# Računarske mreže

**Mrežna oprema, PASIVNE i AKTIVNE KOMPONENTE**
**Kablovi, konektori, WiFi, ripiter, svič, ruter**

## LAN, WAN, MAN
## BUS, STAR, RING, P2P, Client/Server

## Mrežni model OSI
## Mrežni protokol TCP/IP

## Ping, IPCONFIG, arp
## SNA, IoT

# Uvodne napomene

Osnovni problem kod priručnika ovakvog tipa je očuvanje konzistentnosti bez ponavljanja. To je kod mreža gotovo nemoguće. Na neke pojmove se jednostavno mora vraćati i moraju se više puta objasniti. Npr. Ako se objašnjavaju uređaju podrazumjevano je da se znaju modeli, a kasnije se objašnjavaju modeli podrazumjevano je da se znaju uređaji i njihova funkcija i odnos prema protokolima. Tako su pojmovi kao Ethernet, LAN, modeli i slojevi modela objašnjeni više puta, a specijalo adresiranje (pogotovo MAC). Ovdje se pokušalo da svaki put kad je to učinjeno to učini iz drukčijeg ugla, koji daje novu dimenziju i dodatno obaješnjava taj pojam. Da bi se izbjeglao ovo ponavljanje vjerovatno bi bilo ispravnije, konzistentnije i sa manje redundanse da se odvojeno obrade protokoli i uređaji. Možda to i uradim nekom drugom prilikom. Ali, to bi zahtjevalo promjenu ciljne grupe i koncepta da se (bar pokuša) svaka tema obraditi tako da se ne podrazumjeva predznanje. Ili da čitate knjigu u formi hiperteksta, a PDF format Vam to dopušta i nadam se da ćete ga koristiti i na taj način.

Ciljna grupa su napredni i ambiciozni početnici kojima priručnik može da posluži kao osnov za kasniji rad na temi računarskih mreža koja su temelj moderne tehnologije.

U ovoj formi priručnik je korišten kao pomoćno nastvno sredstvo za predmet Računarske mreže. Priručnik je nastao prema uzorku knjige *Računarske mreže*: Mladen Veinović, Aleksandar Jevremović (i oni su zaslužni za inicijalni sadržaj). Materijal je preuzet sa sajta www.racunarskemreze.com/ 2015. godine, kad je prvi put izvršeno djelimično preuređenje i interna prezentacija knjige u ovakvoj (sličnoj) formi). Nažalost sajt više nije aktivan, pa ako želite da preuzmete neki od materijala potrudite se i kontaktirajte autore. Ostale reference i izvore možete potražiti na kraju knjige.

Izvršena su brojna prilagođenja i proširenja kao i usklađivanje sa novim rješenjima koja su se u međuvremenu pojavila. Dopisano je pet potpuno novih poglavlja i 15 novih tema. (*Ukupno više od trideset novih tematskih cjelina*). Sadržaj je obogaćen sa mnogobrojnim novim ilustracijama. *Prva verzija priručnika imala je samo 80 strana, a aktuelna 217.*

Nadam se da je u ovoj formi solidna polazna tačka za početak rada sa mrežama.

**Miroslav Mihaljišin**

*Ovaj priručnik ima isključivo edukativnu namjenu.*

Drugo prošireno izdanje
Banjaluka, *mojTim*, januar 2023.

# Računarske mreže

*Sadržaj:*

**Uvodne napomene ..... 2**
**Računarske mreže ..... 7**
Šta čini računarsku mrežu? ..... 8
Razlozi za umrežavanje ..... 9
Zajedničko korišćenje informacija (podataka) ..... 9
Zajedničko korišćenje hardvera i softvera ..... 10
**Mrežni softver ..... 11**
**Komunikacioni sistem ..... 13**
Direktna komunikacija ..... 14
Zajednički komunikacijski mediji ..... 15
**Klasifikacija mreža ..... 16**
Klasifikacija mreža prema prostoru koji obuhvataju ..... 16
Lokalna računarska mreža (Local Area Network, LAN) ..... 16
Regionalna računarska mreža (Wide Area Network, WAN) ..... 19
**Internet ..... 21**
Mrežne arhitekture sa aspekta međusobnog odnosa i tehnike pristupa ..... 23
P2P mreže ravnopravnih računara (peer-to-peer mreža) ..... 24
Namjena i tipovi servera ..... 25
Klijent server arhitektura ..... 29
Standardne mrežne topologije ..... 30
BUS magistrala (sabirnica) ..... 31
STAR mreže ..... 32
Token Ring mreže - Prstenaste mreže ..... 33
Dodatne i izvedene mrežne topologije ..... 35
Podjela računarskih mreža prema tehnologiji prenosa ..... 37
**Vrste prenosa podataka ..... 39**
Multipleksovanje (Multipleksiranje: Multiplexing' ili 'Muxing') ..... 40
Pojam paketa i paketne mreže ..... 41
Pojam okvira -frame- ..... 42
Prenos podataka sa komutacijom veza (circuit switched) ..... 42
Prenos podataka sa komutacijom paketa (packett switched) ..... 43
Prenos podataka virtuelnom vezom (virtual circuit) ..... 44
Metode pristupa ..... 45
Metoda višestrukog pristupa sa osluškivanjem i otkrivanjem kolizije ..... 45
Metoda višestrukog pristupa sa osluškivanjem i izbjegavanjem kolizije ..... 46
Metoda prioriteta zahtjeva ..... 48

**Mrežna oprema ..... 49**
Pasivna mrežna oprema ..... 49
Mrežni kablovi ..... 50
Koaksijalni kabl ..... 50
Kabl sa upredenim paricama ..... 51
Šta je Ethernet? ..... 51
Ethernet kablovi i konektori ..... 52
Načini povezivanja kod UTP kablova ..... 53
Standardi za konektore i kablove ..... 55
Optički kablovi ..... 56
Standardi i tipovi optičkih kablova ..... 59
Konvertor media pretvarač: Fiber Media Converter ..... 60
Tipovi veza koje koriste telefonske mreže ..... 62
PSTN Klasična (dial-up) telefonska veza sa modemom ..... 62
Integrisani digitalni mrežni servisi ISDN ..... 64
Digitalne pretplatničke veze DSL/ADSL ..... 65
Bežični mediji ..... 67
Svojstva radio talasa ..... 67
Svojstva mikrotalasa ..... 68
Svojstva infracrvenih zraka ..... 69
Svojstva laserskih zraka ..... 69
Bežična mrežna komunikacija WLAN i WiFi ..... 71
Žarišna tačka -Hot spot- i WIFi ..... 72
Bežična pristupna tačka Access point ..... 74
Bežični LAN uređaji i LAN Adapteri ..... 75
Skup servisnih usluga SSID ..... 76
Bluetooth ..... 77
Bluetooth proizvodi ..... 77
Princip rada Bluetooth-a ..... 78
Ad hoc umrežavanje Bluetooth uređaja ..... 79
Bežične mreže prema prostoru koji obuhvataju ..... 83
Mrežna kartica, interfejs mreža-računar ..... 84
Adresa kontrole pristupa medijima -MAC- ..... 85
Aktivni mrežni uređaji ..... 87
Ripiter (Obnavljač signala-Repeater) ..... 87
Hab (Hub) ..... 88
Mrežni most (Bridge) ..... 89
Svič – skretnica-komutator- (Switch) ..... 91
Usmjerivač (Router) ..... 93
Mrežni prolaz (gateway) ..... 95
Bezbjednosna barijera (firewall) zaštita lokalne od javne mreže ..... 97

**Mobilni telefon i računarske mreže ..... 99**
**Strukturno kabliranje ..... 100**
**Protokoli ..... 102**
Nadležnost i posao protokola ..... 103
Protokoli bez uspostavljanja veze ..... 103
Protokoli sa uspostavljanjem veze ..... 104
Upravljanje greškama ..... 105
Provjera parnosti ..... 106
Metoda Kontrolna suma - Checksum - ..... 107
Ciklična provjera redundancije -CRC- ..... 108
Ispravljanje grešaka ..... 109
**OSI model ..... 110**
Enkapsulacija ..... 115
**TCP/IP mrežni model ..... 116**
Standard koji nije postao praksa i praksa koja je postala standard ..... 116
IP - Internet protokol ..... 117
TCP ..... 118
Razmjena podataka ..... 119
Portovi ..... 120
ICMP protokol za slanje kontrolnih poruka o greškama ..... 122
TCP/IP protokol stek ..... 123
Odnos OSI i TCP/IP modela ..... 124
IPv4 ..... 125
IPv6 ..... 126
UDP: Protokol korisničkih datagrama ..... 129
**Klase mreža (Adresni razredi) kod Ipv4 ..... 130**
Mrežna maska ..... 132
Rezervisane IP adrese ..... 134
Besklasno adresiranje - classless addressing- ..... 134
**Adresiranje ..... 138**
Hardversko MAC adresiranje ..... 139
Dodjeljivanje LAN adresa i utvrđivanje sadržaja ..... 141
Pretvaranje IP-adrese u hardversku ARP Protokol za rješavanje adresa ..... 144
DNS sistem ..... 146
Domensko ime i potpuno kvalificirano ime domena FQDN ..... 147
Vršne domene TLD i domenski registri ..... 148
DNS rezolucija i DNS serveri ..... 150
DHCP: Dinamički protokol konfiguracije hosta ..... 153
Web adresa ili Jedinstvena adresa mrežnog resursa URL ..... 155
Pregled adresiranja po slojevima ..... 158

**Operativni sistemi računara i podrška za mreže ..... 159**
Koncept Windows socketa ..... 160
WebSocket, protokol koji definiše priključak na web ..... 162
**Osnovni alati za provjeru rada mreže ..... 164**
Kako saznati ime računara: Hostname ..... 164
Pingovanje ..... 165
Komanda tracert/traceroute ..... 167
Pathping ..... 170
Komanda IPCONFIG ..... 171
Komanda ARP ..... 173
Rad i opasnosti korištenja ARP protokola ..... 174
*Otkrivanje mreže- Network discovery- kod Windowsa* ..... 176
Promjena TCP/IP postavki kod Windowsa – Majkrosoft uputstvo: ..... 179
Popravite probleme sa mrežnom vezom u Windowsu ..... 181
**Softver za upravljanje mrežama ..... 182**
Jednostavni protokol za upravljanje mrežom – SNMP ..... 183
Baza upravljačkih informacija – MIB ..... 185
SNMP komande ..... 186
Opis rada protokola SNMP ..... 188
Programske implementacije koje koriste SNMB ..... 189
Instalacija i korištenje SNMP protokola kod Windowsa ..... 192
**Sigurna mreža i sigurnosna politika ..... 193**
Tehnologije za sigurnost ..... 194
SSL/TLS protokol ..... 196
SSL/TLS digitalni serifikat ..... 199
**SDN Softverski definisane mreže ..... 200**
SDN arhitektura ..... 202
SDN kontroler ..... 202
OpenFlow ..... 205
Northbound API ..... 206
SDN aplikacije ..... 206
**IoT, ili Internet stvari ..... 208**
Osnovne komponente i način rada IoT ..... 210
Mrežne tehnologije kod IoT ..... 213
IIoT, industrijski IoT ..... 214
**Standardi, referentna tijela i organizacije ..... 215**
**Reference ..... 217**

# Računarske mreže

**computer network**
*računarska mreža, dva ili više računara koji su međusobno povezani u svrhu elektronske komunikacije.*

Encyclopedia Britannica

Računarska mreža je pojam koji se odnosi na računare **i druge uređaje** koji su međusobno povezani kablovima ili na drugi način, a u svrhu međusobne **komunikacije i djeljenja** podataka i drugih resursa.
Računarske mreže omogućavaju međusobno komuniciranje računara pomoću neke stalne ili privremene veze.
Veza između dva računara koji dijele svoje resurse **može** da se nazove računarskom mrežom (najjednostavnija računarska mreža).

Računarska mreža se može posmatrati kao **komunikacioni sistem**, gdje se informacija generisana na predajnoj strani (izvorište poruke) dostavlja željenom odredištu.
Osnovni elementi komunikacionog sistema su: **izvor, predajnik, prenosni medijum, prijemnik i odredište**. Ključni poslovi u komuniciranju su: povezivanje, generisanje signala, sinhronizacija, razmjena podataka, otkrivanje i ispravljanje grešaka, kontrola toka, adresiranje i usmjeravanje, zaštita, upravljanje i nadgledanje mreže itd. U računarsim mrežama razlikujemo prenos podataka komutacijom veza (čvrsta direktna veza) ili komutacijom paketa.

Prenos podataka kroz mrežu se obavlja po protokolima - pravilima i procedurama koje upravljaju komunikacijom i saradnjom umreženih računara.

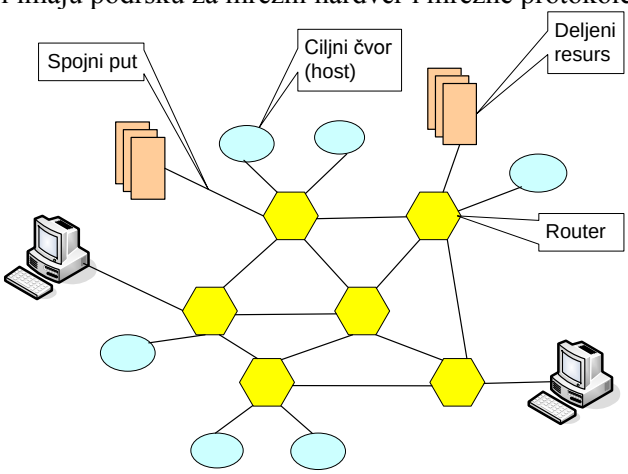
Potreba za informacijama naterala je čoveka da uspostavlja veze sa raznim izvorima informacija i da stvara mreže preko kojih će sebi olakšati prikupljanje, prenos, skladištenje i obradu podataka. Naglim razvojem računarske tehnologije posljednjih godina (povećanje performansi uz pad cijena) i sa pravom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

Počeci umrežavanja vezuju se za prve telegrafske i telefonske linije kojima su se prenosile informacije do udaljenih lokacija. Dostupnost i fleksibilnost tehnologija današnjih savremenih računarskih mreža omogućava da se sa bilo koje tačke na planeti može povezati na mrežu i doći do željenih informacija. U poređenju sa nekadašnjom cijenom korišćenja servisa mreža, cijena eksploatisanja današnjih mreža je sve niža. Računarske mreže su danas nezamjenjivi dio poslovne infrastrukture kako malih, tako i velikih organizacija. U mnogim segmentima poslovanja primjena računarskih mreža može da obezbjedi prednost organizacijama na tržištu (npr. elektronska trgovina omogućava i malim firmama konkurentnost na tržištu).

# Šta čini računarsku mrežu?

**Računarsku mrežu čine: računari, komunikacioni medijum, komunikacioni hardver i komunikacioni softver.** Realizacija i implementacija i hardverskih i softverskih elemenata računarskih mreža obavlja se strogim skupom pravila koji se nazivaju protokoli.
Računarska mreža može biti prost skup dva ili više računara, koji su povezani medijumom za povezivanje i koji međusobno mogu da komuniciraju i dijele resurse. Koristi se za prenos kako digitalnih tako i analognih podataka, koji moraju biti prilagođeni odgovarajućim sistemima za prenos. Mrežom se prenose računarski podaci, govor, slika, video, a aplikacije na stranama korisnika mogu biti takve da se zahtjeva prenos podataka u realnom vremenu (govor, video i sl.) ili to ne mora biti uslov (elektronska pošta, prenos datoteka i sl.). **Mreža se sastoji od računara, medijuma za prenos** (žica, optičko vlakno, vazduh) **i uređaja** kao što su čvorišta, svičevi, ruteri itd. **koji čine infrastrukturu mreže**. Neki od uređaja, kao što su mrežne kartice, služe kao veza između računara i mreže.

Svaka mreža se može svesti na sljedeće dvije osnovne cjeline: hardversku i softversku.
**Hardversku cjelinu** sačinjavaju mrežni čvorovi (*nods*) u kojima se vrši obrada informacija, fizički spojni putevi i dijeljeni resursi.
**Čvorovi** su dijelovi mreža u kojima dolazi do obrade podataka. Postoje dvije vrste čvorova: čvorovi u kojima se vrši stvarna obrada i oni predstavljaju ciljne čvorove (*hosts*), i čvorovi kojima je uloga da usmjeravaju informacije (*routers*).
Dijeljeni resursi su hardverski (štampači, ploteri, faks mašine, diskovi i sl.) ili softverski elementi (datoteke, baze, aplikacije i sl.).
**Softversku cjelinu** mreže čine protokoli – pravila po kojima se vrši komuniciranje (razmjena podataka) u mreži i operativni sistemi koji su u direktnoj komunikaciji sa hardverom računarskog sistema i imaju podršku za mrežni hardver i mrežne protokole.




*Osnovna arhitektura mreže*

Komunikacionl medijum služi za fizičko povezivanje računara. **Osnovna podjela je mreža prema medijima** koji koriste za povezivanje i prenos informacija:

1. **kablovsk**i (žični -bounded) žični mediji mogu biti:
   - Bakrene žice – ili kratko “bakar”
   - Optička vlakna – u žargonu “staklo” ili “optika”

2. **bežični** (unbounded) Bežični mediji su:
   - Radio talasi
   - Mikrotalasi
   - Infracrvene zrake
   - Laserske zrake.

## Razlozi za umrežavanje

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

- zajedničko korišćenje informacija – efikasno komuniciranje učesnika,
- zajedničko korišćenje hardvera i softvera.

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

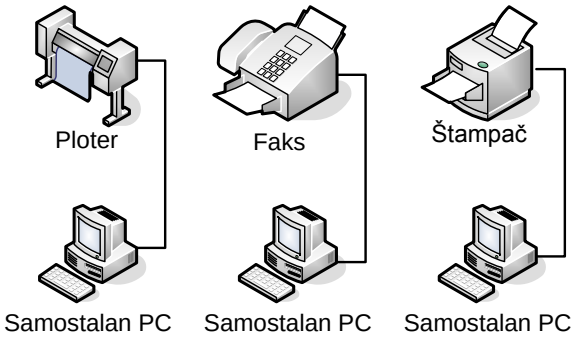
- dokumente (memorandume, tabelarne proračune, fakture)
- elektronsku poštu
- softver za obradu teksta
- softver za praćenje projekata
- ilustracije, fotografije, video i audio datoteke
- štampače
- modeme
- DVD/CD-ROM jedinice i druge prenosive jedinice
- Diskove ...

## Zajedničko korišćenje informacija (podataka)

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

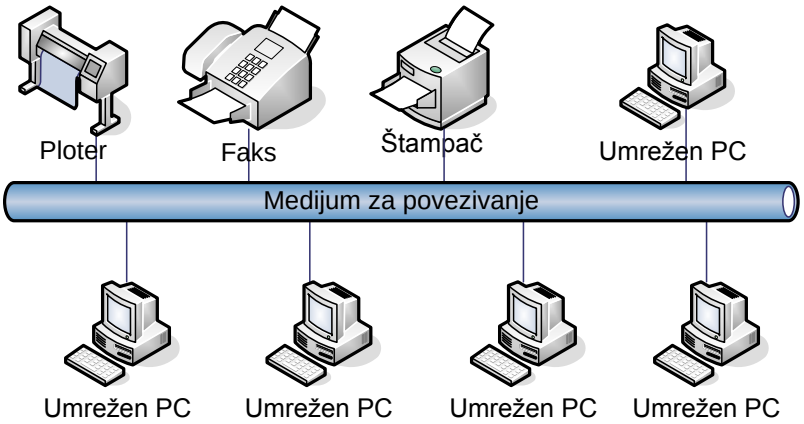
## Zajedničko korišćenje hardvera i softvera

Pre pojave računarskih mreža, bilo je neophodno da svaki korisnik ima svoj štampač, ploter, faks i druge periferijske uređaje. Jedini način da više korisnika koristi isti uređaj je bio da se naizmjenično koristi računar sa kojim je taj uređaj povezan.




*Samostalne PC konfiguracije*

Pojava mreža je otvorila mogućnost da više korisnika istovremeno koristi zajedničke informacije, ali i periferijske uređaje. Ukoliko je štampač neophodan većem broju korisnika koji su u mreži, svi mogu da koriste zajednički mrežni štampač.




*Zajedničko korišćenje hardvera u mrežnom okruženju*

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

# Mrežni softver

Sama mreža ne može ničemu da posluži bez odredene inteligencije koja će joj omogućiti da funkcioniše. Ulogu te inteligencije ima mrežni softver.
Mrežni softver se definiše kao širok spektar softvera koji pojednostavljuje operacije, dizajn, praćenje i implementaciju računarskih mreža. To je krovni termin koji se koristi za opisivanje širokog spektra softvera koji pojednostavljuje operacije, dizajn, praćenje i implementaciju računarskih mreža.
*Postoje mnogobrojne klasifikacije mrežnog softvera. Ako bi pokušali da ih damo i objasnimovjerovatno bi nam treba još jedan priručnik većeg obima od ovoga.*

*Softver za umrežavanje omogućava kontrolu, upravljanje i praćenje mreža.*

Definicija koju na svom sajtu daje Cisco, jedan od vodećih proizvođača mrežne opreme

Kako bi se savladala kompleksnost računarskih mreža, mrežni softver se organizuje hijerarhijski. Npr. programer pregledača Veba (*web browser*) ne treba da misli o tome da li će Veb stranice primati preko bežične mreže ili preko Ethernet mreže. On treba da se koncentriše samo na aspekte značajne za njegovu konkretnu aplikaciju, a da sve niže detalje mrežne komunikacije prepusti nižem sloju mrežnog softvera (prisutnom u okviru operativnog sistema, ili čak samog mrežnog hardvera).
Najgrublje posmatrano, mrežni softver može da se podeli na dva nivoa.
Mrežni softver koji omogućuje korišćenje različitih mrežnih uredaja, npr. mrežnih kartica ili modema, jeste mrežni softver **niskog nivoa.**
Ova vrsta softvera nalazi se obično u jezgru operativnog sistema računara, uglavnom u obliku upravljača perifernim uredajima, tzv. drajvera (eng. driver). On upravlja računarskim hardverom i komunikacionom opremom. Korisnik računara nikada ne koristi ovaj softver direktno, u opštem slučaju on nije ni svestan da taj softver postoji. Osnovni zadatak ovog softvera je da pruži usluge mrežnim aplikacijama (tj. njihovim programerima) koje korisnici koriste.
Ove aplikacije čine mrežni softver **visokog nivoa** i pružaju različite usluge i servise korisnicima na mreži, kao što je slanje i prijem elektronske pošte, pregledanje Veba i sl.

Generalno, funkcije mrežnog softvera su:

• Upravljanje korisnicima (User management) omogućava administratorima da dodaju ili uklanjaju korisnike sa mreže. Ovo je posebno korisno pri zapošljavanju ili smjenjivanju

• Upravljanje datotekama (File management) omogućava administratorima da odluče o lokaciji skladištenja podataka i kontrolišu pristup korisnika tim podacima.

• Pristup (Access) omogućava korisnicima da uživaju u neprekidnom pristupu mrežnim resursima.

• Mrežni sigurnosni sistemi (Network security systems) pomažu administratorima u brizi o sigurnosti i sprečavanju kršenja podataka.

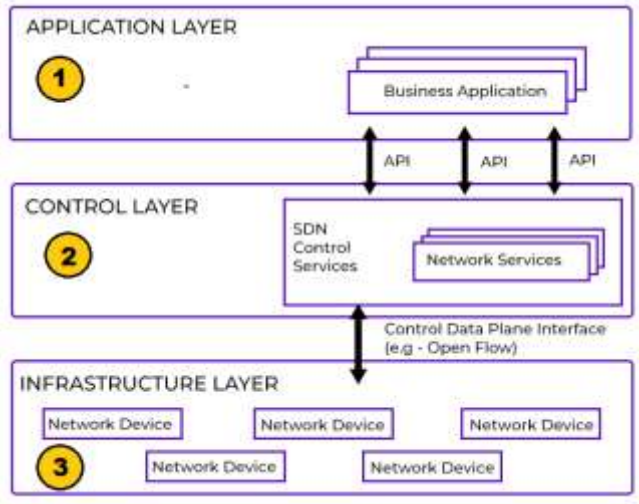
Tradicionalne mreže bile su zasnovane na hardveru koji su činili ruteri i svičevi sa ugrađenim softverom. Odvajanje softvera od hardvera, nazvano softverski definisano umrežavanje (SDN-software-defined networking), što je omogućilo pojednostavljivanju upravljanja infrastrukturom, čineći je prilagodljivijom u odnosu na tehnologije koje su se (i još uvijekse) izutetno brzo razvijaju i mijenjaju.

Uvođenje SDN-a bilo je prekretnica i potpuno je promijenilo način na koji se radi umrežavanje. Softver za umrežavanje—zajedno sa softverski definisanim mrežama (SDN) koje kreira—pomaže inženjerima da odgovore na te izazove omogućavajući **stvaranje mreža zasnovanih na namjeri** (IBN **intent-based networks**).

IBN-ovi smanjuju IT opterećenje i vrijeme implementacije, efikasnije koriste resurse i poboljšavaju agilnost. Oni pružaju te prednosti automatskim prevođenjem poslovnih ciljeva u prilagođene mrežne konfiguracije.

Mi ćemo se u priručniku uglavnom držati tradicionalnog pristupa. Razlog je ciljna grupa (napredni početnici) koji prvo treba da se upoznaju sa osnovnim komponentama i principima tradicionalnog umrežavanja, pa da nakon tog upoznavanja pređu na napredne tehnike i nove tehnološke pristupe.

Za početak (i kraj razmatranja) mrežnog softvera pogledajte ilustraciju konfiguracije osnovnih komponenti mrežnog softvera ((kod softverski definisanih mreža)) i nekoliko osnovnih napomena vezanih za njega. *U pručniku će se na nekoliko mjesta koristiti ovaj pristup.*




*Komponente i slojevi mrežnog softvera*

1. Aplikacioni sloj

Sloj aplikacije (ili ravan aplikacije) koji se odnosi na aplikacije i usluge koje rade na mreži. To su programi koji prenosi mrežne informacije, status mreže i mrežne zahtjeve za određenu dostupnost resursa i primjenu. Ovo se radi preko kontrolnog sloja preko interfejsa za programiranje aplikacija (API). Sastoji od logike aplikacije i jednog ili više API drajvera.

2. Kontrolni sloj

Kontrolni sloj je centralni dio mrežne središtu arhitekture. Mogli bi nazvati mozgom cijelog sistema. Ovaj sloj uključuje softver za kontrolu mreže i mrežni operativni sistem unutar njega. To je entitet zadužen za primanje zahtjeva iz aplikacija i njihovo prevođenje u mrežne komponente. Kontrola infrastrukturnog sloja ili uređaja za obradu i prenos podataka se vrši preko kontrolera. Kontrolni sloj je interfejs-posrednik koji olakšava komunikaciju između gornjih i donjih slojeva preko API interfejsa.

3. Infrastrukturni sloj

Infrastrukturni sloj, koji se naziva i ravan podataka, sastoji se od stvarnih mrežnih uređaja (i fizičkih i virtualnih) koji se nalaze u ovom sloju. Oni su prvenstveno odgovorni za premještanje ili prosljeđivanje paketa podataka nakon primanja odgovarajućih instrukcija od kontrolnog sloja. Jednostavno rečeno, ravan podataka u komponentama mrežne arhitekture fizički upravlja korisničkim prometom na osnovu naredbi koje prima kontroler.

Interfejs aplikacijskog programa (API) povezuje sve tri komponente zajedno. Komunikacija između ova tri sloja je olakšana preko interfejsa aplikacijskih programa koji naviše povezuje komunikaciju između aplikacije i kontrolnih slojeva, dok naniže omogućava komunikaciju između infrastrukture i kontrolnih slojeva.

Za kraj ovog poglavlja još jedna Cisco uputa:
Softver za umrežavanje prima instrukcije o namjeri i prevodi ih u politike koje definišu mrežu.
ALI: prije nego što budete u mogućnost da koristite IBN softver trebali bi da znate koje su osnovne mogućnosti mreža da bi mogli da deklarišete svoje namjere. *A tu će Vam pomoći ovaj priručnik.*

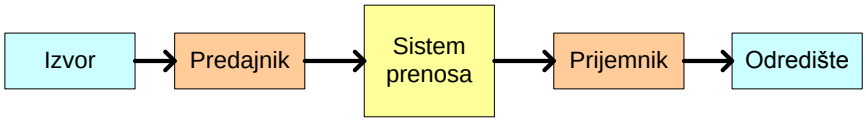
# Komunikacioni sistem

Mrežni komunikacijski sistem označava bilo koju ili sve komponente koje posjedujete ili kontrolišete, uključujući hardver, računare ili prenosne uređaje i njihov odgovarajući softver, koji im omogućavaju elektroničku komunikaciju s drugim računarskim sistemima.
Komponente komunikacijskog sistema služe zajedničkoj svrsi, tehnički su kompatibilne, koriste zajedničke procedure, odgovaraju na kontrole i rade u zajednici.

Računarska mreža se može posmatrati kao komunikacioni sistem, gdje se informacija generisana na predajnoj strani (izvorište poruke) dostavlja željenom odredištu.

Osnovni elementi komunikacionog sistema su:

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




*Model komunikacionog sistema*[1]

Ključni poslovi u komunikacionom sistemu su:

- Povezivanje (*interfacing*) uređaja na komunikacioni sistem
- Generisanje signala (*signal generation*) – propagacija, regeneracija, domet itd.
- Sinhronizacija (*synchronization*) predajnika i prijemnika
- Razmjena podataka (*exchange management*) – prema odgovarajućem protokolu
- Otkrivanje i ispravljanje grešaka (*error detection and correction*) npr. kod slanja datoteka
- Kontrola toka (*flow control*) usaglašavanje brzine slanja i brzine prijema podataka
- Adresiranje i usmjeravanje (*addressing and routing*) – čim postoje više od dva učesnika
- Oporavak (*recovery*) – mogućnost da se transfer podataka nastavi od mjesta prekida
- Formatiranje podataka (*message formatting*) dogovor učesnika
- Zaštita (*security*), na prenosnom putu, autentičnost podataka
- Upravljanje mrežom (*network management*) – mreža je kompleksan sistem, koji ne radi sam po sebi. Neophodno je mrežu konfigurisati, nadgledati (monitorisati), intervenisati i inteligentno planirati za buduću namjenu.

Za ostvarivanja komunikacije neophodni su mediji koji će omogućiti prenos poruka. **Pojam mrežni medij** odnosi se na komunikacione kanale koji se koriste za međusobno povezivanje čvorova na računarskoj mreži.

Prema načinu uspostavljanja komunikacije moguće da komunikaciju ostvarimo na dva načina:

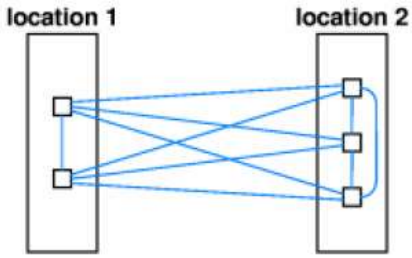
- direktom komunikacijom
- korištenjem zajedničkih komunikacionih medija.

## Direktna komunikacija

Najjednostavnija ideja kako povezati računare je uspostavljanje posebne veze (žice) između svakog para računara. Ovakvo rješenje ima određenih prednosti, no **gotovo se nikad ne primjenjuje** u praksi jer je skupo i ne-skalabilno[2].

[1] Ovo je pojednostavljeni Šenonov (Shannon Weaver) model komunikacija, ali bez najznačajnije komponente, šuma-smetnji. Smetnje nam u komunikacionom sistemu ne trebaju, ali one su uvijek prisutne. „Osnovni problem komunikacije je reprodukcija poruke poslane iz jedne tačke, bilo tačno ili približno, do druge tačke" (Shannon, 1948.).

[2] Generalno: Skalabilnost je osobina sistema da se prilagodi sve većoj količinu posla dodavanjem resursa u sistem.
U IT okruženju, skalabilnost je karakteristika sistema ili aplikacije koja ukazuje na njegovu sposobnost da i dalje dobro radi pod povećanim ili rastućim opterećenjem. Mrežni sistem koji se dobro skalira može održati ili čak povećati nivo performansi ili efikasnosti, čak i kad se povećavaju operativni zahtjevi.




Broj veza potrebnih za ovakvo povezivanje *n* računara je $n(n-1)/2$, dakle raste kao $n^2$.

Kod imalo većeg broja računara broj kablova bi bio tako velik da bi imali problema s njihovim fizičkim polaganjem.

Ipak se ponekad primjenjuje iz sigurnosnih razloga.

## Zajednički komunikacijski mediji

Komunikacijski mediji odnose se na načine isporuke i primanja podataka ili informacija. Komunikacijski mediji djeluju kao kanal za povezivanje različitih računarskih uređaja kako bi mogli međusobno komunicirati. U telekomunikacijama, ta sredstva su alati za prenos i pohranu ili kanali za pohranu i prenos podataka.

S obzirom da direkno povezivanje računar ne dolazi u obzir razvijale su se takozvane LAN tehnologije.
Sve su one imaju kao osnov djeljenje komunikacijskog medija. LAN tehnologije pokazale su se kao djelimično sigurne, dovoljno brze, prilično jeftine, te u većoj ili manjoj mjeri skalabilne.
Da bi se moglo komunicirati preko zajedničkog medija, moraju se propisati pravila i protokoli korištenja koji osiguravaju da neće doći do kolizije u korištenju medija, te da će svaki računar prije ili kasnije ostvariti svoje pravo na komuniciranje.

*Mi ćemo se u ovom priručniku baviti mrežama koji koriste zajedničke komunikacione medije*[3].
Komunikacioni kanal je put kroz mrežu između izvora i odredišta koji se dodjeljuje na zahtjev (npr. pozivanjem), ili trajno (npr. Iznajmljivanjem) za vrijeme trajanja komunikacije.

Povezivanje telekomunikacija i računara u svjetsku međumrežu (Internet) omogućuje konvergiranje tradicionalnih medija, poput knjiga i novina (nastajanje elektronskih knjiga i e-novina), s posve novim oblicima komunikacije, kao što su e-mail, chat, web sites, te prenos mnogih aktivnosti i usluga, kao što su poslovanje, robna razmjena, javna uprava, pa čak i izbori i sl., na WWW.

Ovdje se skalabinost odnosi na mogućnost naknadnog dodavanja čvorova-računara, koji ćine mrežu.
[3] Ustvari mi ćemo se baviti kanalima koji omogućavaju realizaciju komunikacije. Uobičajeno pojam medija predstavlja način komunikacije (npr. novine, časopis, radio, televizija, ili društvene mreže; pa se govori o Twiteru kao mediju, Facebook mediju i slično. Mi ćemo ovdje uglavnom pod medijom govoriti o kanalima koji odgovaraju fizičkom sredstvu za prenos informacija u medijskom prostoru.

# Klasifikacija mreža

Računarske mreže možemo podeliti na osnovu četiri osnovna kriterija: na osnovu veličine, topologije, tehnologije prenosa podataka i pristupa umrežavanju (arhitekture):

1. Na osovu dosega-prostora koji obuhvataju: veličine (LAN/WAN)
2. Pristupa umrežavanju: arhitektura (P2P- C/S)
3. Topologije -logička i fizička-prsten/zvijezda/magistrala
4. Tehnologija prenosa/žično-bežično/

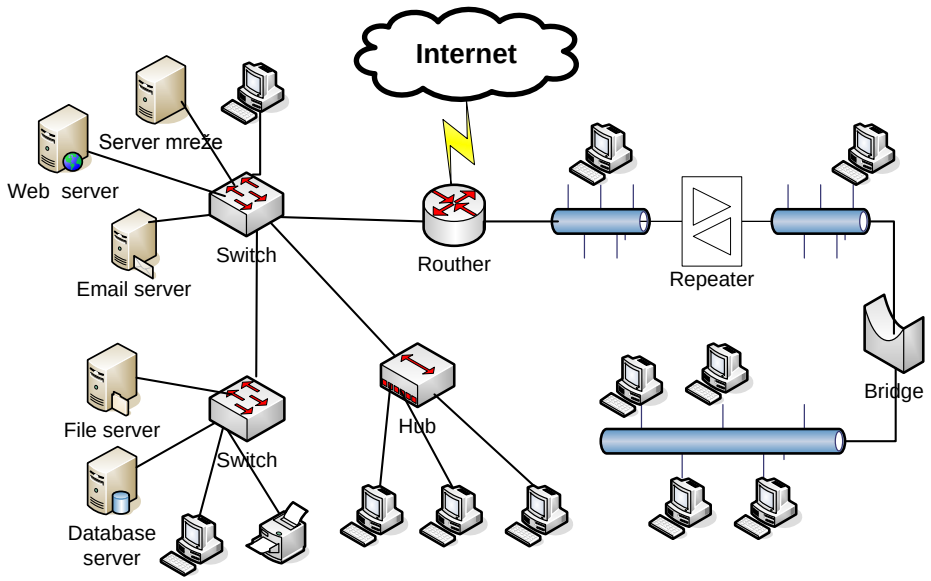
## Klasifikacija mreža prema prostoru koji obuhvataju

Prema prostoru koji obuhvataju, računarske mreže se mogu podijeliti na

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

## Lokalna računarska mreža (Local Area Network, LAN)

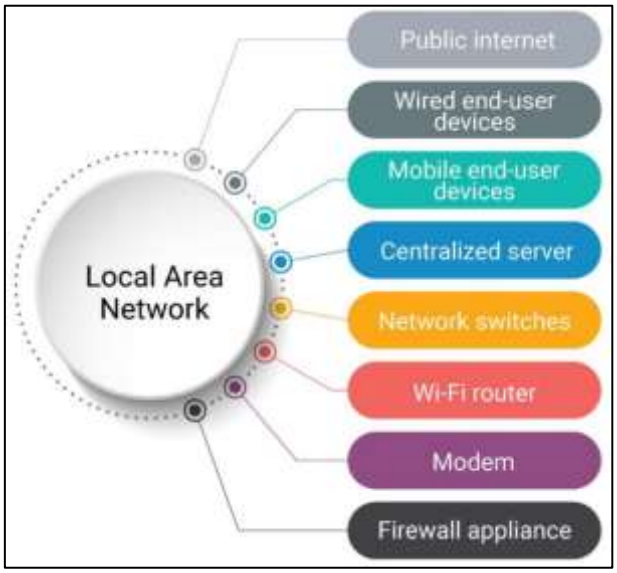
Predstavlja **osnovni tip mreže**. Ona može biti jednostavna kada imamo dva računara povezana kablom, ili složena kada su povezani na stotine računara i periferijskih uređaja u jednoj velikoj organizaciji. Osnovno obilježje lokalne računarske mreže je to što je ona **prostorno ograničena**.



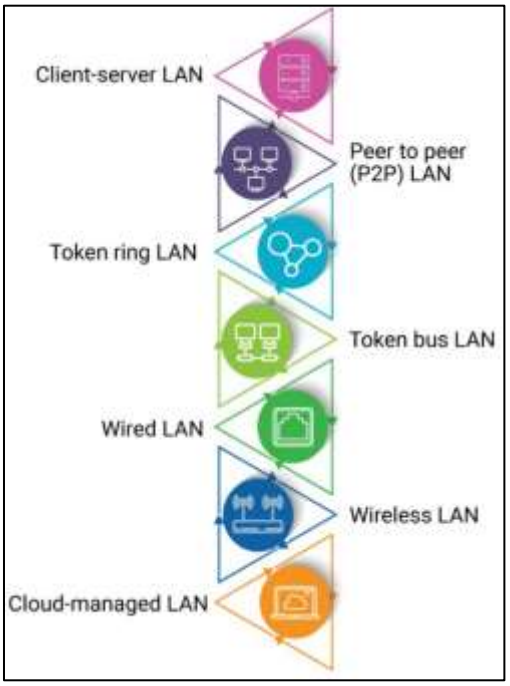

*Lokalna računarska mreža (LAN) sa vezom ka Internetu*

Tradicionalni Ethernet LAN se sastoji od jednog ili više čvorišta, prekidača ili tradicionalnih rutera koje pojedinačni uređaji povezuju preko Ethernet kablova.

Lokalne mreže se mogu klasifikovati na osnovu tipova uređaja koje povezuju, dizajna osnovne arhitekture i medija koji se koristi. Kao posebna klasa izdvaja se LAN ostvaren sa vezama prema oblaku (Cloud-managed LAN).

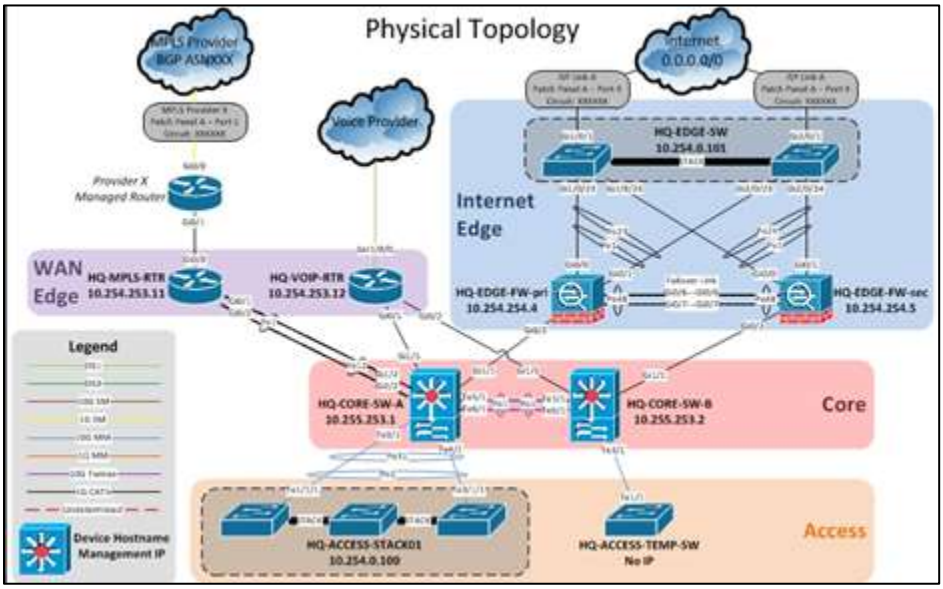



*Osnovne komponente koje određuju LAN mrežu*



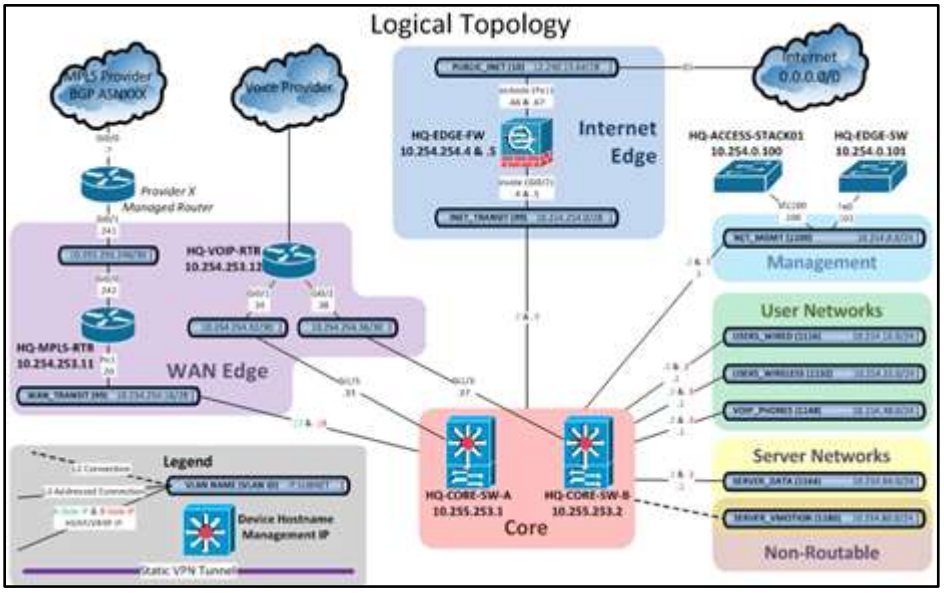

*Osnovni tipovi LAN mreža*

**LAN dijagram** je vizuelni prikaz rasporeda različitih komponenti LAN mreža, tj. čvorova i prikaza kako su te komponente povezane. Raspored različitih čvorova LAN dijagrama se naziva topologijama. LAN dijagram se sastoji od dvije različite topologije, fizičke i logičke topologije.




*Primjer LAN dijagrama koji ilustruje fizičku topologiju*

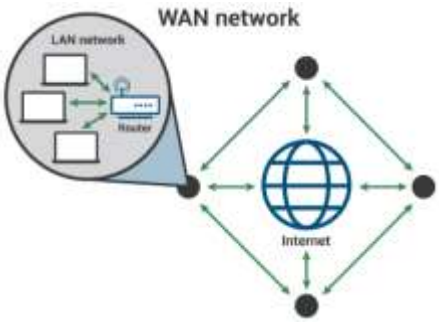
Fizička topologija se odnosi na sve uređaje unutar mreže (od svičeva do rutera i računara). Logička topologija, s druge strane, predstavlja vizualni prikaz kako podaci putuju od i do različitih čvorova LAN mreže.




*Primjer LAN dijagrama koji ilustruje kogičku topologiju*

Profesionalni projektanti mreža za kreiranje dijagrama koriste različite softverske pakete kao što su npr.: EdrawMax, LanFlow, SolarWinds NTM, Intermapper, Creately, Lucidchart, SmartDraw...

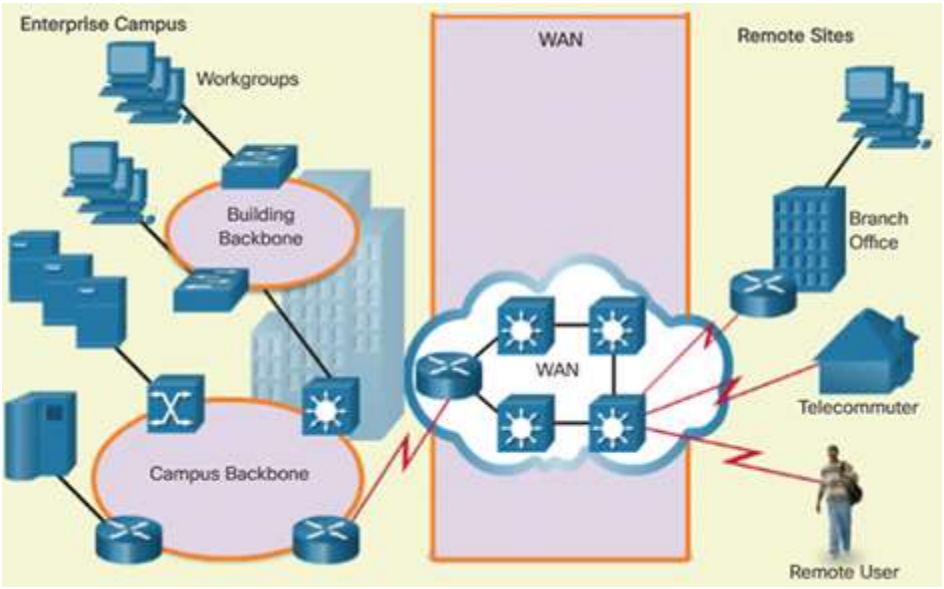
# Regionalna računarska mreža (Wide Area Network, WAN)




U svom najjednostavnijem obliku, WAN mreža je skup lokalnih mreža (LAN) ili drugih mreža koje komuniciraju jedna s drugom.
**Nisu prostorno ograničene**.

Regionalnu računarsku mrežu čini veliki broj povezanih lokalnih mreža. WAN mreže su najveći i najširi oblici kompjuterskih mreža. One mogue da poveže računare i uređaje širom svijeta.

Problem koji se javlja kod LAN mreža ogledao se u tome da mogu da povezuju računare i uređaje na relativno malim rastojanjima. Međutim, velike organizacije i institucije, koje imaju ekspoziture na raznim geografskim lokacijama, teže da sve lokalne mreže svojih centara povežu u jednu veliku mrežu.




WAN mreže (*Wide Area Network*) predstavljaju skup više povezanih LAN mreža, koje se nalaze na različitim geografskim lokacijama. Za povezivanje međusobno udaljenih LAN mreža upotrebljava se tehnologija koja obezbjeđuje nesmetan prenos podataka na velikim rastojanjima. Ove mreže se nazivaju i okosnice ili kičma-mreže (*backbone*).
WAN ruter, poznat i kao rubni ruter ili granični ruter, je uređaj koji usmjerava pakete podataka između WAN lokacija, dajući korisniku (obično nekoj većoj firmi, ili korporaciji) pristup mreži operatera.
WAN topologija je obično point-to-point, odnosno tačka-tačka. To znači da **podržava samo dva krajnja uređaja za slanje i prijem podataka, pri čemu se LAN mreže nalaze iza tih uređaja i preko njih komuniciraju**.
WAN mreže se često grade korištenjem iznajmljenih linija. Na svakom kraju iznajmljene linije, ruter povezuje LAN s jedne strane s drugim ruterom unutar LAN-a s druge strane.

Budući da iznajmljene linije mogu biti vrlo skupe, umjesto korištenja iznajmljenih linija, WAN-ovi se također mogu izgraditi korištenjem jeftinijih metoda komutacije kola ili komutacije paketa.

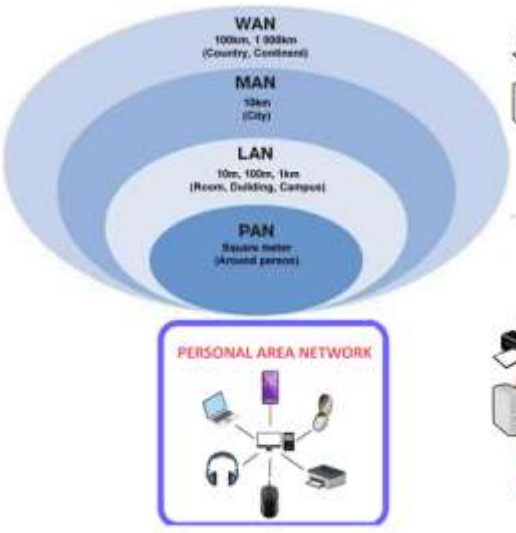
WAN-ovi mogu postojati globalno, bez veza sa fizičkom lokacijom kroz korištenje iznajmljenog mrežnog provajdera, LAN-ovi postoje unutar ograničenog područja. LAN mreže se mogu koristiti za pristup većem WAN-u (kao što je internet), ali samo unutar područja do kojeg može doći LAN infrastruktura.

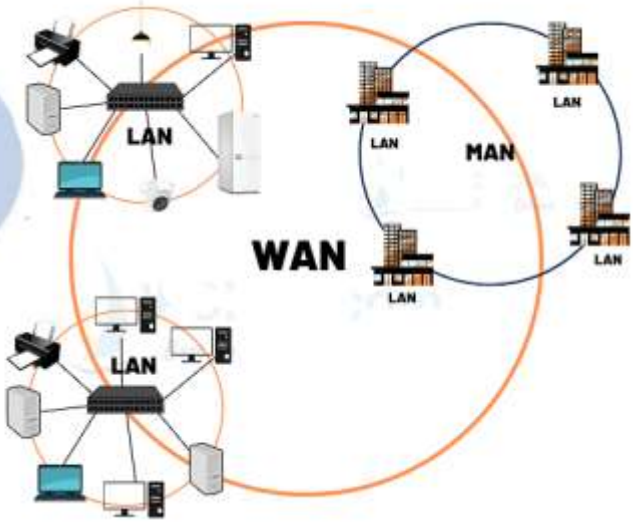
Da WAN veze ne postoje, LAN-ovi bi omogućili organizacijama da rade unutar svojih zgrada, ili bližeg okruženj, ali pristup u udaljene oblasti ili čak različite zemlje - ne bi bio moguć jer bi povezana infrastruktura bila prezahtjevna. WAN-ovi im omogućavaju da komuniciraju između dislociranih podružnica, dijele informacije i ostanu povezani.
**WAN-as-a-service** (WAN-kao-usluga) je WAN model baziran na oblaku. Ovaj model usluge je dizajniran da zamijene zastarjele WAN konfiguracije koje se oslanjaju na hardver. Kako se WAN-kao-usluga nudi putem oblaka, korisnicima je potrebna samo internet konekcija i mogu konfiguririsati svoj WAN koristeći softver, umjesto da koriste hardverske uređaje.

---

U klasifikaciji se rjeđe sreću

- Personal Area Network (**PAN**) Mreža u krugu 10 m oko osobe. Npr. bežična mreža koja povezuje tastaturu, miš ili štampač sa računarom. Drugi primjer ovakve mreže su bluetooth uređaji.
- Metropolitan Area Network (**MAN**) Mreža koja pokriva veća područja od LAN mreže (nekoliko kvartova, grad ili nekoliko gradova), povezuje različite LAN mreže. Većinom je održavana od strane većih korporacija i firmi, a koristi ju mnogo korisnika. Doseg MAN mreže je obično do 50 km.



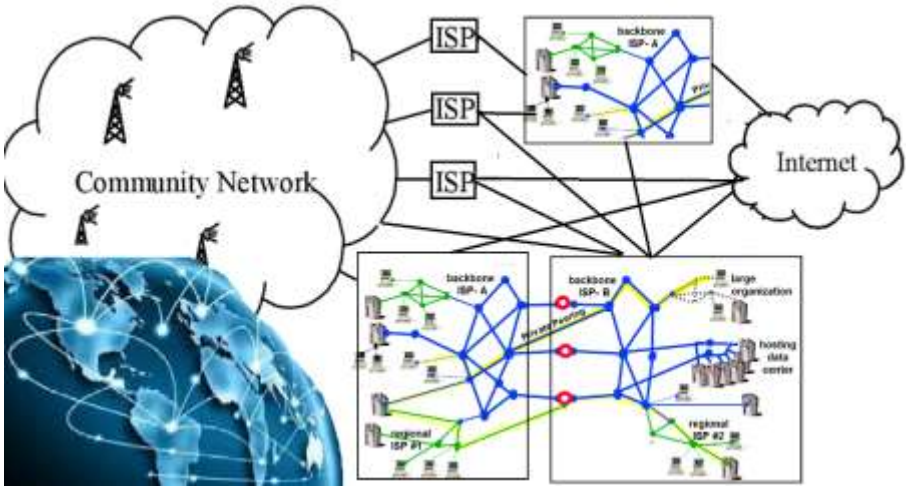




*Internet, kao skup mreža na različitim geografskim lokacijama **nije WAN mreža**. Iako koristi neke od WAN tehnologija, za Internet bi se prije moglo reći da je **međumreža** sa ugrađenim servisima koji su dostupni širom svijeta.*

# Internet

Internet[4], koji se ponekad naziva jednostavno „Mreža"-"Net", je **svjetski sistem** računarskih mreža - u kojoj korisnici na bilo kojem računaru mogu, ako imaju dozvolu, dobiti informacije sa bilo kojeg drugog računara (i ponekad ostvariti direktnu vezu i direktno razgovarati sa korisnika na drugim računarima).

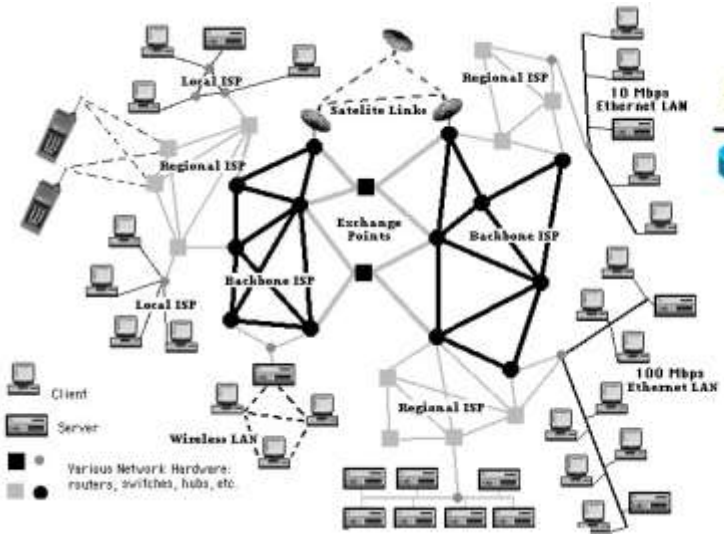
Mada se pod pojmom Internet uobičajeno podrazumjeva svjetska računarska mreža, Internet je prije svega globalni informacioni sistem. Tehnički, taj sistem se ostvaruje kao „**mreža svih mreža",** logički **povezan jedinstvenim sistemom adresiranja putem internet protokola (TCP/IP**), ili drugih protokola kompatibilnih sa internet protokolom, i koji obezbeđuje, koristi ili omogućava servise visokog nivoa za ličnu i poslovnu upotrebu **uz primjenu odgovarajuće telekomunikacione infrastrukture**.
Korisnici interneta informacije razmjenjuju putem mrežnih usluga (servisa). Najznačajnije internet usluge, **internet servisi** su: elektronska pošta (*e-mail*), prenos datoteka (skraćeno ftp, od *ftp, File Transfer Protocol*), pričaonice - ćaskanje-čat *IRC (Internet Relay Chat*) omogućuje da jedan ili više korisnika internet koristeći isti kanal istovremeno vide tekst koji kucaju na svom računaru, kao i tekstove ostalih aktivnih korisnika, koji unose na svom kompjuteru, telnet servis Interneta omogućuje korisnik ovog servisa radi na udaljenom računaru i mnogi drugi a prije svega **veb** ili povezane stranice (ili *www*, skraćeno od *World Wide Web*). Pojam web se često poistovjećuje sa internetom, pa kad se govori o web mrežama gotovo uvijek semisli na internet, mada kako smo naveli web je samo jedan (vjerovatno najvažniji, a zasigurno nakorištenijii ) servis Interneta.

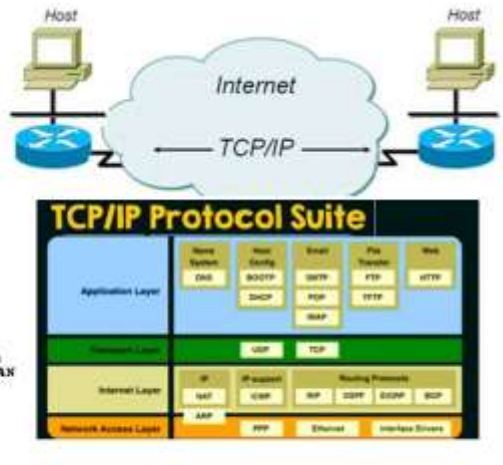



[4] Ostaje nerješeno pitanje: Da li se internet piše sa velikim ili malim slovom?
"...pošto se nalaze u kategoriji opštih (tj. apelativnih) reči, svi anglicizmi se pišu malim početnim slovom (osim ukoliko se javljaju u sastavu vlastitog imena, kada, zavisno od pozicije, podležu pisanju velikim početnim slovom); jedini izuzetak predstavlja reč internet, koja zadržava izvesna svojstva vlastitog imena (preuzeta iz engleskog), pa se zato može alternativno pisati i velikim početnim slovom — Internet" T. Prćić, Rečnik novijih anglicizama.
I. Klajn kaže da to još nije raspravljeno te da zasad oboje dopušteno.

Osnovu internet mreže čine (mrežni) čvorovi međusobno povezani kvalitetnim optičkim vezama, preko kojih se vrši razmjena informacija između udaljenih dielova mreže. Čvorove čine pružaoci internet usluga (**ISP** - Internet Service Providers), velika preduzeća ili akademske institucije. Oni su posrednici između mreže, odnosno Interneta, i pojedinačnih računara koji su u određenom momentu i na određeni način sa njima povezani.
Internet se pojavio u Sjedinjenim Državama 1970-ih, ali je u masovnoj upotrebi od ranih 1990-ih. Procjenjuje se da je 2020. godine približno 4 milijardi ljudi imalo i koristilo pristup internetu.

Kao rodonačelik interneta smatra se ARPANET.
ARPANET je uspostavio prvu mrežnu vezu host-host 29. oktobra 1969. Stvorila ga je Agencija za napredne istraživačke projekte (ARPA)Ministarstvo obrane SAD-a. ARPANET je bila jedna od prvih računarskih mreža opšte namjene (ranije su mreže koristile samo vladine institucije i velike korporacije). Povezao je računare na istraživačkim mjestima koje podržava vlada SAD-e, uglavnom na Univerzitetima u Evropi i SAD. Nezvanično cilj je bio testiranje alternativnih mogućnosti komunikacije u slučaju nukleranog rata.
Ubrzo su se pojavili alati i aplikacije – poput jednostavnog protokola za prenos pošte (SMTP, koji se obično naziva e-pošta), za slanje kratkih poruka i protokola za prenos datoteka (FTP), za duže prenose.
Kako bi se postigla isplativa interaktivna komunikacija između računara, koja obično komuniciraju u kratkim nizovima podataka, ARPANET je koristio novu tehnologiju komutacija paketa. Ova tehnologija, za razliku od tradicionalnih telefonskih komunikacija paketa ne zahtijeva jedno namjensko kolo između svakog para korisnika (što je značilo disperziju potencijalnih ciljeva: telefonskih centrala i čvorova za koje se predpostavljalo da su moguća meta u slučaju rata).
Ovakve komercijalne paketne mreže uvedene su 1970-ih, ali one su prvenstveno dizajnirane da omoguće efikasan pristup udaljenim računarima putem namjenskih terminala. Zamijenili su modemske veze na velike udaljenosti manje skupim "virtualnim" sklopovima preko paketnih mreža. U Sjedinjenim Državama, Telenet i Tymnet bile su dvije takve paketne mreže. Nijedna nije podržana komunikacija između hosta; 70-ih godina prošlog vijeka to je još uvijek bilo područje istraživačkih mreža.
Zemaljski paketni radio sistem omogućio je mobilni pristup računarskim resursima, dok je paketna satelitska mreža Uvođenjem paketnog prenosa postalo je izvedivo povezivanje mobilnog terminala s računarskom mrežom. DARPA je koristila paketnu satelitsku mrežu za povezivanje Sjedinjenih Država sa satelitskim terminalima koji su morali biti spojeni na druge mreže u evropskim zemljama kako bi došli do krajnjih korisnika. Tako se javila potreba za povezivanjem paketne satelitske mreže, kao i paketne radio mreže, s drugim mrežama.
DARPA je pokrenula program za istraživanje međusobnog povezivanja “heterogenih mreža”. Ovaj program, nazvan **Internetting**, ne samo zbog imena smatra se pretečom sadašnjeg interneta, Pa bi se moglo reći da je internet "rođen" prije IP protokola, mada ga oni danas definišu.
Interneting je bio zasnovan na konceptu umrežavanja otvorene arhitekture, u kojem bi mreže sa definisanim standardnim interfejsima bile međusobno povezane „gatewayima“. Planirana je radna demonstracija koncepta. Da bi koncept funkcionirao, morao je biti dizajniran i razvijen novi protokol; zaista, bila je potrebna i sistemska arhitektura.
Godine 1974. Vinton Cerf, tada na Univerzitetu Stanford u Kaliforniji, kao saradnik DARPA-i prvi je opisao takav protokol i arhitekturu sistema, Bio je kontrolisani protokol prenosa (TCP), koji je omogućio komunikaciju različitih tipova mašina na mrežama širom svijeta za usmjeravanje i sastavljanje paketa podataka. TCP je sa ranijim Internet protokolom (IP) formirao TCP/IP paket, standard, koji je usvojilo Ministarstvo odbrane SAD 1980. godine.
**Tako je krajem osamdesetih godina prošlog vijeka nastao internet u formi koju ima i danas.**
Internet kakav danas poznajemo ima ključnu tehnološku ideju – ideju mreže otvorene arhitekture. Izbor neke mrežne tehnologije nije diktiran određenom arhitekturom, već je ostavljeno korisniku da slobodno bira i poveže se sa ostatkom mreže.




## Mrežne arhitekture sa aspekta međusobnog odnosa i tehnike pristupa

Postoje tri osnovna odnosa između umrežemih računara (preciznije komunikatora) u mreži. To su:

1. Terminalski odnos
2. Arhitektura ravnopravnih računara: P2P i
3. Klijent server arhitektura

Pošto su terminali uglavnom stvar prošlosti pozabavićemo se nešto detaljnije sa ostale dvije arhitekture.


Ovu tvrdnju treba uzeti sa određenom rezervom.

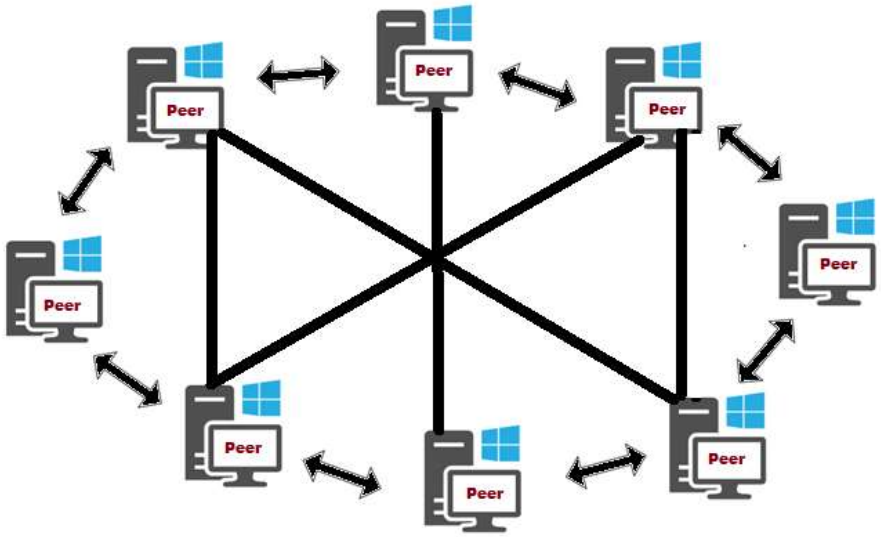
Moderne tehnologije su dale novi smisao terminalskom odnosu i terminalskim mrežama, ali ovdje se nećemo baviti time.

# P2P mreže ravnopravnih računara (peer-to-peer mreža)

Kod mreža ravnopravnih računara ne postoje namjenski serveri niti hijerarhija računara.

**Peer-to-peer** je mreža ravnopravnih računara, server ne postoji, svaki računar u mreži ima ulogu i klijenta i servera, a korisnik odlučuje koliki dio informacija će biti dostupan ostalima. Ovaj sistem organizacije se primjenjuje u posebno malim mrežama, a nikako u većim preduzećima, upravo zbog prevelike izloženosti podataka i niskom nivou sigurnosti važnih informacija.

Svi računari su jednaki, odnosno ravnopravni. Nude jednostavan pristup povezivanju računara radi zajedničkog korišćenja resursa i međusobne komunikacije. Svaki računar funkcioniše i kao klijent i kao server, pa ne postoji administrator koji bi bio odgovoran za cijelu mrežu. Korisnik svakog računara sam određuje koji se resursi na njegovom računaru mogu dijeliti preko mreže..




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

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

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

- Umrežavanje je jednostavno.
- Ne zahtjeva se kupovina posebnog softvera za umrežavanje.
- Korisnici su sami sebi administratori i sami planiraju bezbjednost.
- Ispad nekog računara iz mreže ima uticaj samo na eventualno dijeljene resurse na datom računaru. Ostali računari mogu da nastave rad.

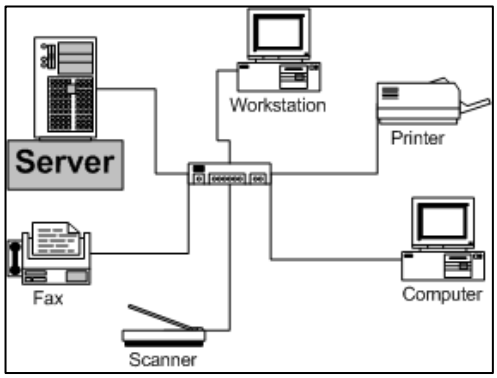
Ove mreže su dobar izbor u sljedećim situacijama:

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

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

## Namjena i tipovi servera

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




Mrežni server je računar dizajniran da djeluje kao centralno mjesto i repozitorij koji pomaže u pružanju različitih usluga i resursa kao što su pristup hardveru, prostor na disku, pristup štampaču, itd. na druge računare u mreži.
Mrežni server se ne mora da razlikuje od radne stanice[5] po hardveru, ali funkcionalnost koju obavlja jasno ga razlikuje od drugih radnih stanica.
Usluge koje server pruža klijentima se realizuju preko namjenskih softverskih paketa (ili su zasnovane na mogućnosti-ma operativnog sistema). Na jednom računaru je moguće instalirati više različitih softverskih paketa i na taj način dobiti multifunkcionalni server. Ovakav pristup je opravdan ukoliko hardverska moć računara može da podrži istovremeno izvršavanje pomenutog softvera i ukoliko sve usluge koristi uglavnom ista grupa korisnika. U protivnom, kombinovanje servisa na jednom računaru može u slučaju greške u jednom softverskom paketu ugroziti bezbjednost i dostupnost ostalih servisa na tom računaru. Noviji odgovor za ovaj problem leži u virtualizaciji.

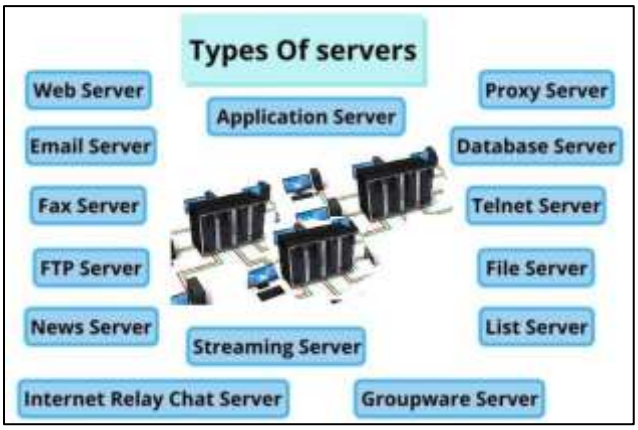
[5] Kod mreža radna stanica je čvor koji može upravljati lokalnom obradom informacija. Koristi se i kao sinonim za klijentski računar, ali često se tim terminom naglašava da je to računar manje snage u odnosu na cetralni – serverski računar. Ranije (u vrijeme ranih PC računara) radna stanica je opisivala moćniji i brži personalni računar koji je imao veće mogućnost multitaskinga zbog dodatne RAM memorije i grafičkih adaptera veće brzine i kao takav bio glavni terminal na LAN-u.

**Virtualizacija servera** predstavlja korišćenje specijalnog sistemskog proširenja operativnog sistema koje omogućava kreiranje većeg broja "logičkih" računara koji dijele stvarne (fizičke) resurse. Na svakom od logičkih servera se može instalirati različit operativni sistem sa različitim softverskim paketima i na taj način omogućiti određeni servis u mreži.
Postoji i situacija kada hardverske mogućnosti jednog računara nisu u stanju da odgovore potrebama velikog broja korisnika servisa istovremeno. U tom slučaju se ista uloga raspodijeljuje na veći broj fizičkih servera. Ukoliko se veći broj fizičkih servera krajnjima korisnicima predstavi kao jedna (logička) jedinica, takva konfiguracija servera se naziva **klaster**.

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

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

Raznovrsnost i složenost poslova koje serveri treba da obave je velika. Mnoge velike mreže imaju različite vrste servera:



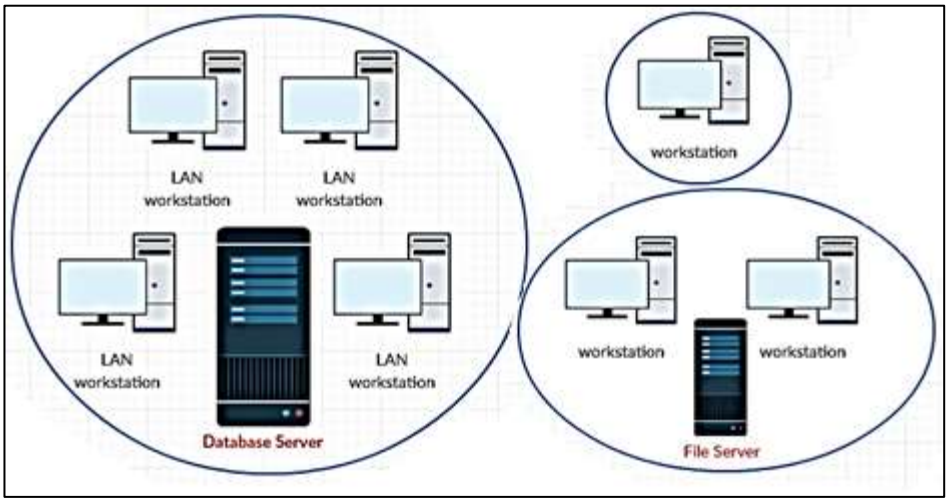

- **Server za datoteke i štampanje (File serveri)**

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

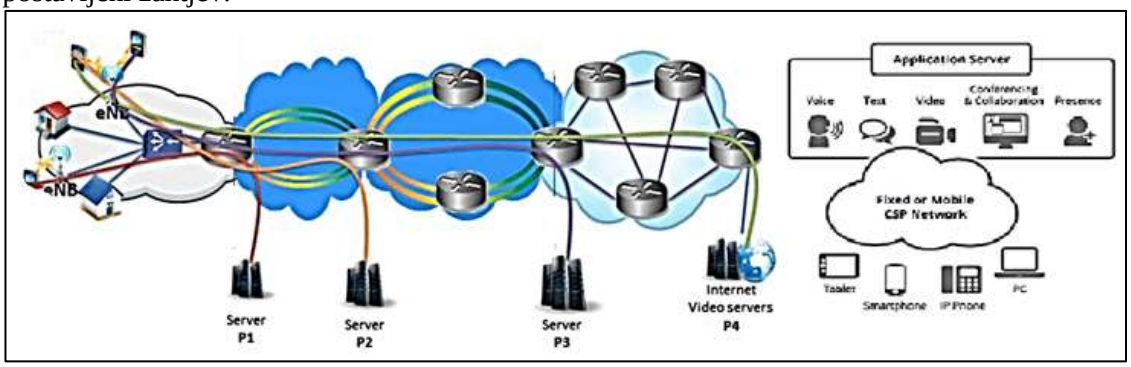
- **Server za aplikacije**

Host web aplikacije (računarski programi koji se pokreću unutar web pretraživača) omogućuju korisnicima u mreži da ih pokreću i koriste, bez potrebe da instaliraju kopiju na svoje računare. Server za aplikacije klijentu na raspolaganje stavlja klijentsku stranu klijent/server aplikacije. U serverima se nalazi velika količina različitih podataka koji su organizovani tako da je njihovo pozivanje jednostavno.

Razlika između servera za datoteke i štampanje i servera za aplikacije nalazi se u načinu odgovora na zahtjev računara koji je zatražio podatke. U slučaju servera za datoteke i štampanje, podaci ili datoteke se učitavaju u računar koji ih zatraži.




Međutim, kod servera za aplikacije, centralna logika aplikacije i osnovni podaci ostaju na serveru, a u računar koji je zatražio podatke učitavaju se samo rezultati zahtjeva. Klijentska aplikacija radi lokalno i pristupa podacima iz serverske aplikacije. Umjesto da se u lokalni računar učitava čitava baza podataka, učitavaju se samo rezultati koji se dobijaju kao odgovor na upit. Na primjer, ukoliko nam je iz baze podataka radnika potrebno da izdvojimo one koji su rođeni u novembru, server za aplikacije nam, na naš zahtjev, neće odgovoriti učitavanjem čitave baze podataka. Umjesto toga, na lokalni računar će biti poslat samo odgovor na postavljeni zahtjev.




- **Komunikacioni server**

Komunikacioni serveri upravljaju protokom podataka i elektronskih poruka između mreže u kojoj je sam server i drugih mreža, glavnih računara (engl. mainframe) i udaljenih korisnika koji putem modema i telefonskih linija pristupaju serveru. Održava okruženje koje je potrebno da jedna krajnja tačka komunikacije (korisnik ili uređaji) pronađe druge krajnje tačke i komunicira s njima.

- **Serveri za organizaciju podataka**

Ovi serveri omogućavaju korisnicima da pronađu, smjeste i zaštite podatke u mreži. Na primjer, mrežni softver može računare da grupiše u logički organizovane grupe koje se zovu domeni, a to omogućava svim korisnicima mreže pristup svakom mrežnom resursu.

Sa širenjem mreže, planiranje specijalizovanih servera dobija na značaju. Planer mreže mora da uzme u obzir očekivani rast mreže tako da se mreža ne poremeti ukoliko se javi potreba da se uloga nekog servera promeni.

- **Kataloški serveri**

Ovi serveri održavaju i kreiraju indeks ili tabelu sadržaja informacija koje se mogu pronaći u velikoj distribuiranoj mreži, poput računara, korisnika, datoteka dijeljenih na fajl serverima serverima i web aplikacija. Primjeri su Server imenika i Server imena kao što su (kasnije objašnjeni) DNS serveri. Ovo mož biti bilo koji računar koji treba pronaći nešto na mreži, kao što je član Domene koji se pokušava prijaviti, klijent e-maila koji traži adresu e-maila ili korisnik koji traži datoteku

Tradicionalno postoje još neki tipovi servera:

• **Mail serveri**: Omogućavaju vam premještanje i pohranjivanje pošte putem lokalne mreže, široke mreže i putem interneta

• **Web serveri**: su serveri koji vam omogućavaju skladištenje i upravljanje podacima na web stranici. Uobičajeni web serveri su Apache, Microsoft Internet Information Services (IIS) i Nginx.

• **Serveri protokola** za prenos datoteka (**FTP**): Oni olakšavaju siguran prenos datoteka sa jednog računara na drugi.

• Posrednički-**Proxy server**: Nalazi se između klijentskog programa i eksternog servera. Djeluje kao posrednik između klijenta i drugih servera, prihvaćajući dolazni promet od klijenta kojeg onda proslijeđuje serveru. Razlozi za to uključuju kontrolu i filtriranje sadržaja, poboljšanje performansi u prometu, sprečavanje neovlaštenog pristupa mreži ili jednostavno usmjeravanje prometa preko velike i komplikovane mreže.

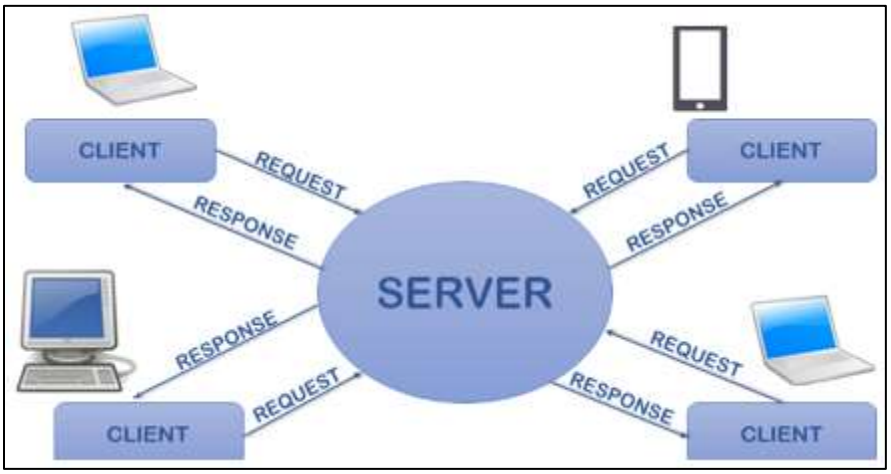
• **Virtualni server** Dijeli hardverske i softverske resurse s drugim virtualnim serverima. Postoji samo kako je definisan u specijaliziranom softveru zvanom hipervizor. Virtuelizacija servera omogućava efikasniju infrastrukturu.

Često se vrši klasifikacija servera i prema operativnom sistemu koji koristi. Danas postoji veliki broj operativnih sistema.
Prema nekim statistikama, otprilike 80% svih servera koristi neku varijaciju Linuxa, dok oko 20% servera koristi Windows.

Administrator servera ili admin ima ukupnu kontrolu nad serverom.
Ovo je obično u kontekstu poslovne organizacije, gdje administrator servera nadgleda performanse i stanje više servera u poslovnoj organizaciji, ali može biti u kontekstu jedne osobe koja pokreće server za igre.

# Klijent server arhitektura

**Klijent-server** je arhitektura gdje su klijent (korisnik) i server odvojeni ili neravnopravni.
U **mrežama sa serverom**, postoji najmanje jedan računar u mreži koji vrši ulogu servera. To znači da jedini podaci koje klijenti mreže dijele i kojima imaju pristup su podaci koji se nalaze na serveru. **Centralni server funkcioniše, u tom slučaju, kao baza podataka dostupna svima u mreži**. Ovakav sistem primjenjuju najčešće velika preduzeća i korporacije.




*Klijent server arhitektura*

Klijent je obično aktivan korisnik, koji šalje zahtjeve i čeka dok se isti ne ispune, dok je server pasivan, čeka da dobije zahtjev koji ispunjava i šalje korisniku. Serveri su obično veoma jake mašine sa dobrim konfiguracijama i karakteristikama.
Obično servere pogone i posebni operativni sistemi za razliku od običnih – klijent operativnih sistema, serverski operativni sistemi su u više segmenata bolji i sadrže naprednije opcije.
Klijenti i serveri razmjenjuju poruke u obrascu razmjene poruka zahtjev-odgovor. Klijenti pokreću komunikacijske sesije sa serverima, koji čekaju dolazne zahtjeve; klijent šalje zahtjev, a server vraća odgovor.
Ova razmjena poruka je primjer međuprocesne komunikacije. Da bi komunicirali, računari moraju imati zajednički jezik i moraju slijediti pravila tako da i klijent i server znaju šta mogu očekivati.
Jezik i pravila komunikacije definisani su komuni-kacionim protokolima.
Klijent obično ne dijeli nijedan od svojih resursa, ali zahtijeva sadržaj ili uslugu od servera.
Većina mrežnih aplikacija koristi model klijent-server (na njemu je zasnovan World Wide Web i e-pošta npr.) Komunikacijskim protokolima definisana je strukturu i za zahtjeve između klijenta i servera u mreži. Na primjer, web pretraživač na računaru korisnika (klijent) koristi HTTP protokol za traženje informacija od web stranice na serveru.

| Protokol bez državljanstva - **Stateless Protocol**<br>Klijentski zahtjev prema serveru se često opisuje kao "atomski, potpun i bez državljanstva". Odgovor servera je opisan kao "potpun" i obično trenutan.<br>"Atomska" priroda zahtjeva klijenta znači da zahtjev postoji kao samostalni element podataka u mrežnom okruženju. Mnogi klijenti mogu uputiti potpuno isti zahtjev serveru. Ali da bi zahtjev bio "isti", svaki takav zahtjev mora poslati potpuno iste informacije. |
|---|

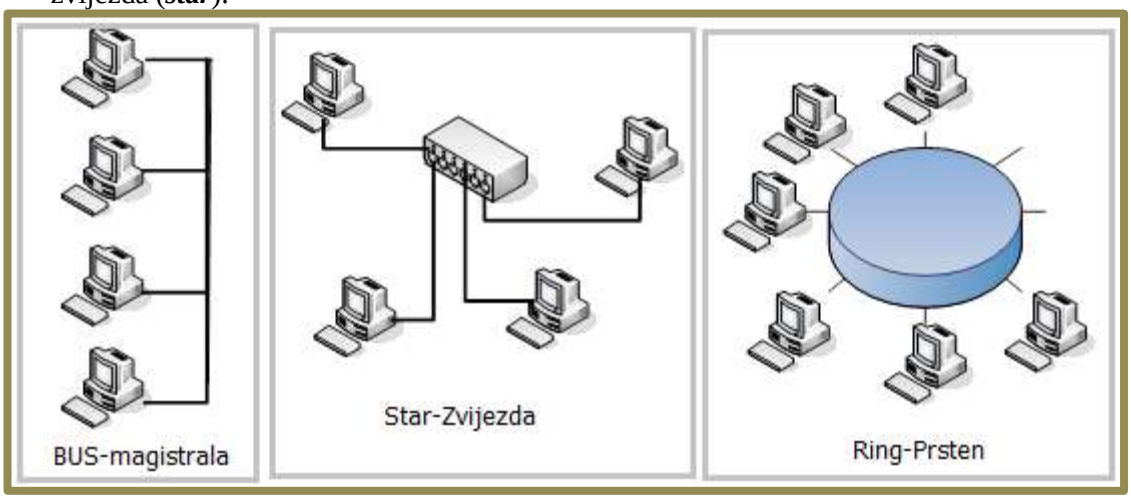
U HTTP protokolu, zahtjev se sastoji od URL-a, zaglavlja (uključujući HTTP kolačiće) i podataka koje dostavlja klijent. I kao element, zahtjev ne može biti podijeljen.
"Kompletna" priroda zahtjeva klijenta znači da zahtjev sadrži sve vanjske informacije koje server može koristiti da odgovori na zahtjev. Server se ne može vratiti klijentu da dobije više informacija. Zahtjev je jednosmjerna komunikacija. Kada se jednom pošalje, klijent više nema šta da kaže serveru. (Mada server može koristiti druge informacije bez zahtjeva da odgovori klijentu, ali to nije isto što i dobijanje dodatnih informacija od klijenta.)
Priroda zahtjeva klijenta bez državljanstva je složenija. To znači, generalno, da klijent i server ne znaju ništa jedno o drugom osim onoga što je predstavljeno u zahtjevu i vraćeno u odgovoru. U trenutnom okruženju web interaktivnosti, ova istina može biti zamagljena. Svi znamo da se možemo "logirati" na web stranicu i da web stranica "pamti" naš status, koje se postiže upotrebom HTTP kolačića i baza podataka na strani servera.

Napomena:
I klijent i server mogu biti u istom sistemu, ali to neće biti predmet naše pažnje.

## Standardne mrežne topologije

LAN topologija definiše način povezivanja računara i ostalih uređaja u mreži. Lokalna mrežna topologija može se opisati sa stanovišta fizičke ili logičke perspektive.
**Fizička topologija opisuje geometrijsko uređenje komponenti koje sadrži LAN**, odnosno proučava i objašnjava kako se mrežne komponente stvarno, fizički povezuju odgovarajućim medijumom.
**Logička topologija opisuje mogućnost veze između dvijekrajnje tačke mreže** koje komuniciraju, odnosno objašnjava kako informacija putuje kroz mrežu.
**Postoje tri osnovne LAN topologije**:

- magistrala (***bus***),
- prsten (***ring***) i
- zvijezda (***star***).




*Tri osnovne topologije LAN mreža*

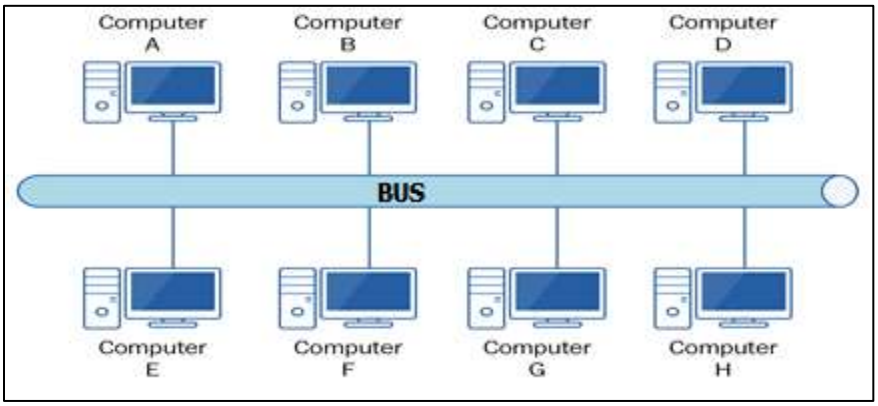
*Naravno, ove se mreže mogu i kombinovati, pa tako možemo naprimjer povezati dvije star mreže kao dva mrežna segmenta magistalne mreže.*

Ove topologije predstavljaju logičku arhitekturu mreže, ali **fizički, uređaji ne moraju da budu stvarno raspoređeni u ovom obliku**. Bus i ring logičke topologije su često fizički organozovane kao star topologija odnosno u obliku zvijezde.

Izbor i specifikacija topologije LAN mreže zavisi od: fizičkih lokacija na kojima se nalaze korisnici sistema, količine podataka u lokalnim bazama podataka i količine potrebnog ažuriranja tih baza, od frekvancije pristupa bazama na drugim lokacijama i zahtjeva za komuniciranjem između dvije korisničke lokacije.

## BUS magistrala (sabirnica)

**Najjednostavnija metoda**. Jedan kabal povezuje sve računare, servere i periferijske uređaje. Podaci se u mreži šalju preko kabla direktno na fizičku adresu odredišnog računara.




Ponovo dolazimo do pojma *ethernet*.

Najpoznatiji primjer LAN tehnologije sa sabirnicom je verzija *Ethernet*-a. *Riječ je o tehnologiji koja se razvija od ranih 1970-tih godina (Xerox, DEC, Intel, IEEE), doživjela je nekoliko generacija, te danas dominira tržištem. U originalnoj verziji postojala je sabirnica - **koaksijalni kabel zvani ether**. Taj kabel nije smio biti dulji od 500 m, a spojevi na njega morali su biti udaljeni barem 3 m.* **Ethernet** je najzastupljeniji tip kod implementacije bus mreža. **Ethernet standard** propisuje format okvira, te način slanja bitova kroz sabirnicu neposrednim pretvaranjem bitova u promjenu napona.

Pošiljatelj šalje okvir u obliku električnog signala koji se širi od pošiljatelja o oba smjera po kablu. Svi računari "vide" signal. Primatelj iz signala reprodukuje okvir.

Šta podrazumjeva ova metoda?

Najvažnije je da se zna da u datom trenutku samo jedan računar šalje podatke na mrežu. Podaci se šalju svima, a preuzima ih računar kome su upućeni. Ukoliko neki drugi računar u mreži pokuša da u istom trenutku pošalje nešto mrežom, on dobija signal da se nečiji podaci već nalaze na njoj, tj. na mreži postoji saobraćaj i čeka da se mreža oslobodi. Ako u istom trenutku dva računara pokušaju da pristume mreži dolazi do kolizije.

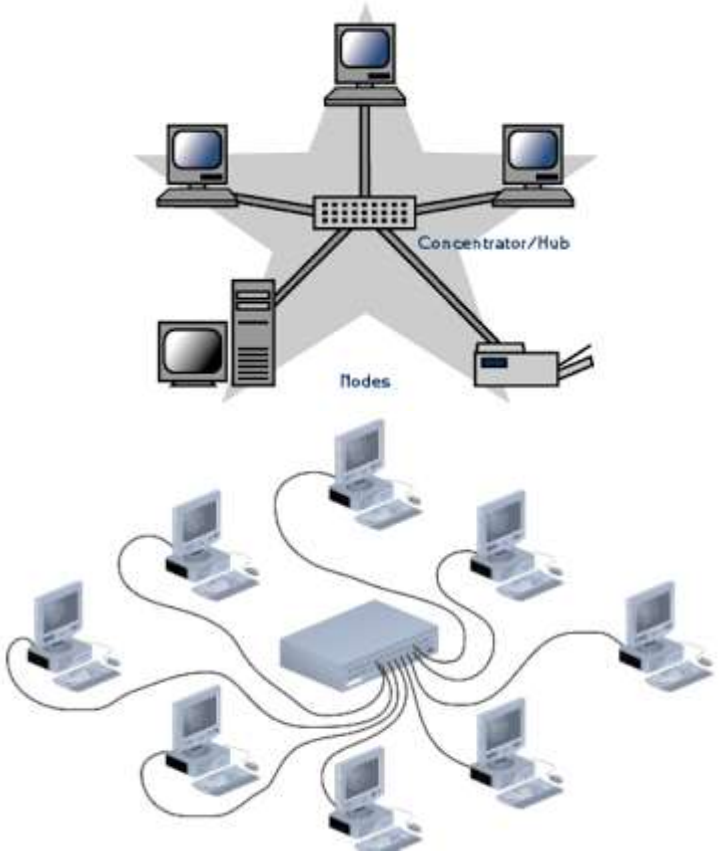
Ethernet zbog toga koristi uređaj CSMA/CD (*Carrier Sense and Multiple Access with Collision Detection*).

Računari dobijaju informaciju o koliziji i jedan od njih šalje ometajući signal kojim obavještava ostale korisnike. Poslije toga, svaki od njih odlaže slanje podataka na mrežu u cilju sprečavanja ponovne kolizije na određeno vrijeme.

Prednosti topologije magistrale: lako je dodati novi mrežni uređaj ovoj topologiji, zahtjeva daleko manje kabla nego ostale topologije.
Mane: cijela mreža može biti u prekidu ako negdje postoji prekid na glavnom kablu; teško je otkriti problem kod mreže.

## STAR mreže

Star topologija ili topologija zvijezde predstavlja takav oblik arhitekture gdje su krajnji čvorovi na mreži povezani preko posebne veze na centralni hub ili svič.
Prednosti ove topologije: lako se instalira i povezuje; nema prekida u mreži pri dodavanju novog uređaja ili uklanjanja; lako je otkriti greške i zamjeniti dijelove i sl. Mane ove topologije: podložna je zagušenjima sobraćaja, zahtjeva više kabla nego linearna topologija; ako se hub ili switch pokvari svi čvorovi su ugašeni; mnogo skuplja topologija od npr. bus topologije.




Kod ovih mreža postoji centralna tačka na koju se povezuju svi računari u mreži. Taj uređaj se naziva hub ili koncetrator.

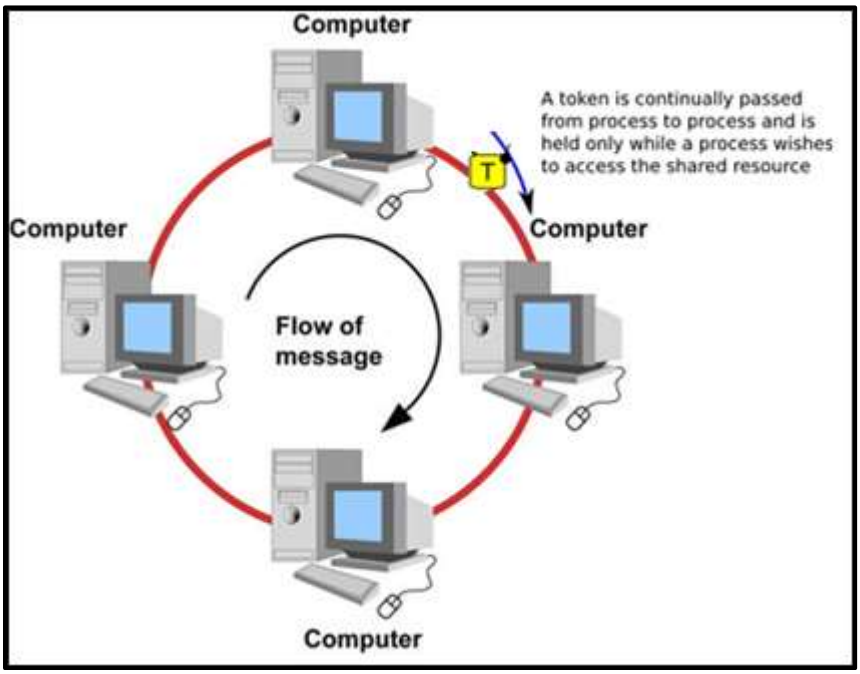
Topologija zvijezde je linearna LAN arhitektura, kod koje se prenos podataka obavlja cijelom dužinim fizičkog mediuma kojim se prenose podaci i podaci se prenose svim radnim stanicama.

Ovaj vid mrežne topologije je **najzastupljeniji danas**, jer u slučaju da jedan dio mreže otkaže, ostatak nastavlja sa radom. Takođe, brz rast mreže omogućava lako dodavanje mrežnih priključaka, sve što trebamo uraditi je povezati više hubova. U slučaju korišćenja aktivnog huba moguće je kontrolisati mrežni saobraćaj pomoću protokola za nadgledanje mreže poput SNMP-a.

*Kako to da smo u predhodnom poglavlju tvdili da je Eternet (kao sabirnica-magistrala) najzastupljeniji, a sad je to zvijezda?*
*Pa jednostavno, zbog razlike u logičkom i fizičkom pristupu. Fizički je to star, a logički bus.*
Logičke bus ili ring topologije su često fizički implementirane kao star topologije.

## Token Ring mreže - Prstenaste mreže

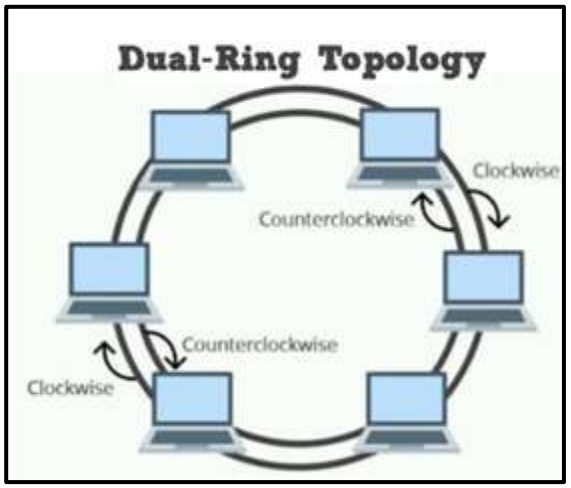
Ring topologija[6] ili topologija prstena predstavlja način na koji su uređaji međusobno logički povezani. Ovakva vrsta mreže se sastoji od više uređaja povezanih jedan sa drugim tako da se obrazuje zatvorena kružna putanja.
Računari u ovim mrežama se povezuju u logički krug kroz koji putuju podaci i prolaze kroz svaki računar u mreži. Kod prenosa se koristi tzv. **token passing metoda**.



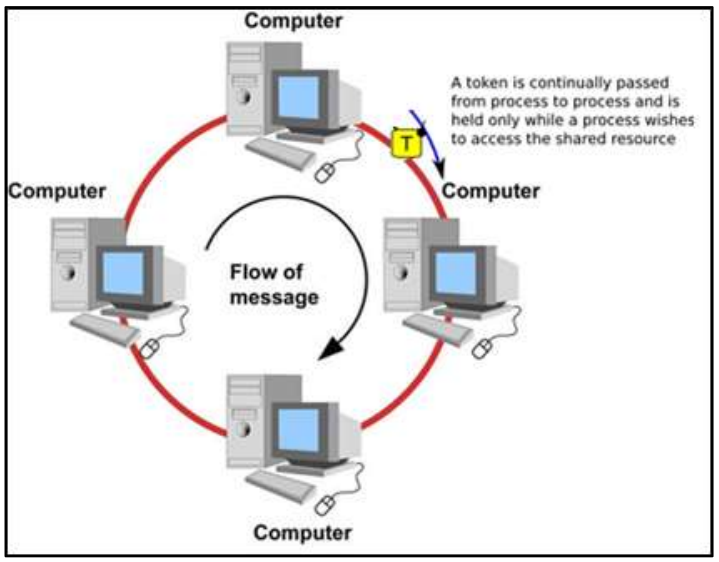

[6] *Token Ring je protokol sloja veze podataka. Token Ring koristi drugačije specifikacije fizičkog sloja, drugačije MAC mehanizme i drugačije formate okvira od Ethernet mreža. Izvorni standard za token ring mreže bio je intelektualna svojina kompanije IBM. Kasnije je* **IEEE** *je ovaj protokol standardizovala pod imenom* **802.5**.

Kod ove metode **poseban paket** podatak, tzv. **Token (žeton), putuje kroz mrežu od računara do računara**. Kada token dođe do računara koji želi da pošalje podatke, on ga menja (između ostalog dodaje MAC adresu pošiljaoca, adresu primaoca i podatke koje treba poslati) i šalje dalje kroz mrežu, sljedećem računaru, ovaj sljedećem i tako redom. Podaci prolaze kroz mrežu od računara do računara redom, sve dok ne stignu do odredišta. Odredišni čvor (računar) mijenja token kopira podatke i dodaje im potvrdu o prijemu. Ovakav token sada kruži dalje do računara koji je poslao podatke. Poslije toga se sa mreže uklanjaju kontrolni podaci, da bi se mreža oslobodila. *Ovo nije ni u kom slučaju neefikasno ili sporo, jer token signal mrežom putuje brzinom svjetlosti.*

Na mreži, kao i kod bus mreža, može da postoji u jednom trenutku samo jedan token. Ako neko želi da koristi mrežu, mora da sačeka da se saobraćaj na njoj oslobodi. S obzirom da podatke može da šalje samo računar kod kojeg se nalazi token, **ne može** se desiti da dva računara istovremeno šalju podatke, pa je samim tim isključena mogućnost pojave sukoba.



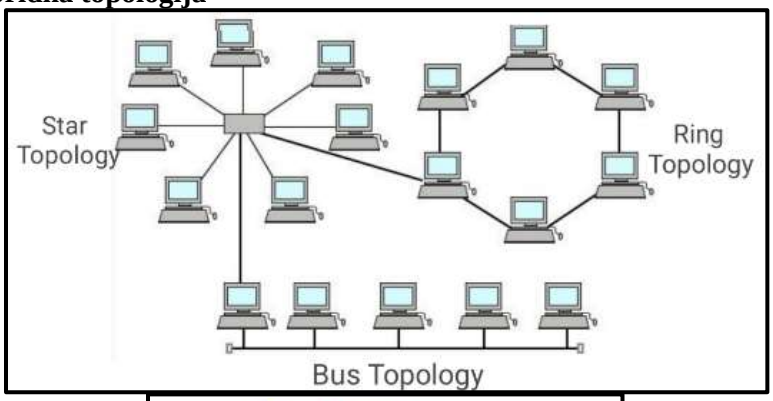

Takođe, postoje i dual ring mreže gdje postoje primarni i sekundarni krug. U normalnoj razmjeni se koristi primarni prsten, međutim, u slučaju njegovog prekida, mreža se automatski konfiguriše da koristi sekundarni u kome se saobraćaj kreće u suprotnom smjeru od primarnog.



# Dodatne i izvedene mrežne topologije

Već smo rekli da postoji mogućnost kombinovanja predhodno opisane tri osnovne mrežne topologije.
Nevešćemo i ilustrovati neke od mogućih rješenja.

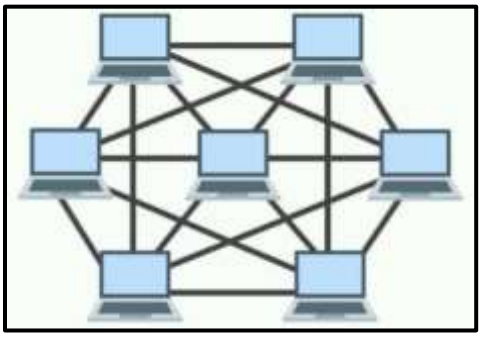
**Hybrid - Hibridna topologija**





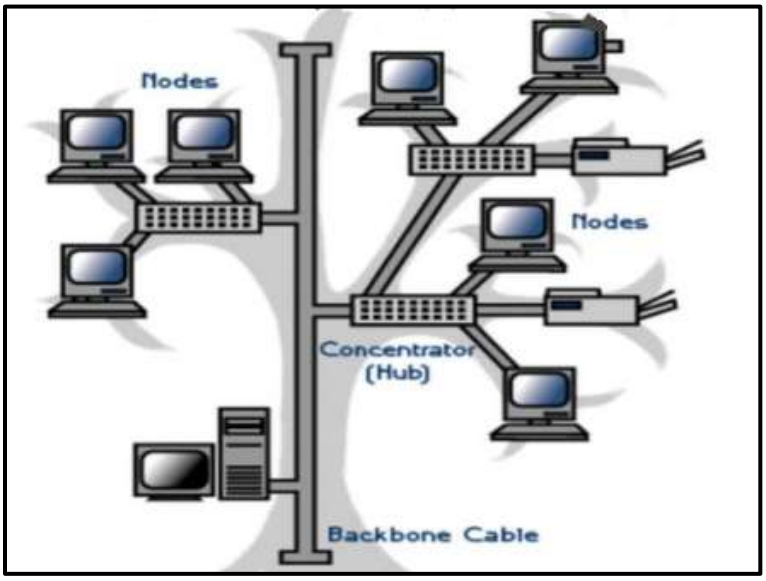
Topologija koja koristi dvije ili više mrežnih topologija naziva se hibridna topologija. Svi čvorovi povezani na svaku zvjezdastu mrežu imat će centralni uređaj, koji će biti ili čvorište, ili svič, a kablovi magistrale će se povezati na čvorište ili prekidač za međusobno povezivanje svake topologije zvijezde.

**Mesh-zamršena topologija**



Višestruka mrežna veza između računara kako bi se obezbijedilo više putanja za prenos podataka.

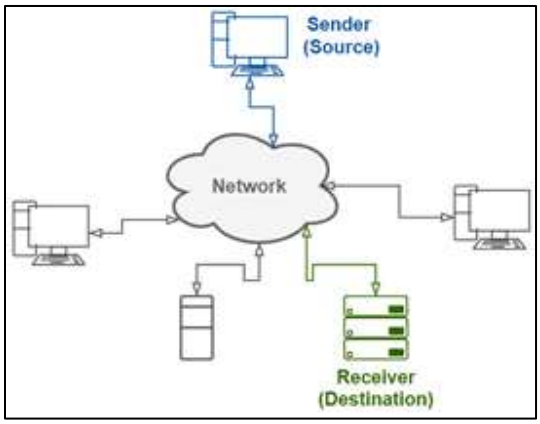
**Tree Topology-Topologija stabla**




U topologiji stabla, može se povezati više segmenata sa jednom vrstom topologije kao što je sabirnica, prsten-prsten, zvijezda-star. Budući da bilo koja **dva čvora mogu imati samo jednu međusobnu** vezu, topologije stabla stvaraju prirodnu roditeljsku i podređenu hijerarhiju (**parent/child**) .

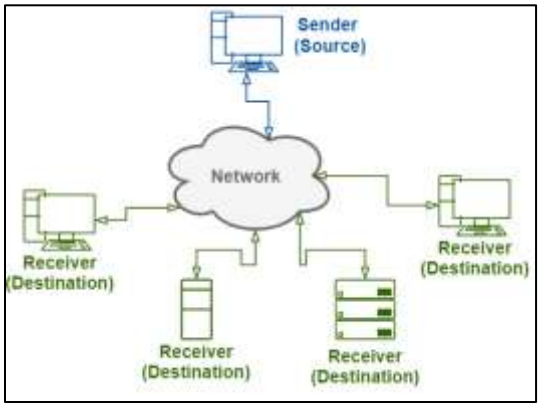
# Podjela računarskih mreža prema tehnologiji prenosa

Prenos podataka u LAN mreži se dijeli na tri klase: *unicast, broadcast i multicast.*



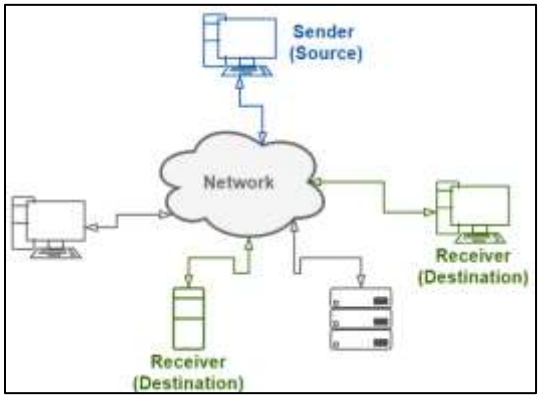

Kod *unicast* prenosa jedan paket je poslat od izvora do odredišta na mreži. Izvorni čvor adresira paket koristeći adresu koja će biti na odredištu, potom se paket šalje na mrežu, i konačno na odredište.

Unicast isporučuje poruku jednom specifičnom čvoru koristeći asocijaciju jedan na jedan između pošiljaoca i odredišta: svaka odredišna adresa jedinstveno identificira jednu krajnju tačku primatelja.

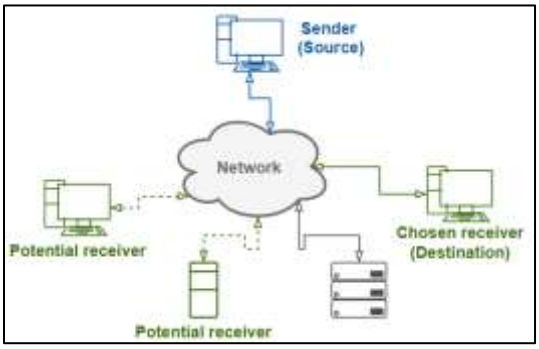



*Broadcast* prenos podatak se sastoji od jednog paketa podataka koji se kopira te šalje svim čvorovima koji se nalaze u mreži.

Broadcast isporučuje poruku svim čvorovima u mreži koristeći asocijaciju jedan na sve; jedan datagram (ili paket) od jednog pošiljaoca se usmjerava na više krajnjih tačaka (sve moguće) povezanih s adresom emitiranja. Mreža automatski replicira datagrame po potrebi kako bi dosegla sve primaoce unutar opsega emitiranja, što su generalno sve podmreže mreže.

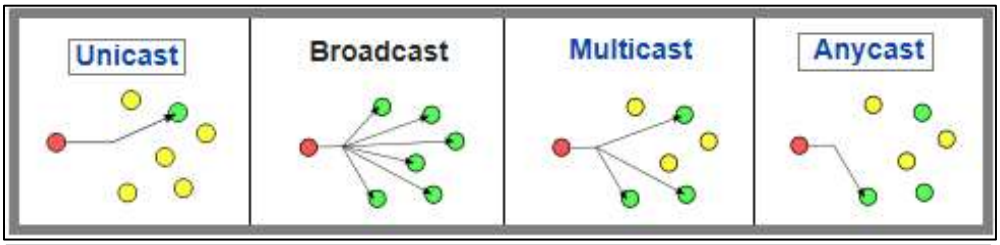



*Multicast* prenos podataka se sadrži od jednog paketa podataka koji se kopira i šalje na specifične podskupove uređaja na mreži. Multicast isporučuje poruku grupi čvorova koji su izrazili interes za primanje poruke koristeći asocijaciju jedan-prema-mnogo-od-više ili mnogo-prema-mnogo-od-više; datagrami se rutiraju istovremeno u jednom prenosu na više primalaca. Multicast se razlikuje od Broadcast emitiranja po tome što odredišna adresa označava podskup, ne nužno sve, dostupnih čvorova.




*Anyast* ili usmjereni prenos je u osnovi vrsta Unicast prenosa.

Anycast isporučuje poruku bilo kojem iz grupe čvorova, obično onom najbližem izvoru koristeći asocijaciju jedan-na-jedan-od-više gdje se datagrami usmjeravaju na bilo kojeg pojedinačnog člana grupe potencijalnih primatelja koji su svi identifikovani istom adresom odredišta. Algoritam usmjeravanja bira pojedinačni prijemnik iz grupe na osnovu kojeg je najbliži prema nekoj mjeri udaljenosti ili cijene.




Message Addressing Methods

| Method | Source-to-Destination | How many potential destinations? | How many destinations receive the message? |
|---|---|---|---|
| Unicast | One-to-One | One | One |
| Broadcast | One-to-All | Multiple | Multiple |
| Multicast | One-to-Many | Multiple | Multiple |
| Anycast | One-to-Any | Multiple | One |

Razlikujemo dva tipa mreža:

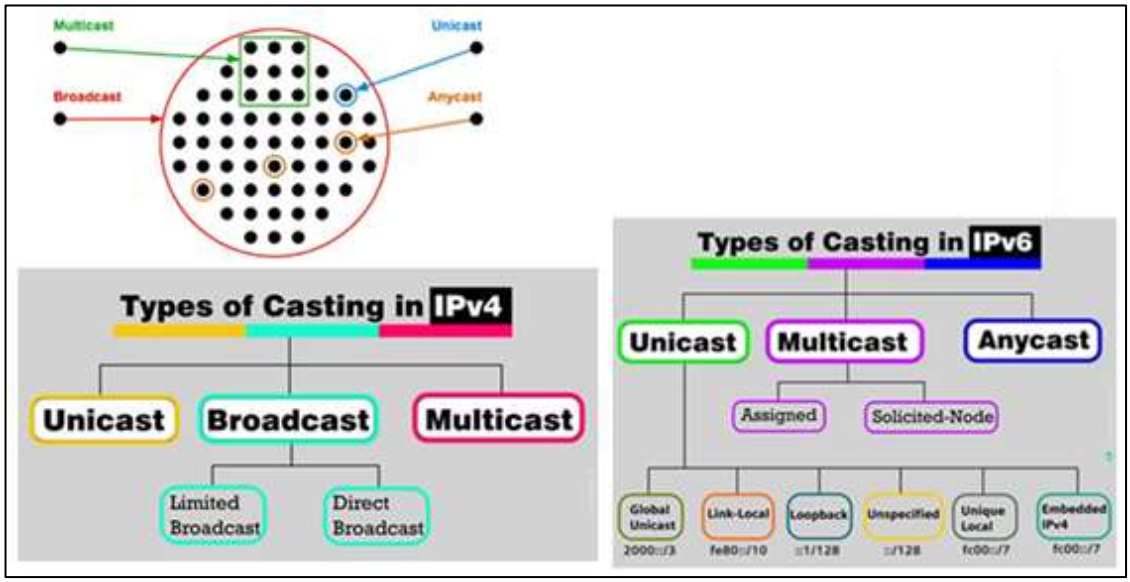
- difuzijske mreže (*broadcast network*)
- mreže od tačke do tačke (*point-to-point network*)

Kod difuzijskih mreža postoji jedan komunikacijski kanal koji dijele svi uređaji na mreži. Ovo je način prenošenja poruke svim primaocima istovremeno U paketu koji se šalje mrežom postoji adresno polje koje određuje kojem uređaju je paket namijenjen. Primjeri su sabirnica i prsten, (gdje paket putuje do svih, a mogu da ga prihvate samo ovlašteni).

Mreže od tačke do tačke sastoje se od mnogo međusobno spojenih uređaja. Paket na svom putu od izvora ka odredištu može proći više čvorova. Jedan par čvorova povezan linijom. Podaci od izvora ka odredištu putuju preko više međučvorova.

U lokalnoj mreži, repetitorska čvorišta ili prekidači pružaju osnovnu povezanost. Čvorište pruža krug od tačke do više tačaka u kojem svi povezani klijentski čvorovi dijele mrežni propusni opseg. Svič sa druge strane obezbeđuje seriju kola od tačke do tačke, putem mikrosegmentacije, što omogućava svakom klijentskom čvorunicastu da ima namjensko kolo i dodatnu prednost pune dupleks veze.

Iz perspektive sloja OSI modela, i svičevi i čvorišta repetitora pružaju veze od tačke do tačke na fizičkom sloju. Međutim, na sloju veze podataka, čvorište repetitora pruža povezivanje od tačke do više tačaka – svaki okvir se prosljeđuje svim čvorovima – dok svič (komutator) obezbjeđuje virtuelne veze od tačke do tačke – svaki unikast okvir se prosljeđuje samo do odredišnog čvora.




*Ilustracija korištenja različitih tehnologija prenosa podataka i pristupa čvorovima sa aspekta protokola (koji će kasnije biti objašnjeni)*

Kasnije ćemo se pozabaviti OSI modelom pa gornji komentar, zasad, shvatite samo kao napomenu (važnu) da mrežnii uređaji mogu i koriste različite tehnologije i da mogu da pripadaju različitim mrežama.

## Vrste prenosa podataka

U računarskim mrežama postoje **dva** dijametralno suprotna načina prenosa podataka.

Kod prvog načina, koji je stariji, veza između izvorišta poruke i odredišta uspostavlja se kroz čvorove mreže, na način da se **zauzima kompletan spojni put**. Karakterističan primjer je javna telefonska komutirana mreža.

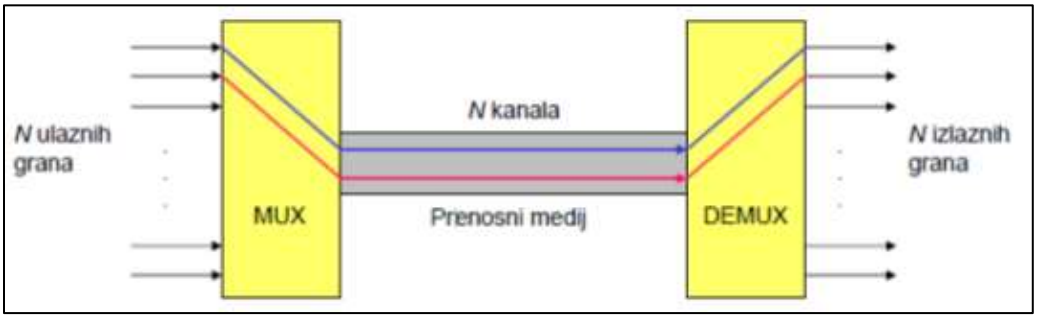
Drugi tip je paketski način prenosa, gdje se poruka **dijeli u manje cjeline** – pakete (okviri), a kroz mrežu se paketi mogu preusmjeravati po različitim spojnim putevima. Ovakav način prenosa je karakterističan kod Interneta.

# Multipleksovanje (Multipleksiranje: Multiplexing' ili 'Muxing')

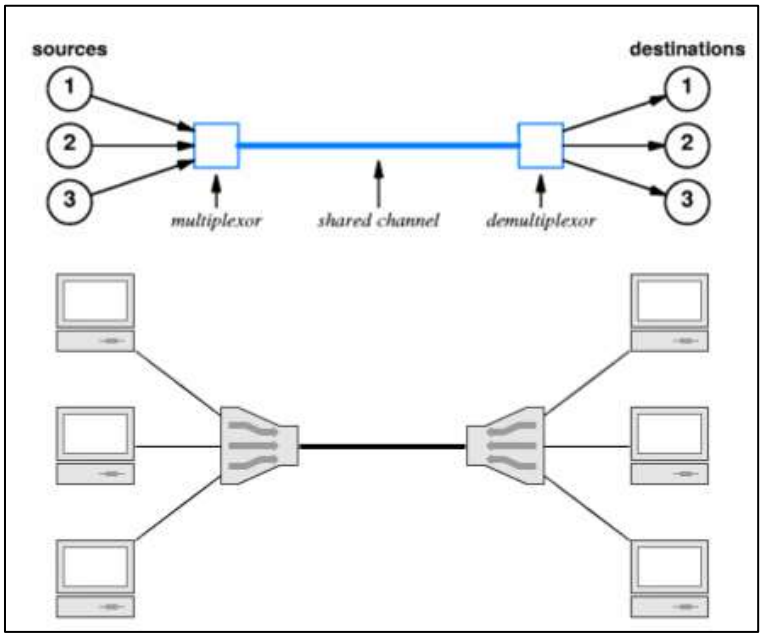
U elektronici, telekomunikacijama i računarskim mrežama multipleksiranje je proces u kome se **više** analognih **ili** digitalnih signala kombinuje **u jedan** signal i prenosi nekim prenosnim medijumom do željenog prijemnika.

Multipleksiranjem ili višestrukim iskorištenjem se većem broju izvora i odredišta omogućuje istovremena upotreba iste veze u mreži tj. prenosni medij se može višestruko koristiti.

Za multipeksiranje se koristi multipleksor (MUX) u koga ulazi N grana koje se kombinuju u jedan signal. Prenosni medij se dijeli na N kanala (N korisnika).




Demultipleksor (DEMUX) i multipleksor su povezani prenosnim medijem. DEMUX će izdvajati pojedine podatke iz odreñenog kanala i proslijediti ih na izlaz koji je predodreñen nekoj od N pripadajućih grana




*Ilustracija multipleksiranja (multipleksovanja) kod računarskih mreža*

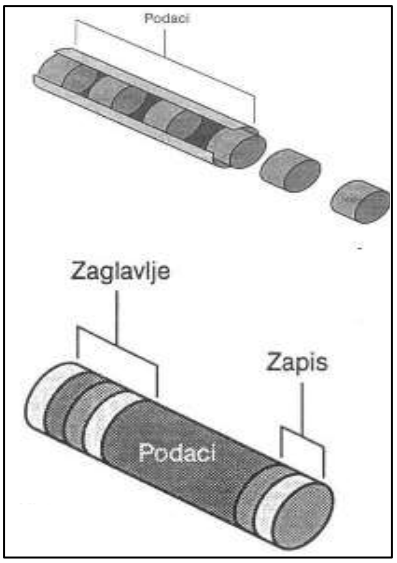
# Pojam paketa i paketne mreže

Kroz mrežu se podaci ne kreću kontinuirano već su razbijeni na manje jedinice koje nazivamo paketima (packets, frames). U većini mreža poruka se ne prenosi kao jedan kontinuirani niz bitova. Umjesto toga, svaka poruka dijeli se u male dijelove koji se zovu *paketi* i koji se šalju zasebno. Dakle pošiljatelj dijeli poruku u pakete, svaki paket putuje nezavisno kroz mrežu, a primatelj skuplja pakete pa ih ponovo sastavlja u poruku.

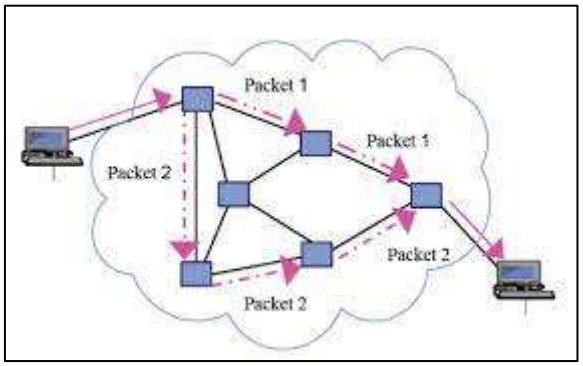
Zbog upotrebe paketa, mreže računara često se nazivaju *mreže s prospajanjem paketa* (**packet switching networks**). To je bitna razlika u odnosu na telefonske mreže, koje rade na drukčijem principu i nazivaju se *mreže s prospajanjem linija* (**circuit switching networks**).

Svaki paket sadrži:

1. **Zaglavlje paketa**
   - Adresa izvora, računar koji je poslao podatke
   - Adresu odredišta, računar koji prima podatke
   - Upravljački i kontrolni podaci
2. **Podatke koji se prenose** (512B-4KB)
3. **Prateći zapis**
   - Informacije o provjeri greške kojima se provjerava da li su paketi stigli neoštećeni (CRC).




***Paketna* mreža** je mreža koja omogućava prenos podataka preko više konekcija. Kada se podaci pošalju na mrežu, nije poznata putanja kojom će stići do odredišta. Podatak koji se šalje rastavlja se na više paketa koji sadrže, između ostalog redne brojeve i adrese pošiljaoca i odredišta. Podaci se zatim šalju kroz najpovoljnije putanje koje se dobijaju uzimanjem u obzir kvalitet veze na tim dijelovima mreže, cijene itd.




Paketi stižu do odredišnog računara, gdje se sastavljaju prema rednim brojevima. Ako neki paket nedostaje, šalje se zahtjev pošiljaocu za tim dijelom. On ga šalje ponovo, ovaj put drugom putanjom.

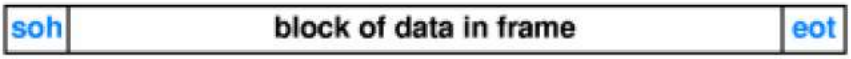
Glavna prednost paketnog prenosa je efikasnije i pravednije korištenje zajedničkih resursa.

Naime, kad bi se kroz zajednički resurs slale kontinuirane poruke, tada bi jedan par računara mogao zauzeti resurs, a drugi bi morali dugo čekati da dođu na red.

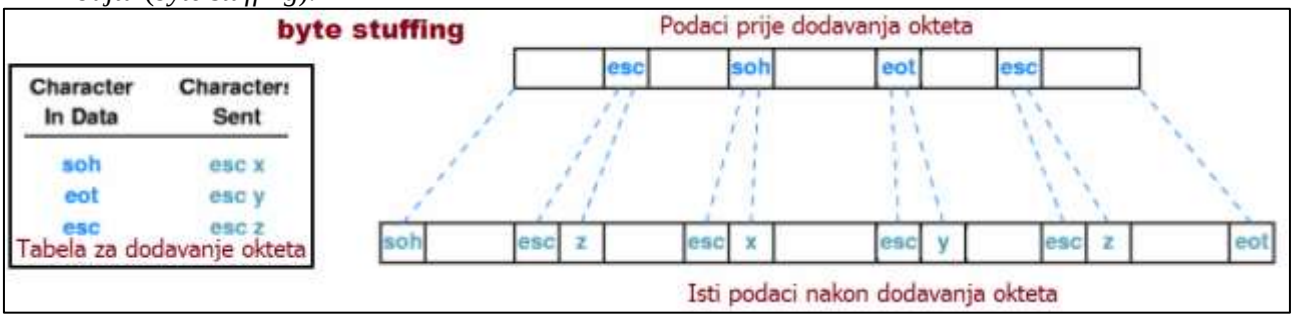
Paketna mreža obezbjeđuje mnogo veći stepen sigurnosti i brzine.

## Pojam okvira -frame-

Svaka mrežna tehnologija definiše u detalje kako izgledaju paketi koji se mogu prenositi kroz tu mrežu. **Okvir (frame) je paket s precizno definisanim formatom koji se koristi unutar određenog tipa mreže**.
Na primjer, neka mrežna tehnologija mogla bi koristiti okvire varijabilne dužine koji se sastoje od ASCII znakova. Pretpostavimo da specijalni znakovi soh odnosno eot služe za označavanje početka odnosno kraja okvira.




Tako se okvir sastoji od stvarnih podataka koje treba prenijeti i od specijalnih-kontrolnih podataka početka i kraja. Tu se javlja problem kad i sama poruka ima unutar sebe te iste znakove. To se rješava dodavanjem-umetanjem dodatnog kontrolnog bajta-okteta, tzv.*tehnikom umetanja bajta* (*byte stuffing*).

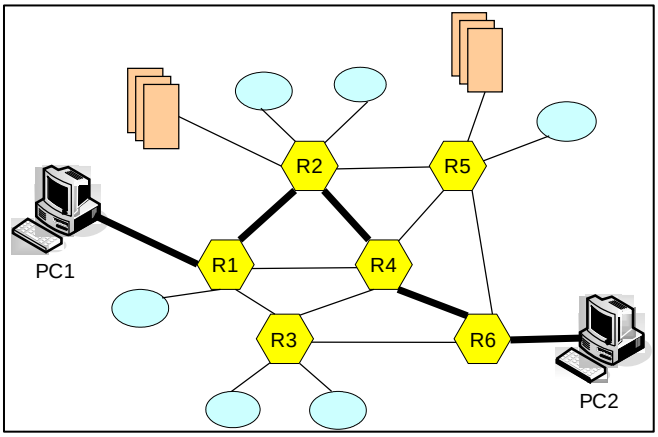



Npr. Kod okvira s dva rezervisana znaka soh i eot, dodavanje okteta zahtjeva da se uvede i treći rezervisani znak, na primjer esc.
Prije slanja, pošiljatelj prolazi kroz podatke i zamjenjuje pojavu bilo kojeg rezerviranog znaka s kombinacijom od dva znaka prema ranije definisanoj tabeli preslikavanja. Nakon ove zamjene, unutar dijela okvira s podacima više se ne pojavljuju ni soh ni eot, pa primatelj može da odredi početak i kraj okvira i izdvojiti podatke.

## Prenos podataka sa komutacijom veza (circuit switched)

U ovom tipu prenosa podataka između dva učesnika u komunikaciji uspostavlja se čvrsta direktna veza, a ukupna informacija se prenosi putanjom koja je utvrđena u toku uspostave veze. Na primjer, ako računar PC1 želi da komunicira sa računarom PC2 prvo se uspostavlja veza između ova dva računara i ta veza postoji samo za dati prenos podataka. Ako neki treći računar poželi da komunicira sa računarom PC2 u tom trenutku, to neće biti moguće po istom spojnom putu.

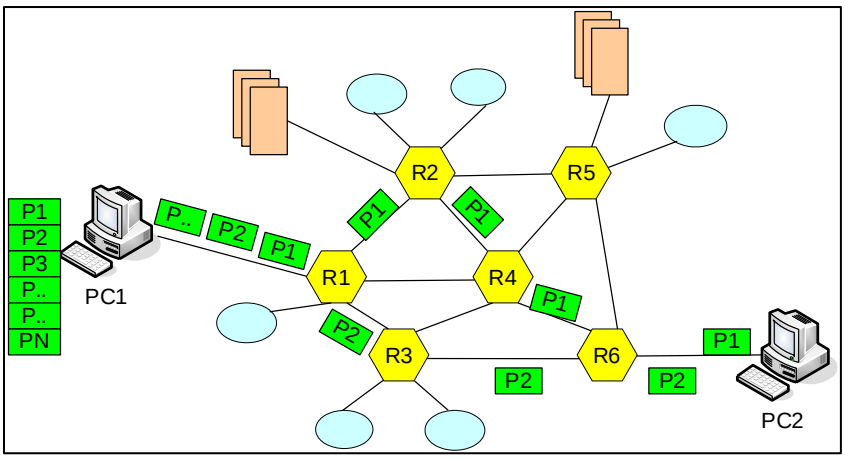
Osnovna karakteristika ovakvog načina prenosa podataka je da se podaci mogu prenositi uspostavljenom vezom maksimalnom brzinom koja je moguća, tj. u potpunosti se može koristiti kompletan frekvencijski opseg uspostavljenog spojnog puta (komunikacionog kanala) za prenos podataka.




*Prenos podataka sa komutacijom veza*

## Prenos podataka sa komutacijom paketa (packett switched)

Kod ovog načina prenosa podataka između dva učesnika, prvo se informacija koja se razmjenjuje dijeli u pakete, odgovarajuće strukture (dužina paketa, redni broj, adresa odredišta, prioritet i sl.). Paketi se upućuju do prvog čvora u mreži (rutera), a u svakom ruteru se vrši nezavisno usmjeravanje paketa. Izbor putanje u ruterima se vrši na osnovu više kriterijuma koji važe u datom trenutku. Paketi prolaze različite putanje od izvorišta do odredišta. Na odredištu se vrši slaganje paketa u prvobitan redosljed da bi se dobila potpuna informacija.



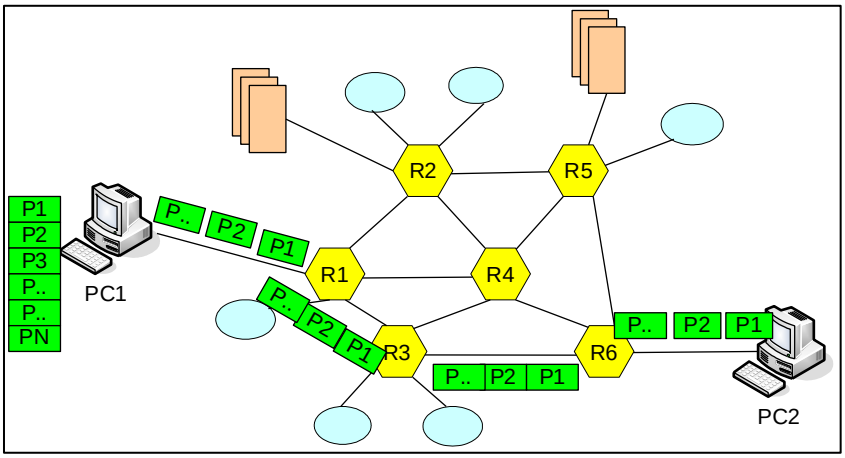

*Prenos podataka sa komutacijom paketa*

Ovakav način prenosa podataka je karakterističan za računarske mreže gdje većinu mrežnog saobraćaja čine kratki naleti podataka sa praznim prostorom između i koji su obično vremenski duži od "popunjenih".
Suština ovakvog načina prenosa podataka je da se u praznim prostorima mogu slati paketi koje šalje neki treći učesnik.

Dakle, podaci od različitih izvorišta mogu prolaziti istim spojnim putem. Ovo je daleko zahtjevniji način prenosa, zato što paketi najčešće mogu da nađu bar jedan slobodan spojni put. Mana je što je efektivna brzina slanja podataka na ovaj način manja od maksimalne koju dozvoljava propusni opseg kanala, zato što ga koriste više učesnika u komunikaciji.

## Prenos podataka virtuelnom vezom (virtual circuit)

Ovaj način prenosa podataka se takođe odnosi na paketski prenos. Međutim, paketi se usmjeravaju na isti spojni put između dva računara.
Virtuelna kola su permanentnog tipa što znači da kada se jednom definišu putanje, rijetko ili nikada se ne mijenjaju. Ovo je zapravo **softverska zamjena** za hardverska rješenja ovog tipa. Podaci i dalje putuju kroz mrežu (povezani čvorovi) ali tačno određenom putanjom.




*Prenos podataka virtuelnim kolima*

Svaki paket, pored karakterističnih polja koje nosi, ima i obilježje koje ukazuje na datu virtuelnu vezu. Skoro sve mreže koje imaju intenzivan saobraćaj na mreži koriste ovu metodu definisanja putanje.
Prednost ovakvog načina prenosa paketa je da se krajnjim aplikacijama može obezbjediti odgovarajući kvalitet usluge.

Na primjer, kod interaktivnog prenosa govora kroz mrežu, važno je obezbjediti da paketi podataka, kojima je kodovan govor, do prijemnika stižu istom brzinom, tj. da ne postoji varijacija u kašnjenju.
U mrežama sa komutacijom paketa, pojedini paketi mogu da pronalaze drastično različite putanje (različito vrijeme prenosa), što može dovesti do problema na prijemu – nerazumljiv govor.
Samo virtuelnim kolima se može obezbjediti zahtjevani kvalitet usluge. Zbog prenosa kroz mrežu postoji kašnjenje, ali je ono identično za sve pakete.

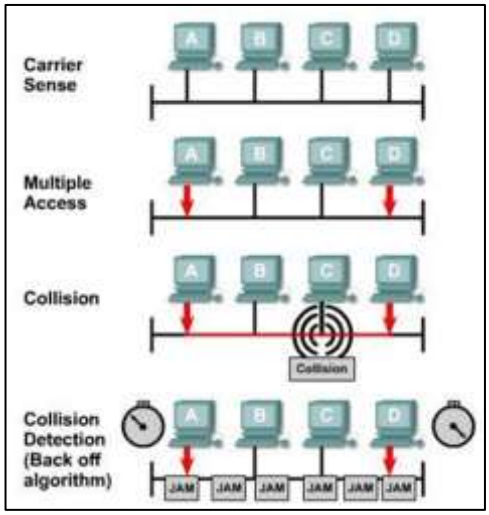
# Metode pristupa

Metode pristupa su **pravila** kojima se reguliše **kada koji računar u mreži može da šalje podatke**. Na ovaj način se unosi red u procese slanja i primanja podataka.
**Šta ako se desi da dva računara istovremeno počnu da šalju podatke**? U tom slučaju dolazi do sudara podataka i podaci se odbacuju.
Kako riješiti taj problem? Ovo može da se riješi na dva načina: da ne dozvolimo uopšte mogućnost da dva računara istovremeno pošalju podatke, ili da takvu mogućnost sudara podataka dozvoli, ali da onda na neki način riješimo i kontrolišemo takvu situaciju.
**ALOHA pristup**
Predajnik šalje podatak kada ima podatak za slanje ne proveravajući da li je kanal slobodan. Aloha na havajskom znači zdravo, pa bi naziv trebao da sugeriše da je svako dobro došao.

Ovaj metod razvijen je za paketske radio-prenose. Svaki korisnik pristupa kanalu kada ima podatke spremne za slanje, ne ispitujući da li je kanal već zauzet. Ukoliko je kanal već bio zauzet doći će do sukoba (kolizije) i svi podaci će biti oštećeni. Poslije određenog vremena ukoliko ne dobije potvrdu o uspješnom prijemu od odredišne stanice, predajna stanica će ponovo poslati podatke.
Zbog velikog broja sukobljavanja smatra se da je ova metoda **neupotrebljiva za LAN** mreže.
Postoji i vremenski raspodjeljena ALOHA gdje predajne stanice mogu da šalju podatke u tačno određenim vremenskim trenucima. Kod ove modifikovane metode je manja kolizija.

## Metoda višestrukog pristupa sa osluškivanjem i otkrivanjem kolizije

*Mehanizam za kontrolu pristupa medijumu (engl. Media Access Control, MAC) zove se Višestruki pristup sa osluškivanjem nosioca i detektovanjem sukoba (engl. Carrier Sense Multiple Access with Collision Detection, CSMA/CD). On je najprepoznatljiviji i najćešće korišten metod Ethernet standarda.*




Metodu višestrukog pristupa zajedničkom mediju sa osluškivanjem nosećeg signala i sa otkrivanjem kolizije (engl. Carrier Sense Multiple Access with Collision Detection, CSMA/CD) možemo uporediti sa grupom ljudi koji sjede, za početak ćutke, u zatamnjenoj sobi. Svako od njih ima podjednako pravo da progovori (faza višestrukog pristupa). Ako neko čuje da neko drugi priča, nema pravo da progovori (faza osluškivanja nosećeg signala). Ako dvije osobe progovore u istom trenutku, obje će ustanoviti tu činjenicu i prestati da pričaju (faza otkrivanja sukoba).

Kako to izgleda u mreži, među računarima?
Svaki računar osluškuje da li je mreža slobodna za prenos podataka (tj. osluškuje noseći signal), odnosno da li se njom već šalju neki podaci (faza osluškivanja nosećeg signala).

Ako je mreža zauzeta, računar sačeka neko vrijeme, pa ponovo provjerava da li je mreža slobodna. Ako utvrdi da je mreža slobodna, računar šalje paket podataka (faza višestrukog pristupa). Može se desiti da u jednom trenutku dva (ili više) računara istovremeno počnu slanje podataka. Tada dolazi do sudara podataka i oni se odbacuju. Kažemo da je došlo **do kolizije**, ili sukoba. Računari koji su učestvovali u sukobu sada detektuju da je došlo do sukoba[7], (faza otkrivanja sukoba) i prestaju sa emitovanjem podataka[8].
Svi sukobljeni računari biraju slučajno izabran vremenski period tokom kojeg čekaju pre nego što pokušaju ponovo da pošalju podatke (period zaostajanja).
Sukobi su potpuno uobičajena stvar u Ethernet mrežama[9], čak habovi imaju na prednjoj strani indikator, koji kada zatrepti, obavještava da se desio sudar. Sukobi se rješavaju vrlo brzo, (u mikrosekundama).
Sukobi mogu biti problem kada se dešavaju suviše često, i samim tim bitno usporavaju mrežu. Do ovoga može doći kada je mrežni saobraćaj obiman.
Na obimnost mrežnog saobraćaja utiče broj računara u mreži, ali aplikacije koje koriste korisnici na tim računarima. Recimo, aplikacije za rad sa bazama podataka stvaraju obimniji mreži saobraćaj od aplikacija za obradu teksta.
Takođe, kod ove metode pristupa, dužina kabla ne treba da bude veća od 2500m[10].

Metoda višestrukog pristupa sa osluškivanjem nosećeg signala i sa otkrivanjem kolizije zove se još i metoda rivaliteta, jer se računari u mreži takmiče za prvenstvo slanja podataka.

## Metoda višestrukog pristupa sa osluškivanjem i izbjegavanjem kolizije

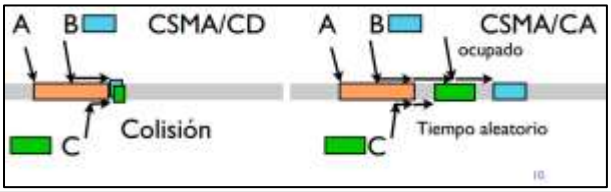
Metoda višestrukog pristupa zajedničkom mediju sa osluškivanjem nosećeg signala i sa izbjegavanjem kolizije (engl. Carrier Sense Multiple Access with Collision Avoidance, CSMA/CA) podrazumjeva da računar koji hoće da pošalje podatke, ostalim računarima prethodno pošalje signal kojima to najavljuje. Ovim su ostali računari obavješteni da ne šalju svoje podatke, pa je sukob podataka izbjegnut.

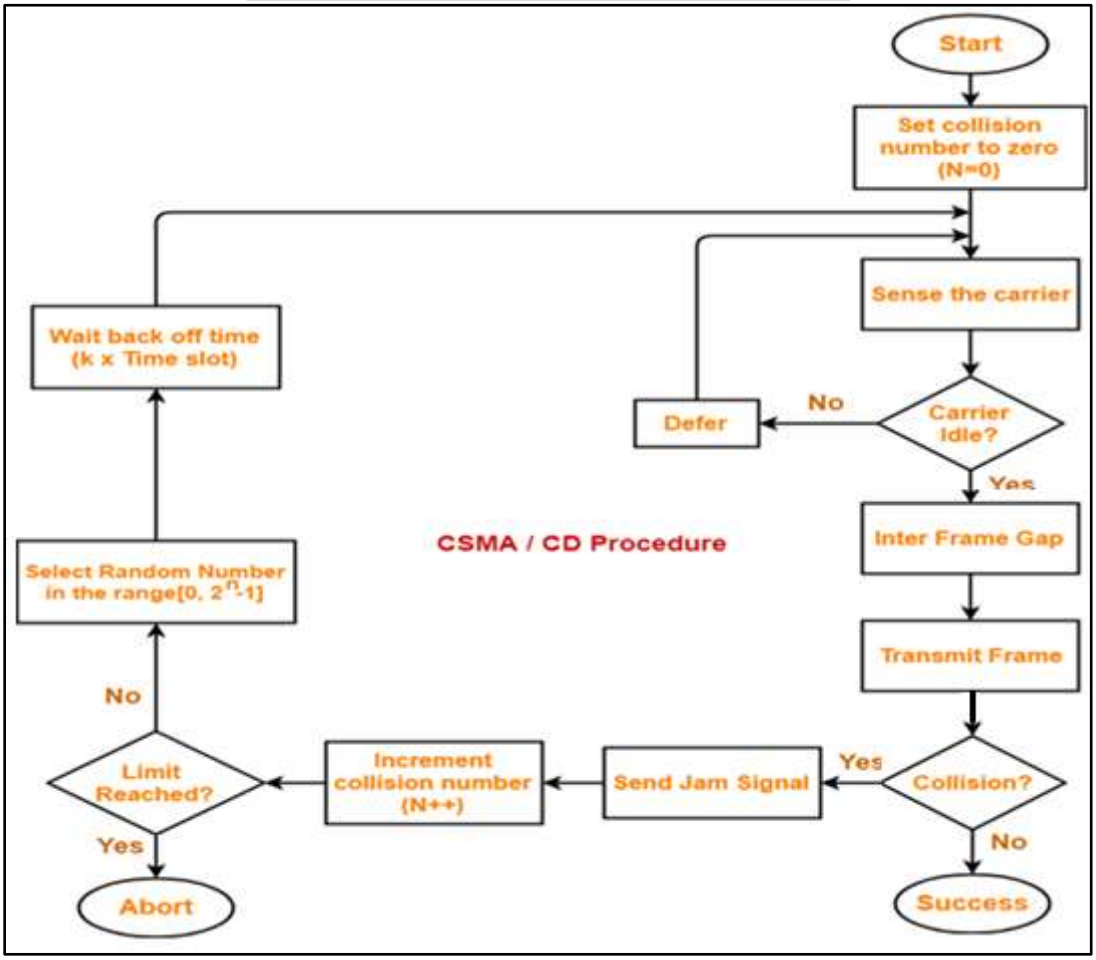
[7] Računar pretpostavlja da se u koaksijalnom kablu desio sukob ako se izmjeri naponski impuls velike amplitude. U režimu rada poludupleks, na optičkim kablovima ili UTP kablovima, računar pretpostavlja da se desio sukob kada se na kanalima za prijem i predaju (kod optičkog kabla), odnosno paricama za prijem i predaju (kod UTP kabla), istovremeno pojavi signal.

[8] Računar koji detektuje sukob šalje poruku o zagušenju svim računarima u mreži da se desio sukob i da treba odbaciti sve nepotpuno primljene pakete podataka. Kada dođe do sukoba podataka, oni se pomešaju i postanu neprepoznatljivi. Ako sukob ne bi bio detektovan, narušeni podaci mogli bi biti uzeti kao ispravni. Tek nakon poruke o sukobu, sukobljeni podaci se odbacuju.

[9] Postoji tzv. zakašnjeli sukob, koji ne spada u normalnu pojavu na Ethernetu. To je sukob koji se desi kada i posljednji bit nekog paketa podataka bude predat od strane računara pošiljaoca. Do ovoga može doći kada je paket veoma kratak (kraći od 64 bajta) ili je mrežni kabl suviše dugačak, pa računar završi predaju podataka prije nego što se sukob i desi, negdje daleko od računara

[10] Ako je kabl predugačak, onda računar sa jednog kraja kabla neće biti u stanju da blagovremeno ”osjeti” signal poslat sa drugog kraja kabla, i može i sam početi slanje podataka. Tako će češće dolaziti do sukoba.



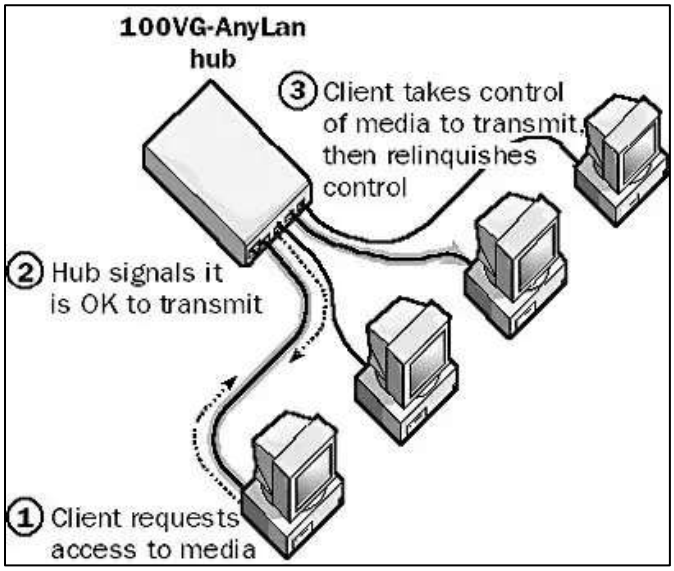




*Dijagram toka koji pokazuke algoritam CSMA/CD*

Evo koraka koji objašnjavaju proceduru ove metode predstavljenu na gornjoj slici:
Prvo, predajnik koja želi poslati podatke, prepoznaje nosača je li zauzeta ili neaktivna. Ako je medij u stanju mirovanja-slobodan, tada se prenos vrši.
Prenosna stanica otkriva sudar, ako postoji, koristeći uslov: Tt> = 2*Tp gdje je Tt kašnjenje prijenosa, a Tp kašnjenje rasprostiranja-širenja.
Stanica otpušta signal zaglavljivanja čim otkrije sudar.
Nakon što se sudar dogodio, predajna stanica prestaje s odašiljanjem i čeka neko slučajno vrijeme koje se naziva ' vrijeme povlačenja '. Nakon tog vremena, stanica se ponovno emitira.
Ova metoda se koristila u ranijim Ethernet mrežama. Danas se koriste modifikovane metode ovog pristupa. Glavne mane su šro slanje najava povećava obim saobraćaja u mreži i dodatno usporava mrežu i ograničenje dužine kabla (na 2500 m kao i kod CSMA).

## Metoda prioriteta zahtjeva

Metoda prioriteta zahtjeva (*Demand Priority Access Method* - **DPAM**) definisana je IEEE 802.12 standardom. Koristi se kod prenosa podataka preko LAN-a mreža kontrolisanih repetitorom sa topologijom zvijezda. Kada računar šalje podatke, oni se **ne šalju svim računarima** u mreži, nego idu kroz hab do računara kojem su namjenjeni.
Kad više uređaja šalje istovremeno poruku nastaje kolizija koja se rješava postupkom arbitraže. Poruke se međusobno upoređuju, a prioritet u slanju ima onaj uređaj koji u tom trenutku šalje dominantni bit ili logičku '0'. Sve ostale poruke koje imaju u tom trenutku recesivni bit ili logičku '1' prestaju sa slanjem. Na kraju postupka arbitraže slanje nastavlja samo uređaj koji šalje poruku sa sa najvećim prioritetom ili najnižom binarnom vrijednošću.




Ako se pokaže da su oba zahtjeva sa istim prioritetom, računari se opslužuju naizmjenično.
Kod metode pristupa moguće je da računar istovremeno i šalje i prima podatke.
Repetitor ili hab su zaduženi da primjete sve adrese, veze i krajnje čvorove i provjere da li svi oni funkcionišu. Repetitori upravljaju pristupom mreži, kružno ispitujući da li postoje zahtjevi za slanje podataka sa bilo kog čvora na mreži.

*Metoda prioriteta zahtjeva je poznat i kao **AnyLAN** po najčešće korištenoj Ethernet tehnologiji koja je koristi. Za ovu vrstu tehnologije se koriste i termini: 100VG-AnyLAN, 100BaseVG. Ona kombinuje elemente Ethernet i Token Ring arhitektura. Ovu mrežnu tehnologiju je prvobitno razvio Hewlett-Packard, a zatim je dodatno uobličena i ratifikovana od strane IEEE..*

Prema definiciji 100VG-AnyLAN, krajnji čvor može biti računar, most (bridge), ruter ili komutator (switch). Prioritet zahtjeva se zasniva na činjenici da su repetitori i krajnji čvorovi komponente koje čine svaku 100VG-AnyLAN mrežu. Kod metode **prioriteta habovi i repetitori upravljaju pristupom mreži**, kružno ispitujući da li postoje zahtjevi za slanje podataka sa bilo kog čvora u mreži[11].

[11] Krajnji čvor može biti računar, most, ruter ili svič

# Mrežna oprema

Računarske mreže se sastoje 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:

- prema kriteriju potrebe energiije za samo funkcionisanje opreme (pasivna oprema ne treba struju za rad, aktivna treba)
- prema mogućnosti logičkog odlučivanja za potrebe usmjeravanja podataka (pasivni elementi mrežne opreme nemaju mogućnost odlučivanja, a aktivni imaju)

Aktivnu mrežnu opremu čine uređaji koji prihvaćaju i distribuiraju saobraćaj unutar mreža, dok pasivnu opremu sačinjava sistem za povezivanje koji služi za povezivanje aktivne opreme.


## Pasivna mrežna oprema

*pojačivači/konektori/kablovi/ormari/kanalice*

Pasivna mrežna oprema su oni dijelovi računarske mreže koji su uključeni u prenos podataka u mreži, ali oni ne mijenjaju niti utiču na podatke.

Pod pasivnom opremom se ranije podrazumjevao sistem za kabliranje (kog su činili kablovi i konektori), što se kao termin obesmislilo pojavom bežične tehnologije.

Pasivna oprema se sastoji od kablova, konektora, razvodnog panela (patch panel, switching panel, punch-down panel), komunikacijskih ormara i sistema za napajanje električnom energijom (vodovi, sklopke i naponske letve, sistem za hlađenje).

# Mrežni kablovi

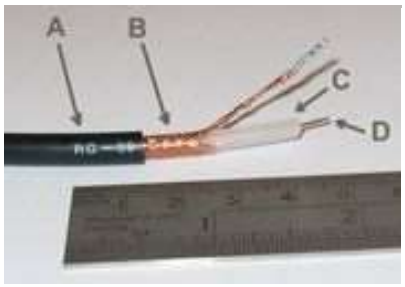
Za prenos signala između računara većina današnjih mreža koristi kablove koji se ponašaju kao mrežni prenosni medijumi.
Prenos podataka kablovima ostvaruje se kroz bakrenu žicu e pomoću električne struje. Bakar se koristi, jer je on dobar vodič električne struje, a još uvijek je relativno jeftin žice se lagano se savijaju i spajaju.
Loša osobina bakrenih žica je pojava problema interferencije – dvije žice indukuju struju jedna u drugoj i tako proizvode smetnju. Konstrukcija pojedinih tipova žica nastoji smanjiti interferenciju.
Postoji mnogo različitih tipova kablova koji mogu da se primjene u različitim situacijama. Njihov broj je izuzetno veliki i obuhvata više od 2200 različitih tipova.

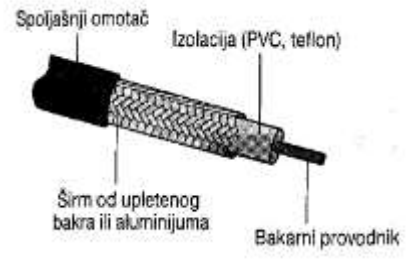
Većina današnjih mreža koristi tri osnovne vrste kablova:

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

## Koaksijalni kabl

U jednom trenutku ovo su bili najrasprostranjeniji mrežni kablovi, i to iz više razloga: relativno su jeftini, laki, fleksibilni i jednostavni za rad. U svom najjednostavnijem obliku, koaksijalni kabl se sastoji od bakarne žice u sredini, oko koje se nalazi najpre izolacija, a zatim sloj od upletenog metala - širm i, na kraju, spoljašnji zaštitni omotač .




*Slojevi koaksijalnog kabla*

Svrha ovog oklopa je da apsorbuje elektromagnetne smetnje ili šum, i time spreči njihovo mešanje sa podacima koji se prenose. Kablovi koji imaju jedan sloj izolacije i jedan sloj od upletenog metala zovu se i kablovi sa dvostrukom zaštitom.

Postoje, takođe, i kablovi sa četvorostrukom zaštitom (dva sloja izolacije i dva sloja širma), koji se primjenjuju u sredinama sa jakim elektromagnetnim smetnjama.

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

## Kabl sa upredenim paricama

Kabl sa upredenim paricama se sastoji od dvije izolovane bakarne žice koje su obmotane (upredene) jedna oko druge. Na slici 2.x prikazana su dva tipa ovog kabla: kabl sa neoklopljenim (*Unshielded Twisted-Pair, UTP*) i oklopljenim paricama (*Shielded Twisted-Pair, STP*).

*Kablovi sa neoklopljenim i oklopljenim paricama*

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

## Šta je Ethernet?

Da bi objasnili klasu kablova poznatu kao Eternet kablovi započećemo razjašnjenje pojma Ethernet (koji će nas pratiti dobar dio ovog priručnika).
Ethernet ili IEEE standard 802.3 je danas najčešće korištena tehnologija za lokalne mreže (LAN).
*Specifikacije i prava na tehnologiju bila su dostupna svakome, što je jedan od glavnih razloga zašto je ova tehnologija tako raširena u računarnoj industriji.* Kao najvažnijeg proizvođača Ethernet komponenti možemo navesti Cisco Systems, Intel i 3Com.
Ethernet je zasnovan na CSMA/CD metodi (*Metodi višestrukog pristupa*, gdje jedan uređaj šalje paket mrežnom segmentu, prisiljavajući sve ostale uređaje u tom segmentu da obrate pažnju na paket. Istovremeno, drugi uređaj pokušava izvršiti prenos što dovodi do kolizije, nakon čega oba uređaja moraju izvršiti ponovni prenos, koji ćemo nešto detaljnije objasniti kasnije).
Tako uglavnom jeste međutim:

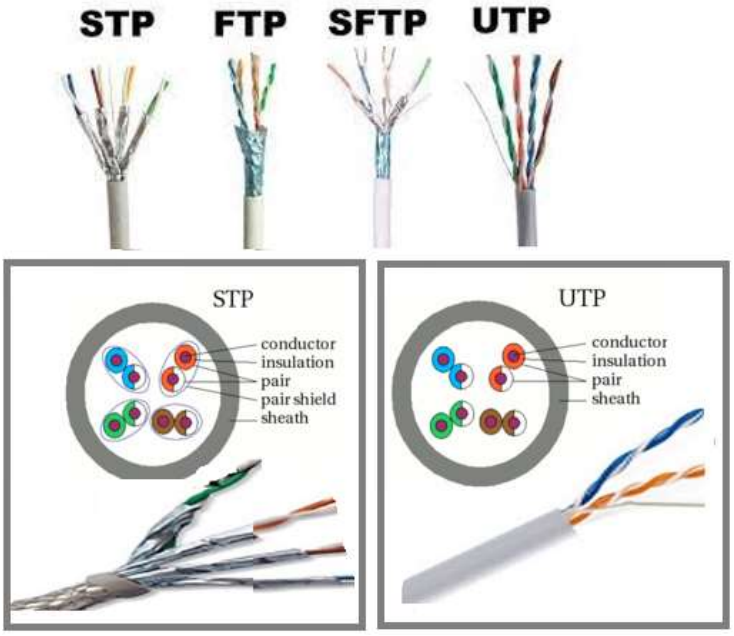
*Moderni Eternet sistemi su izvedeni sa dvosmjernim linkovima. Ovakvi sistemi nemaju ograničenja dužine kablova i brzine prenosa podataka kao kod originalnih sistema koji koriste CSMA/CD protokol. Većina izmjena kod eternet sistema se upravo odigrala na fizičkom sloju, od primjene koaksijalnih kablova kao medijuma do primene optičih kablova. Od djeljenog eterneta izvedenog u topologiji magistrale do eterneta koji radi u potpunom dupleksu na topologiji zvijezde sa komutatorom kao centalnim dijelom i linkovima od tačke do tačke ka računarima. Dužine segmenata u modernim sistemima su ograničene samo fizičkim karakteristikama.*

## Ethernet kablovi i konektori

Ethernet se obično koristi fizičkom infrastrukturom izvedenom na principima strukturnog kabliranja.
*Ranije su se za realizaciju Eternet LAN mreža koristili koaksijalni kablovi, ali su oni danas samo istorijska kategorija.*

Uobičajeno se koriste skraćeni nazivi za ove kablove:

- STP (od shielded twisted pair - oklopljena upletena parica)
- FTP (od foiled twisted pair - upletena parica zaštićena od smetnji folijom)
- S/FTP (od shielded/foiled twisted pair - upletena parica zaštićena od smetnji folijom i žičnim opletom)
- UTP (od unshielded twisted pair - neoklopljena upletena parica)



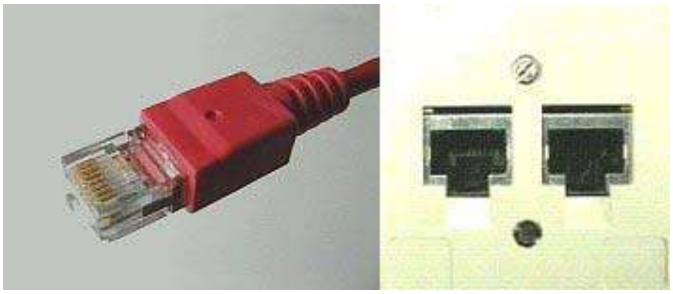

Svaki od ovih kablova ima 8 žica ili 4 parice (po dve upredene bakarne žice). Da bi ste povezali računare međusobno ili sa uređajima kao što su switch ili ruter potrebno je u pravilnom rasporedu povezati žice na konektore.
FTP kabl je napravljen tako da su četiri parice potpuno obavijene tankom metalnom folijom. Ova folija svoju zastitnu funkciju obavlja tako što zahvaljujući visokoj impedansi reflektuje spoljne, ometajuće, elektromagnetne signale na učestanostima većim od 5 MHz i tako im onemogućava prodor do samih parica.

**Kod LAN mreža se najviše koriste UTP kablovi.** Unutar UTP kabla se nalazi do četiri upletena para bakrenih žica, zatvorenih u zaštitnu plastiku. Dvije pojedinačne žice u jednom paru upletene su jedna oko druge, a zatim su i parovi upleteni.

Postoji pet kategorija UTP kabla. Tih pet kategorija je definisano standardom TIA 568. Prva kategorija je CAT3 i danas se rijetko koristi, a kada se koristi, onda se najčešće koristi u telefonskim linijama. Podržava 10 Mbps do 100 metara. CAT4 je druga kategorija i koristi se u mrežama s token ring-om i podržava 16 Mbps do 100 metara. Treća kategorija je CAT5 i koristi se u LAN-ovima utemeljenima na Ethernetu. CAT5 sadrži dva upletena para i podržava 100 Mbps do 100 metara. Četvrta kategorija je CAT5e koja sadrži četiri upletena para te podržava 1 Gbps na 100 metara.

Kategorija je CAT6 koji se koristi u LAN-ovima zasnovanim temelje na Ethernetu i mrežama podatkovnih centara. CAT6 sadrži četiri čvrsto upletena para. Podržava 1 Gbps do 100 metara i 10 Gbps do 50 metara.

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

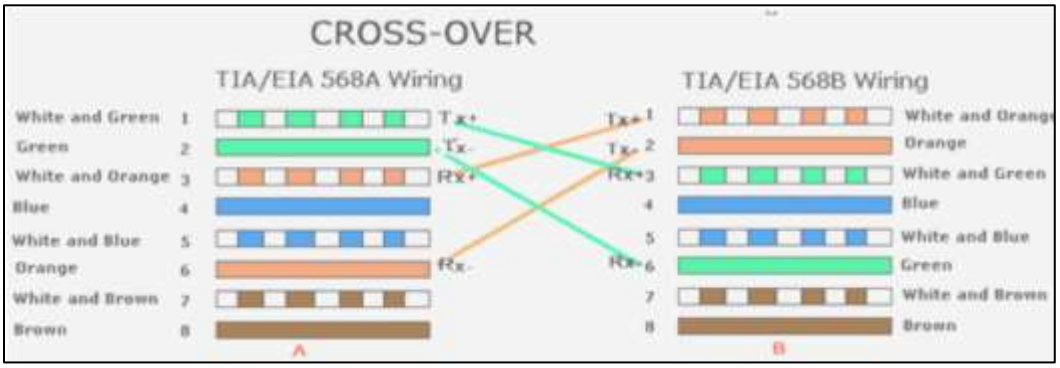


*Konektor RJ45 i utičnica*

## Načini povezivanja kod UTP kablova

*Kako ćete izukrštati žice odnosno hoćete li ih ukrstiti?*
Da bi ste povezali bilo koja dva uređaja potrebo je pravilno povezati 4 žice ili 2 parice.
Postoje tri načina kabliranja da povežete bilo koji aktivni mrežni uređaj sa računarom ili računare međusobno. Kako spojiti žice na prijemnoj i predajnoj strani zavisi od uređaja koji se povezuju.

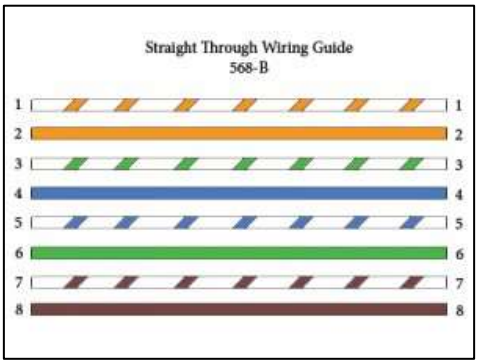
Ako povezujete iste uređaje: Dva računara, 2 switcha ili 2 rutera međusobno povezuju se **Crossover načinom kabliranja ili ukrštenim načinom.**

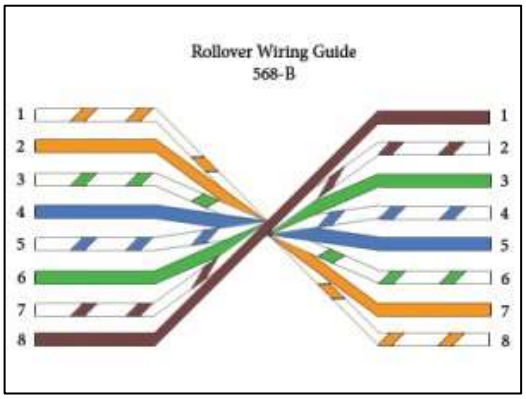



Potrebno je povezati prvu žici sa trećom i drugu sa šestom, takođe isto i u drugom smeru. Ukoliko ostale žice želite da koristite za funkcionalnosti poput PoE (Power Over Ethernet) ostale 4 žice povežite kao na slici, ali to nije obavezno.

Ukoliko želite da povežete, uslovno rečeno, raznorodne uređaje npr. PC-Switch, Switch-Router povezujete **Streight-trough kablom, ravnim ili jedan-na-jedan** načinom.

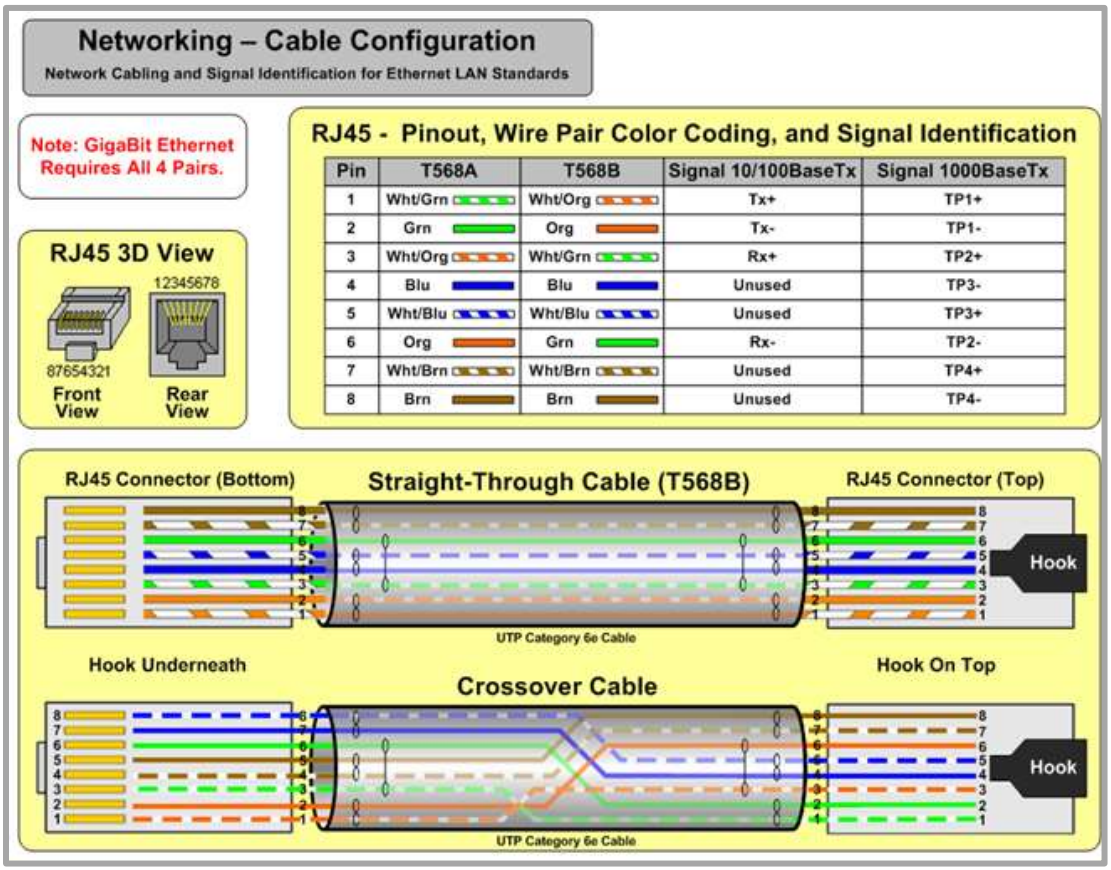
Kod oveg kabla potrebno je povezati pinove na konektoru na sljedeći način: prvi na prvi, drugi na drugi, treći na treći i šesti na šesti. Kao i kod Cross kabla ostale je potrebno povezati za PoE funkcionalnost.




Postoji **još jedan način** kabliranja UTP kablom, koji se inače ne koristi za prenos podataka već **za programiranje aktivnih mrežnih uređaja**, odnosno za povezivanje na njihov interfejs.

Ovo **je Rollover** način povezivanje gde se prva bakarna žica povezuje na 8 pin na RJ45 konektoru, a onda redom 2-7, 3-6, 4-5, 5-4...



## Standardi za konektore i kablove

Industrijski standardi za računarsku mrežu napravljeni su od strane TIA/EIA[12]. Ustanovljene su četiri osnovne kategorije UTP kablova u zavisnosti od garantovanog kvaliteta prenosa.
Evo i dijela specifikacije kablova koji zadovoljavaju Ethernet standarde:

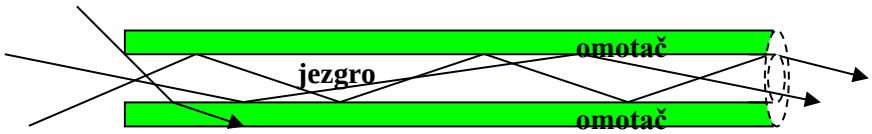
| Tabela uporednih karakteristika tipova eterneta | | | | |
|---|---|---|---|---|
| **Tip eterneta** | **Brzina** | **Tip kabla** | **Dupleks** | **Maks. rastojanje** |
| Desetomegabitni eternet | | | | |
| 10Base5 | 10 Mb/s | Koaksijalni debeli | polu | 500 m |
| 10Base2 | 10 Mb/s | Koaksijalni tanki | polu | 185 m |
| 10Base-T | 10 Mb/s | UTP kategorije 3/5 | polu | 100 m |
| 10Base-F | 10 Mb/s | Optičko vlakno | polu | 100 m |
| 10Base-FL | 10 Mb/s | Optičko vlakno | polu | 100 m |
| Stomegabitni eternet | | | | |
| 100Base-T | 100 Mb/s | UTP kategorije 5 | polu | 100 m |
| 100Base-T4 | 100 Mb/s | UTP kategorije 5 | polu | 100 m |
| 100Base-T2 | 100 Mb/s | UTP kategorije 5 | polu | 100 m |
| 100Base-TX | 100 Mb/s | UTP kategorije 5 | polu | 100 m |
| 100Base-TX | 200 Mb/s | UTP kategorije 5 | potpun | 100 m |
| 100Base-FX | 100 Mb/s | Višerežimsko vlakno | polu | 400 m |
| 100Base-FX | 200 Mb/s | Višerežimsko vlakno | potpun | 2 km |
| Gigabitni eternet | | | | |
| 1000Base-T | 1 Gb/s | UTP kategorije 5e | potpun | 100 m |
| 1000Base-TX | 1 Gb/s | UTP kategorije 6 | potpun | 100 m |
| 1000Base-CX | 1 Gb/s | STP tvinaksijalni | potpun | 25 m |
| 1000Base-SX | 1 Gb/s | Višerežimsko vlakno | potpun | 550 m |
| 1000Base-LX | 1 Gb/s | Jednorežimsko vlakno | potpun | 10 km |
| 1000Base-ZX | 1 Gb/s | Jednorežimsko vlakno | potpun | 70-100 km |
| Desetogigabitni eternet | | | | |
| 10GBase-CX4 | 10 Gb/s | STP tvinaksijalni | potpun | 100 m |
| 10GBase-T | 10 Gb/s | UTP kategorije 6a/7 | potpun | 100 m |
| 10GBase-LX4 | 10 Gb/s | Višerežimsko vlakno | potpun | 300 m |
| 10GBase-LX4 | 10 Gb/s | Jednorežimsko vlakno | potpun | 10 km |
| 10GBASE-SR/W | 10 Gb/s | Višerežimsko vlakno | potpun | 300 m |
| 10GBASE-LR/W | 10 Gb/s | Jednorežimsko vlakno | potpun | 10 km |
| 10GBASE-ER/W | 10 Gb/s | Jednorežimsko vlakno | potpun | 40 km |

[12] TIA/EIA znači Udruženje telekomunikacijskih industrija/Udruženje elektronskih industrija (*Telecommunications Industry Association/ Electronic Industries Alliance*) koje objavljuje TIA/EIA standarde ožičenja. Standarde i publikacije usvaja TIA/EIA u skladu sa patentnom politikom Američkog nacionalnog instituta za standarde (ANSI). TIA/EIA-568 uspostavlja široko rasprostranjene standarde telekomunikacionih kablova koji podržavaju interoperabilnost. Standard **568B** postavlja minimalne zahtjeve za različite kategorije kablova.

# Optički kablovi

Optički kabl, poznat i kao kabl s optičkim vlaknima (**fiber-optic cable**, optical-fiber cable,), je sklop sličan električnom kablu, ali koji sadrži jedno ili više optičkih vlakana koja se koriste za prenos svjetlosti.

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



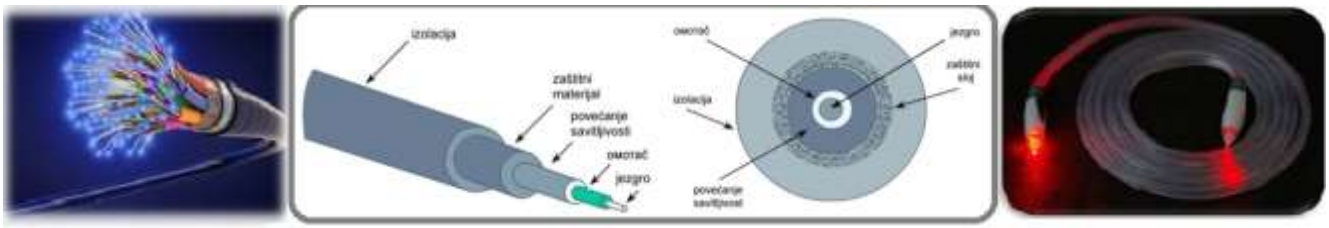

*Totalna refleksija kod prenosa kroz optičko vlakno*

Sistemi prenosa sa optičkim kablovima se sastoje iz tri osnovna funkcionalna dijela, a to su:

- predajnik (izvor svetlosti – LED ili laserska dioda),
- optičko vlakno i
- prijemnik (foto senzor).

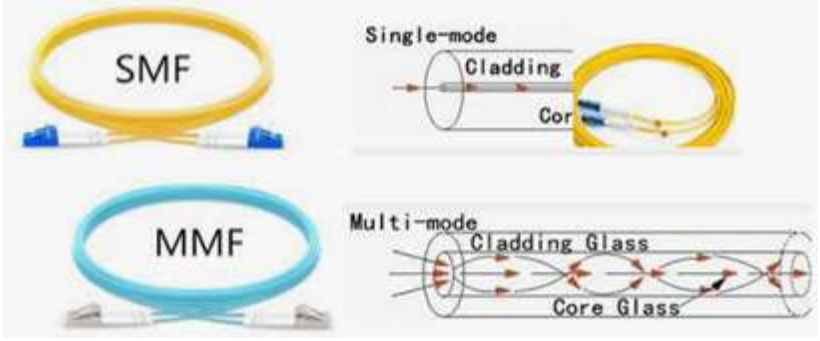
Standardni električni signal se dovodi na LED ili lasersku diodu koje vrše konverziju u svetlost, zatim se svetlost "ubacuje" u optičko vlakno na čijem drugom kraju je prijemnik koji vrši opto-električnu konverziju posle koje se dobija standardni električni signal.

Princip po kome se informacija prenosi po optičkom vlaknu bazira se na fizičkom fenomenu pod nazivom totalna refleksija. Svako optičko vlakno se sastoji iz jezgra koga čini staklo određenog indeksa prelamanja i omotača presvučenog preko jezgra. Ovaj omotač je takođe od stakla, ali ono ima drugu vrijednost indeksa prelamanja. Svketlost se ubacuje u jezgro pod određenim uglom potrebnim da dođe do totalne refleksije, zbog koje se svijetlosni zrak neprestalno odbija od granične površine jezgro/omotač putujući tako kroz vlakno do prijemnika.




*Kablovi sa optičkim vlaknom*

Optička vlakna se mogu podijeliti u dvije osnovne grupe: na **monomodna** (*singlemode*) koja su tanja i omogućavaju prostiranje samo jednog svijetlosnog zraka, i **multimodna** (*multimode*) koja su deblja i omogućavaju istovremeno prostiranje više zraka od više različitih izvora.
U tehnološkom procesu je mnogo jednostavnije (a time i jeftinije) proizvesti vlakno većeg prečnika jezgra. To je razlog zbog kog se multimodna vlakna češće koriste. Pored toga, u veće jezgro je mnogo lakše "ubaciti" svijetlost iz izvora, pa su i predajnici jeftiniji jer svijetlosni snop izvora ne mora biti toliko fokusiran kao u slučaju korišćenja monomodnog vlakna. Dakle, cjelokupni sistem baziran na multimodnom vlaknu je jeftiniji i takvi sistemi su danas dominantni kod lokalnih računarskih mreža. Sa druge strane, zbog većih rastojanja koja je potrebno premostiti, u telekomunikacijama su dominantna monomodna vlakna.
Optičko vlakno se sastoji od jezgre i sloja omotača, odabranih za potpunu unutrašnju refleksiju zbog razlike u indeksu prelamanja između njih. Obloga je obično presvučena slojem akrilatnog polimera ili poliimida. Ovaj premaz štiti vlakno od oštećenja, ali ne doprinosi njegovim svojstvima optičkog talasovoda. Pojedinačna obložena vlakna (ili vlakna formirana u trake ili snopove) zatim imaju čvrsti puferski sloj ili cijev(e) jezgre ekstrudirane oko njih kako bi formirali jezgro kabla.
Nekoliko slojeva zaštitnog omotača, zavisno od primjeni, dodaje se kako bi se formirao kabel. Čvrsti sklopovi vlakana ponekad stavljaju staklo koje apsorbira svjetlost ("tamno") između vlakana, kako bi spriječilo da svjetlost koja curi iz jednog vlakna uđe u druga. Ovo smanjuje preslušavanje između vlakana ili smanjuje odbljesak u aplikacijama za snimanje snopova vlakana.



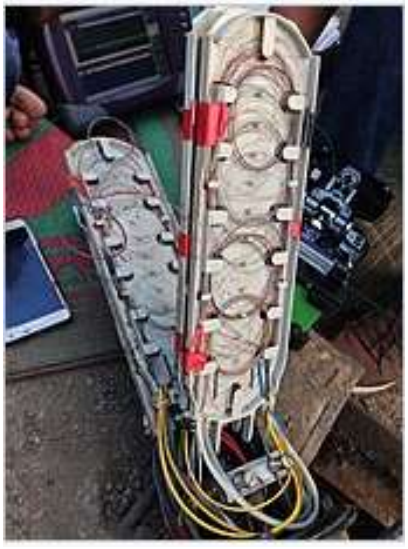

Vlaknasti kablovi mogu sadržavati do hiljadu vlakana u jednom kablu, iako se najčešće proizvodi jednomodni vlaknasti kabel s najvećim brojem žica, koji se sastoji od 36 traka od kojih svaka sadrži 24 vlakna.

**Kod računarskih mreža svaki link (veza) zahtjeva dva vlakna – jedan za predaju a drugi za prijem**.
*Optička vlakna obično se primjenjuju se u WAN mrežama za povezivanje udaljenih lokacija*. 2012. godine, japanska kompanija NTT je demonstrirala kabl sa jednim vlaknom koji je mogao prenijeti 1 petabit u sekundi (1015bit/s) na udaljenosti od 50 kilometara.

Moderni optički kablovi dolaze u širokom spektru omotača i oklopa, dizajnirani za primjene kao što su direktno zakopavanje u rovovima, dvostruka upotreba kao dalekovodi, instalacija u kanalima, pričvršćivanje na zračne telefonske stupove, podmorska instalacija i umetanje u popločane ulice.

*Polaganje optičkog kabla u podzermne instalacije*

Napomena: *Optička vlakna su podložna procesu gubitka kvaliteta tokom "starenja" što bi trebalo da se uzme u obzir, prilikom dizajniranja ili prilikom narudžbe da se provjeri deklaracija na vrijeme eksploatacije.*
*Naime: Optička vlakna su vrlo jaka, ali je čvrstoća drastično smanjena zbog neizbježnih mikroskopskih površinskih nedostataka svojstvenih proizvodnom procesu. Početna čvrstoća vlakna, kao i njena promjena s vremenom, moraju se uzeti u obzir u odnosu na naprezanje nametnuto vlaknu tokom rukovanja, kabliranja i instalacije za dati skup uslova okoline. Postoje tri osnovna scenarija koji mogu dovesti do degradacije čvrstoće i kvara izazivanjem rasta nedostataka: dinamički zamor, statički zamor i starenje bez stresa.*



*Optički kabl u razvodnoj kutiji za kablove*
Vidljive su pojedinačne žice optičkog kabla unutar razvodne kutije.

# Standardi i tipovi optičkih kablova

| MULTIMODE FIBRE | | | | |
|---|---|---|---|---|
| Cable type | Wavelength | Maximum attenuation | Minimum overfilled modal bandwidth length | Minimum effective modal bandwidth length |
| OM1 62.5-/125-micron multimode fibre | 850-nm | 3.5 dB/km | 200 MHz-km | Not required |
| | 1300-nm | 1.5 dB/km | 500 MHz-km | Not required |
| OM2 50-/125-micron multimode fibre | 850-nm | 3.5 dB/km | 500 MHz-km | Not required |
| | 1300-nm | 1.5 dB/km | 500 MHz-km | Not required |
| OM3 50-/125-micron multimode fibre | 850-nm | 3.0 dB/km | 1500 MHz-km | 2000 MHz-km |
| | 1300-nm | 1.5 dB/km | 500 MHz-km | Not required |
| OM4 50-/125-micron multimode fibre | 850-nm | 3.0 dB/km | 3500 MHz-km | 4700 MHz-km |
| | 1300-nm | 1.5 dB/km | 500 MHz-km | Not required |
| OM5 50-/125- micron multimode fibre | 850-nm | 3.0 dB/km | 3500 MHz-km | 4700 MHz-km |
| | 953-nm | 2.3 dB/km | 1850 MHz-km | 2470 MHz-km |
| | 1300-nm | 1.5 dB/km | 500 MHz-km | Not required |

| SINGLE-MODE FIBRE | | | | |
|---|---|---|---|---|
| Cable type | Wavelength | Maximum attenuation | Minimum overfilled modal bandwidth length | Minimum effective modal bandwidth length |
| Single-mode indoor-outdoor | 1310-nm | 0.5 dB/km | N/A | N/A |
| | 1383-nm | 0.5 dB/km | N/A | N/A |
| | 1550-nm | 0.5 dB/km | N/A | N/A |
| Single-mode indoor plant | 1310-nm | 1.0 dB/km | N/A | N/A |
| | 1383-nm | 1.0 dB/km | N/A | N/A |
| | 1550-nm | 1.0 dB/km | N/A | N/A |
| Single-mode outside plant | 1310-nm | 0.4 dB/km | N/A | N/A |
| | 1383-nm | 0.4 dB/km | N/A | N/A |
| | 1550-nm | 0.4 dB/km | N/A | N/A |

# Konvertor media pretvarač: Fiber Media Converter

Fiber media pretvarač je dodatni mrežni uređaj koji se koristi za povezivanje optičkih i različitih tipova medija. Standardno povezuje optičke kablove sa UTP (bakarnim) kablovima) pretvaranjem optičkih signala u električne signale i obrnuto.

Konverter medija obično ima tri interfejsa: PoE[13] port, SFP slot i port za napajanje.

Sama jedinica prima električne signale od PSE-a, kao što je PoE svič i PoE injektor, pretvara signale u optičke i prenosi ih niz optički kabl do drugog medijskog pretvarača. A drugi uređaj će zatim pretvoriti signale natrag u električne signale koje rubni uređaj (podržan za PoE) može primiti.

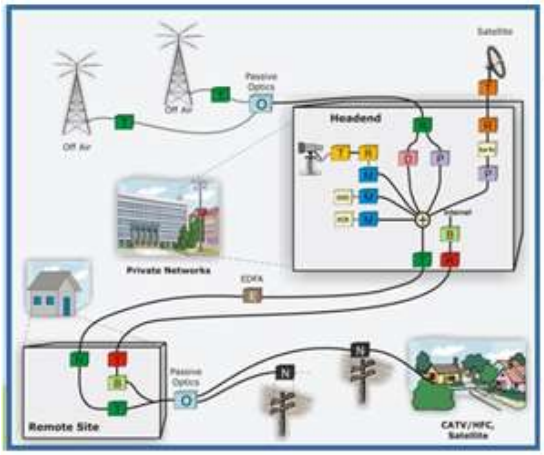

*Gigabit Fiber Ethernet komplet za konverziju medija sa 100m gotovim optičkim kablom*

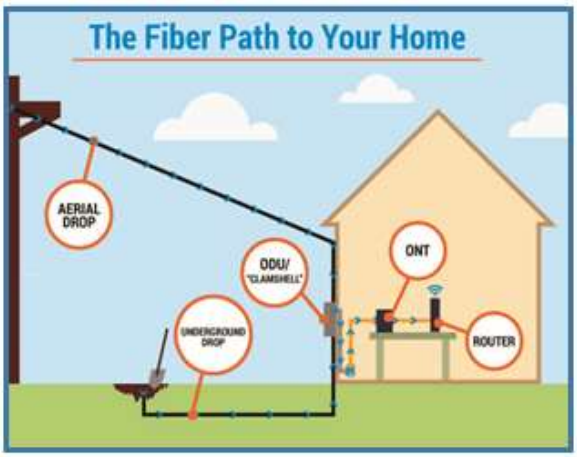
Konverter medija predstavlja ekonomičan način da se unaprijede postojeće konfiguracije ožičenja uz minimalan uticaj na stare uređaje, ali uz značajno povećanje brzine mreže.


*Jednoportni fiber media pretvarač*

[13] Power over Ethernet, ili PoE, opisuje bilo koji od nekoliko standarda ili ad hoc sistema (pa i sistemima sa optičkim kablovima) koji prenose električnu energiju zajedno sa podacima o UTP Ethernet kablovima.
PoE tehnologija omogućuje običnim Ethernet mrežnim kabelima da funkcioniraju kao kabeli za napajanje. U PoE-omogućenoj mreži jednosmjerna struja (DC) teče preko mrežnog kabla zajedno s normalnim Ethernet protokom podataka. Većina PoE uređaja slijedi IEEE standard 802.3af ili 802.3at.


*Ilustracija realizacije priključka konvertora (sa PoE napajanjem) optičkog u žični signal*



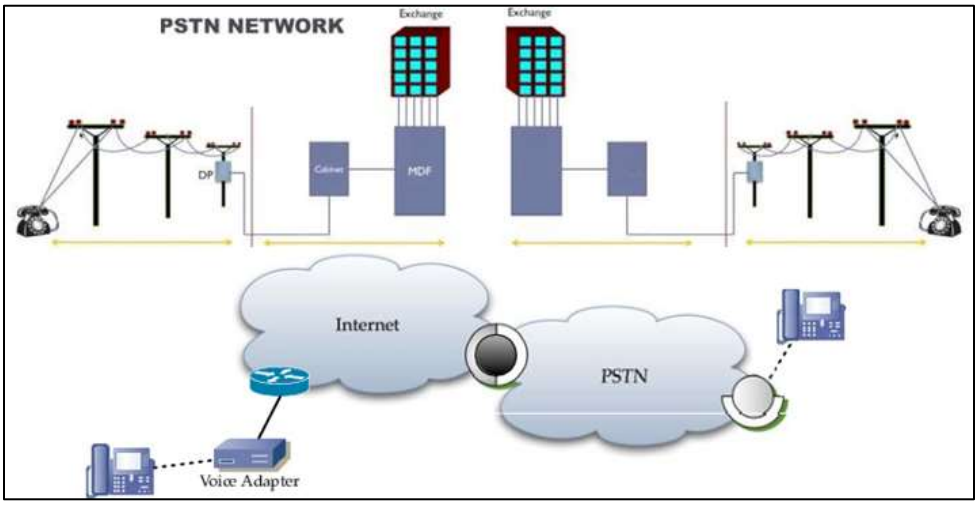




*Mada se (zbog cijena) optičke mreže realizuju kao dio WAN mreža moguće je da se implementira i kao kućna verzija LAN-a*

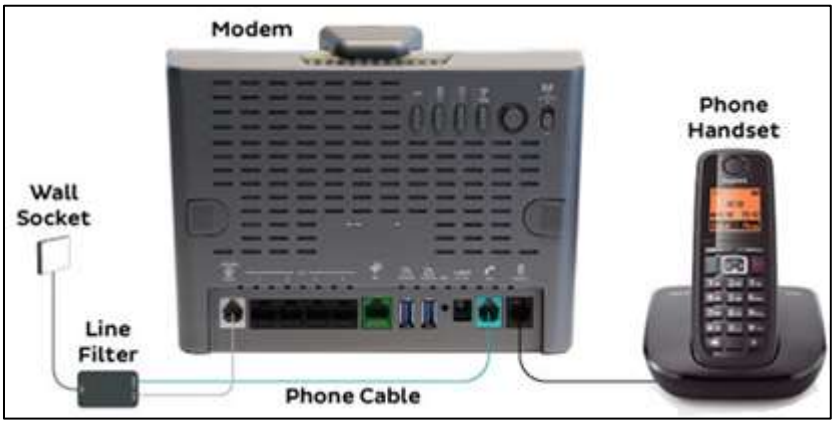
# Tipovi veza koje koriste telefonske mreže

## PSTN Klasična (dial-up) telefonska veza sa modemom

Dial-up pristup Internetu je oblik pristupa Internetu koji koristi mogućnosti PSTN javne komutirane telefonske mreže (*Public Switched Telephone Network*) za uspostavljanje veze sa provajderom Internet usluga (ISP) biranjem telefonskog broja na konvencionalnoj telefonskoj liniji.




PSTN je projektovan davno sa osnovnim ciljem da se uspješno prenese govorni signal. Karakteristika komutacione mreže je da se u fazi uspostave veze bira jedan od mogućih puteva prenosa, a za vrijeme održavanja veze informacija se prenosi uspostavljenim fizičkim putem. Sasvim je moguće, da se za dvije uzastopne uspostave veze sa istih lokacija izabere potpuno različit fizički put prenosa informacije. Često se kaže da su ovo primjeri čvrste direktne veze.
Da bi se ovom mrežom mogli prenositi podaci, potrebno je na oba kraja veze postaviti modeme, uređaje koji vrše modulaciju i demodulaciju digitalnog signala iz računara. Signali u računaru su digitalni, a telefonske linije su analogne tako da **modem na izlazu vrši konverziju digitalnog signala u analogni, a na ulazu u računar prevodi analogni signal u digitalni**.



Računarski modemi mogu biti interni i eksterni:

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

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

Pošto je telefonska mreža konstruisana za prenos govora, njen propusni opseg je mali - do 3.4 kHz što dovodi do toga da su brzine prenosa podataka kilobitskog, a ne megabitskog reda veličine.

Analogna transmisija i primjena modemske tehnologije dostiže maksimalnu brzinu od 56 kbit/s pomoću savremenih modulacionih tehnika, kao i tehnika kompresije (koristeći V.90 ili V.92 protokol). Što je protok veći, veći je i uticaj šuma. Osim toga, šum se javlja i pri D/A i A/D konverziji. Takođe, brzine prenosa čak i pri uslovima bliskim idealnim ne postižu maksimalne nominovane vrijednosti. Na primjer, modem od 56 kbit/s pri najboljim uslovima može postići brzinu između 45 i 50 kbit/s.

Brzina interneta pomoću ove tehnologije može pasti na 21,6 kbit/s ili manje. Loše stanje telefonske linije, visok nivo buke i drugi faktori utiču na brzinu dial-up-a. Iz tog razloga se popularno naziva **sindrom 21600.**

U posljednjih dvadesetak godina Dial-up je doživio značajan pad u upotrebi, s zraženom tendencijom da u bliskoj budućnosti potpuno nestane, kako se sve više korisnika prelazi na širokopojasnu vezu.

Jedan od faktora koji doprinose su zahtjevi za propusnim opsegom novijih kompjuterskih programa, kao što su operativni sistemi i antivirusni softver, koji automatski preuzimaju značajna ažuriranja u pozadini kada se prvi put uspostavi veza s Internetom. Ova preuzimanja u pozadini mogu potrajati nekoliko minuta ili duže i, dok se sva ažuriranja ne završe, mogu ozbiljno utjecati na količinu propusnog opsega dostupnog drugim aplikacijama kao što su web pretraživači.

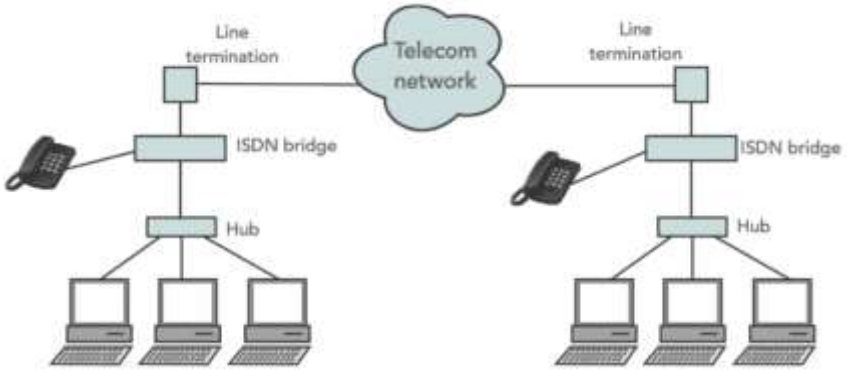
Istraživanje provedeno 2018. procjenjuje da je 0,3% Amerikanaca koristilo dial-up.

# Integrisani digitalni mrežni servisi ISDN

ISDN (*Integrated Services Digital Network*) predstavlja digitalni ekvivalent analognoj telefonskoj mreži, a u odnosu na nju obezbjeđuje bolji kvalitet i veću brzinu prenosa.

Početkom 70-tih godina XX vijeka prvi put se javila ideja o integrisanim servisima tj. ideja da se preko jedne jedinstvene mreže korisnicima osim standardnih servisa telefonije korisnicima bi se ponudio i prenos faksa, zvuka, muzike i videa. 1984. donešen je prvi paket preporuka za realizaciju i primjenu ISDN-a.
**Danas se smatra zastarjelom** tehnologijom koja se mijenja VoP uređajima baziranim na SIP tehnologijama.

ISDN predstavlja **nadgradnju**, odnosno viši stepen postojeće **javne komutirane telefonske mreže**. Veći dio komutacionih sistema (telefonskih centrala) i prenosnih sistema između centrala je digitalizovan. Međutim, pretplatnički dio mreže je ostao analogan. Uvođenjem ISDN-a i pretplatnički dio mreže postaje digitalan, i to korišćenjem postojećih bakarnih parica.




*ISDN obezbjeđuje kompletan digitalni prenos od kraja do kraja*

Uređaj povezan na ISDN uslugu i konvertovan za upotrebu na običnih telefona pretvaranjem digitalnih signala u analogne, ili obrnuto. Ovo je bilo brže od modema od 56Kb koji su koristili konvencionalni zvuk. ISDN poziv za razmjenu podataka je bio telefonski poziv na određeni broj, tako da je broj koji je pozvan takođe morao imati ISDN, biti u mogućnosti da obavlja komunikaciju i razmjenu podataka, a i obje strane su morale koristiti isti komunikacijski protokol. (Ovo je bilo i prije masovnog i obavezujućeg korištenja Interneta, tako da je bilo puno različitih protokola u zajedničkoj upotrebi).

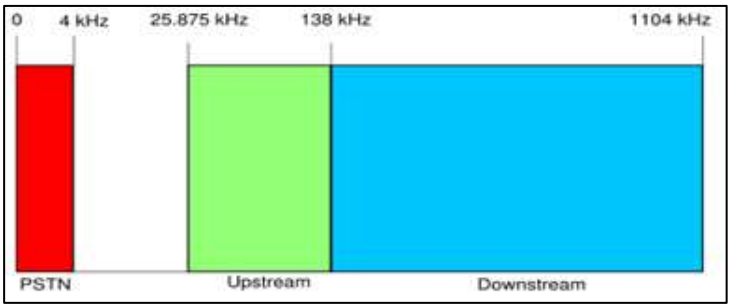
## Digitalne pretplatničke veze DSL/ADSL

Termin DSL (*Digital Subscriber Line*) (ili xDSL) opšte uzevši predstavlja način prenosa digitalnih signala po bakarnim paricama većim brzinama (počev od 144 kb/s pa sve do 50 Mb/s).

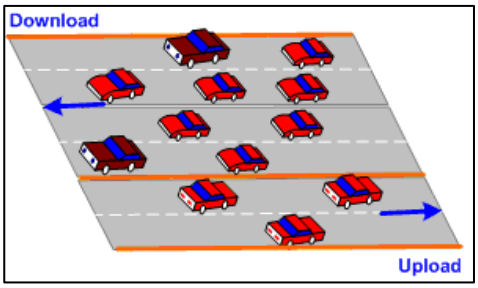
| *Ime* | *Značenje* | *Protok* | *Način rada* | *Aplikacije* |
|---|---|---|---|---|
| DSL | **Digital Subscriber Line** | 160 kb/s | Duplex | ISDN, prenos govora i podataka |
| HDSL | **High data rate Digital Subscriber Line** | 2.048 Mb/s (1.544 Mpbs) | Duplex | T1/E1 servisi, WAN i LAN pristup |
| SDSL | **Single line Digital Subscriber Line** | 2.048 Mb/s (1.544 Mpbs) | Duplex | Isto kao HDSL uz opremu za simetričan pristup |
| ADSL | **Asymmetric Digital Subscriber Line** | 1.5 - 9 Mb/s (Down) | 16 - 640 kb/s (Up) | Pristup Internetu, udaljenom LAN-u, VoD |
| VDSL | **Very high data rate Digital Subscriber Line** | 13 - 52 Mb/s (Down) | 1.5 - 2.3 Mb/s (Up) | Isto kao ADSL uz prenos HDTV signala |

*Tabela sa pregledom osnovnih xDSL tehnologija*

Najpoznatija je takozvana asimetrična digitalna pretplatnička linija (ADSL-*Asymetric Digital Subscriber Line*). Kao što joj i samo ime kaže, osnovna karakteristika ove vrste DSL realizacije je asimetričnost. Asimetričnost, zapravo, znači mogućnost mnogo bržeg prenosa podataka od mreže ka korisniku (*downstream*) nego što slanje podataka od korisnika ka mreži (*upstream*).




*Princip ADSL-a – podijela frekvencijskog opsega*



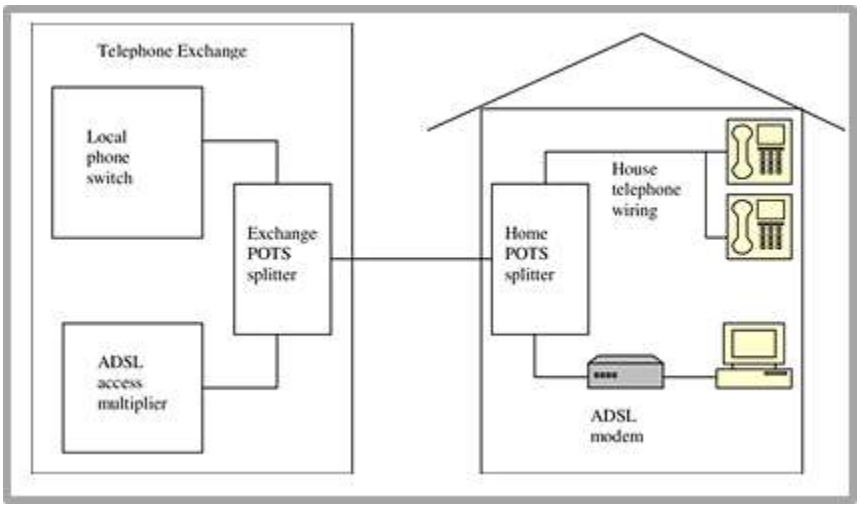

*Plastičan prikaz ADSL-a*

ADSL usluga se realizuje instalacijom dva uređaja na strani korisnika gdje se nalazi djelitelj frekvencije (spliter) ADSL primopredajnik (ADSL modem). i može se realizovati preko obične telefonske linije ili baznog ISDN priključka. ADSL kolo povezuje ADSL modem na svakom kraju parice telefonske linije formirajući tri informaciona kanala:

- downstream kanal velike brzine
- dupleks kanal srednje brzine i
- POTS ili ISDN kanal.

Telefonski par žica je povezan na uređaj mrežnog interfejsa (NID), gdje frekvencijski spliter, takođe poznat i kao POTS spliter, razdvaja niskofrekventne govorne signale od visokofrekventnih signala podataka.
Telefonski izlazni port interfejsa je povezan na postojeće telefonske žice.

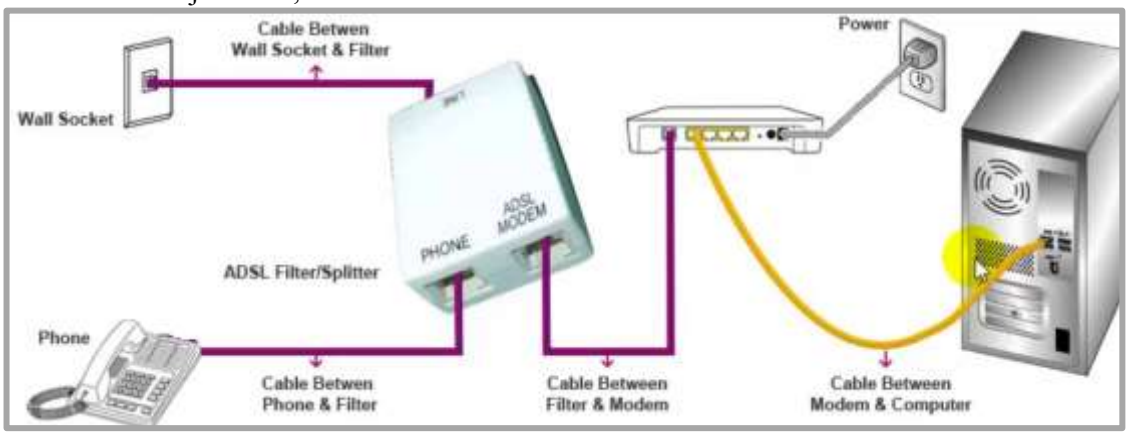
Izlazni port za podatke je povezan na ADSL modem, koji je zatim spregnut sa Ethernet mrežnom interfejsnom karticom instaliranom unutar PC-a.
Frekvencijski spliter može biti van ili u okviru interfejsnog uređaja.




Frekvencijski opseg koji se koristi za puni ADSL podjeljen je u tri dijela :

- opseg od 0 do 4 kHz je rezervisan za govornu telefoniju,
- dio između 25 kHz i 138 kHz za upstream podatke do Interneta,
- ostatak opsega do 1.1 MHz za downstream podatke od ISP-a do korisnika.

POTS kanal je odvojen filtrima od digitalnog modema, što garantuje neprekidni POTS/ISDN servis, čak i ako ADSL ne uspije. Velike brzine kanala su u opsegu od 1.5 do 6.1 Mb/s, dok su dupleks brzine u opsegu od 16 do 64 kb/s. Svaki kanal može biti podmultipleksiran do forme više kanala manje brzine, zavisno od sistema.

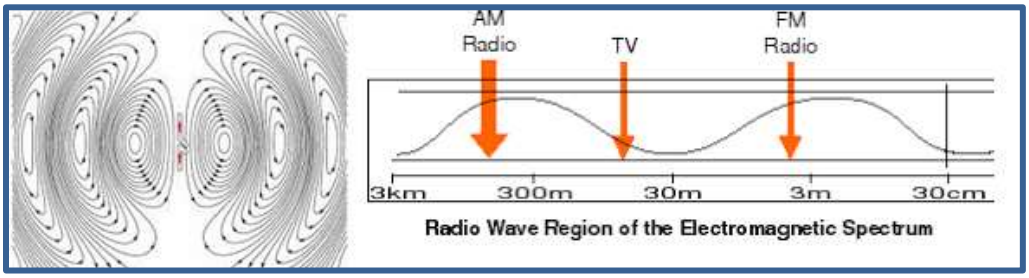



Minimum konfiguracije obezbeđuje 1.5 ili 2 Mb/s downstream i 16 kb/s dupleks kanal; standardno objezbjeđuju protoke od 6.1 Mb/s downstream i 64 kb/s u full-dupleksu.
Danas se umjesto žične forme često koriste se ADSL WiFi modemi zbog jednostavne i jeftine infrastrukture.
Međutim, žična forma obezbjeđuje mnogo bolje sigurnosno okruženje, pa je i dalje u upotrebi.

# Bežični mediji

## Svojstva radio talasa

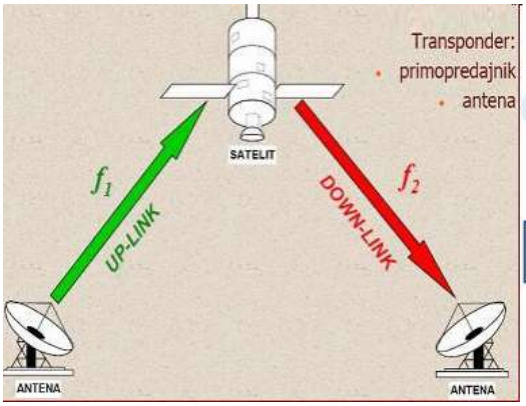
Riječ je o elektromagnetskim talasima iz frekventnog raspona koji se inače koristi za radio ili televiziju. Podaci se prenose preko talasa određene frekvencije, slično kao radio program.

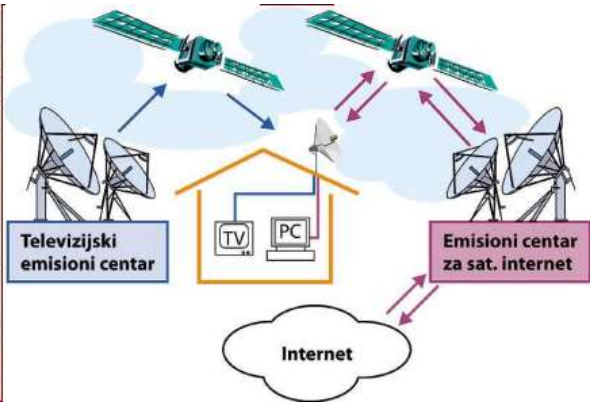



Računari koji koriste radio talase moraju imati antene za emitiranje i primanje talasa. Domet zavisi o izabranoj frekvenciji talasa.

| Naziv pojasa | Frekvencija | Talasna dužina | Upotreba |
|---|---|---|---|
| | < 3 Hz | > 100 000 km | H.A.A.R.P. projekti i vojna upotreba |
| ekstremno niske frekvencija | 3—30 Hz | 100 000 km – 10 000 km | komunikacije sa podmornicama |
| super niske frekvencije | 30—300 Hz | 10 000 km – 1000 km | komunikacije sa podmornicama |
| ultra niske frekvencije | 300—3000 Hz | 1000 km – 100 km | podzemne komunikacije - rudnik |
| vrlo niske frekvencije | 3—30 kHz | 100 km – 10 km | podmornice, geofizika, nadzor medicinskih uređaja |
| niske frekvencije | 30—300 kHz | 10 km – 1 km | navigacija, AM radio, časovni signali |
| srednje frekvencije | 300—3000 kHz | 1 km – 100 m | AM radio |
| visoke frekvencije | 3—30 MHz | 100 m – 10 m | radio-amateri |
| vrlo visoke frekvencije | 30—300 MHz | 10 m – 1 m | FM radio, televizija, avioni |
| ultra visoke frekvencije | 300—3000 MHz | 1 m – 100 mm | televizija, mobilni telefoni, avijacija, bežični internet (LAN) |
| super visoke frekvencije | 3—30 GHz | 100 mm – 10 mm | mikrotalasna peć, avijacija, radar |
| ekstremno visoke frekvencije | 30—300 GHz | 10 mm – 1 mm | radioastronomija |
| | iznad 300 GHz | < 1 mm | |

Primjenjuju se za bežične (“wireless”) LAN-ove, pogotovo za spajanje laptopa na mrežu.
Primjenjuju za uspostavljanje interkontinentalnih veza između dijelova Interneta – tada su potrebni sateliti. Svrha satelita u interkontinentalnim vezama je pojačavanje radio signala i svladavanje zakrivljenosti zemlje.

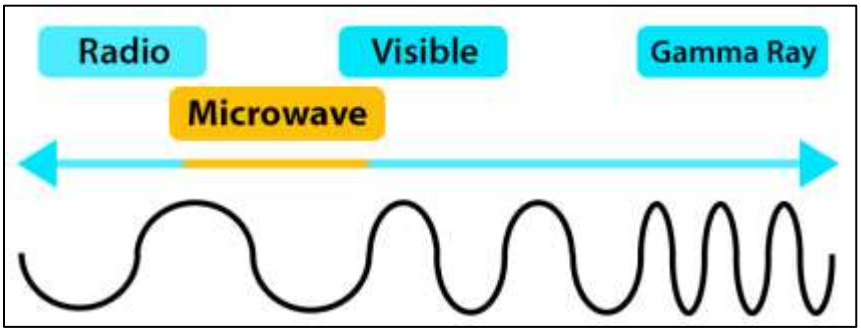



Kasnije ćemo se nešto detaljnije pozabaviti nekim od uređaja baziranih na bežičnoj tehnologiji, a zasad ćemo se upoznati sa osnovnim karakteristikama talasa koji omogućavaju ovu tehnologiju.

## Svojstva mikrotalasa

Riječ je o elektromagnetskim talasima iz frekventnog raspona iznad onog koji se koristi za radio ili televiziju.



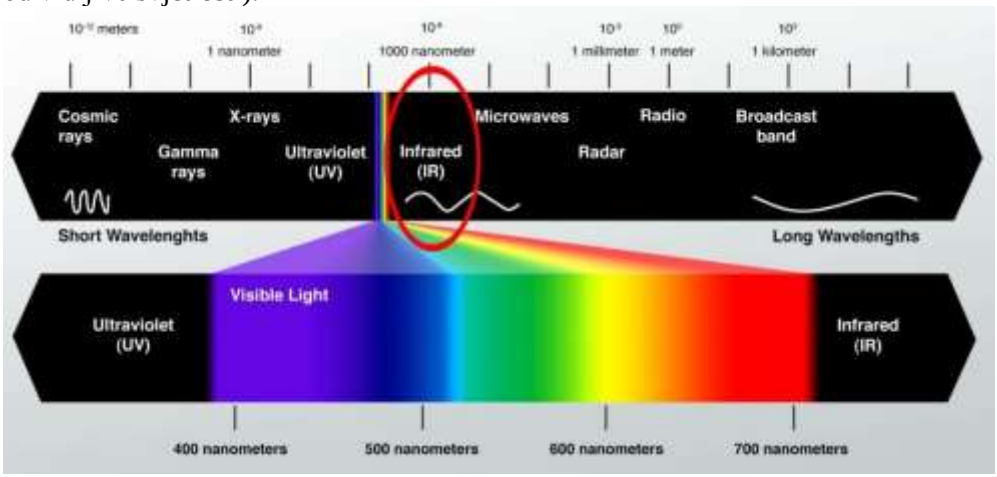

Mikrotalasi su zajednički naziv za decimetarsko, centimetarsko i milimetarsko područje radiotalasa. Tradicionalno to obuhvata područje frekvencija iznad 300 MHz, međutim danas se često kao donja granica mikrotalasa uzima i frekvencija od 1 GHz.

Podaci se opet prenose preko talasa određene frekvencije, slično kao radio program. Za razliku od radio talasa, mikrotalasi se mogu usmjeriti prema jednoj tački, čime se štedi energija i sprečava "prisluškivanje". Takođe, mikrotalasi mogu nositi više informacija nego radio talasi. Mana im je da ne mogu proći kroz neke vrste zapreka. Antene se zato moraju postaviti tako da među njima postoji "optička vidljivost".

Primjena je u gradskim WAN-ovima, tamo gdje bi inače bilo skupo polaganje žica.

## Svojstva infracrvenih zraka

Opet je riječ o elektromagnetskim talasima, no ovaj put iz infracrvenog (toplinskog) spektra, dakle ispod frekventnog raspona vidljive svjetlosti. Infracrveni talasi su oni između frekvencija 300GHz i 400THz u elektromagnetnom spektru (talasne dužine im je kraća od mikrotalasa, ali duže od vidljive svjetlosti).

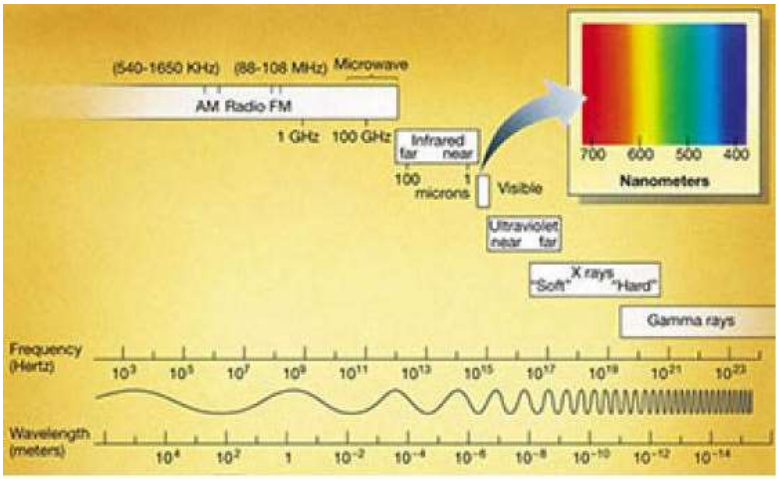



Ne mogu prodrijeti kroz zidove i sunčevi infracrveni zraci ometaju te zrake. (Dakle, ne može se koristiti za komunikaciju na daljinu.) Kako je njihova upotreba ograničena unutar zatvorenog prostora, ne trebaju im nikakve vladine dozvole za svoje aplikacije.

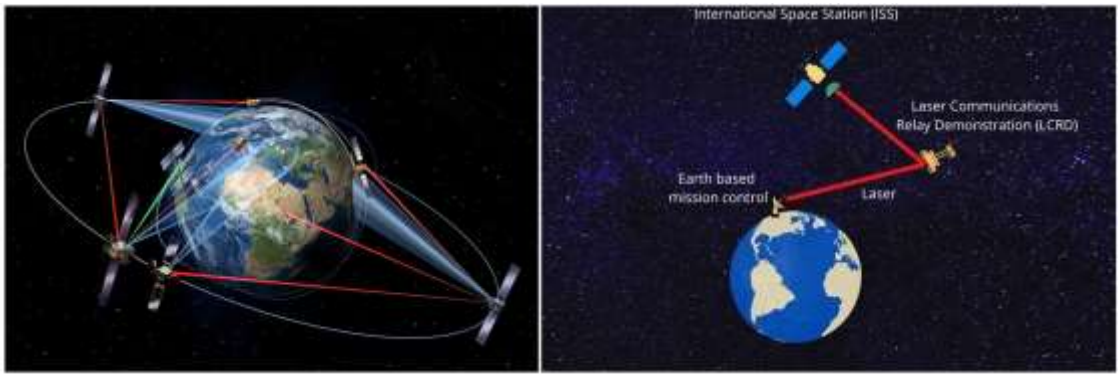
Infracrvene zrake predstavljaju jeftino rješenje u odnosu na druge bežične medije jer ne zahtijevaju antene. No one imaju mali domet, svega nekoliko metara.
Koriste se za bežično povezivanje uređaja unutar jedne sobe: na primjer laptop, tasture i miševi.

## Svojstva laserskih zraka

Riječ laser je akronim za Pojačavanje svjetlosti stimulisanom emisijom zračenja (*Light Amplification by Stimulated Emission of Radiation*).



Koristi se da opiše uređaje uređaje koji emituju elektromagnetno zračenje koji koriste pojačavanje svjetlosti stimulisanom emisijom zračenja na talasnim dužinama od 180 nanometara do 1 milimetra.
Kod laserskih zraka podaci se pretvaraju u svjetlo, koji se **umjesto optičkim vlaknima prenosi zrakom, odnosno vakumom i svemirskim prostorom**. Koristi se lasersko svjetlo, zato jer ono ima relativno veliki domet i može se usmjeriti prema jednoj tački.




*Laserski zraci nisu pogodni za zemaljski prenos pošto laserske zrake ometaju fizički objekti*

Aktivni laserski medij smješten je između dva ogledala, "rezonatora". Jedno od tih ogledala je i jednosmjerno ogledalo. Zračenje aktivnog laserskog medija pojačano je u rezonatoru. Istovremeno, samo određeno zračenje može izaći iz rezonatora kroz jednosmjerno ogledalo. Ovo zračenje je lasersko zračenje.

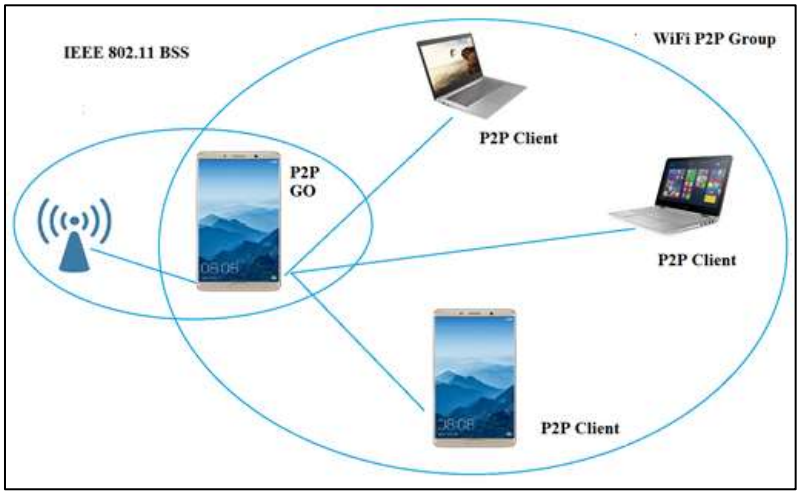
Računarske mreže s laserskim prenosom podataka koristi slobodan prostor kao medij za prenos podataka (Free Space Optical Link). Komunikacija između usmjerenih uređaja se ostvaruje putem moduliranog laserskog snopa u vidljivom i IC talasnom području. Posebno su pogodni za izgradnju gradskih komunikacijskih mreža, MAN (Metropolitan Area Network).
Komunikacija između usmjerenih uređaja se ostvaruje putem moduliranog laserskog snopa u vidljivom i IC talasnom području.

Napomena: Ne treba ih mješati sa optičkim medijima realizovanih kao svjetlovodi – fiber laser i laser **nisu** sinonimi.

# Bežična mrežna komunikacija WLAN i WiFi

Kao sve prisutniju tehnologiju izdvojićemo bežičnu komunikaciju. Pošto ima određene specifičnosti teško bi bilo da se univerzalno prate i prave razlike u zasnovanu na „žičnoj"-„bakar" komunikaciji.

Bežična lokalna mreža (**WLAN**, *wireless local area network*) je metoda bežičnog povezivanja dva ili više uređaja koji koriste visokofrekventne radio talase i često uključuju pristupnu tačku internetu. WLAN je fleksibilan komunikacioni sistem implementiran u početku kao dodatak ili kao alternativa žičnom LAN-u u zgradama, bolnicama, aerodromima itd. Ova tehnologija još se naziva i **WiFi** (***Wireless Fidelity***) i danas je jedna od dominantnih tehnologija implementacije LAN mreža. Ova tehnologija omogućava brzi i jeftin bežični prenos podataka sa brzinom do 45 Mbps u P2P režimu prenosa na rastojanjima do 60 km. (Oba podatka: i brzina i domet su samo moguća, realno oboje je mnogo manje.)




Slaba strana kao i kod svih *wireless* rješenja predstavlja činjenica da je takva veza podložna spoljnim uticajima koji mogu dovesti do anomalija (i zloupotreba) u prenosu. Dobra strana je da je brzo i jeftino rješenje za povezivanje što ga čini pravim izborom u slučajevima kada ne postoje tehničke mogućnosti korištenja infrastrukture fiksne telefonije

Danas, koristi se treća generacija WLAN tehnologije koju je standardizacijsko tijelo IEEE oformilo pod nazivom 802.11. IEEE 802.11 prvi je standard za bežične lokalne mreže objavljen 1997. godine, nakon toga javljaju se verzije. Zadnja važeća verzija objavljena 2021. je 802.11ax, poznatija kao "Wi-Fi 6", radi u opsezima od 2,4 GHz i 5 GHz sa brzinama podataka u višegigabitnom opsegu.

Radio komunikacija kod WLAN-ova se obavlja u tzv. **ISM** (*Industrial, Scientific & Medical*) opsegu frekvencija koji je svuda u svijetu prihvaćen kao **opseg za čije korišćenje nije potrebna dozvola-licenca od strane regulatornih agencija** (vlasti) - takozvani FTA (*free to air*) spektar. ISM čine tri opsega frekvencija:

- 902 - 928 MHz,
- 2400 - 2483,5 MHz (koja se najčešće koristi) i
- 5728 - 5750 MHz.

IEEE 802.11 standardi određuju dva načina rada: **infrastrukturni i ad hoc način rada**.
Infrastrukturni način rada koristi se za povezivanje bežičnih krajnjih uređaja, poznatim i pod nazivom bežični klijenti, na postojeću ožičenu mrežu uz pomoć bežičnog usmjerivača ili pristupne tačke.
Ad hoc način rada koristi se za direktno povezivanje bežičnih klijenata, bez potrebe za bežičnim usmjerivačem ili pristupnom tačkom. Ad hoc mreža sastoji se od bežičnih klijenata koji svoje podatke šalju direktno jedni drugima.

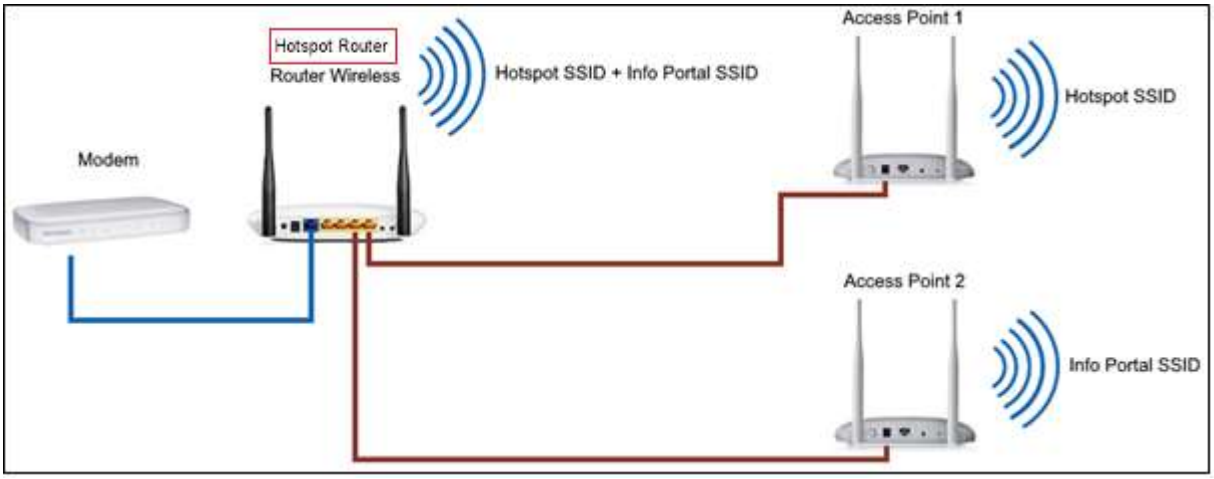
## Žarišna tačka -Hot spot- i WIFi

*Wi-Fi i hotspot su opšti pojmovi koji se često koriste kao sinonim za pristup Internetu.*

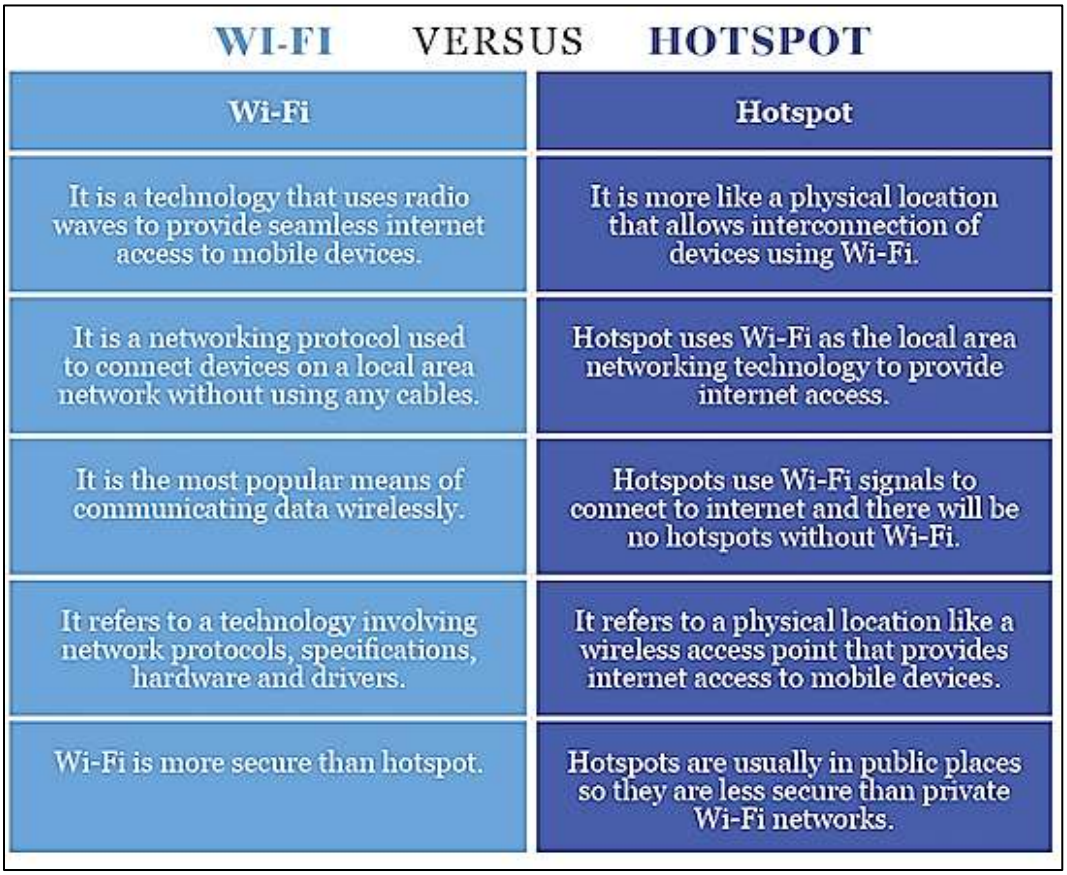
Iako se ovi izrazi obično koriste naizmjenično, postoje neke bitne razlike između Wi-Fi-ja i žarišne tačke naročito u pogledu načina pristupa, efikasnosti, sigurnosti i sigurnosnog područja.

WiFi prenosi i prima radio talase unutar uređaja zasnovanih na IEEE 802.11 mrežnim standardima.

Žarišna tačka nije ništa drugo nego **fizička lokacija** (obično javna mjesta poput kafića, hotela ili aerodroma) koja omogućava pristup Internetu mobilnim uređajima koji obično koriste Wi-Fi.




Omogućava uređajima da međusobno komuniciraju putem bežične lokalne mreže. Ove WLAN mreže kreiraju prenosnu žarišnu tačku koristeći modem ili bežični ruter koji je povezan s ISP-om, provajderom koji omogućuje konekciju na Internet.
Wi-Fi je vrsta servisa internet usluga, dok je hot spot lokacija koja omogućava pristup tim servisima.
Vruće tačke su obično lokacije gdje svako može pristupiti internetu što ga čini pogodnim mjestom za cyber napade.

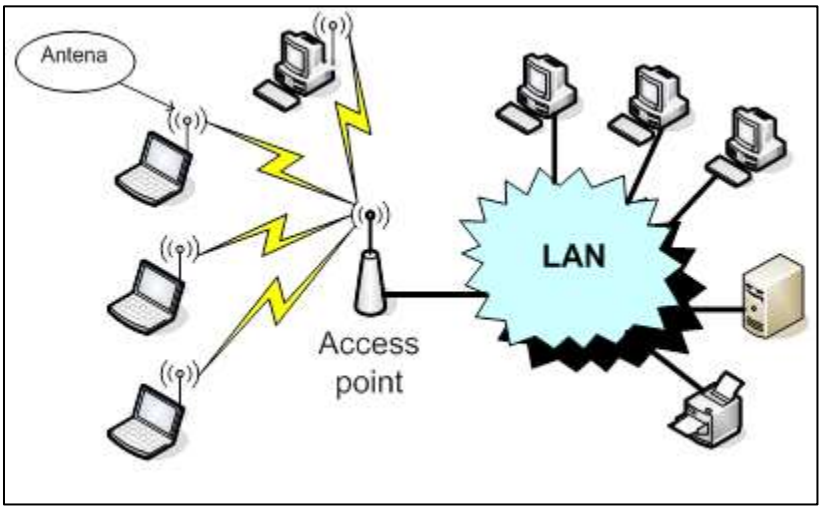



*Osnovne karakteristike i poređenje WiFi i HotSpot-a*

# Bežična pristupna tačka Access point

BPT Bežična pristupna tačka (*Wireless Access Point* ***WAP***) je uređaj koji omogućava bežičnim uređajima priključivanje na računarsku mrežu koristeći Wi-Fi, Bluetooth ili neki drugi bežični standard.

**BPT** je uređaj koji objedinjuje par odašiljač/prijemnik i koristi se umjesto Dail-In servera ili Ethernet habova kod žičnih mreža. Access Point je uređaj koji služi za međusobno povezivanje klijenata i predstavlja centralni dio jedne mreže. Takođe, može da se koristi i za spajanje wireless klijenata sa LAN-om ili sa izlazom na Internet. Access pointi igraju ulogu mostova (*bridges*) izmedu bežičnih stanica i resursa u žičnom LAN-u (serveri i ruteri za pristup internetu). U tipičnoj WLAN konfiguraciji povezuje se na žičnu mrežu sa fiksne lokacije koristeći standardan Ethernet kabl.




*Bežičan pristup LAN-u preko Access point uređaja*

Svaki access point ima integrisan konektor za antenu kao i konektor za LAN. Može da radi u nekoliko modova (čije prisustvo varira u zavisnosti od uređaja i proizvođača):

- *client* mod (pomoću njega se spaja na mrežu isto kao i pomoću obične kartice),
- *bridge* mod (koristi se za spajanje dvije mreže ili više mreža u jednu cjelinu),
- *repeater* mod (kao ripiter – onnavljač signala, koristi se ako je potrebno dodatno povećati domet mreže).

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


*Antene*

Pristupna tačka prima, obrađuje i šalje podatke između WLAN-a i žične mrežne infrastrukture.

## Bežični LAN uređaji i LAN Adapteri

Bežični LAN uređaji su uređaji kojima je potrebna bežična veza do mrežne infrastukture. Krajnji korisnici pristupaju WLAN-u preko bežičnih LAN adaptera, koji se često se nazivaju i Wifi adapteri ili Wifi ključevi.

*Lijevo WiFi adapter u obliku USB-a:, desno primjer PCI/PCIe bežičnog adaptera*

Bežični adapter je uređaj koji dodaje bežično povezivanje/bežično na laptop ili desktop računar. Ovi uređaji su dostupni kao eksterni USB moduli (dongle), kao i PCI ili PCI Express (PCIe) kartice koje se priključe u prazne slotove na matičnoj ploči.
Za razliku od laptopa koji već imaju interni bežični modul, PC ili desktop računari ga obično nemaju, pa je ovaj bežični adapter neophodan kako bi se računar mogao povezati na dostupne Wifi rutere/hotspotove oko lokacije, koji se zatim mogu koristiti za pristup internetu.
Napomena:
*Bežični adapter može sadržavati i Bluetooth modul, tako da računar može pristupiti Bluetooth uređajima u blizini, kao što su slušalice i zvučnici. Bluetooth modul i internet modul se razlikuju, stoga nemojte samo kupiti bežični bluetooth adapter ako želite pristupiti internetu, i nemojte kupovati bežični internet adapter ako želite pristupiti bluetooth-u, osim ako uređaj nema oba modula u njemu i to je jasno navedeno u specifikacijama.*
Korištenjem sličnih adaptera mogu se realizovati i drugi bežični uređaji kao npr. bežični most (*Wireless Bridge*) ili bežični gatewayi.

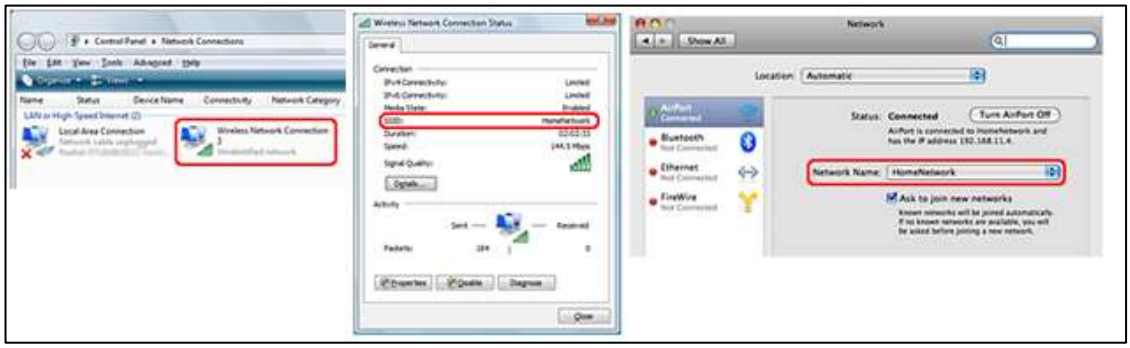
## Skup servisnih usluga SSID

SSID znači "Service Set Identifier"- "Identifikator skupa usluga". Prema standardu IEEE 802.11 za bežično umrežavanje, "skup usluga" odnosi se na skup bežičnih mrežnih uređaja s istim parametrima. Dakle, SSID je identifikator (ime) koji vam govori koji skup usluga (ili mreža) se pridružuje. SSID-ovi su dizajnirani kao jedinstveno ime za razlikovanje više WiFi mreža u području tako da se možete povezati s željenom.

Identifikatori skupa usluga razlikuju bežične LAN mreže dodjeljujući svakom jedinstvenom 32-bitnom alfanumerički identifikator znakova.

Identifikator skupa usluga prvenstveno je osmišljen da razlikuje bežičnu lokalnu mrežu na mjestima na kojima bi drugi WLAN također mogao istovremeno emitirati. Identifikator skupa usluga funkcionira u suradnji s osnovnim servisnim setom (BSS), kombinacijom pristupnih tačaka i povezanim klijentima i proširenim skupom usluga (ESS).

SSID za Wi-Fi mrežu tehnički je naziv imena mreže.




*Primjer definisanja SSID usluga iz Conttrol panela kod Windows-a*

Na primjer, ako vidite znak koji vam govori da se pridružite mreži s SSID-om "Airport WiFi", samo trebate pronaći popis bežičnih mreža u blizini i pridružiti se "Airport WiFi" mreži.

*SSID omogućuje razne opcije - možete ga promijeniti, sakriti ga i onemogućiti pristup drugih uređaja ili ga koristiti za stvaranje više zasebnih mreža s različitim imenima i parametrima pristupa. To vam omogućuje udobno korištenje jednog uređaja s Wi-Fi tačkom, u potpunosti prilagođavajući ga tako da odgovara vašim zadacima i potrebama.*

## Bluetooth

Bluetooth[14] je bežična tehnologija prenosa podataka i govora, razvijena od strane proizvođača raznovrsne elektronske opreme, sa ciljem da se njihovi proizvodi – od kompjutera i telefona do tastatura i bežičnih slušalica, umreže na malim udaljenostima (do 10 metara) bez upotrebe kablova, brzo i jednostavno.

Ideja iz koje je potekao bluetooth, nastala je 1994. godine kada je *Ericsson Mobile Communications* odlučio da ispita mogućnosti povezivanja mobilnih telefona sa njihovim dodacima preko jeftine radio veze sa malom potrošnjom struje. Ideja je bila da se u svaki uredjaj ugradi mali radio i na taj način iz upotrebe izbace kablovi. Godinu dana kasnije, pravi potencijal te ideje je počeo da se kristališe. Glavna istraživanja obavljana su u Ericsson-ovim laboratorijama. Ericsson je prije usvajanja imena bluetooth tehnologiju nazivao „*Multi-Communicator Link*“ (MC Link).

Originalna zamisao bila je da se poveže bežična slušalica sa mobilnim telefonom, a to što su otkrili da na isti način mogu da povežu većinu elektronskih uređaja, bila je, po njihovim rečima – srećna slučajnost. Početkom 1998[15]. godine Ericsson je uradio nešto sasvim neočekivano – odlučio je da tehnologiju ne naplaćuje, i svim zaintresovanim kompanija dao besplatne licence, što se pokazalo kao najbolji način da tehnologija postane globalni standard. Ericsson je započeo razgovore sa kompanijama iz različitih sfera proizvodnje elektronske opreme (Nokia – mobilni telefoni, IBM i Toshiba – prenosni kompjuteri i Intel – čipovi za digitalnu obradu signala) sa ciljem da se osnuje konzorcijum koji će dalje razvijati i promovisati tehnologiju otvorene specifikacije za bežično umrežavanje.

## Bluetooth proizvodi

Danas je bluetooth standard za umrežavanje na malim udaljenostima. Mogućnosti bluetooth tehnologije su razne i teško ih je nabrojati – od originalne zamisli, povezivanje bežične slušalice sa mobilnim telefonom, preko upravljanja kompjuterom uz pomoć mobilnog telefona i razmjena podataka između dva mobilna telefona, pa do nalaženja parkiranog automobila, ali i partnera (toothing), kontrole zamrzivača i mikrotalasne pećnice, kao i „bežičnog“ pisanja sa bluetooth olovkom...

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

*Bluetooth USB adapter*

*COM Bluetooth bežična PC kartica*

[14] Samo ime duguje danskom kraluj Harald Bluetooth koji je živio u X vijeku

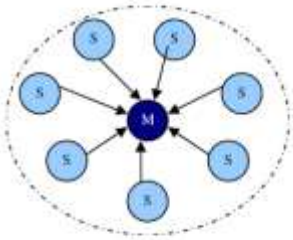
[15] Bluetooth tehnologija javnosti je zvanično predstavljena 20. maja 1998. godine kada je pet kompanija, Ericsson, IBM, Intel, Nokia i Toshiba, održalo simultanu konferenciju za štampu u Londonu, Tokiju i San Hozeu

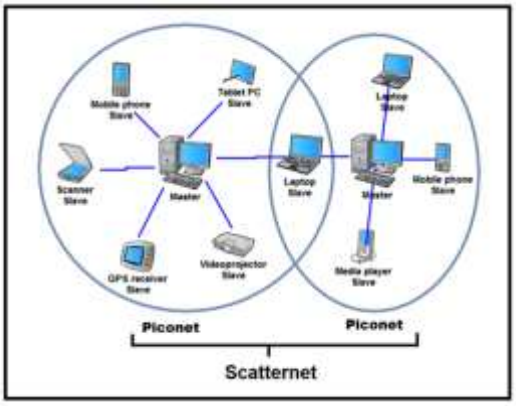
*Bluetooth adapter za kola*

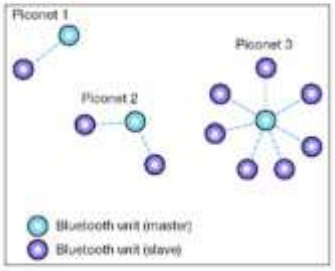
*Logitech Bluetooth bežična slušalica*

## Princip rada Bluetooth-a

Konfiguracija mreža Bletooth tehnologijom moguće je ostvariti tri osnovne topologije: point-to-point, piconet mrežu i scatternet mrežu, koje koriste radio talase za transfere govora i podataka u radijusu od 10 metara.

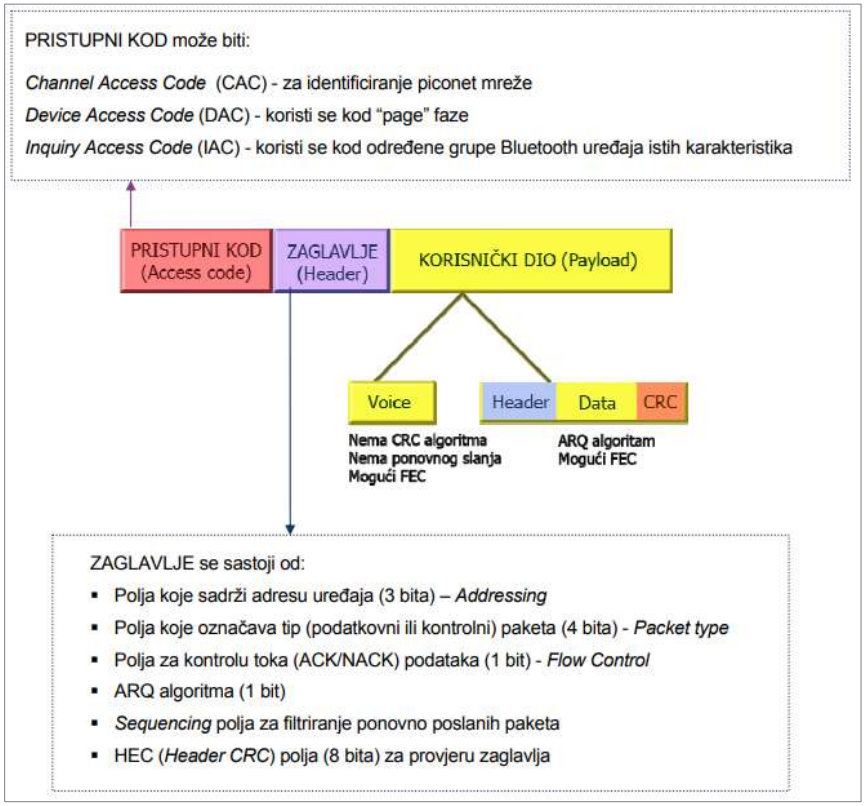





Kada se dva ili više Bluetooth uređaja spoje, kreira se tzv. **piconet**. Svaki piconet može da sadrži do 8 različitih uređaja (jedan master i sedam slave uređaja). U njoj se jedna jedinica ponaša kao nadređena (master), kontrolišući promet, a ostale jedinice su podređene (slave).
Više piconeta može biti spojeno u **scatternet**. Veza između scatternet mreža ostvaruje se preko jednog Bluetooth uređaja koji može biti slave u dvije ili više piconet mreža, ali master u samo jednoj piconet mreži. Takav uređaj može biti gateway propuštajući promet iz jedne mreže u drugu.
Pristupni kod služi za identifikaciju i sinhronizaciju uređaja i temelji se na identitetu master-a i njegovog sistemskog takta (clock-a) koji služi za sinhronizaciju rada s ostalim uređajima u mreži. Pristupni kod je jedinstven za svaki kanal i koriste ga svi paketi koji se prenose tim kanalom. Zaglavlje sadrži upravljačke informacije: bitove za korekciju greške, podatke o ponovnom slanju podataka i kontroli toka podataka.

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




*Format paketa određen Bluetooth standardom*

Frekvencijski opeseg za bluetooth prenos je definisan u granicama 2.4GHz do 2.48 GHz. Teoretska najveća moguća brzina prenosa po Bluetooth specifikaciji iznosi 2.1 Mb/s. U praksi je to naravno malo drugačije. Maksimalna dvosmerna brzina prenosa (fullduplex, komunikacija u oba pravca u isto vrijeme) je 462 Kbps. Asimetrična transmisija omogućava brzinu prenosa od 721 Kbps u jednom pravcu, i 56 Kbps u drugom. U slučaju prenosa govora, koriste se tri sinhrona kanala brzine od 64 Kbps (svaki).

## Ad hoc umrežavanje Bluetooth uređaja

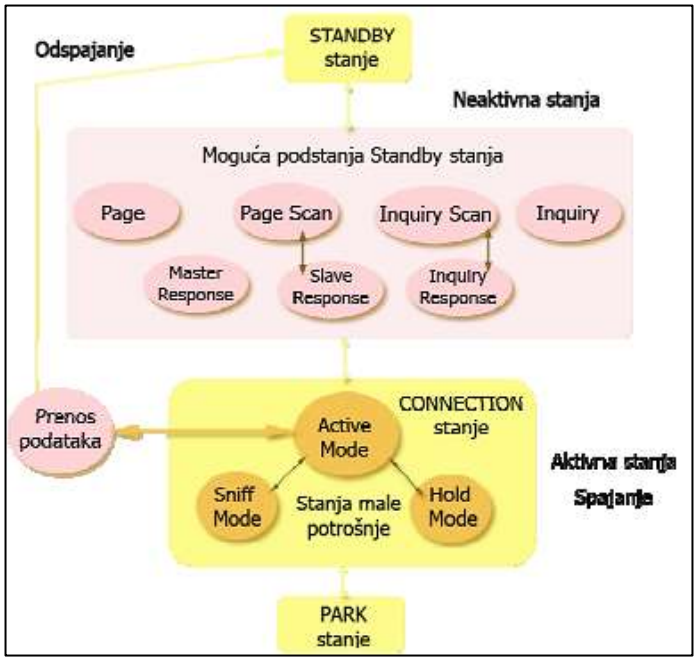
Bluetooth uređaji mogu slati i primati pakete unutar jedne piconet mreže, njihovo sudjelovanje u ostalim mrežama temelji se na vremenskom multipleksiranju TDM-u (*Time Division Multiplex*). To znači da iako uređaji mogu sudjelovati u radu ostalih mreža, oni mogu biti aktivni samo unutar jednog piconet-a u nekom određenom trenutku, odnosno dijele svoje vrijeme prema broju piconet-a, radeći jedan dio vremena u jednoj, a drugi dio vremena u drugoj mreži.
Da bi se izbegla interferencija bluetooh uređaja sa drugim uređajima iz ISM opsega (a i da bi se povećala sigurnost), koristi se tehnika frekvencijskog preskakivanja s raspršenim spektrom (FHSS: *frequency hopping spread spectrum).* Kod FHSS modulacije definišu se frekvencijski skokovi unutar spektra, gdje se pod skokovima misli na ekstremno brze promjene frekvencija na kojima se prenose. Svako „osluškivanje" se obavlja na 32 različite frekvencije.

Odašiljač i prijemnik moraju biti sinhronizirani prema nizu preskakivanja kako bi održali logički kanal, jer u suprotnom dolazi do gubitka podataka.
Cijeli frekventni pojas na 2.4 GHz, (2.4 GHZ – 2.4835 GHZ) dijeli se na 75 do 79 neprekrivajućih podkanala pri čemu je širina svakog kanala 1MHz. Zahvaljujući FHSS tehnici istovremeno može postojati 10 nezavisnih piconet mreža (ili do 80 uređaja). Iznad tog broja mreža postaje preoptrećena.

Kada se Bluetooth uređaji nađu unutar dometa oni uspostavljaju ad hoc mrežu. U toj mreži jedan od uređaja postaje master, a svi ostali uređaji su slave (podređeni). Bilo koji uređaj može postati master. Uređaj koji uspostavlja vezu, prema definiciji, preuzima tu funkciju.
Umrežavanje uređaja unutar piconet mreža i uspostava međusobne komunikacije ide u nekoliko koraka:

1. Uređaj je prvo u Standby stanju. Zatim ulazi u Inquiry podstanje u kojem traži prisutnost drugih uređaja u mreži (trajanje ~2s). Bluetooth specifikacija definiše Inquiry pristupne kodove pomoću kojih uređaj specificira koji tip uređaja traži u mreži (npr. kao PDA, printer ili LAN pristupna tačka). Za vrijeme Inquiry upita, uređaj iz vlastitog lokalnog clock-a i Inquiry pristupnog koda generira niz frekvencijskog preskakivanja. Taj niz pokriva 32 kanala od mogućih 79 (FHS tehnika). Prema generisanom nizu uređaj šalje Inquiry upit na svakom kanalu (broadcast upit),
2. Ostali uređaji se u mreži u određenim vremenskim intervalima (periodično) nalaze u Inquiry scan podstanju i osluškuju medij. Ti uređaji također generišu niz fekvencijskog preskakivaja iz svog lokalnog clock-a i pristupnog koda. Ako uređaj koji se nalazi u Inquiry scan podstanju dobije Inquiry upit, on tada ulazi u Inquiry response podstanje i odgovara s Inquiry response porukom koja uključuje adresu tog uređaja i njegov clock (za sinhronizaciju),
3. Svi uređaji koji su broadcast inquiry porukom pronađeni unutar 10 m (dometa), odgovoriće na Inquiry poruku. Zbog toga često korisnik sam mora selektovati željeni Bluetooth uređaj s liste pronađenih uređaja,
4. Uređaj koji je slao Inquiry upit, sada prima Inquiry response poruku i ulazi u Page podstanje kako bi uspostavio vezu. U page podstanju, uređaj generiše frekvencijski niz preskakivanja na temelju adrese i vrijednosti clock-a pronađenog uređaja koje dobiva iz Inquiry response poruke. Prema tom nizu na svakom od 32 kanala šalje Page poruku. Ako u međuvremenu u mreži postoje uređaji koji žele komunicirati s njim, on će u nekim vremenskim intervalima ulaziti u Page scan podstanje. Uređaj osluškuje medij za odgovor svakih 1.25 s na 16 kanala od mogućih 32,
5. Traženi uređaj u mreži (sada već slave) prima Page poruku i odgovara s Page response paketom onome ko je posalo Page poruku (sada kao master),
6. Kada master primi odgovor, šalje FHS paket slave uređaju. FHS paket sastoji se od Bluetooth adrese i clock-a mastera. Nakon što slave primi FHS paket, on šalje ACK paket da je primio FHS paket. To dobiva master i generira novi niz frekvencijskog preskakivanja iz vlastite adrese i vlastitog clock-a. Slave tada koristi masterovu adresu i clock za generiranje identičnog niza. Time se je master sinhronizova sa slave uređajem i moguće je uspostaviti komunikaciju,

7. Nakon što je Page proces gotov, uređaji prelaze u Connection stanje (trajanje Page-Connected procesa ~0.6s). Master tada šalje poll paket slave uređajima kako bi potvrdio uspješan prelaz iz niza frekvencijsog preskakivanja koji je bio prisutan u Page stanju u novi niz koji se temelji na njegovom vlastitom clock-u i adresi.




Bluetooth uređaji se u svakom trenutku nalaze u neka od tri glavna stanja:

- stanje uspostavljene konekcije (*Connection*)
- stanje osluškivanja (*Standby*) i
- stanje pripravnosti (Park)

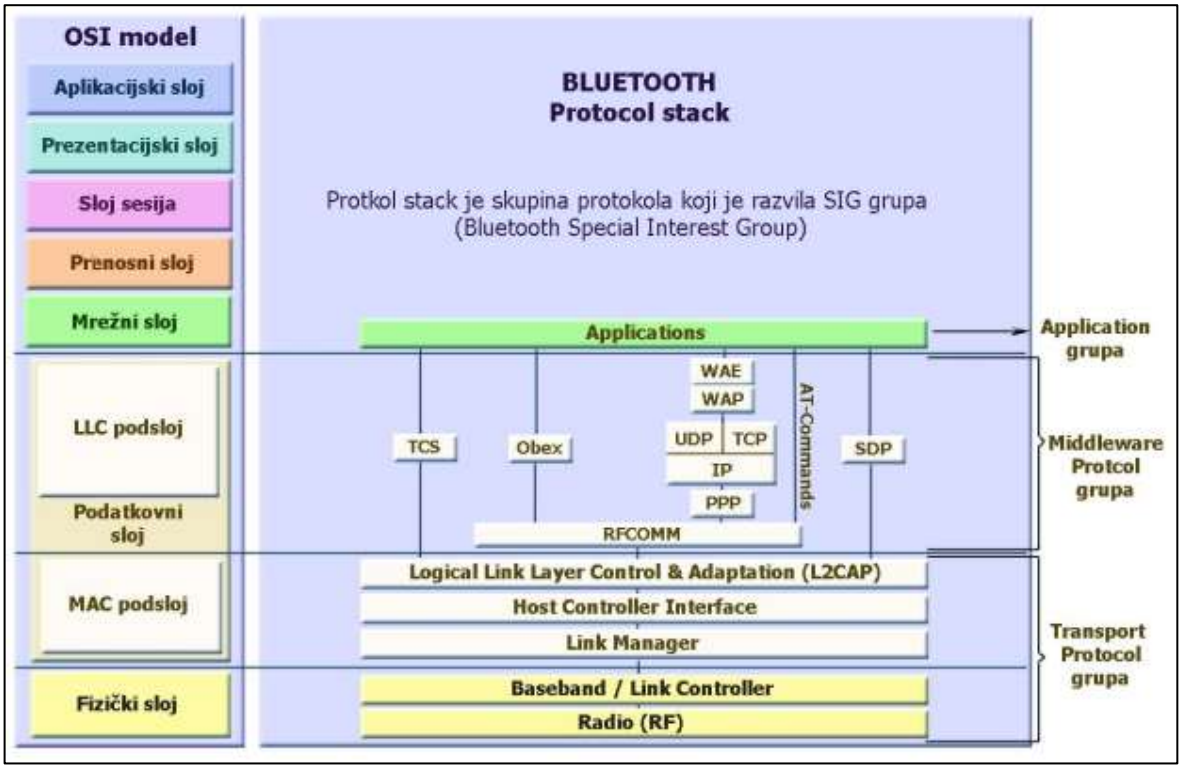
Uređaj je u stanju connection ako ima uspostavljenu vezu sa drugim uređajem (ili uređajima) i ako obavlja neku aktivnost (primanje/slanje). Uz svoju 48-bitnu MAC adresu, uređaj ima i 3-bitnu Active Member Address (AM_ADDR).

U Standby stanju Bluetooth uređaj čeka da se priključi piconet mreži. Uređaj osluškuje medij svakih 1.25 sekundi na 32 različite frekvencije (kanala) u vremenu od 10 ms na pojedinom kanalu.

Park stanje: Bluetooth uređaj ulazi u ovo stanje kada više ne želi biti aktivan čvor piconet mreže, ali želi ostati dio njega tako da se kasnije može uključiti u komunikaciju. Zato uređaj ostaje sinhroniziran s master-om i osluškuje broadcast medij. Uz svoju 48-bitnu MAC adresu uređaj dobiva i 8-bitnu Parked Member address (PM_ADDR). Ovo stanje je korisno ako ima više od 7 uređaja koji žele biti dio istog piconet-a. Parkirani slave uređaji se tada iz park moda bude regularno, slušaju na određenom kanalu, vrše re-sinhornizaciju i provjeravaju ima li broadcast poruka poslanih od strane master-a.

U bluetooth specifikaciji, definisana su tri moguća bezbjednosna moda:

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

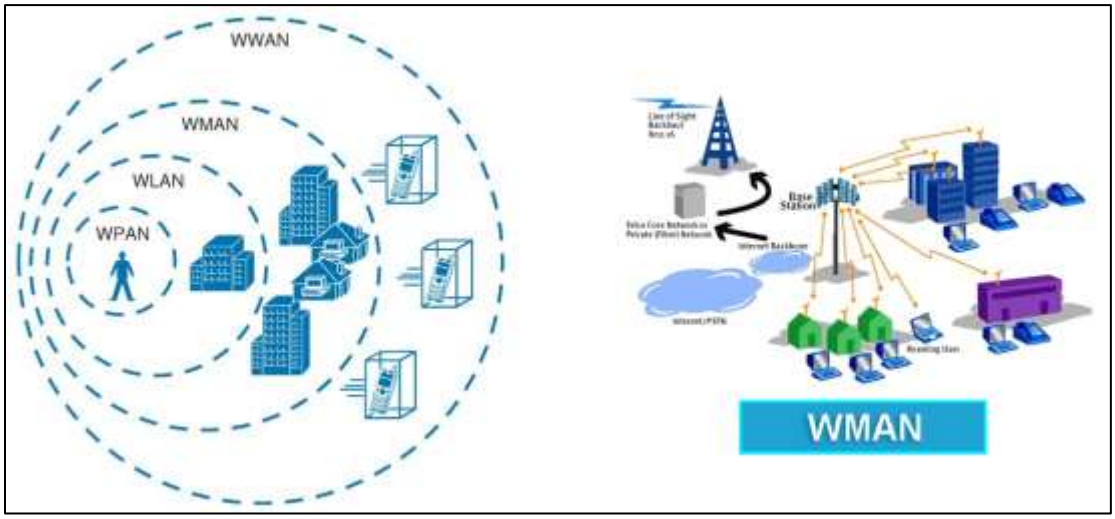



*Pozicija Bluetoth-a u OSI modelu*

Za razumjevanje gornje ilustracije potrrbno bi bilo da se upoznamo sa osnovnim modelima i protokolima koji se koriste pri realizaciji mreža (što ćemo pokušati razjasniti kasnije). Recimo da su za potrebe Blutoth uređaja razvijeni posebani protokoli i koji odgovaraju standardnim (OSI i TCP/IP) protokolima i modelima.

# Bežične mreže prema prostoru koji obuhvataju

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




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

**Lokalne bežične mreže** (*Wireless Local Area Network* – WLAN) omogućavaju da računari na jednoj geografskoj lokaciji dijele informacije i zajedničke uređaje (štampači, baze podataka, itd.). U okviru ove mreže omogućeni su isti servisi kao i u žičnim mrežama, a imaju niz prednosti u odnosu na žični LAN – mobilnost, fleksibilnost, skalabilnost, brzina protoka, jednostavnost i smanjenje troškova instalacije. WLAN su neophodne u situacijama kada, zbog arhitektonskih, geografskih ili drugih razloga, nije moguće ostvariti druge načine formiranja mreže. Ograničavajući faktor primjene je relativno kraći domet veze (30–300m) i frekvencijski opseg. Ako je potrebno premostiti veća rastojanja koriste se dodatne antene sa pojačivačima za podizanje nivoa signala.

**Bežične personalne ili lične mreže** (*WPAN – Wireless Personal Area Network)* koristi se za povezivanje računara koji su locirani u jednoj sobi. Udaljenost uređaja manja je od 10 metara. Za povezivanje se koristi IrDA, Wireless USB, ili Bluetooth.

# Mrežna kartica, interfejs mreža-računar

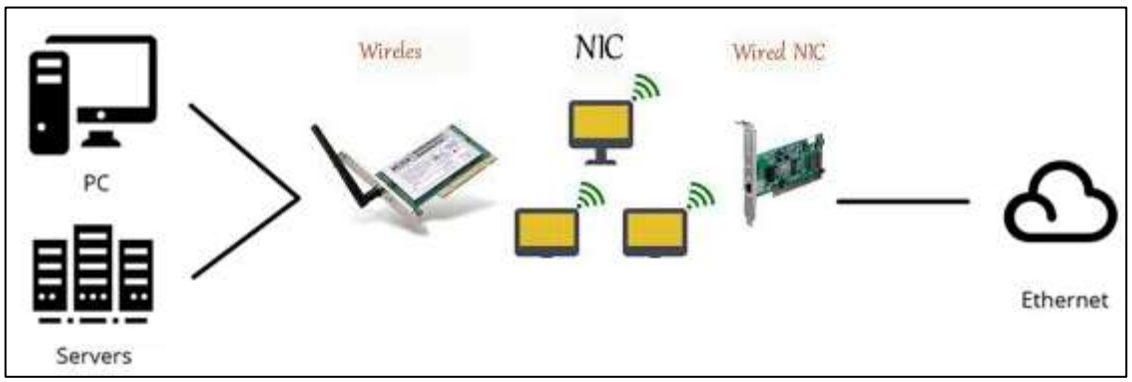
**Mrežna kartica je uređaj koji povezuje računar sa računarskom mrežom**. Često se naziva: mrežni adapter, mrežni interfejs, *NIC*...

Mrežne kartice pakuju podatke u frejm i prenose podatke iz računara, a potom primaju, raspakuju i dekonvertuju primljeno sa mreže.

Da CPU računara ne bi bio trajno opterećen poslom stalnog praćenja sobraćaja na mreži u računar se ugrađuje posebni hardverski sklop – *mrežni* ili *LAN* interfejs poznat kao mrežna kartica, koji radi bez pomoći procesora i memorije. Osnovni zadatak mrežne kartice je da se brine za sve detalje vezane uz slanje i primanje okvira podataka pristiglih sa mreže, ili poslatih na mrežu.

Mrežne kartice su se ranije u računarima mogle naći najčešće u vidu zasebnih kartica dok se **danas uglavnom integrišu u matične ploče računar**a. Ako se koristi odvojena mrežna kartice, obično se uzima kao dodatna kartica (uz integrisanu) zbog mogućnosti priključivanja više mrežnih uređaja (npr. ADSL modem (Ethernet) i mrežni hub) , iako neke matične ploče dolaze i sa dva čipa, odnosno priključka. U tom slučaju kartice mogu funkcionisati zasebno ili udruženo.

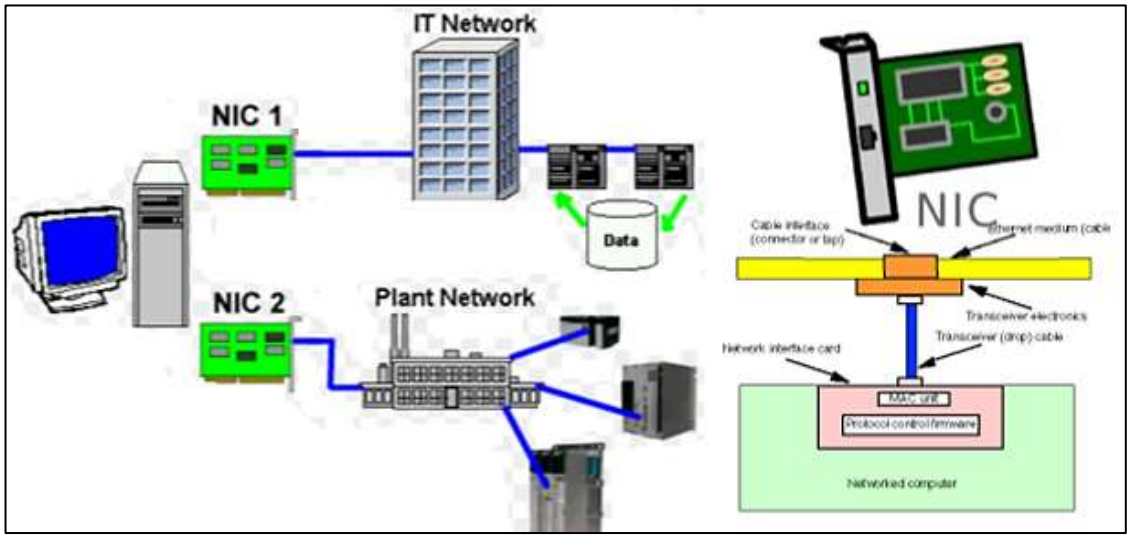
Mrežne kartice uglavnom imaju *RJ-45* (za *UTP* kablove), *BNC*, odnosno *AUI* (*Attachment Unit Interface*) konektore, dizajnirane za eternet arhitekturu. Takođe, na mrežnim karticama se uglavnom nalaze i *LED* diode koje služe za praćenje aktivnosti kartice. Glavni proizvođači mrežnih kartica su *3Com, Intel, Realtek, Marvell, VIA*... Postoje mrežne kartice u 10, 100, i 1000 Mbit/s (Gigabit) izvedbama, što označava propusnost podataka koju može podnijeti jedna mrežna kartica.




Mrežna kartica se sastoji od tri osnovna dijela:

1. Sprege fizičke sredine za prenos - odgovorna za električno slanje i prijem podataka. Sastoji se **od prenosnika** koji šalje ili prima podatke **i konvertora koda.**
2. Kontrolera linka podataka - odgovara MAC podsloju
3. Računarska sprega

Gotovo obavezan je četvri dio memorijski bafer u koji se vrši privremeno smještanje podataka.




## Adresa kontrole pristupa medijima -MAC-

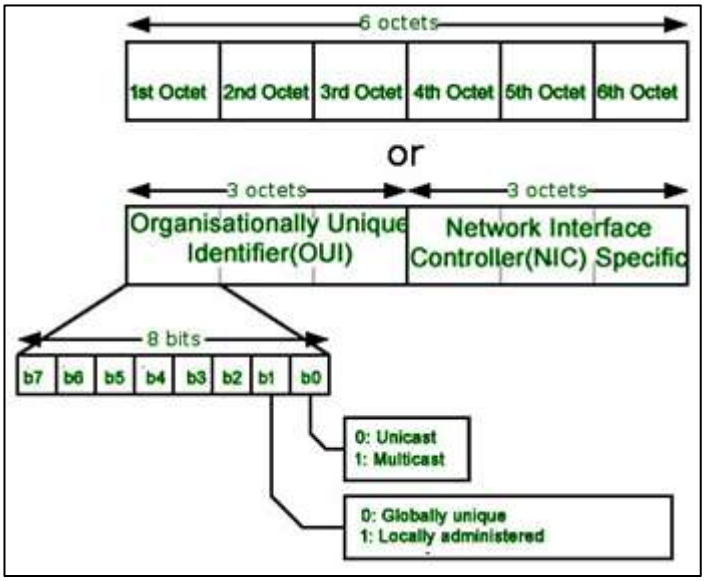
Jedan od važnijih elemenata svake mrežne kartice je *MAC* (**Media Access Control**) adresa. *MAC* adresa predstavlja 48-bitni serijski broj iz opsega koji dodjeljuje proizvođaču.
Svaka od mrežnih kartica ima ovaj MAC broj sa adresom zapisan u svom ROM čipu.

Adresa kontrole pristupa medijima je jedinstveni identifikator koji se dodjeljuje kontroleru mrežnog interfejsa za korištenje kao mrežna adresa u komunikacijama unutar mrežnog segmenta.
Treba naglasiti da **upotreba MAC adresa nije vezana samo za mrežne kartice, već za bilo koji drugi mrežni uređaj fizičkog sloja koji jedinstveno identifikuje uređaj na mreži zasnovanoj na Ethernetu**; upotreba je uobičajena u većini IEEE 802 mrežnih tehnologija, uključujući Ethernet, Wi-Fi i Bluetooth. MAC adresa je poznata i kao *Ethernet adresa, hardverska adresa, fizička adresa ili PHY adresa.*

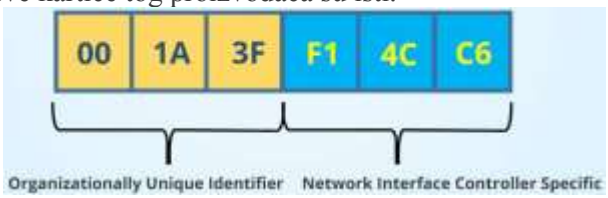
Dio MAC adrese sadrži informacije o proizvođaču, a dio je jedinstven serijski broj uređaja.

MAC adresa se sastoji se od 48 bitova (6 okteta) koji se zapisuje u obliku 12 hexadecimalnih cifri sa više različitih načina grupisanja i odvajanja cifri. Najčešće se koriste tri:

- 6 parova cifri odvojenih crticom (01-23-45-67-89-ab)
- 6 parova cifri odvojenih dvotačkom (01:23:45:67:89:ab)
- 3 skupine po 4 cifre odvojene sa tačkom (0123.4567.89ab)




MAC adresa je logički podjeljena u dva dijela:
Prva tri okteta (24 bita ili prvih 6 hexadecimalnih cifri) predstavljaju **oznaku proizvođača** mrežnih uređaja i za sve kartice tog proizvođača su isti.




Druga tri okteta (drugih 6 hexadecimalnih cifri) su **jedinstveni za svaku** karticu (*isti proizvođač ne može da prodaje dvije iste kartice*).

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

Svi uređaji na istoj mrežnoj podmreži imaju različite MAC adrese. MAC adrese su vrlo korisne u dijagnosticiranju mrežnih problema kao što su problemi s IP adresama.
MAC adrese su korisne za dijagnostiku mreže jer se nikada ne mijenjaju, za razliku od dinamičke IP adrese, koja se s vremena na vrijeme može promijeniti. Za mrežnog administratora, to čini MAC adresu pouzdanijim načinom identifikacije pošiljatelja i primaoca podataka na mreži.

Skraćenica **OUI** (organizationally unique identifie) Organizacioni jedinstveni identifikator je 24-bitni broj koji jedinstveno identifikuje dobavljača, proizvođača ili drugu organizaciju. OUI se kupuju i dodjeljuje od Zavoda za registraciju *IEEE* (*Institute of Electrical and Electronics Engineers*).

Neki OUI poznatih proizvođača:

```
CC:46:D6 - Cisco
3C:5A:B4 - Google, Inc
3C:D9:2B - Hewlett Packard
00:9A:CD - HUAWEI TECHNOLOGIES CO.,LTD
```

# Aktivni mrežni uređaji

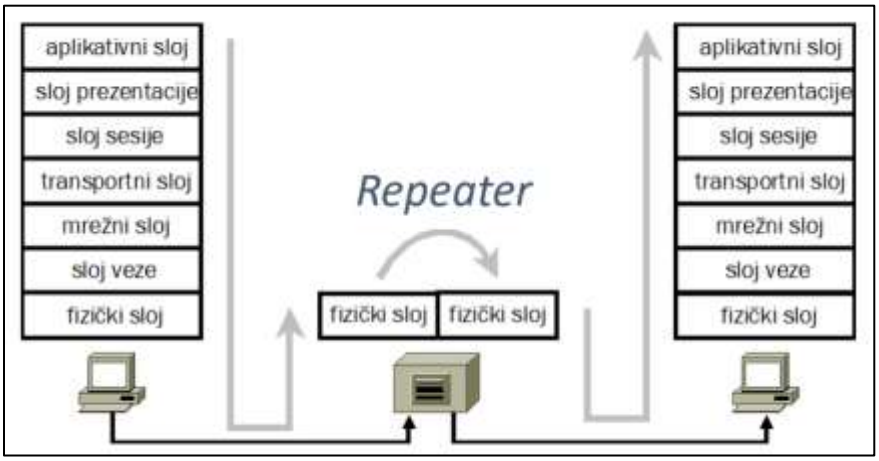
Aktivne mrežne komponente su uređaji koji upravljaju saobraćajem na mreži.
U nastavku su opisani uređaji koji se koriste u realizaciji mreža, počev od onih neophodnih za realizaciju svih vrsta mreža pa sve do uređaja potrebnih za realizaciju WAN mreža. Tu spadaju ripiteri, habovi, mostovi, svičevi, ruteri i *firewall*-ovi.

## Ripiter (Obnavljač signala-Repeater)

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

1. obnavljaju amplitudu (*Reamply*),
2. obnavljaju oblik (*Reshape*) i
3. obnavljaju vremenske reference primljenog signala (*Retime*)

prije nego što signal proslijede na izlazni port.
Ripiter nema informacija o signalu koji pojačava, što znači da se podjednako odnosi i prema ispravnom i prema neispravnom signalu.




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

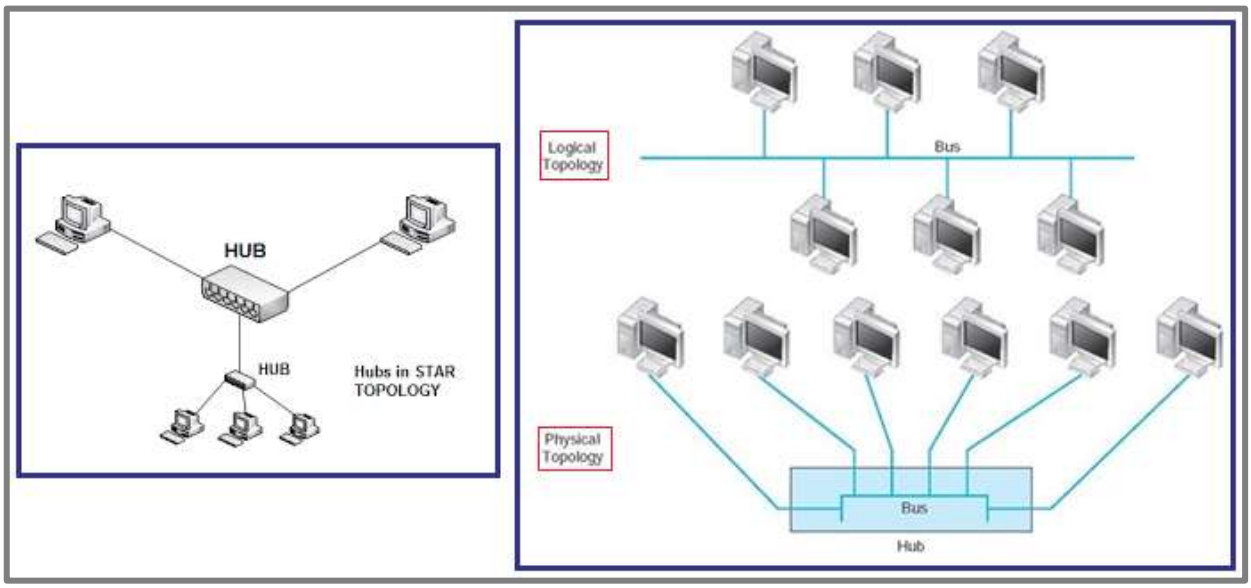
# Hab (Hub)

Hab je uređaj koji objedinjuje više ripitera u jednom kućištu. Može se posmatrati kao višeportni ripiter.
Na habu postoji više konektora (obično su to RJ-45 konektori). Na svaki konektor se priključuje po jedan kabl, preko kojeg se povezuje po jedna radna stanica ili server. Omogućava povezivanje više segmenata mreže u jedan segment.

*Različite veličine habova*

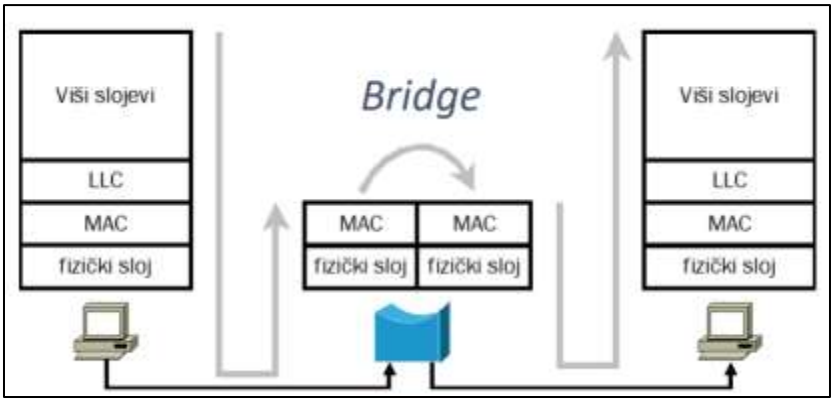
Hab funkcioniše slično kao ripiter: ono što primi na jednom svom portu hab emituje na svim ostalim portovima. **U Ethernet mrežama sa UTP i optičkim kablovima hab je čvor koji povezuje stanice i servere.** Može se koristiti kao centralna tačka u topologiji zvijezde.

Habovi sadrže između 6 i 24 porta i mogu se postavljati i uklanjati u zavisnosti od potreba i u skladu sa razvojem mreže. Najčešće se koriste pri konfigurisanju mreža.
Svaki hab ima još jedan dodatni port koji se naziva *uplink* port. On služi za međusobno povezivanje dva haba. Povezivanje se vrši tako što se spaja uplink port jednog haba sa običnim portom drugog haba.
Hab kao uređaj nestaje (bolje rečeno već je nestao) iz računarskih mreža zbog sve niže cijene svič uređaja koji nude znatno bolje performanse.
**! ! !** Pošto nemaju aktivnu LOGIČKU ulogu i repiter i hab možemo smatrati dijelom pasivne mrežne opreme. Mogu se smatrati pasivnom opremom sa gledišta da nema nikakvu logičku funkciju. Samo pojačavaju primljeni signal i prosljeđuje ga dalje na sve svoje portove.

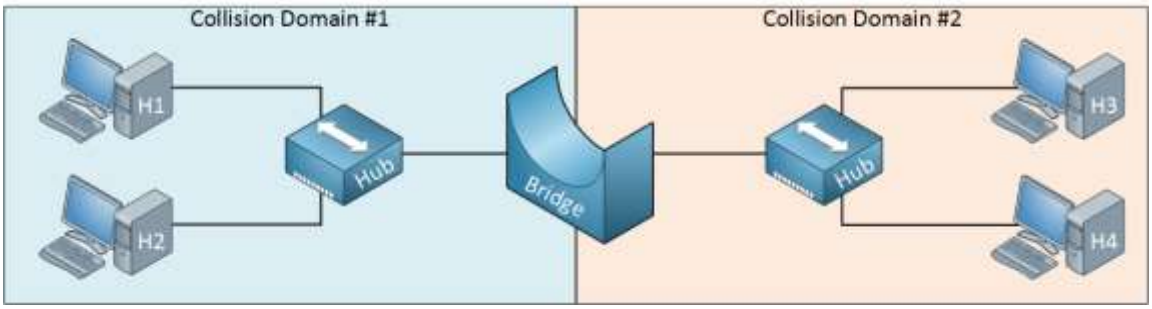


# Mrežni most (Bridge)

To je uređaj koji povezuje udaljene mrežne segmente. Radi u drugom sloju OSI modela, tj. u sloju veze podataka.

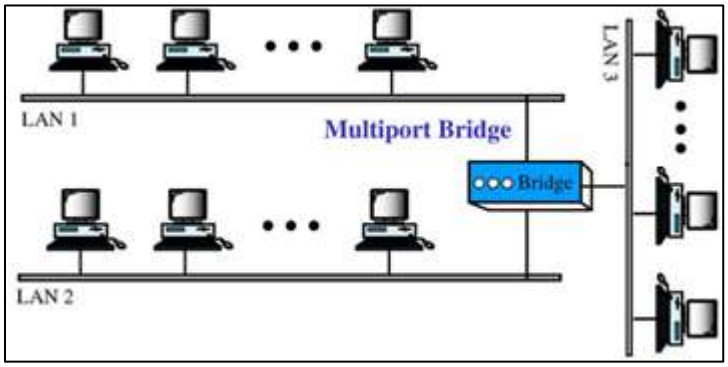



Do sada smo vidjeli da u datom trenutku na mreži može da emituje samo jedna stanica. Ostale stanice osluškuju saobraćaj i kada zaključe da je medijum slobodan šalju svoje pakete.
Može se zaključiti da bi bilo veoma zgodno logički **podijeliti mrežu na segmente koji se sastoje iz stanica koje međusobno najviše komuniciraju.** To bi značilo da po dvije stanice u različitim segmentima mogu da komuniciraju istovremeno. Ako stanica iz jednog segmenta šalje podatke stanici u drugom segmentu, tada ostalim stanicama nije dozvoljeno da komuniciraju.



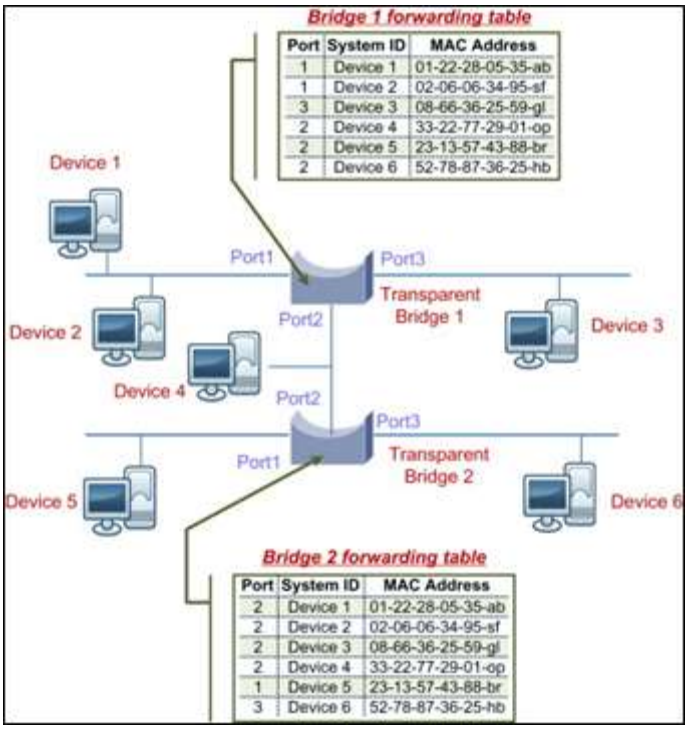

Segmentaciju mreže možemo izvršiti uređajem koji se zove mrežni most. Spolja je sličan ripiteru, a funkciono ima sve njegove osobine uz dodatak nekoliko novih koje su veoma značajne. Most provjerava sadržaj zaglavlja primljenog paketa da bi saznao MAC (fizičku) adresu izvora i odredišta. Na osnovu toga, on **formira tabelu MAC adresa** za svaki port.
Pojedini segmenti mreže se nazivaju kolizioni domeni.
Kada dobije broadcast paket (paket za sve računare u mreži), mrežni most ga samo prosljeđuje i ne pamti MAC adresu iz njegovog zaglavlja.
Postoji pravilo u segmentiranju mreže po kome 80% saobraćaja treba da se odvija u okviru kolizionih domena, a 20% da ide preko mosta. To znači da ukoliko neke dvije stanice često međusobno komuniciraju (npr. neka radna stanica i određeni server), ne treba stavljati most između njih. Mrežni most unosi određeno kašnjenje kao posljedicu obrade paketa, ali se ono uglavnom ne osjeća.

**Jednostavan most** - povezuje dva segmenta i sadrži tabelu sa spiskom svih stanica u svakom od njih- Tabela se popunjava "ručno" - pre nego što se jednostavan most pusti u rad, operator mora da unese u tabelu adrese svih stanica. Kada se nova stanica priključi na mrežu, tabela se mora modifikovati. Kada se stanica isključi sa mreže, njena adresa mora biti izbrisana iz tabele.




**Višeportni most** - povezuje više od dva LAN-a. Svaki LAN se povezuje na jedan port mosta. Za svaki port u mostu postoji jedna tabela koja sadrži spisak fizičkih adresa svih stanica iz odgovarajućeg LAN-a.

**Transparentni most** - posjeduje mogućnost učenja i sam se brine o svojim tabelama. Kada nije priključen na mrežu, njegove tabele su prazne.




U toku rada, most analizira odredišnu i izvorišnu adresu svakog okvira koji primi. Kao i standardni most, pretragom tabela po odredišnoj adresi okvira odlučuje na koji segment će poslati okvir.

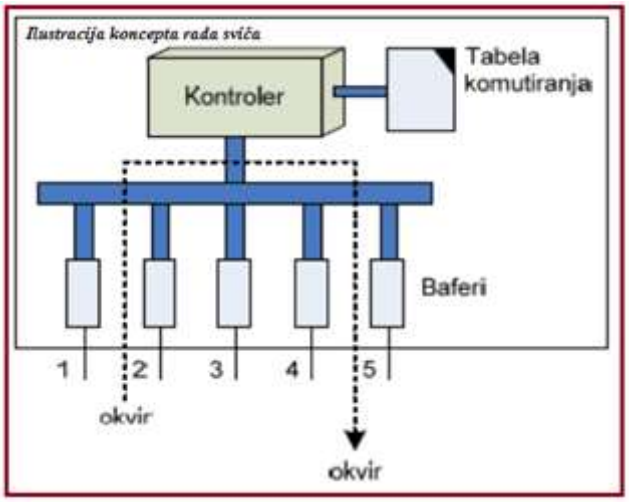
## Svič – skretnica-komutator- (Switch)

Svič je za mrežni most isto što je i hab za ripiter, tj. Ona je multiportni most.

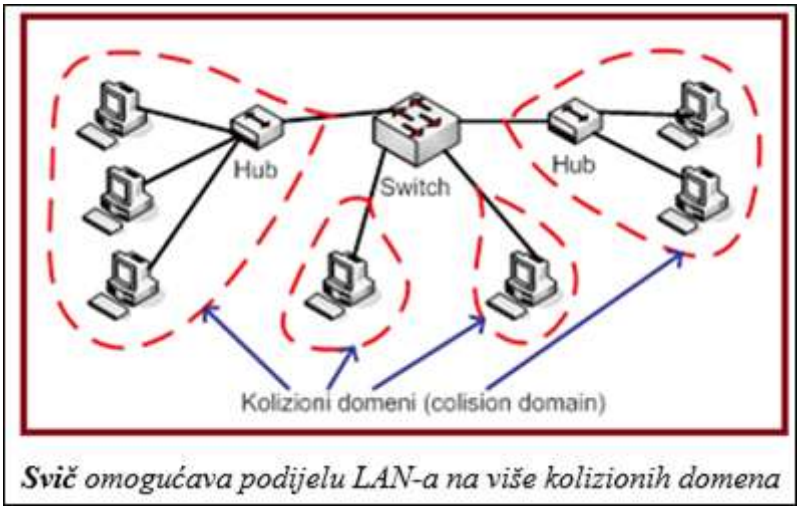
Skretnica se može koristiti kao zy povezivanje uređaja ili segmenata u jedinstveni LAN. Za razliku od klasičnog, višeportnog mosta, **komutator poseduje bafere za svaki link (mrežu) na koji je povezan.** Skretnica realizuje funkcije mosta na efikasniji način.

Skretnica na sebi ima veći broj portova. Svaki port, kao i kod mosta, ima izvestan stepen inteligencije, odnosno ne vrši samo retransmisiju paketa, već upisuje MAC adrese u odgovarajuću tabelu.

Veoma značajna mogućnost koju svič posjeduje je da se na svaki port sviča može priključiti stanica, a ne segment mreže.

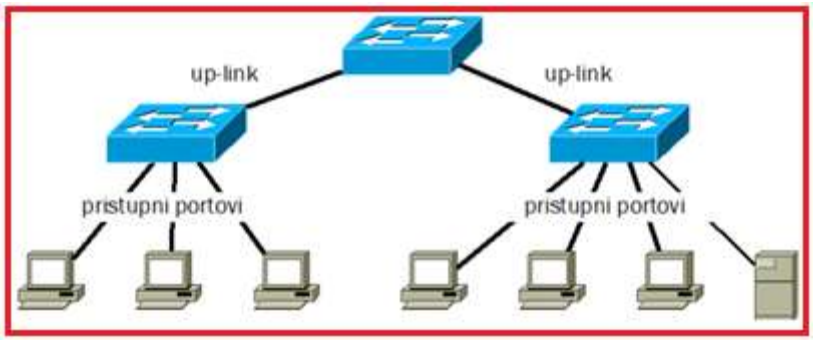



Kolizioni domen u ovom slučaju čini stanica sa odgovarajućim portom. U ovom slučaju, saobraćaj koji vidi stanica je samo onaj koji je direktno upućen za nju, kao i broadcast poruke.




*Svič omogućava podijelu LAN-a na više kolizionih domena*

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

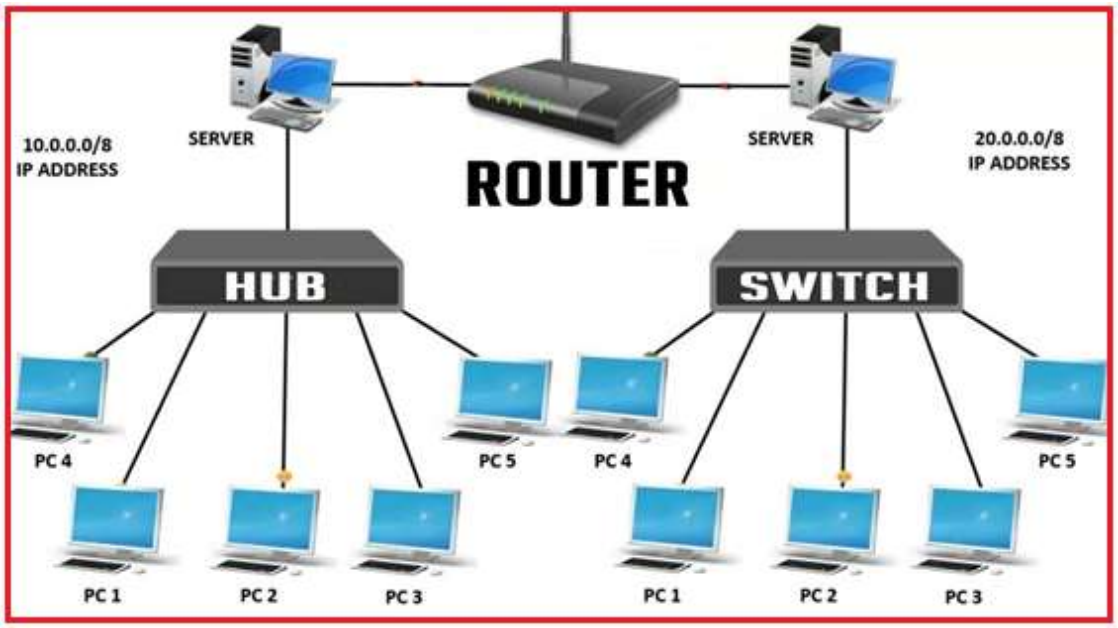



Postoje dvije vrste portova:

• Pristupni portovi (**access ports**): fizički interfejsi kojima se switch povezuje sa krajnjim sistemima na mreži.

• Mrežni up-link portovi (**network uplink ports**) koji služe za povezivanje na druge svičeve-komutatore.

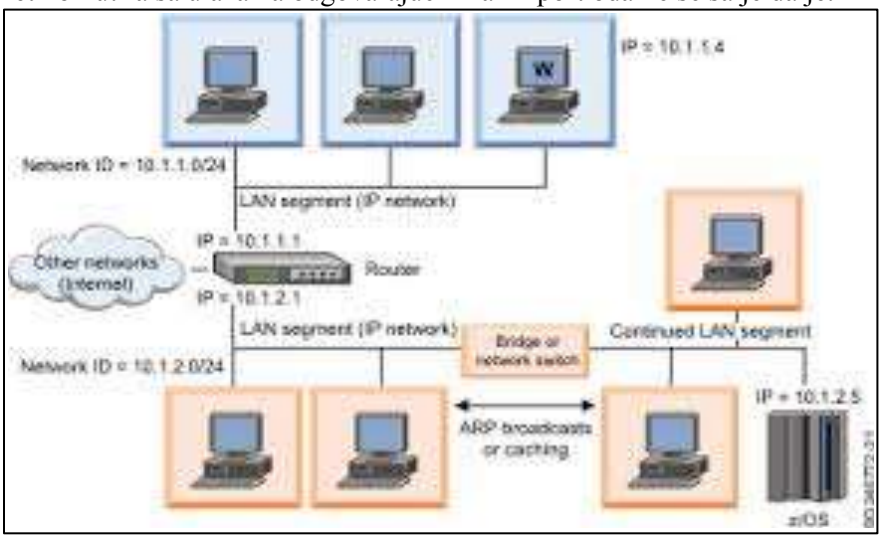
Mreža ne mora sadržati samo svičeve ili samo habove, već je treba balansirati u zavisnosti od potreba. Na primjer, veoma je čest slučaj u praksi da se na jedan port sviča poveže hab, a na taj hab, naravno, više stanica.



## Usmjerivač (Router)

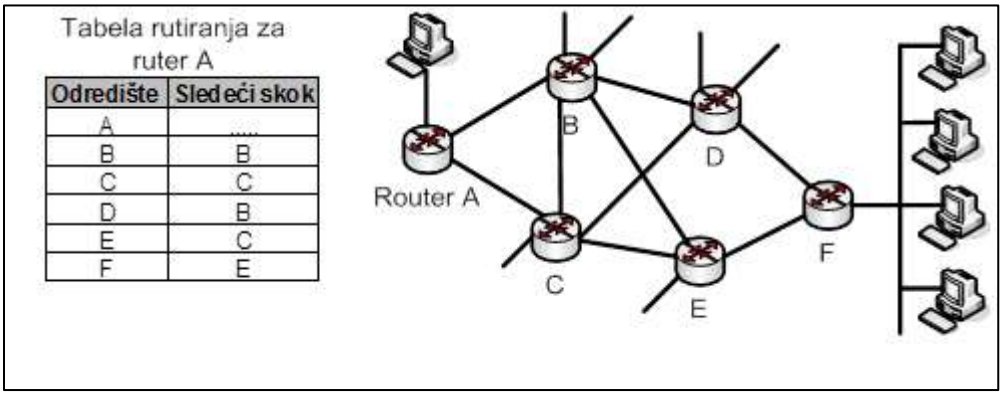
Za razliku od mrežnih uređaja koje smo do sada vidjeli i koji rade na prvom i drugom OSI nivou, ruteri rade na trećem nivou, odnosno mrežnom sloju. Sadrže softver koji određuje kojom od više mogućih putanja u mreži složene topologije je najbolje prenijeti primljeni paket.

**Glavna uloga** rutera u mreži je da rutiraju (usmjeravanje) pakete kako bi oni stigli do svog odredišta. Informacija koja se koristi za ovu funkciju je odredišna adresa smještena u paketu. Ruter obavlja ovu funkciju tako što po prispjeću paketa izvuče odredišnu adresu, zatim nađe odgovarajući zapis u tabeli rutiranja gdje su smješteni podaci na koji port treba paket da se proslijedi i odredi adresu sljedećeg rutera na putu ka kojem se paket usmjerava. Ovaj proces se naziva „*address lookup*“. Kada se dobije ova informacija vrši se proces komutacije (*switching*) gdje se paket komutira sa ulaza na odgovarajući izlazni port odakle se šalje dalje.




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

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

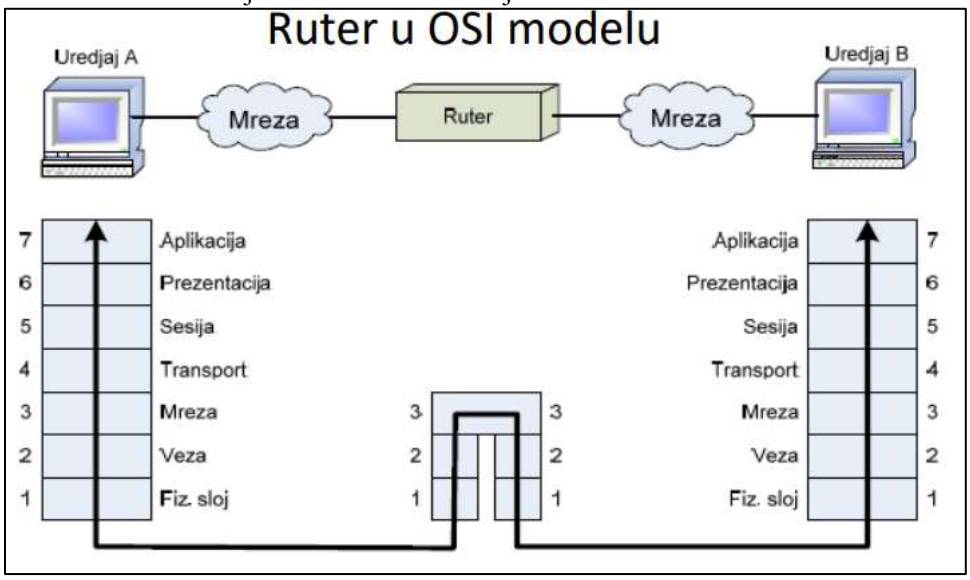



*Ruteri usmjeravaju pakete na osnovu tabele rutiranja*

Svaki protokol rutiranja koristi različiti algoritam za utvrđivanje kada su dostupne nove rute i koja je ruta najbolja na osnovu metrike.
Prosljeđivanje paketa do mreža sa kojima ruter nije u direktnoj vezi može da se vrši na dva načina:

1. **Statičke putanje** - Reč je o putanjama koje administrator ručno ustanovljava. Kada god topologija mreže iziskuje ažuriranje (na primjer, prilikom kvara na vezi), administrator mreže ovakvu putanju mora da ažurira.
2. **Dinamičke putanje** - Ove putanje ruter automatski saznaje nakon što administrator konfiguriše protokol rutiranja. Za razliku od statičkih putanja, čim mrežni administrator uključi dinamičko rutiranje, informacije o rutiranju se samim procesom rutiranja automatski ažuriraju svaki put kada se od nekog rutera u okviru mreže primi informacija o novoj topologiji.

Ruteri rade na fizičkom sloju veze i mrežnom sloju u OSI modelu.

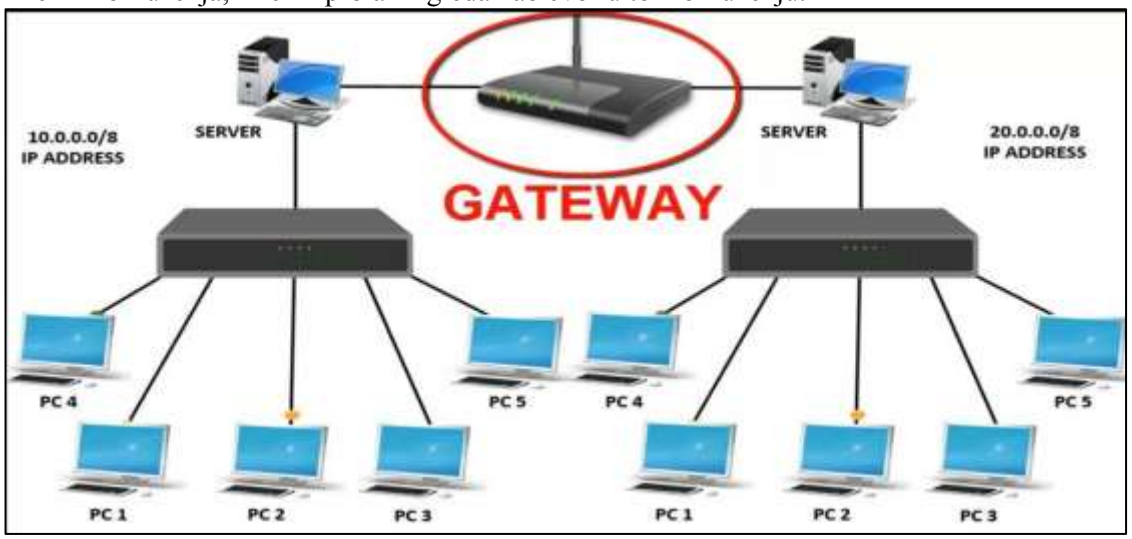



Ruteri pripadaju svim mrežama na koje su povezani i za svaku mrežu imaju posebnu mrežnu adresu.

*Bežični ruter namjenjen za mala preduzeća*

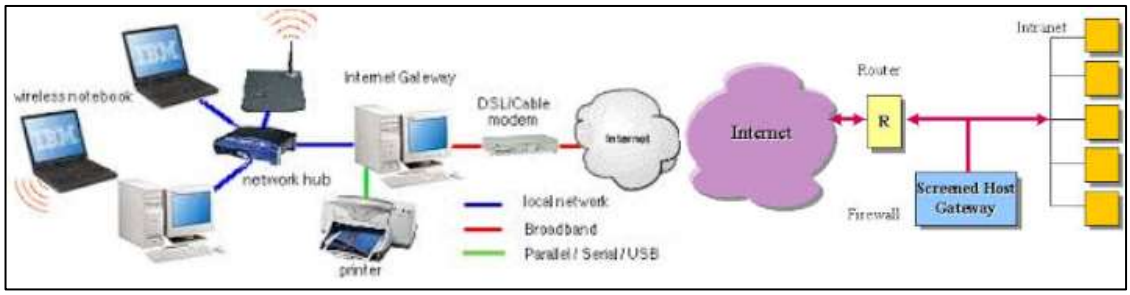
## Mrežni prolaz (gateway)

Mrežni prolaz je hardverski urežaj i/ili softverski paket koji povezuje dva **različita** mrežna okruženja. Omogućava komunikaciju između različitih arhitektura i okruženja. Vrši prepakivanje i pretvaranje podataka koji se razmjenjuju između potpuno drugačijih mreža, tako da svaka od njih može razumjeti podatke iz one druge. Mrežni prolaz je obično namjenski računar, koji mora biti sposoban da podrži oba okruženja koja povezuje. Svakom od povezanih mrežnih okruženja, mrežni prolaz izgleda kao čvor u tom okruženju.



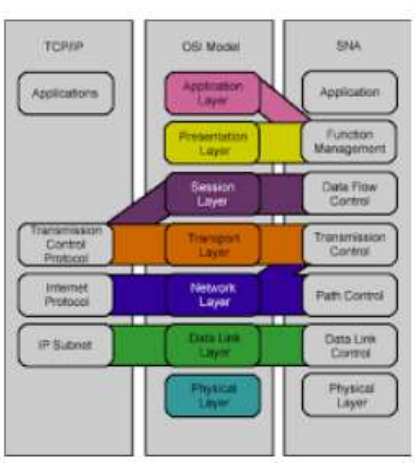

Zahtjeva značajne količina RAM memorije za čuvanje i obradu podataka. Radi u sloju sesije i aplikativnom sloju. Kako povezuje različite mreže, **mrežni prolaz mijenja format poruka** da bi ih prilagodio krajnjim aplikacijama kojima su namjenjene, vrši prevođenje podataka (iz ASCII u EBCDIC kod, na primjer) kompresiju ili ekspanziju, šifrovanje ili dešifrovanje, i drugo. Drugi naziv za gateway je i **prevodilac protokola**. Dakle, **osnovna namjena mrežnih prolaza je konverzija protokola**. Faktički - gateway je konvertor protokola.

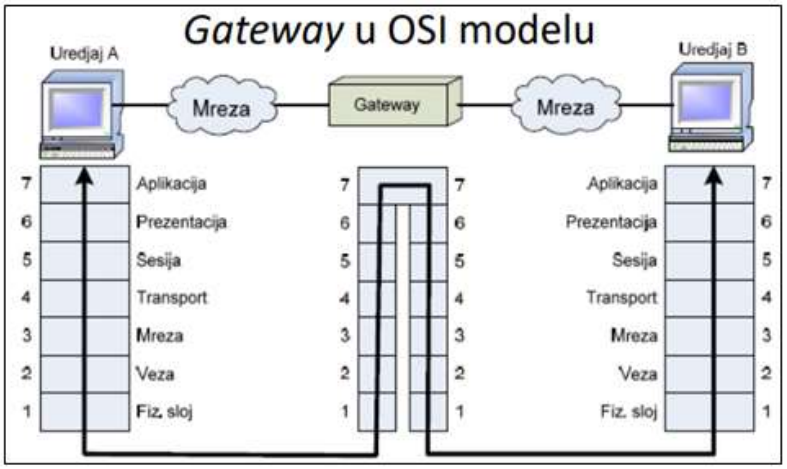
Transformacija se odnosi samo na zaglavlje i završni zapis paketa. Mora da se prilagodi brzinu prenosa, veličinu i format okvira i sl.




Radi između transportnog i aplikativnog sloja OSI modela. ALI to je Uređaj za međumrežno povezivanje koji je aktivan na svih sedam nivoa OSI modela. Omogućavaju komunikaciju između mreža, a da u isto vreme ne remete nezavisno funkcionisanje pojedinačnih mreža.

Danas u svijetu postoji veliki broj autonomnih mreža, svaka sa svojim različitim hardverom i softverom.



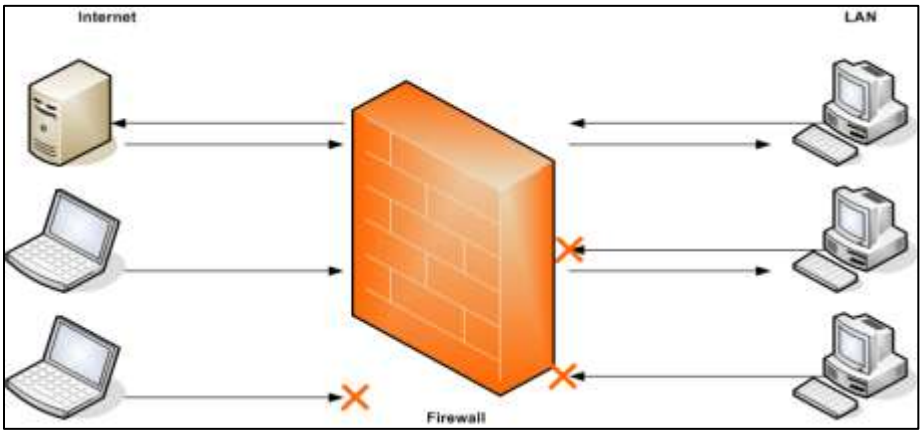




Autonomne mreže međusobno se mogu razlikovati po više karakteristika: algoritmima za rutiranje, implemen-tiranim protokolima, procedurama za administriranje i vođenje politike mreže i dr.

No nezavisno od nabrojanih razlika, korisnici jedne mreže imaju potrebu da komuniciraju sa korisnicima povezanim na drugu mrežu i u tome im pomaže gateway.

# Bezbjednosna barijera (firewall) zaštita lokalne od javne mreže

*Firewall* je bezbjednosni uređaj ili softver smješten između neke lokalne mreže i javne mreže (Interneta), čija je namjena da štiti podatke u mreži od neautoriziranih korisnika, (blokiranjem i zabranom pristupa po pravilima koje definiše usvojena bezbjednosna politika), što je u direktnoj vezi sa politikom sigurnosti datog informacionog sistema. Vrlo često ne moraju svi korisnici u LAN-u da imaju jednaka prava pristupa mreži. Postavljanjem *firewall* uređaja između dva ili više mrežnih segmenata mogu se kontrolisati i prava pristupa pojedinih korisnika pojedinim dijelovima mreže.




*Princip rada firewall-a*

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

Da bi *Firewall* obavljao funkciju, potrebno je da:

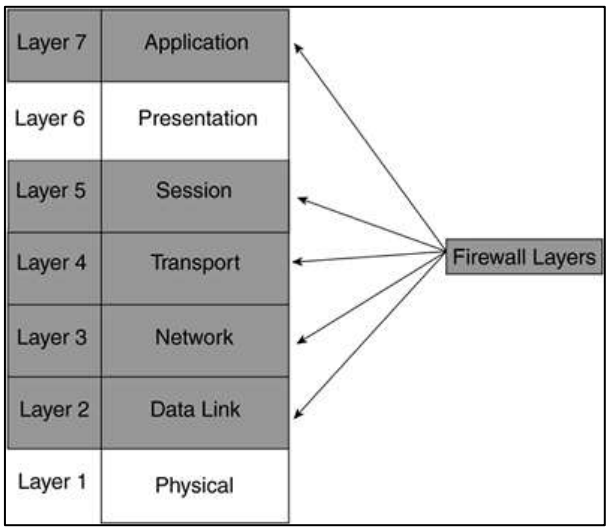
- Sav ulazni saobraćaj prolazi kroz firewall.
- Sav izlazni saobraćaj prolazi kroz firewall.
- Firewall implementira sigurnosnu politiku i odbija saobraćaj koji krši tu politiku.
- Sam firewall bude otporan na sigurnosne napade.

Samo posjedovanje firewall-a (hardverskog ili softverskog) ne znači da je računar/mreža koju on štiti bezbjedan. Naprotiv, firewall predstavlja samo alat koji je moguće iskoristiti za zaštitu ukoliko je dobro podešen (ukoliko su dobro definisana bezbjednosna pravila).

Najbolji način da se firewall podesi (ukoliko administrator nema iskustva u toj oblasti) je da se blokira sav saobraćaj a da zatim za svaku konekciju posebno donese odluka da li je treba dopustiti, trajno ili privremeno, i za koje klijente.

**Osnovni** zadatak koji firewall je *filtriranje paketa*. Administrator ga konfiguriše tako da on propušta samo pakete upućene na određene IP adrese i određene TCP portove. Na primjer, može se postići da vanjski subjekti mogu pristupati samo nekim (osiguranim) računarima unutar organizacije, te da pritom smiju komunicirati samo preko određenih portova (servisa).

**Drugi** zadatak koju obavlja firewall je pokretanje posebnih aplikacijskih programa koji se zovu *appication-layer gateways* ili *proxies*. Na primjer, može se postići da zaposlenici unutar organizacije mogu preuzimati datoteke s Interneta jedino posredstvom FTP proxy-ja na firewall-u. Taj proxy najprije kontroše da li je zaposlenikov zahtjev dozvoljen u smislu sigurnosne politike, zatim firewall preuzima (dowlaoud) datoteku s vanjskog Interneta i provjerava da u njoj nema virusa, na kraju on šalje datoteku zaposleniku.




Pošto se realizuje na različitim modelima (od softverskih koji koriste raznovrsne algoritme do hardverskih rješenja različitih tipova) **pozicija** bezbjedonosne barijere u OSI modelu **nije strogo propisana**.

Generalno Firewall radi na 3. nivou OSI modela. Na ovom nivou se odvija IP adresiranje. Firewall obavlja filtriranje saobraćaja na osnovu broja porta i IP adrese.

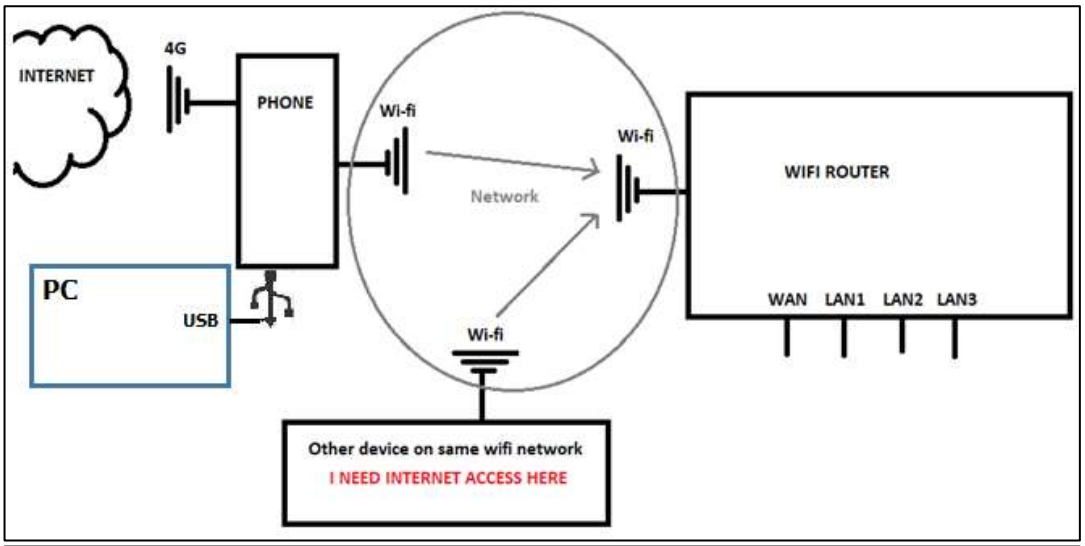
Ako filtrirate određene portove, možete reći da filtrirate na sloju 4. Ako vaš zaštitni zid pregleda određena stanja protokola ili podatke, možete reći da radi na sloju 7.

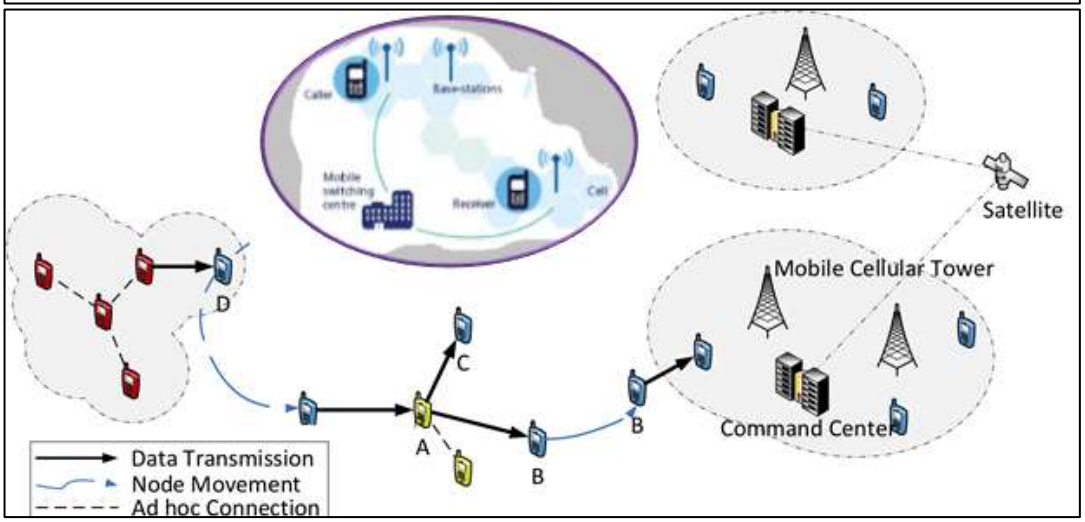
*Izgled Cisco ASA porodice sigurnosnih uređaja namjenjen zaštitii korporativnih mreža, prvi put predstavljen 2005. godine*

# Mobilni telefon i računarske mreže


Svi pametni telefon mogu se konektovati na Internet (inače ne bi bili pametni).
Većina ovih telefona može dijeliti podatke putem Wi-Fija, Bluetootha ili USB-a.

Pošto se u priručniku bavimo računarskim mrežama nećemo objašnjavati kako.
Ovdje je dovoljno reći da mobilni telefon predstavlja (i jeste) računar i kao takav ima sve osobine mrežnog čvora.
Uz odgovarajući softver (i znanje) može obavljati funkcije različitih mrežnih uređaja, ali se najčešće koristi za pristup Internetu i WiFi WLAN mrežama.



# Strukturno kabliranje

Iako se u osnovi pojam kabliranja prvenstveno odnosi na pasivnu opremu, dizajn pasivne opreme nije moguće kvalitetno realizirati bez sagledavanja zahtijeva po pitanju aktivne opreme. Oba navedena segmenta moraju se pažljivo uskladiti prema trenutnim i budućim zahtjevima korisnika.

Strukturno kabliranje je kablovska infrastruktura (uključujući tu obavezno i bežičnu infrastrukturu) u zgradama i naseljima namjenjena telekomunikacionim servisima, koja sadrži određeni broj standardizovanih manjih elemenata koje nazivamo podsistemima strukturnog kablovskog sistema.

Strukturno kabliranje možemo podeliti u šest podsistema:

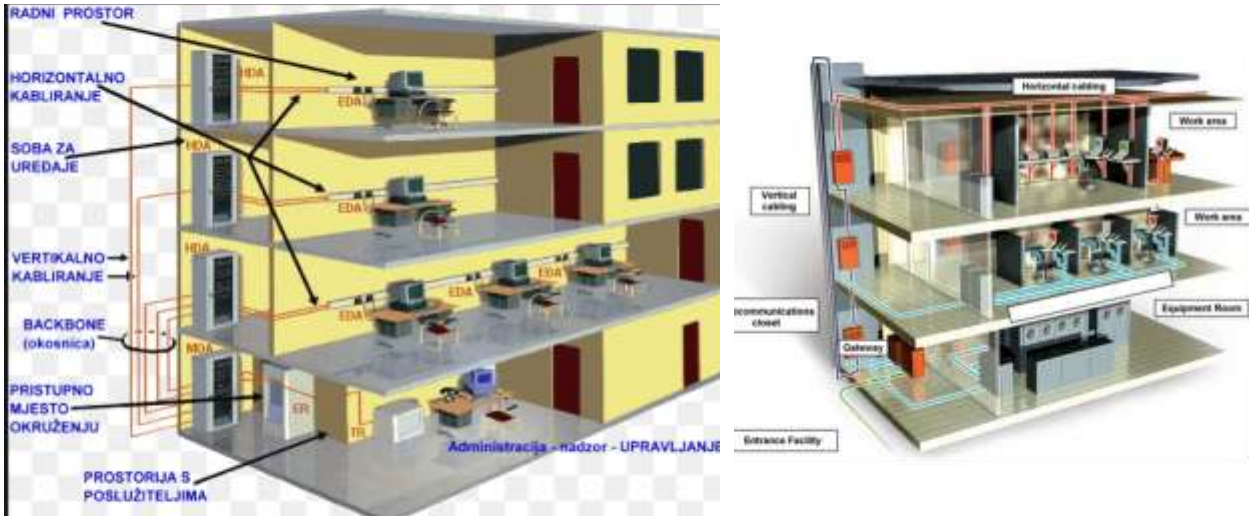
1. Ulazna postrojenja, gdje se strukturna mreža povezuje sa spoljnim svijetom;
2. Prostorije sa opremom, u kojima se nalazi korisnička oprema;
3. Telekomunikacione sobe, u kojima se nalazi oprema koja povezuje magistralne (Backbone) kablovske sisteme sa horizontalnim kablovskim sistemima;
4. Magistralno (Backbone) kabliranje povezuje ulazna postrojenja, prostorije sa opremom i telekomunikacione sobe;
5. Horizontalno kabliranje povezuje telekomunikacione sobe i pojedinačne priključnice na spratu;
6. Krajnje komponente, koje povezuju krajnjeg korisnika sa priključnicom horizontalnog kablovskog sistema.

Projektovanje i instalacija strukturnog kablovskog sistema je rukovođena setom standarda koji specificiraju kabliranje za glasovne i veze podataka u data centrima, radnim prostorima, stambenim objektima, korišćenjem kablova klasa D, E, F i modularnih priključnica. Američki standardi definišu kategorije kablova 5, 5e, 6, 7 (kategorija 7 još uvek nije zvanično ušla u standard).
Svi ovi standardi definišu kako povezivati kablove preko završnih priključnica u prespojnim panelima (koji su obično montirani u 19'' rek) odakle se može izabrati kako upotebiti ovu vezu. Svaka priključnica može biti povezana na port sviča (koji je najčešće u istom reku) ili na panel telefonije, koji predstavlja vezu sa kućnom telefonskom centralom.
Linije povezane na portove mrežnog sviča zahtjevaju prosto prespajanje za sve kablove od sviča do korisničkog računara. Govorne veze ka telefonskoj centrali u nekim zemljama zahtjevaju adapter sa 8P8C modularnih konektora na standardnu telefonsku priključnicu (tj. umjesto telefonskog R11 standardni R45).
Standardi kabliranja zahtjevaju da svih osam provodnika u kablu bude povezano na jednoj priključnici, odnosno zabranjuju paralelno vođenje podataka i glasa jednim kablom.

Za formiranje LAN mreže potrebno je obezbjediti niz tehničkih preduslova. Svaki projekat LAN mreže započinje detaljnim snimanjem lokacije sa ciljem da se prikupe potrebni podaci, kao što su postojeće stanje instalacija, građevinske osnove objekta, kao i detalji energetskog uzemljenja.

Dizajn pasivne opreme nije moguće kvalitetno realizirati bez sagledavanja zahtijeva po pitanju aktivne opreme. Oba navedena segmenta moraju se pažljivo uskladiti prema trenutnim i budućim zahtjevima korisnika

Dalji postupci se sastoje od preliminarnog određivanja horizontalnih i vertikalnih kablovskih trasa i razmještaja razvodnih ormana.




*Implementacija strukturnog LAN kabliranja na primjeru jedne zgrade*

Savremene računarske mreže se u najvećem broju slučaja realizuju po principu strukturiranog kabliranja, što znači da se radni prostor objekta **dijeli na radna mjesta do kojih se sprovodi par signalnih UTP kablova** za prenos podataka i govora. Signalni kablovi se sastoje od 4 bakarne upredene parice (*twisted pair*). **Radno mjesto se projektuje sa najmanje jednim dvostrukim signalnim priključkom na svakih 6 do 8 $m^2$ korisne radne površine**.

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

Vertikalne trase povezuju spratne razvodne ormane.

I horizontalne i vertikalne kablovske trase se izvode u formi zvijezde, da bi se obezbjedilo da u slučaju prekida pojedine trase ostatak sistema radi. Ovaj sistem se osim horizontalnih trasa odnosi i na vertikalne, tako da se i sve vertikalne trase završavaju u jednom centralnom razvodnom ormanu, a **kablovska struktura ima oblik složene zvijezde**, kojoj je početak u centralnom razvodnom ormanu, a kraj u priključnoj kutiji u okviru radnog mjesta.

# Protokoli

Prenos podataka kroz mrežu se obavlja po protokolima – utvrđenim pravilima koja su poznata svim učesnicima u komuniciranju. Ključni elementi protokola kojim se dogovara spremnost za slanje, spremnost za prijem, format podataka i sl. su:

- Sintaksa - format podataka i nivoi signala
- Semantika – kontrolne informacije u prenosu i kontrola grešaka
- Tajming – brzina prenosa

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

Svakom aktivnošću na mreži kojom se podrazumjeva komunikacija dva ili više entiteta upravlja protokol.
Na primjer: protokoli u ruterima određuju putanju paketa od njegovog izvora do odredišta, protokol za kontrolu zagušenja saobraćaja u krajnjim sistemima kontroliše brzinu prenosa paketa između pošiljaoca i primaoca itd. Ovladavanje oblašću umrežavanja računara praktično bi se moglo poistovetiti sa razumjevanjem svih mrežnih protokola.

***Protokol može označavati i softver*** *kojim se realizuje određeni skup pravila za komunikaciju. Razni oblici komunikacije između računara ili programa obično se ne mogu ostvariti jednim velikim protokolom. Umjesto toga,* ***prema modelima stvaraju se porodice protokola koji međusobno surađuju i organizovani u "slojeve" (nivoe -layers), kako je objašnjeno kod OSI modela.***

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

**Na predajnom računaru protokol**:

1. Dijeli podatke u manje cjeline, nazvane paketi, koje može da obrađuje.
2. Paketima dodaje adresne informacije tako da odredišni računar na mreži može da odluči da li oni pripadaju njemu.
3. Priprema podatke za prenos kroz mrežnu karticu i dalje kroz mrežni kabl.

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

1. Preuzimaju se paketi podataka
2. Kroz mrežnu karticu unose se paketi podataka u računar.
3. Iz paketa podataka uklanjaju se sve informacije o prenosu koje je dodao predajni računar.
4. Kopiraju se podaci iz paketa u prihvatnu memoriju (bafer) koja služi za ponovno sklapanje.
5. Ponovno sklopljeni podaci prosljeđuju se aplikaciji u obliku koji ona može da koristi.

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

## Nadležnost i posao protokola

Uspostavljanje veze, prenos podataka i raskid veze određeni su setom protokola od kojih je svaki nadležan za jedan od sljedećih poslova:

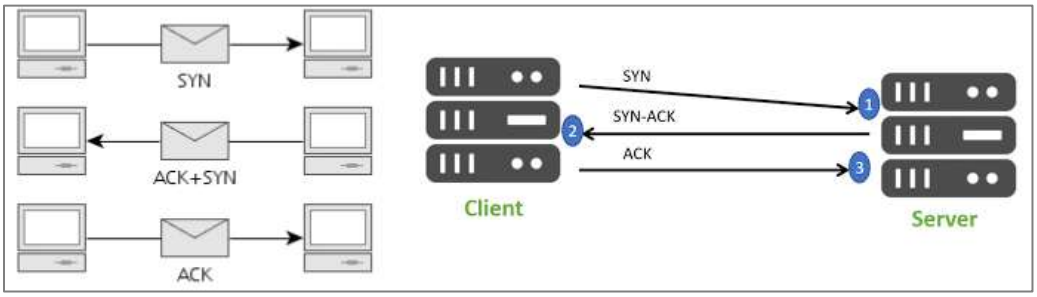
- *Handshaking* - uspostavljanje veze;
- Pregovaranje o različitim karakteristikama veze;
- Definisanje početka i kraja poruke;
- Definisanje formata poruke.
- Definisanje pravila za obradu oštećenih ili nepravilno formatiranih poruka (ispravka grešaka);
- Utvrđivanje neočekivanog prekida veze i definisanje daljih koraka u tom slučaju;
- Prekid veze.

## Protokoli bez uspostavljanja veze

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

## Protokoli sa uspostavljanjem veze

Pri korišćenju protokola sa uspostavljanjem veze dvije strane moraju da uspostave vezu između sebe kao preduslov za razmjen u podataka.




Proces uspostavljanja veze može se porediti sa pozivanjem telefonskog broja:

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

Jasno je da procedura potrebna za uspostavljanje veze zahtjeva određeno vreme i angažovanje obe strane. Međutim, ona obezbeđuje pouzdaniji (ali ne i potpuno pozdan) prenos podataka i umanjuje mogućnost greške. Uspostavljanje veze se praktikuje kod protokola koji imaju za cilj da osiguraju pouzdan prenos podataka.

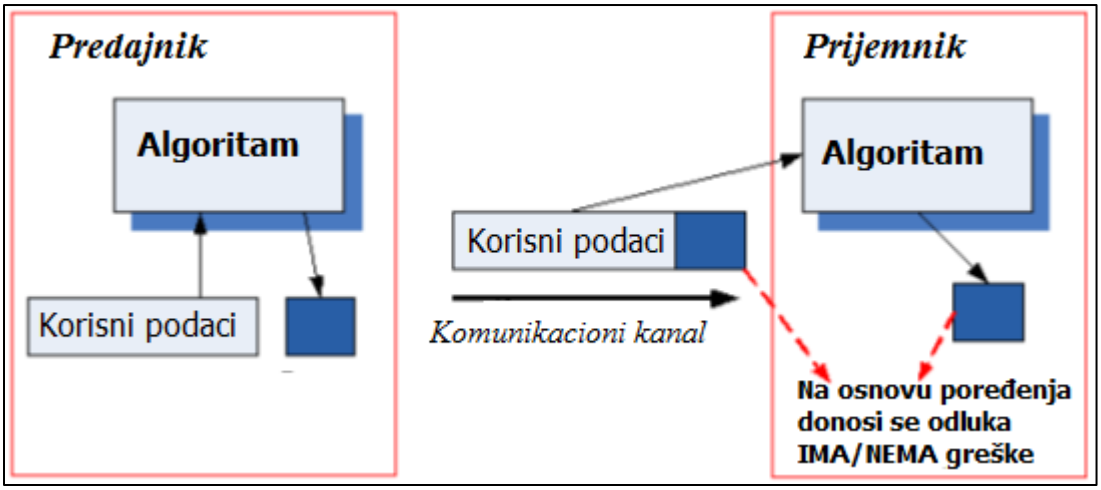
Primjer protokola koji radi sa uspostavljanjem veze je TCP (*Transmission Control Protocol*). Protokoli servisa kod kojih su performanse bitnije od pouzdanog prenosa podataka najčešće ne uključuju uspostavljanje veze.
Za uspostavljanje veze, TCP koristi trosmjerni protokol rukovanja. Prije nego što se klijent može povezati na ciljni server, server se prvo mora povezati na port za uspostavljanje veze; ovo se zove pasivno otvaranje. Kada se uspostavi pasivno otvaranje, klijent može pokrenuti aktivno otvaranje.

# Upravljanje greškama

Upravljanje greškama odnosi se na mehanizme koji otkrivaju i ispravljaju greške koje se javljaju tokom prenosa podataka. Postoji mogućnost pojavljivanja dva tipa grešaka i to: promenjen podatak i izgubljen podatak. Greške na komunikacionom kanalu su neminovne kod realnih komunikacija i nastaju zbog različitih vrsta šumova ili problema u prenosu. Nijedna mreža ne može da odstrani greške, ali većina grešaka može biti sprečena, otkrivena i eventualno ispravljena. Osnovne funkcije kontrole grešaka su sprečavanje i otkrivanje njihovog nastajanja, kao i njihovo ispravljanje.

Osnovni uzroci grešaka su šum na liniji i degradacija signala. Kod žičnih mreža šum je nepoželjan električni signal koji se javlja na komunikacionom kanalu. Može se očekivati na električnim medijima gde se pojavljuje kao neočekivan električni signal. Manifestuje se na dva načina i to: dodatni bitovi – umetanje ili nedostajući bitovi – brisanje.

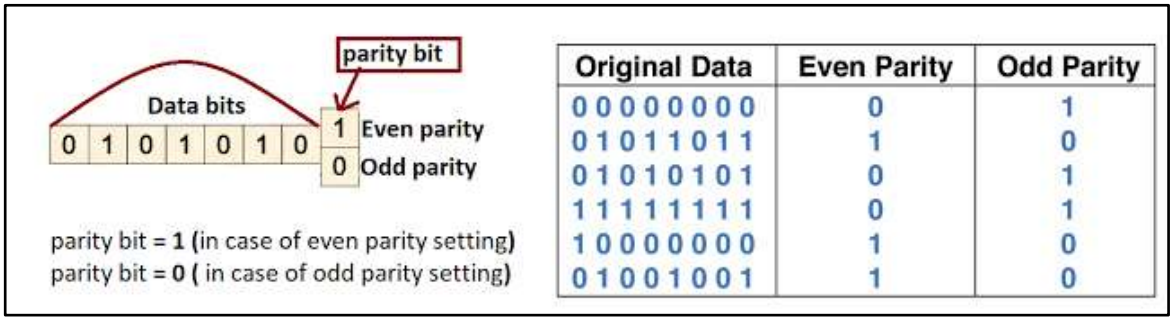
Jedan od ključnih zadataka u računarskim telekomunikacijama je provjera da li su primljeni podaci identični poslatima, odnosno da li je tokom prenosa došlo do njihove izmene.
Za potrebe otkrivanja grešaka pošiljalac izračunava dodatne bitove i šalje ih zajedno sa korisnim podacima. Što se veći broj bitova koristi kao dodatak korisnim podacima, bolje je otkrivanje greške ali je i manja efikasnost prenosa.
Primalac iz dobijenih korisnih podataka izračunava dodatak i poredi ga sa dobijenim. Ako je dodatak isti kao što ga je pošaljilac izračunao, nema greške u prenosu, a ako je različit, postoji greška u prenosu.




*Tehnika otkrivanja greške*

# Provjera parnosti

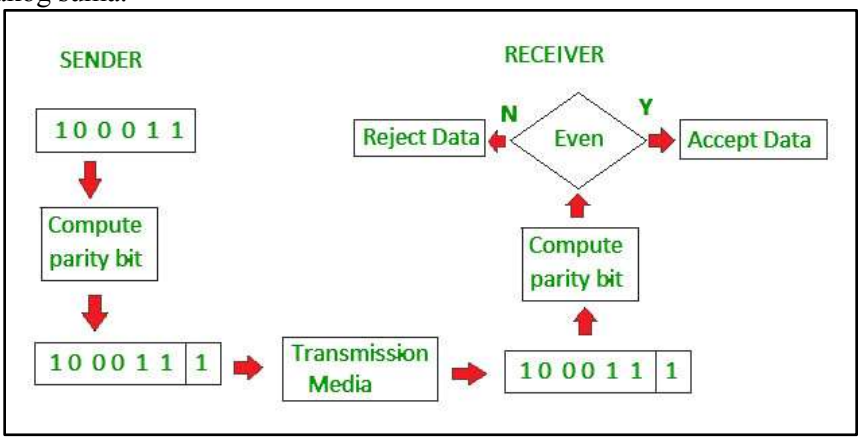
Provjera parnosti predstavlja najstariji i najjednostavniji metod detekcije greške gde se jedan bit dodaje svakom karakteru.
Ako u karakteru koji se prenosi postoji paran broj jedinica i bit koji je dodat ima vrednost 0 to se naziva parna parnost (***even parity***).
Ako u karakteru postoji paran broj jedinica i dodaje se 1 to se naziva neparna parnost (***odd parity***).
Prijemnik prima karakter, ponovo računa bit i poredi ga sa dobijenim bitom parnosti. Na ovaj način se može uočiti neparan broj pogrešnih bitova.




| Original Data | Even Parity | Odd Parity |
|---|---|---|
| 00000000 | 0 | 1 |
| 01011011 | 1 | 0 |
| 01010101 | 0 | 1 |
| 11111111 | 0 | 1 |
| 10000000 | 1 | 0 |
| 01001001 | 1 | 0 |

*Ilustracija metode provjere parnosti*

Ovaj jednostavni metod detektuje 50% grešaka. Primjena provjere parnosti nije jednostavna u prisustvu jakog šuma.



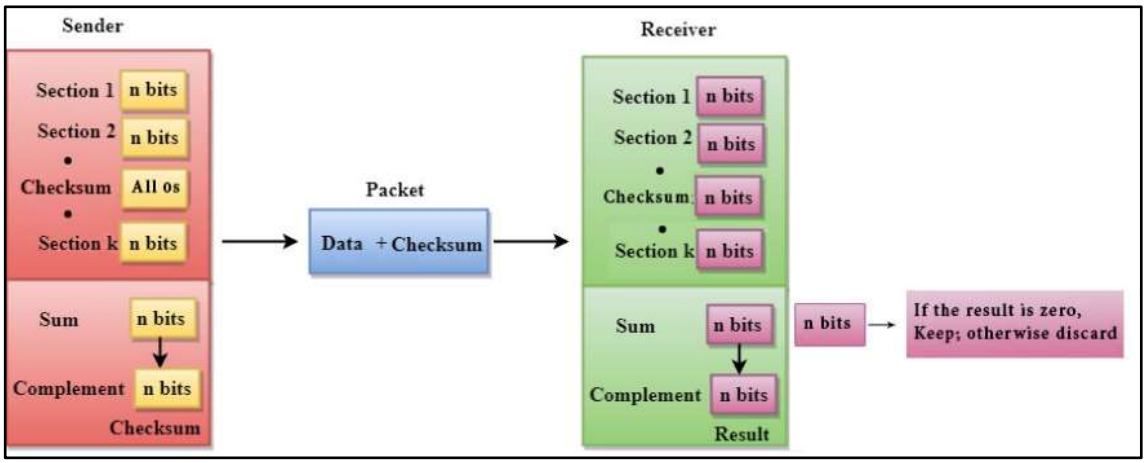

*Primjer metode provjere parnosti u komunikacionom sistemu*

# Metoda Kontrolna suma - Checksum -

Kontrolna suma je tehnika detekcije greške zasnovana na konceptu redundantnosti.
Podijeljen je na dva dijela:

**1. Generator kontrolne sume**

Kontrolna suma se generiše na strani koja šalje. Generator kontrolne sume dijeli podatke na jednake segmente od n bitova svaki, a svi ovi segmenti se sabiraju koristeći nečiju komplementarnu aritmetiku. Zbir se dopunjuje i dodaje originalnim podacima, poznatim kao polje kontrolne sume. Prošireni podaci se prenose preko mreže.




*Ilustracija metode kontrole sume*

Pošiljalac slijedi date korake:

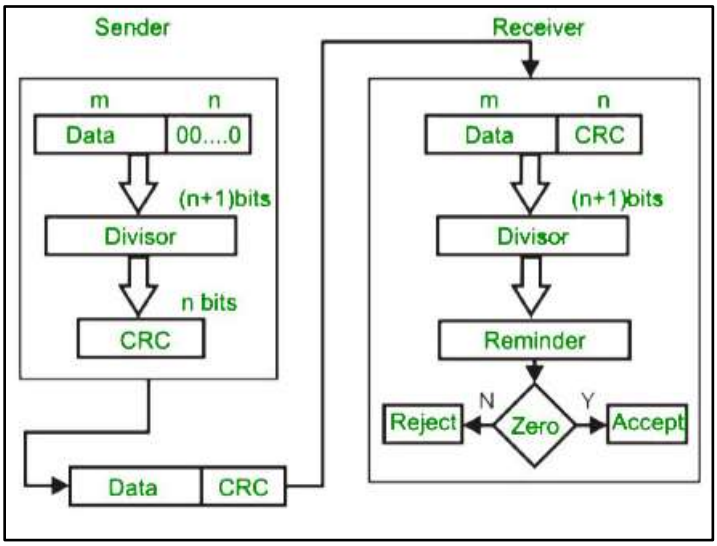
Blok jedinica je podijeljena na k sekcija, i svaki od n bitova.
Svi k sekcija se sabiraju korištenjem jednog komplementa da se dobije zbir.
Zbir se dopunjuje i postaje polje kontrolne sume.
Originalni podaci i polje kontrolne sume se šalju preko mreže.

**2. Provjera kontrolne sume -Checksum Checker-**

Kontrolna suma se provjerava na strani koja prima. Prijemnik dijeli dolazne podatke na jednake segmente od n bitova svaki, i svi ovi segmenti se sabiraju, a zatim se ovaj zbir dopunjuje. Ako je komplement sume nula, tada se podaci prihvataju u suprotnom podaci se odbijaju.

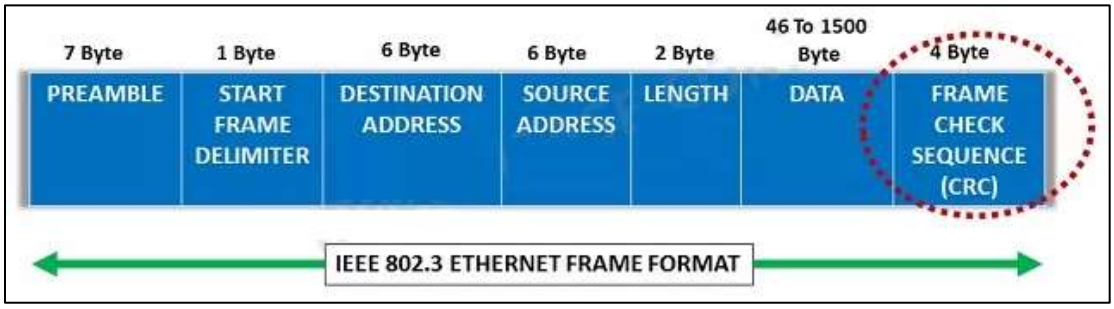
# Ciklična provjera redundancije -CRC-

Ciklička provjera redundanse (Cyclic redundancy check) je kod za otkrivanje grešaka koji se obično koristi u mrežama.




*Ilustracija principa CRC metode otkrivanja greške*

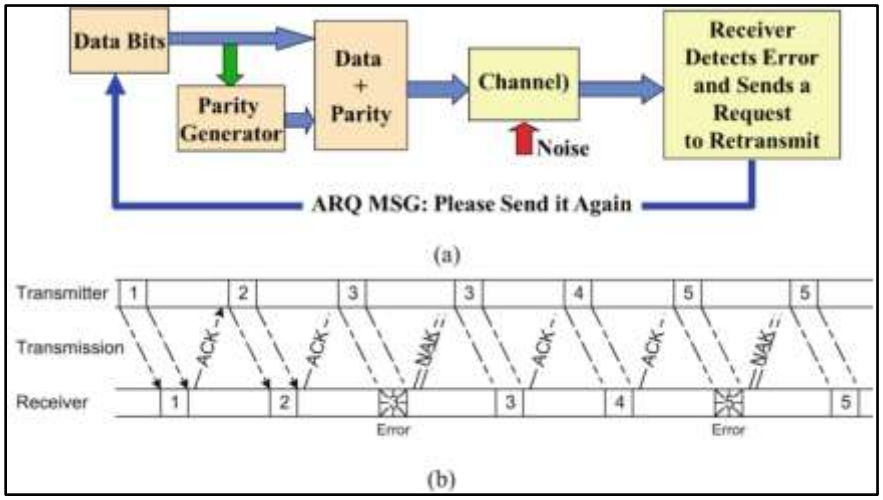
Blokovi podataka koji ulaze u ove sisteme dobijaju kratku vrednost provere, zasnovanu na ostatku polinomske podele njihovog sadržaja. Prilikom pronalaženja, proračun se ponavlja i, u slučaju da se vrijednosti provjere ne poklapaju, može se poduzeti korektivna akcija protiv oštećenja podataka. CRC-ovi se mogu koristiti za ispravljanje grešaka.



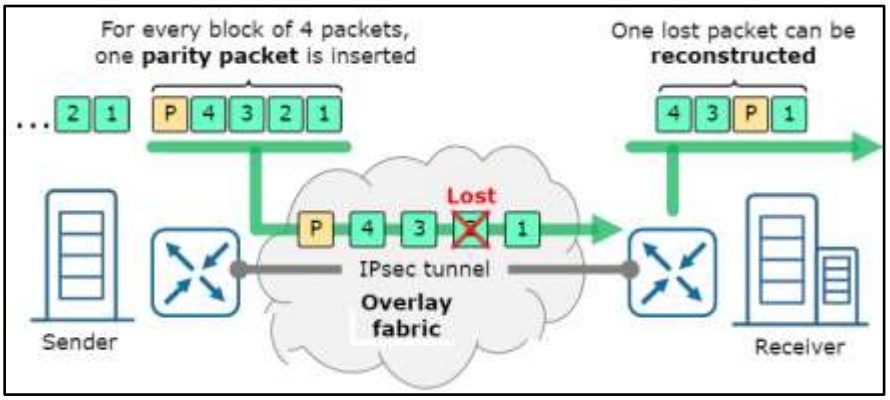

*Standardni Eternet paket koji koristi CRC metod*

## Ispravljanje grešaka

Kada se u primljenim okvirima detektuje greška ona mora da se ispravi ili se takav okvir odbacuje. Jednostavan, efikasan, jeftin i najčešće korišćeni metod za korekciju greške je **retransmisija**. Kod ovog postupka prijemnik, kada detektuje grešku, traži od predajnika da ponovo pošalje poruku sve dok se poruka ne primi bez greške. Čest naziv je automatski zahtjev za ponavljanje (*Automatic Repeat Request, ARQ*). Postoje dva tipa *ARQ* a to su: stani i čekaj i kontinualni *ARQ*.




Korekcija greške unaprijed (*Forward Error Correction*) FEC, je vrsta ispravljanja greške koja uključuje kodiranje poruke na redundantni način, što omogućava prijemniku da rekonstruiše izgubljene bitove bez potrebe za ponovnim prenosom.

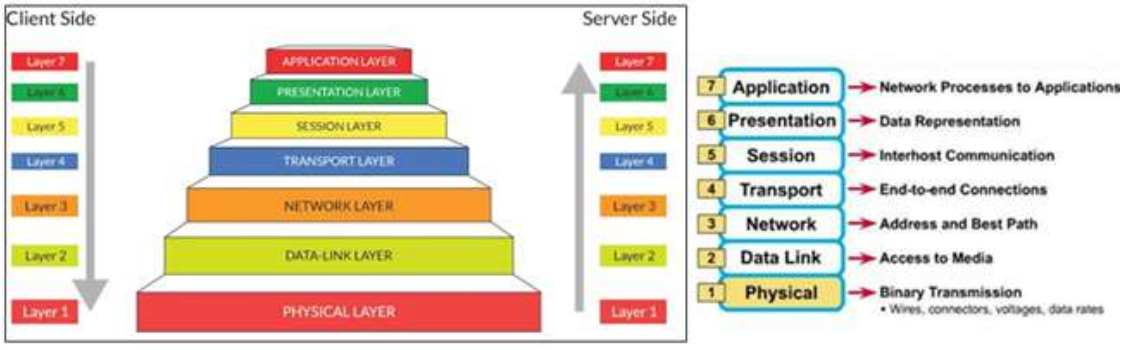



FEC radi dodavanjem "kontrolnih bitova" ("*check bits*") u odlazni tok podataka. Dodavanje više bitova za provjeru smanjuje količinu dostupnog propusnog opsega povećanjem ukupne veličine bloka odlaznih podataka, ali takođe omogućava prijemniku da ispravi više grešaka bez primanja dodatnih prenesenih podataka.
Ova dinamika čini FEC idealnim kada je propusni opseg velik, ali je ponovni prenos skup ili nemoguć.
Dodatni "kontrolni bitovi" ili redundantni bitovi koje pošiljatelj dodaje u tok podataka kodirani su u podatke na vrlo specifičan način (npr. Hamingov kod), što omogućava efikasnu korekciju greške od strane prijemnog uređaja.

# OSI model

Do sad smo mnogo puta pominjali OSI model, pa ćemo (napokon) da ga nešto detaljnije objasnimo. **OSI (referentni model za otvoreno povezivanje - Open Systems Interconection) model** opisuje komunikaciju sklopovlja, programa, software-a i protokola pri mrežnim komunikacijama. **OSI-model je** najkorišteniji **apstraktni opis arhitekture mreže**. To je hijerarhijska struktura sedam slojeva koji definiše zahtjeve za komunikacijama između dva računara.
OSI model opisuje način na koji treba upravljati podacima za vrijeme različitih faza njihovog prenosa. Opisuje komunikaciju uređaja, programa, software-a i protokola pri mrežnim komunikacijama. Koriste ga proizvođači pri projektiranju mreža, kao i stručnjaci pri proučavanju mreža. On je apstraktan model, što znači da stvarna implementacija mreže ne mora striktno da ga slijedi. Referentni model je ustvari samo smjernica. *OSI model nikada nije implementiran do kraja. Njegova mana je da on ne sadrži sloj za Internet, mada ga indirektno podržava.*

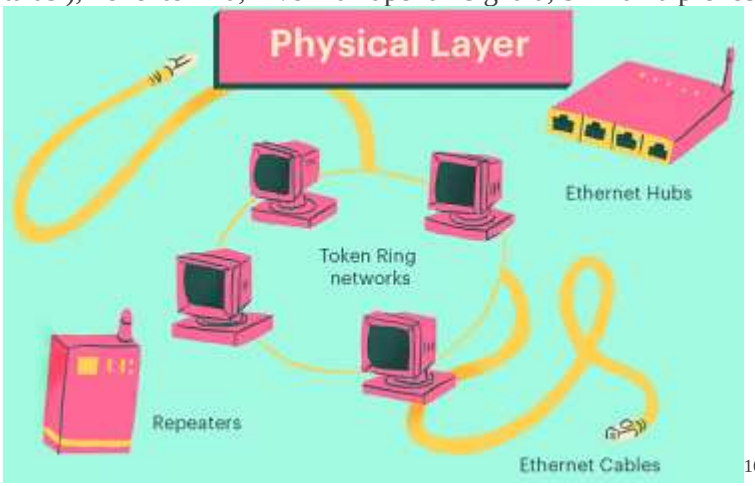
OSI model je apstraktni **opis dizajna protokola računarskih mreža**, predstavljen u obliku sedam slojeva (nivo-layer). Razvijen je 1984. godine od strane Međunarodne organizacije za standarde (International Organization for Standardization, ISO), koja je predstavljala oko 130 država.
Sve današnje mreže su bazirane na OSI standardu.
Slojevi su podijeljeniu dvije glavne skupine: Aplikacijski skup (viši) i Prenosni skup (niži). Prvi se više bavi softverskim prenosom podataka, dok se drugi bavi hardverskim prenosom podataka. OSI definiše sedam nivoa jedinstvene komunikacione infrastrukture koja se može primjeniti za svaki krajnji računar ili čvor u mreži. Svaki nivo ima jasno definisane funkcije koje omogućavaju dio komunikacije sa drugim sistemom. Te funkcije koriste funkcije nižeg nivoa da bi obavile jednostavnije funkcije, a obezbjeđuju odgovarajuće usluge višim nivoima. Svih sedam slojeva zajedno, prikazuju tok podataka od izvora prema odredištu.




*OSI model*

Zašto slojevi?
Slojevi omogućuju razgraničavanje pojedinih funkcija u umrežavanju na način da jedan sloj nema nikakvog utjecaja na susjedne slojeve slojeve. Na taj način omogućen je njihov pojedinačni razvoj te promjena sklopova u ure razvoj te promjena sklopova u uređaju (računaru) bez utjecaja na njegovu funkcionalnost. Mreže različitih proizvođača će međusobno besprijekorno komunicirati, jer moraju da zadovolje protokole definisane u slojevima.

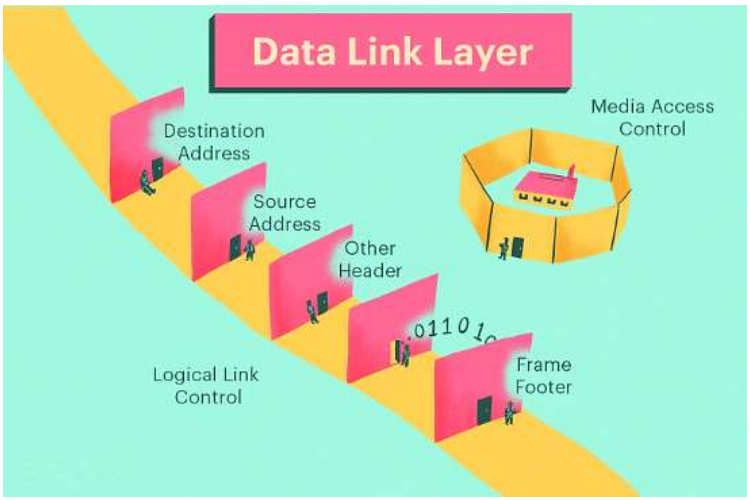
**1. Fizički sloj** (*Physical*) je zadužen za definisanje električnih, mehaničkih i drugih specifikacija vezanih za vezu između dva mrežna uređaja. Odgovoran je za aktiviranje, održavanje i deaktiviranje veze između krajnjih tačaka linka i u slučaju prekida linka da o tome obavjesti drugi nivo. Brine se o fizičkim komponentama mreže: medijima za prenos (bakar, optika, radio talasi), konektorima, nivoima napona i signala, brzinama prenosa podataka, itd.



[16]

Praktično on je zadužen **za prenos bitova (nula i jedinica)** putem komunikacionog kanala. U kontekstu podataka, sloj 1 prenosi podatke u obliku jedinica i nula. Tehnički, ovaj sloj preuzima bitove sa kraja pošiljaoca, kodira ih u signal, šalje signal preko mreže i dekodira signal na kraju prijemnika. Stoga, bez sloja 1, komunikacija bitova podataka preko mrežnih uređaja putem fizičkih medija nije moguća.

2. **Sloj veze** (*Data link*) definiše adresiranje fizičkog sloja, topologiju, otkriva greške u prenosu preko 1. sloja. Brine se o pristupu mediju za prenos podataka. Sloj veze podataka upravlja prenosom putem fizičkog sloja i **omogućava prenos oslobođen grešaka na ovom i fizičkom sloju**. Takođe, s obzirom na to da je jedinica prenosa fizičkog sloja bit, sloj veze upravlja i formatom poruka (definiše početak i kraj poruke).

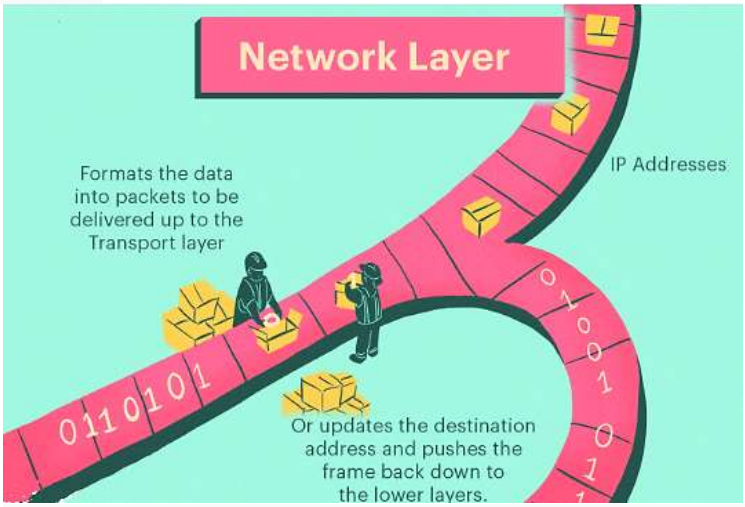



[16] Ilustracije preuzete sa https://www.lifewire.com/layers-of-the-osi-model-illustrated-818017

Takođe, s obzirom na to da je jedinica prenosa fizičkog sloja bit, sloj veze upravlja i formatom poruka (definiše početak i kraj poruke).

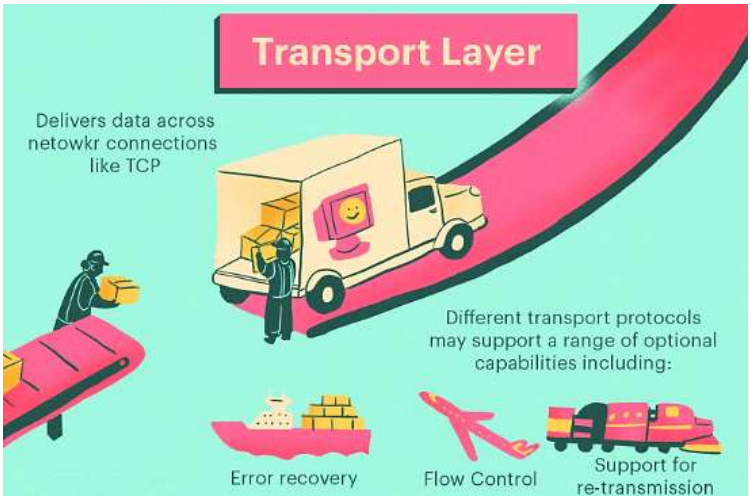
**Sloj 2** je podijeljen na **dva pod-sloja**: kontrolu pristupa medijima (MAC) i kontrolu logičke veze (LLC). *MAC sloj inkapsulira okvire podataka koji se prenose preko medija za povezivanje mreže kao što su žice ili kablovi. U situacijama kada takav prenos podataka ne uspije, LLC pomaže u upravljanju ponovnim prenosom paketa.*

3. **Sloj mreže** *(Network)* obavlja podjelu podataka na pakete i vrši pridruživanje adresa tim paketima.




Određuje rutu-putanju do idućeg mrežnog čvora kojim će tako podjeljeni paketi putovati prema krajnjem-odredišnom čvoru.

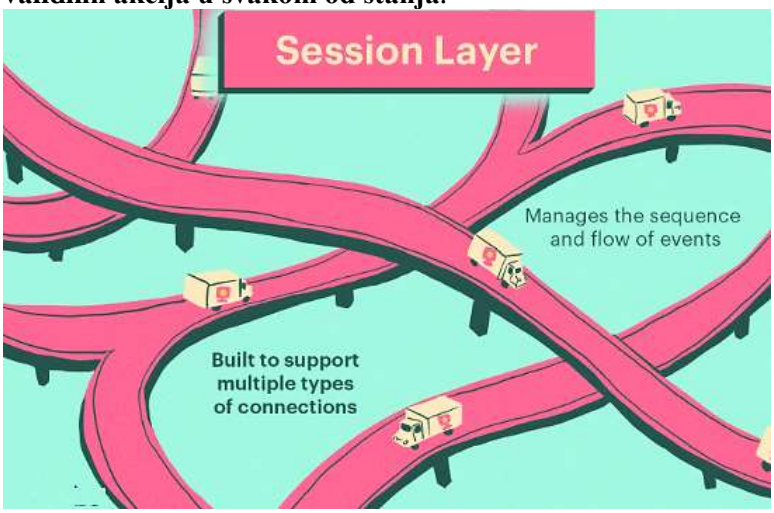
**4. Transpotrni sloj** (*Transport*) obezbjeđuje transparentni transfer podataka od izvora do odredišta Zadatak transportnog sloja jeste **obrada poruka na krajnjim tačkama - izvorištu i odredištu**.




Ovaj sloj uspostavlja, održava i prekida virtuelne veze za prenos podataka između izvorišta i odredišta. Transporni sloj je zadužen za nabavku mrežne adrese odredišta, podjelu podataka u segmente pogodne za slanje, prilagođavanje brzine prenosa mogućnostima strane sa slabijim

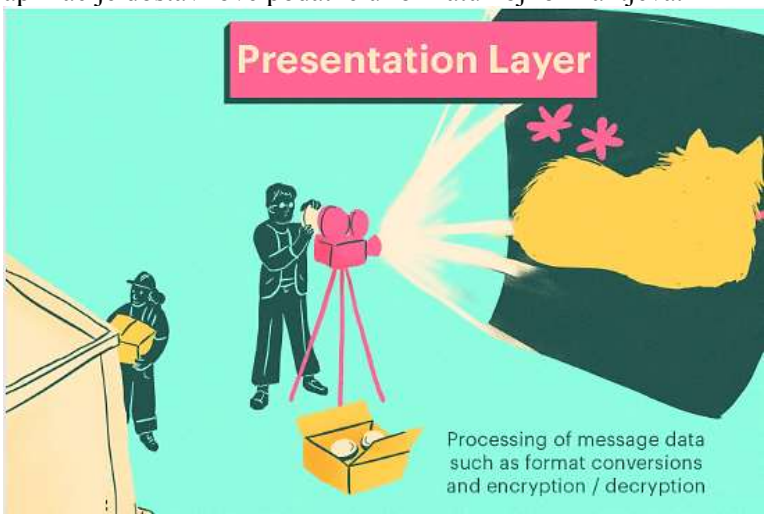
performansama, osiguravanje prenosa svih segmenata, eliminisanje dupliranih segmenata i sl. Takođe, ovaj sloj može izvršiti i dodatnu kontrolu grešaka pri prenosu (dodatnu u smislu da je ona već izvršena na sloju veze).

5. **Sloj sesije** služi za organizovanje i sinhronizaciju razmjene podataka između aplikacija. Sloj sesije je zadužen za uspostavljanje, održavanje i prekid logičkih sesija između krajnjih tačaka. Svrha sesija jeste **definisanje stanja (ili faza) svakog dijaloga radi definisanja validnih akcija u svakom od stanja**.



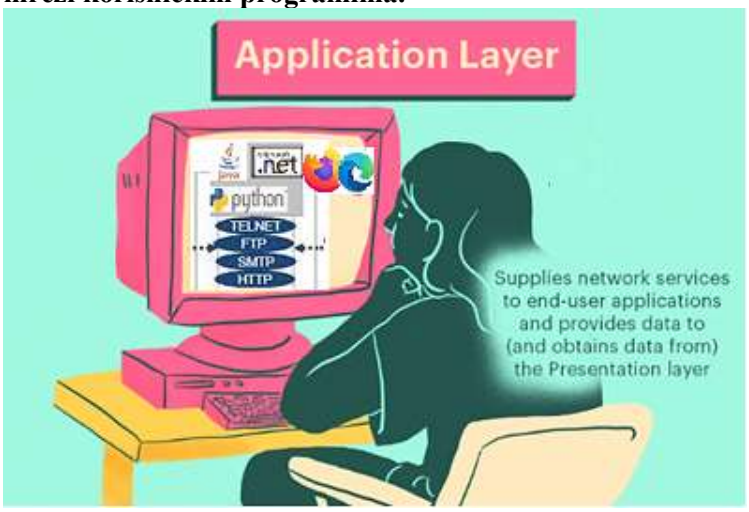

Na osnovu toga se vrši upravljanje transportnim slojem i provjera podataka dobijenih od njega. Dodatna uloga sesija jeste i obračunavanje sesija (engl. *session accounting*).

6. **Sloj prezentacije** (*Prezentation*) prevodi podatke iz aplikativnog oblika u zajednilki oblik uobičajen transport podataka preko mreže i obrnuto kada ti podaci pristižu u obrnutom pravcu. Zadatak ovog sloja jeste **da uskladi format** podataka između učesnika u komunikaciji i sloju aplikacije dostavi ove podatke u formatu koji on zahtjeva.




Na primjer, sloj prezentacije može originalne podatke dobijene od sloja aplikacije kompresovati radi efikasnijeg prenosa. Ovakve podatke sloje prezentacije na strani drugog učesnika ne može direktno proslediti sloju aplikacije već je pre toga neophodno izvršiti dekompresiju.

7. **Sloj aplikacije** (*Application*) predstavlja interfejs prema krajnjem korisniku. Na ovom sloju se započinju i završavaju zahtjevi. Osnovna uloga ovog sloja je **da omogući pristup mreži korisničkim programima.**




| Layer | Application/Example | | Central Device/ Protocols | | | DOD4 Model |
|---|---|---|---|---|---|---|
| **Application** (7)<br>Serves as the window for users and application processes to access the network services. | **End User layer** Program that opens what was sent or creates what is to be sent<br>Resource sharing • Remote file access • Remote printer access • Directory services • Network management | | **User Applications**<br>SMTP | | GATEWAY | Process |
| **Presentation** (6)<br>Formats the data to be presented to the Application layer. It can be viewed as the "Translator" for the network. | **Syntax layer** encrypt & decrypt (if needed)<br>Character code translation • Data conversion • Data compression • Data encryption • **Character Set Translation** | | JPEG/ASCII<br>EBDIC/TIFF/GIF<br>PICT | | | |
| **Session** (5)<br>Allows session establishment between processes running on different stations. | **Synch & send to ports** (logical ports)<br>Session establishment, maintenance and termination • Session support - perform security, name recognition, logging, etc. | | **Logical Ports**<br>RPC/SQL/NFS<br>NetBIOS names | | | |
| **Transport** (4)<br>Ensures that messages are delivered error-free, in sequence, and with no losses or duplications. | **TCP** Host to Host, Flow Control<br>Message segmentation • Message acknowledgement • Message traffic control • Session multiplexing | PACKET FILTERING | TCP/SPX/UDP | | | Host to Host |
| **Network** (3)<br>Controls the operations of the subnet, deciding which physical path the data takes. | **Packets** ("letter", contains IP address)<br>Routing • Subnet traffic control • Frame fragmentation • Logical-physical address mapping • Subnet usage accounting | | **Routers**<br>IP/IPX/ICMP | | Can be used on all layers | Internet |
| **Data Link** (2)<br>Provides error-free transfer of data frames from one node to another over the Physical layer. | **Frames** ("envelopes", contains MAC address)<br>[NIC card — Switch — NIC card] (end to end)<br>Establishes & terminates the logical link between nodes • Frame traffic control • Frame sequencing • Frame acknowledgment • Frame delimiting • Frame error checking • Media access control | | **Switch**<br>**Bridge**<br>**WAP**<br>PPP/SLIP | Land Based Layers | | Network |
| **Physical** (1)<br>Concerned with the transmission and reception of the unstructured raw bit stream over the physical medium. | **Physical structure** Cables, hubs, etc.<br>Data Encoding • Physical medium attachment • Transmission technique - Baseband or Broadband • Physical medium transmission Bits & Volts | | **Hub** | | | |

*Pregled protokola i uređaja po slojevima OSI modela*

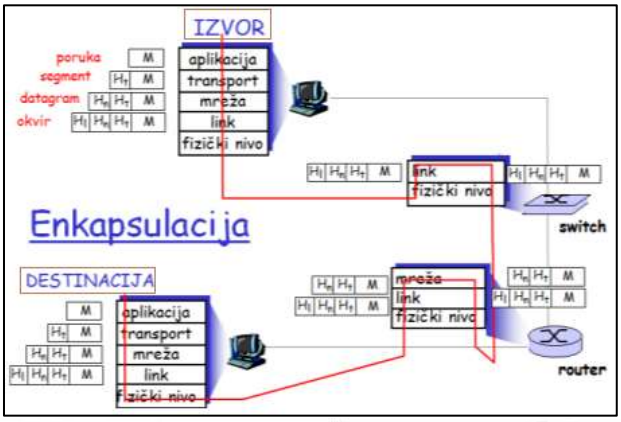
# Enkapsulacija

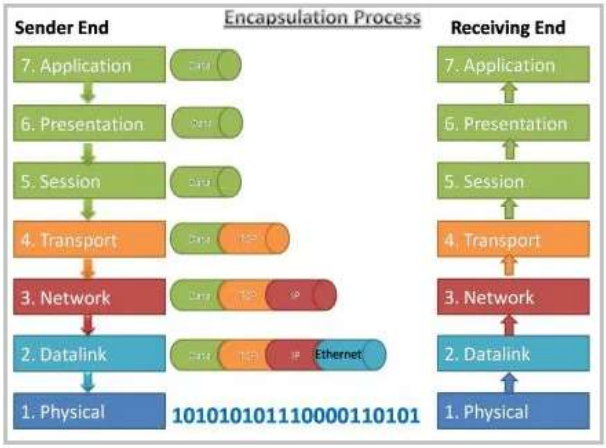
Ranije je objašnjeno da se slanje podataka obavlja korištenjem paketa i okvira-frejmova. Paketi se usmjeravaju po mreži koristeći odredišnu adresu koja je sadržana u paketu. Put kojim paket dolazi od izvora do odredišta nije bitan. Bitno je da svi paketi stignu na odredište. Djeljenje podataka za slanje 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.

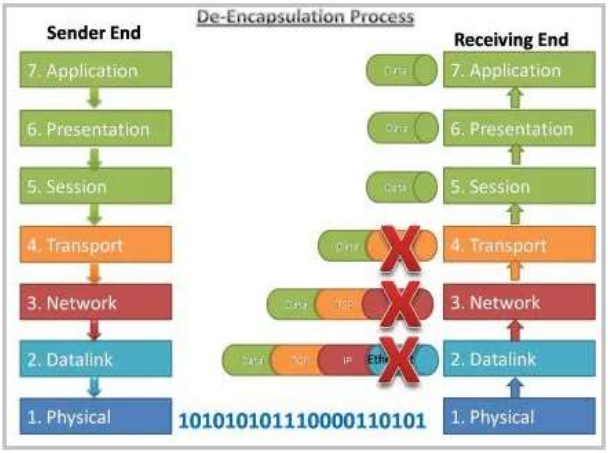
Svaki od slojeva unutar OSI modela ima neki oblik pakovanja podataka. Protokol Data Unit (PDU) je naziv za pojedini oblik pakovanja podataka za odgovarajući sloj:

- Na gornja 3 sloja OSI modela (Application, Presentation, Session) podaci nisu zapakovani.
- Na 4. sloju (Transport) podaci se dijele u segmente. Segment je PDU za 4. sloj.
- Na 3. sloju (Network) segmenti se pakuju u pakete. Paket je PDU za 3. sloj.
- Na 2. sloji (Data Link) paketi se pakuju u okvire. Okvir je PDU za 2. sloj.
- Na 1. sloju (Physical) okviri se rastavljaju u bitove koji se prenose mrežom.

Postupak pakovanja podataka, od 7. sloja prema 1. sloju, u oblik pogodan za prenos 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).



# TCP/IP mrežni model


**Umjesto OSI modela u praksi se koristi TCP/IP model koji je preuzeo mnoge osobine OSI.** Nasuprot *OSI* modelu koji je formalno standardizovan, Internet model (*TCP/IP*) je *de facto* standardni model za razvoj i projektovanje internet mreža. **TCP/IP model** je komunikacijski model koji je omogućio globalni Internet.

*Niti jedan dokument službeno ne određuje TCP/IP model. TCP/IP model je stvar prakse i nastao je obrnuto od OSI modeli: prvo su nastali protokoli, a model je samo opis postojećih protokola.*

## Standard koji nije postao praksa i praksa koja je postala standard

1970-ih, potreba za standardima povezivanja i komunikacije računara postala je takva da su i državne institucije i proizvođači računarske opreme osjetili i obavezu i potrebu za regulacijom. Istraživači iz Francuske, Velike Britanije i SAD-a započeli su dva projekta za razvoj upravo toga. Prvo su to bile neformalne grupe koje su pokušale da razviju skup standarda za prostor računarskog umrežavanja. Njihovi projekti su imali za cilj da definišu standard za kompjutersko umrežavanje i interoperabilnost među dobavljačima i proizvođačima uređaja.
U tome su prednjačila dva tima.
Jedan tim koji je radio na tome bila je Međunarodna organizacija za standardizaciju (ISO). Drugi je radio pod pokroviteljstbom Međunarodnog konsultativnog komiteta za telegraf i telefon, (ITU-CCITT). Svako od ovih tijela izradilo je dokument kojim pokušava standardizirati način na koji će se protokoli za kompjutersko umrežavanje oblikovati u budućnosti.
1983. došlo je do spajanja dva dokumenta i formiranja Osnovnog referentnog modela za međusobnu povezanost otvorenih sistema. Prvobitni cilj nije bio kreiranje modela prvenstveno u obrazovne svrhe – iako mnogi ljudi danas misle da je to bio slučaj. Referentni model OSI trebao je poslužiti kao osnova za uspostavljanje skupa protokola (OSI Protocol Suite) koje će koristiti međunarodne mreže.
No, nije sve išlo po planu. Proizvođači nisu bili zadovoljni ponuđenim modelom. Smatrali su ga prekomplikovanim. A i vrijeme uspostavljanja standardizacije je bilo predugo.
U praksi su se već koristila neka rješenja.
Prethodnik današnjeg TCP protokola razvijen je 1973. i tad se tada zvao *Transmission Control Program.*


Vinton Grey Cerf i Robert Bob Kahn napisali su prvi TCP protokol, pod nazivom Specifikacija programa kontrole internetskog prenosa (RFC 675), objavljen u decembru 1974.
1977. Jonathan Postel objavio je skup komentara u kojima govori o potrebi razdvajanja funkcija tadašnjeg TCP protokola, koji je služio za komunikaciju između krajnjih korisnika, i funkcija za kreiranje i rutiranje Internet paketa.
Postelovi komentari su 1978. godine doveli do kreiranja TCP/IP arhitekture i razdvajanja TCP-a na TCP koji radi na transportnom sloju i IP koji radi na mrežnom sloju.
Otuda i dolazi ime TCP/IP.


Vint Cerf (desno) sa Jonom Postelom i Steveom Crockerom 1994. Njih trojica su bili dio tima koji je radio na ARPAnetu, koji je na kraju postao Internet.

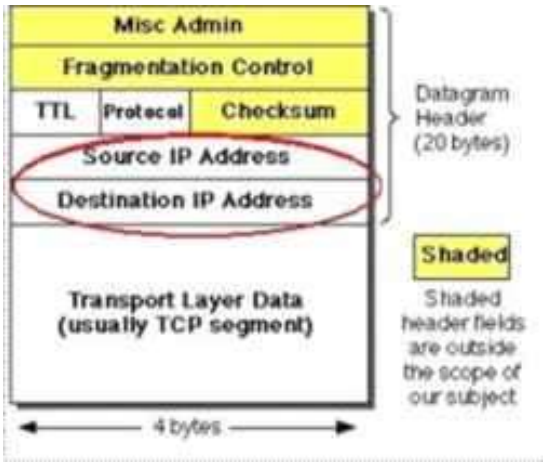
Prvog januara 1983. godine ARPAnet je zemenio Network Control Protocol sa TCP/IP skupom protokola i taj datum na određeni način predstavlja datum rođenja Interneta.

U proteklih 50 godina ova dva modela praktično objedinjena i predstavljaju zajednički model koji funkcioniše.
OSI model je ostao (i danas je) osnov akademskog i obrazovnog pristupa mrežama, a TCP/IP je postao dominantan u praksi.

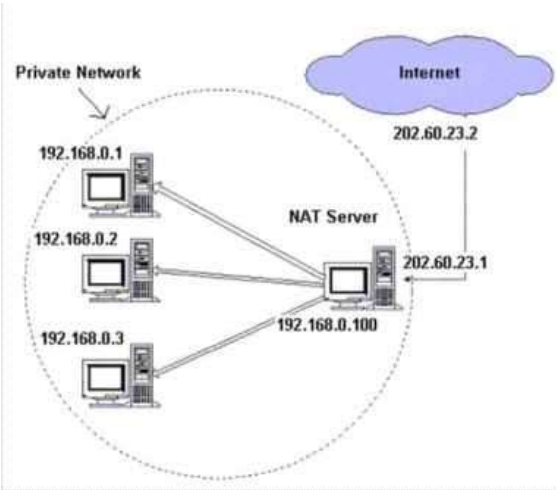
## IP - Internet protokol

Internet Protocol (IP) je protokol za komunikaciju između izvora i korisnika preko Internet mreže.

Osnovni dio IP-a rukuje s mrežnim adresama. Svaki računar na Internetu ima svoju numeričku adresu, a protokol IP "zna" kako slati poruke (pakete s podacima) na tako adresirane računare.
IP protokol osigurava relativno nepouzdanu uslugu prenosa podataka na modelu usluge koji se često naziva najboljom mogućom (**best effort**), što znači da nema gotovo nikave garancije da će poslani paket ili datagram zaista i doći do odredišta nakon što je poslan.
Ukoliko aplikacija zahtijeva pouzdanost, koriste se drugi mehanizmi ili protokoli, najčešće na sloju iznad samog IP protokola.
IP protokol pridružuje podacima izvornu i ciljnu adresu **(source and destination IP address)**.



Podaci u IP mreži se šalju u blokovima koji se nazivaju paketi ili datagrami. Specifično je da se prilikom slanja paketa između izvorišta i odredišta unaprijed ne određuje tačan put preko mreže kojim će podaci ići, te u tom smislu govorimo o IP mreži kao o paketskoj mreži.
Podaci preko IP-a se šalju u paketima i to samo između ruuera-mrežnih usmjerivača (router), a između svičeva-skretnica (switch) u frame-ovima.
IP adrese korisnika koji surfuju po WorldWideWeb-u se koriste da omoguće komunikaciju sa serverom nekog web sajta. Takođe, one se nalaze u zaglavljima elektronske pošte.
U stvari, za sve programe koji koriste TCP/IP protokol, IP adresa korisnika i IP adresa odredišta su neophodni kako bi se uspostavila komunikacija i poslali podaci.




Ono što IP ne zna raditi jest brinuti se o tome da paketi zaista i dođu tamo gdje trebaju, da dođu bez pogrešaka i onako kako su poslani. *Baš ga briga ako se paketi izgube ili uopšte svi ne stignu: on će pokušati isporučiti sve što su mu dali, ali ako ne ide - onda ništa.*
Slično poštaru koji bi bacio preporučena pisma, koja ne može isporučiti, u smeće bez da obavijesti onoga ko ih je poslao.
Zato postoji TCP protokol koji se brine da paketi nakon pristizanja budu poredani dobrim redoslijedom, da ne sadrže pogreške i da svi stignu.

## TCP

TCP (Transmission Control Protocol) je pouzdan (**reliable**) konekciono orijentisan protokol koji dozvoljava da se niz bajtova sa jednog računara isporuči bez greške bilo kom drugom računaru na Internetu. Korišćenjem protokola TCP aplikacija na nekom od hostova kreira virtualnu konekciju prema drugom hostu, te putem te ostvarene konekcije zatim prenosi podatke.
Ovaj protokol se bavi stvarima kao što su:

- **Podjela podataka** koji su mu prosljeđeni iz sloja aplikacije na dijelove čija veličina odgovara sloju ispod tj internet sloju
- **Potvrđivanje prijema** paketa
- **Postavljanje časovnika** (time out) kako bi se osiguralo da drugi kraj potvrdi pakete koji su mu poslati

Prilikom korištenja TCP usluge entiteti prolaze kroz tri faze:
1. Uspostava veze - konekcija
2. Razmjena i provjera podataka
3. Prekid veze

TCP je vrlo kompleksan protokol. On definiše principe slanja i provjere paketa na prijemnoj i predajnoj strani.

## Razmjena podataka

TCP entiteti razmjenjuju podatke u obliku segmenata. Segment se sastoji od zaglavlja koje ima 20 okteta (uz opcionalni dio) za kojim slijedi nula ili više okteta podataka, a nastaje skupljanjem podataka od nekoliko upisivanja ili razbijanjem podataka od jednog upisivanja. Veličina segmenta je varijabilna uz dva ograničenja:

- Svaki segment uključujući i TCP zaglavlje mora stati u 65 535 okteta IP paketa
- Svaka mreža ima svoj **MTU** (*Maximum Transmission Unit*), a to je najveća dopuštena jedinica za prenos koja definiše gornju granicu veličine segmenta.

**Ako** je segment prevelik za mrežu kroz koju mora proći, čvor vrši fragmentaciju u više manjih segmenata od kojih svaki dobiva svoje IP zaglavlje.

Osnovni protokol kojeg koriste TCP entiteti je protokol s klizajućim prozorom (Sliding Window):

1. Nakon slanja segmenta predajnik pokreće brojač (timer)
2. Kad segment stigne na odredište, prijemnik šalje u segmentu potvrdu s brojem jednakim slijedećem broju segmenta kojeg očekuje
3. Ako brojač istekne prije nego što je primljena potvrda, segment se šalje ponovno

TCP Header

| Bit offset | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 | 26 | 27 | 28 | 29 | 30 | 31 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | Source port | | | | | | | | | | | | | | | | Destination port | | | | | | | | | | | | | | | |
| 32 | Sequence number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 64 | Acknowledgment number | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 96 | Data offset | | | | Reserved | | | | CWR | ECE | URG | ACK | PSH | RST | SYN | FIN | Window Size | | | | | | | | | | | | | | | |
| 128 | Checksum | | | | | | | | | | | | | | | | Urgent pointer | | | | | | | | | | | | | | | |
| 160 … | Options (if Data Offset > 5) … | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

*Zaglavlje TCP paketa*

Značenja polja:

- **Source Port** - Broj priključne tačke usluge izvorišta.
- **Destination Port** - Broj priključne tačke usluge odredišta.
- **Sequence Number** - Redni broj prvog okteta podataka u tom segmentu; ako je postavljena zastavica S (SYN), onda je to početni redni broj (ISN - Initial Sequence Number), a prvi oktet podataka ima broj ISN+1.
- **Acknowledgment Number** - Broj potvrde; ako je postavljen A (ACK) bit, polje sadrži redni broj sljedećeg okteta kojeg primatelj očekuje.
- **Offset** - Pomak podataka, pokazuje na početak podataka u TCP segmentu, izraženo u 32-bitnim riječima (TCP zaglavlje je uvijek višekratnik 32-bitne riječi).
- **Reserved** – Polje je rezervirano za buduće potrebe; popunjeno je nulama.
- **Kontrolni bitovi**:

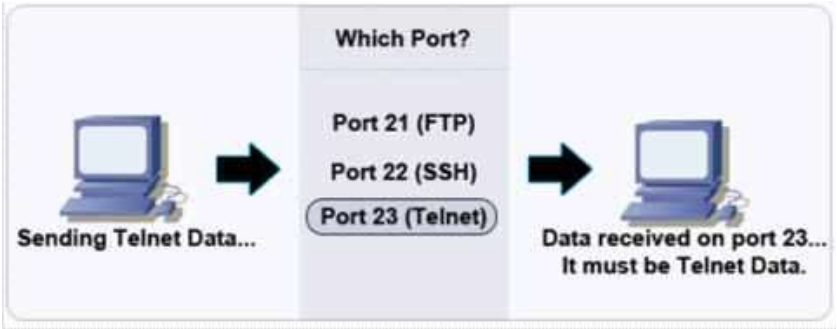
  - **U**RG - Indikator hitnih podataka
  - **A**CK - Indikator paketa potvrde
  - **P**SH - Inicira prosljeđivanje svih do tada neproslijeđenih podataka korisniku
  - **R**ST - Ponovna inicijalizacija veze
  - **S**YN - Sinkronizacija rednih brojeva
  - **F**IN - Izvorište više nema podataka za slanje
- **Window** – Prozor, označava koliko je okteta prijemnik spreman primiti
- **Checksum** - Kontrolni zbroj; računa se kao 16-bitni komplement jedinice komplementa zbroja svih 16-bitnih riječi u zaglavlju i podacima; pokriva i 96 bitova pseudozaglavlja koje sadrži izvorišnu i odredišnu adresu, protokol i duljinu TCP zaglavlja i podataka.
- **Urgent Pointer** - Pokazivač na redni broj okteta gdje se nalaze hitni podaci; polje se gleda jedino ako je postavljena zastavica URG.
- **Options + Padding** - Options mogu, a ne moraju biti uključene; ako postoje, veličine su x×8 bita, Padding je dopuna nulama do 32 bita.
- **Data** - Podaci aplikacijskog nivoa.

## Portovi

Port je virtuelna tačka na kojoj počinju i završavaju mrežne veze. Portovi su softverski zasnovani i njima upravlja operativni sistem računara. Svaki port je povezan sa određenim procesom ili uslugom.

TCP upotrebljava određen raspon portova kojima raspoređuje aplikativne programe na strani pošiljatelja i primatelja. TCP protokol definiše raspon portova od 0 do 65535, tj. ukupno ima 65536 mogućih različitih portova. Svaka strana TCP konekcije ima dodijeljenu 16-bitnu oznaku za obje strane aplikacije (slanje, primanje).
Portovi su u osnovi podijeljeni u 3 kategorije:

- poznati portovi,
- registrovani portovi i
- dinamički/privatni portovi.

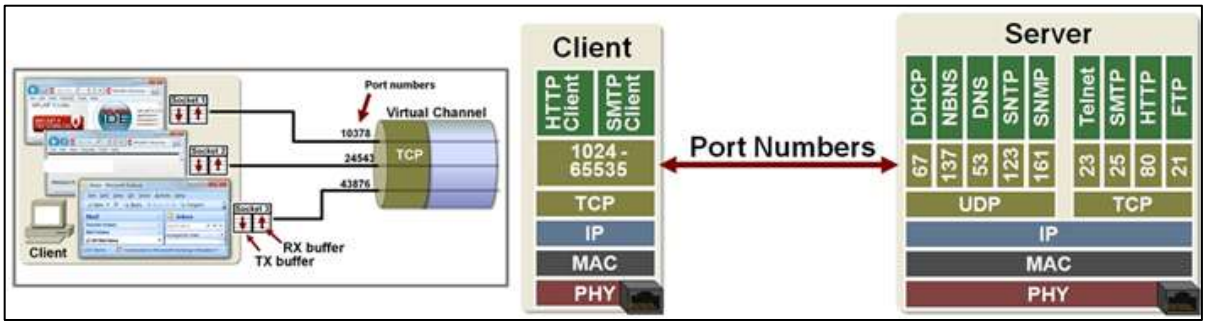



*Slanje i prijem podataka na neke od poznatih portova*

**Opšte poznati portovi** (eng well known ports) dodijeljeni su od strane Internet Assigned Numbers Authority, organizacije koja se brine za IP adresni prostor, vršne domene te druge detalje vezane uz IP Protokol.
Ovi portovi su najčešće korišteni od strane sistemskih procesa, koje koriste poznate aplikacije kada primaju konekcije pasivno slušajući promet na tim portovima. Neki primjeri opšte poznatih portova su: FTP (TCP port 21), Telnet (23), SMTP (25) i HTTP (80).

**Registrovani portovi** se koriste kod aplikacija krajnjih korisnika kao izvorišni portovi prilikom konekcije servera, kao i za identifikaciju servisa registrovanih od trećih strana.

**Dinamički /privatni** portovi se koriste i na strani aplikacija krajnjih korisnika, ali nešto rjeđe. Dinamički/privatni protovi imaju samo lokalno značenje za određenu TCP konekciju.




Portovi omogućavaju računarima da lako razlikuju različite vrste saobraćaja: e-poruke idu na različite portove od web stranica, na primjer, iako oba dolaze do računara putem iste internetske veze.

## ICMP protokol za slanje kontrolnih poruka o greškama

IP definiše mrežnu uslugu kao uslugu u najboljoj namjeri: best-effort delivery. Prilikom komunikacije po ovom principu best-effort delivery je moguće da datagrami budu duplicirani, izgubljeni, kasne ili stignu u slučajnom poretku.

U TCP/IP stogu protokola to rješava kolekcija protokola *ICMP* (Internet Control Message Protocol**)**. Svaka standardna implementacija IP protokola mora sadržavati ICMP protokole. ICMP koristi IP protokol za slanje poruka o grešci. Osim dojave o grešci, ICMP šalje i druge informacije.

Popis svih ICMP poruka može vidjeti na slici lijevo.

Ovdje ćemo navesti neke standardne poruke o grešci koje navodi ICMP.

• *Source Quench*: Ruter šalje ovu poruku kada u međuregistru nema mjesta.

Pošiljatelj mora reagovati smanjivanjem brzine generisana novih datagrama.

• *Time Exceded*: Generira se kada je ruter spustio polje TIME TO LIVE u datagramu na nulu ili kada host pri ponovnom sklapanju fragmentirane poruke prekorači REASSEMBLY TIMER

• *Destination Unreachable*: Šalje se kad ruter ustanovi da se datagram ne može isporučiti na svoje odredište. Iskazuje se razlika između nedostupnog hosta i nedostupne mreže.

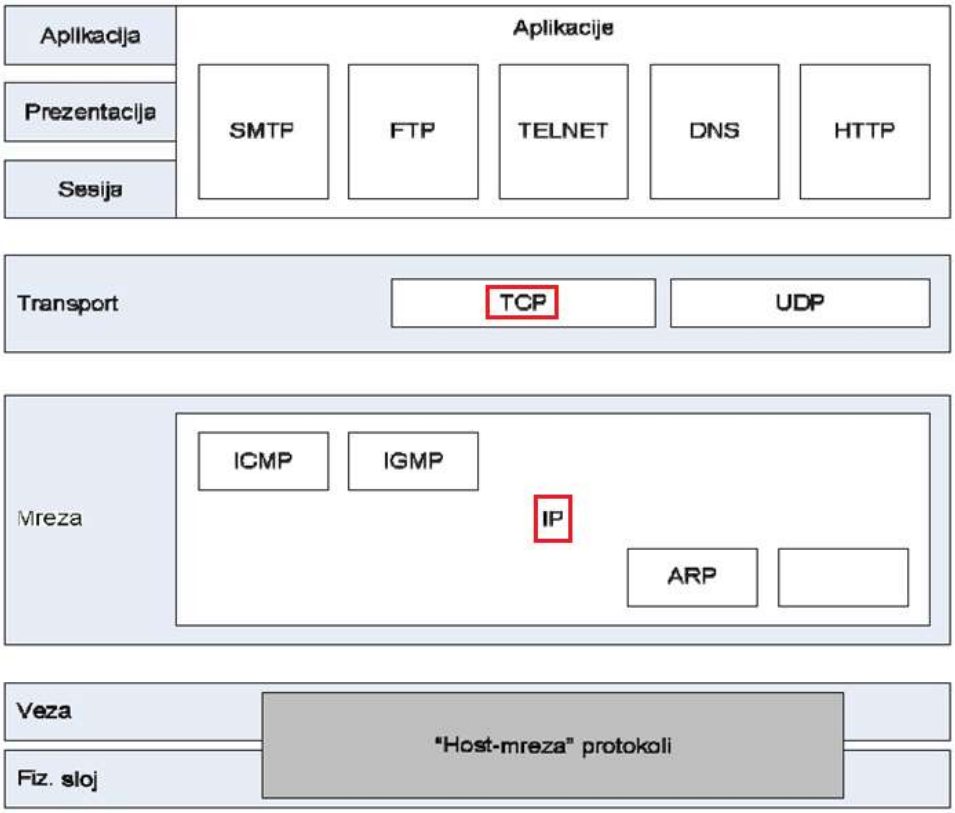
• *Redirect*: Ukoliko ruter utvrdi da bi datagram trebao biti poslan po drugoj ruti, šalje ovu poruku. Može zahtijevati promjenu za host ili za mrežu.

| Type | Name |
|---|---|
| 0 | Echo Reply |
| 1 | Unassigned |
| 2 | Unassigned |
| 3 | Destination Unreachable |
| 4 | Source Quench |
| 5 | Redirect |
| 6 | Alternate Host Address |
| 7 | Unassigned |
| 8 | Echo |
| 9 | Router Advertisement |
| 10 | Router Selection |
| 11 | Time Exceeded |
| 12 | Parameter Problem |
| 13 | Timestamp |
| 14 | Timestamp Reply |
| 15 | Information Request |
| 16 | Information Reply |
| 17 | Address Mask Request |
| 18 | Address Mask Reply |
| 19 | Reserved (for Security) |
| 20-29 | Reserved (for Robustness Experiment) |
| 30 | Traceroute |
| 31 | Datagram Conversion Error |
| 32 | Mobile Host Redirect |
| 33 | IPv6 Where-Are-You |
| 34 | IPv6 I-Am-Here |
| 35 | Mobile Registration Request |
| 36 | Mobile Registration Reply |
| 37-255 | Reserved |

Dva najpoznata alata za ispitivanje povezanosti mreže, *ping* i *traceroute*, koja ćemo kasnije opisati zasnivaju se na korištenju ICMP poruka.

# TCP/IP protokol stek

Stek protokola je kombinacija, odnosno skup protokola.
**Par** koji sačinjavaju internet protokol **IP i** protokol za kontrolu prenosa **TCP** su najbitniji od mrežnih protokola i **termin TCP/IP protokol stek** označava skup najkorišćenijih od njih. Ovaj stek objedinio je i sve druge protokole u svim slojevima.



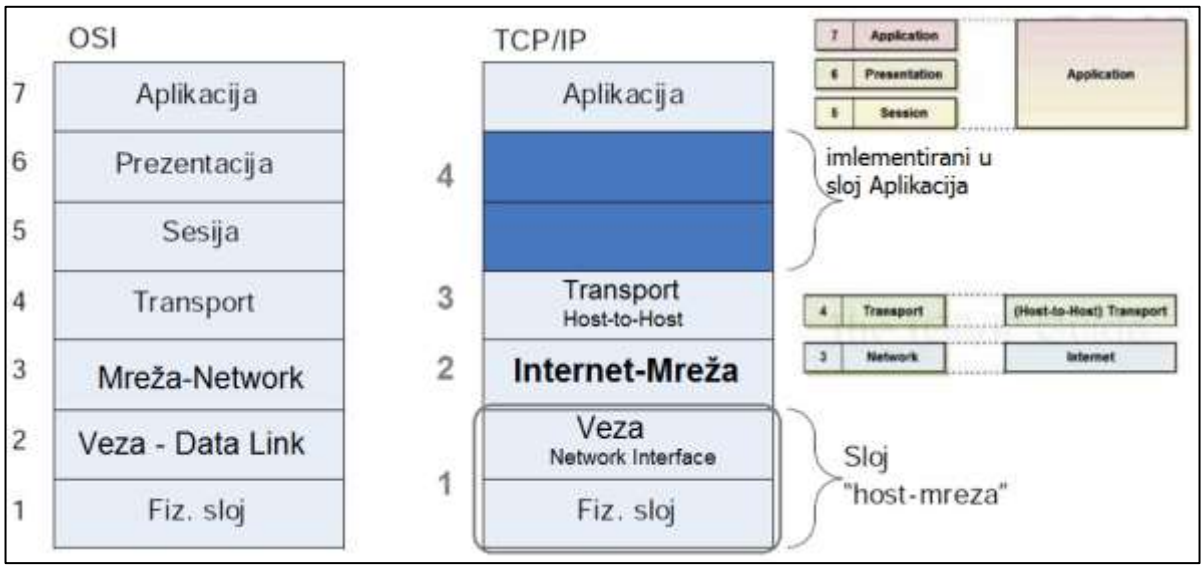

*Struktura TCP/IP modela sa najvažnijim protokolima razvrstanim u slojeve*

**Aplikativni sloj** TCP/IP obuhvata funkcije sloja aplikacije, prezentacije i sloja sesije OSI modela. Mrežni protokoli (i odgovarajući programi) na ovom nivou su Telnet, FTP, SNMP, HTTP i SMTP.
**Transportni sloj** odgovara sloju 4 OSI modela, sa tom razlikom da nema funkcionalnost OSI sesije. Osnovna namjena ovog sloja je da obezbjedi prenosni servis. Najvažniji protokoli na ovom sloju su TCP (Transmission Control Protocol) i UDP (User Datagram Protocol). Oba protokola služe aplikativnom sloju za prenos podataka, a sam izbor zavisi od zahtjeva za pouzdanošću prenosa. TCP je pouzdan, konekcioni protokol koji obezbjeđuje proveru grešaka i kontrolu toka podataka preko virtualne veze, koja se uspostavlja i po završetku prenosa raskida. FTP, HTTP i SNMP servisi koriste TCP da bi obezbjedili prenos podataka bez grešaka i gubitaka. UDP je nepouzdan, prenos bez konekcije, ali sa zato sa manjim opterećenjem mreže. UDP ne obuhvata proveru grešaka pri prenosu, niti ima mehanizme za kontrolu toka podataka.

SNMP i multimedijalne aplikacije koriste UDP, SNMP zbog nadzora mreže (što je proces koji ne bi trebalo da preoptereti mrežu), a multimedijalne aplikacije zbog manjeg opterećenja mreže.
**Internet (mrežni sloj)** je odgovoran za usmjeravanje (rutiranje) podataka preko mreže. Omogućava komunikaciju preko mreža istog ili različitog tipa i obavlja prevođenje između različitih adresnih šema. IP (Internet Protocol) i ARP (Address Resoluton Protocol) se nalaze u ovom sloju.
Pošto koristi vertikalna hijerarhisku komunikacija između različitih protokola na različitim komunikacionim slojevima, neodvojiv dio paketskog prenosa je i proces **enkapsulacije** i **deenkapsulacije** (objašnjen kod OSI modela).
Kompletan proces enkapsulacije se odvija na strani pošiljaoca a kompletan proces deenkapsulacije na strani primaoca podataka.
Međutim, oba procesa se djelimično mogu izvršavati i na posrednicima u komunikaciji, u zavisnosti od toga na kojim nivoima ti posrednici funkcionišu. Na primjer, ruter će iz primljenih okvira izdvojiti pakete mrežnog sloja (dekapsulacija) da bi na osnovu podataka u njihovom zaglavlju doneo odluku o prosleđivanju. Nakon donošenja te odluke, ruter će paket mrežnog sloja upakovati u odgovarajući okvir (inkapsulacija) za prenošenje do sledećeg posrednika ili konačnog odredišta.

## Odnos OSI i TCP/IP modela

TCP/IP je (kao i OSI) hijerarhijski protokol što znači da je svaki protokol višeg nivoa, podržan od strane jednog ili više protokola nižeg nivoa. **ALI** za razliku od OSI modela koji definiše koje funkcije pripadaju kom sloju, slojevi TCP/IP modela sadrže relativno nezavisne protokole koji se mogu kombinovati zavisno od potreba sistema.
Slojevi koje TCP/IP podržava su aplikativni, trasportni, internet i međumrežni, pri čemu se u nekim podijelama međumrežni sloj dijeli na fizički i sloj veze podataka, pa se govori i o pet slojeva TCP/IP modela.



TCP/IP **ne** posvećuje posebnu pažnju i samo se okvirno bavi najnižim slojevima (fizičkim i slojem veze), pretpostavljajući da mreža posjeduje protokole koji pokrivaju funkcije tih slojeva. Zajedno, ova dva sloja se tretiraju kao ″host-mreža ″sloj.
Mrežni i transportni sloj odgovaraju slojevima 3 i 4 OSI modela. Međutim, kod TCP/IP na transportni sloj direktno se nastavlja aplikacioni sloj, koji obuhvata funkcionalnost tri gornja sloja OSI modela.

# IPv4

IPv4 je Internet Protocol verzije 4, prvi put predstavljen u januaru 1983. godine. I danas se koristi za rutiranje većine Internet prometa, čak i uz tekuću implementaciju Internet Protocol verzije 6 (IPv6), njegovog nasljednika
Najvažnija karakteristika IPv4 protokola je da koristi 32-bitnu IP adresu, što znači da je propisana dužina svake IP adrese u ovoj verziji protokola 32 bita.
IPv4 verzija protokola detaljno propisuje izgled paketa, gdje su pojedina polja u zaglavlju detaljno specificirana, dok je sama **dužina podataka u paketu varijabilna**. Prema standardu **minimalna dužina tako formiranog datagrama je 20 bajtova, dok je maksimalna dužina 65535 bajtova**.
IPv4 može generisati 4.3. milijardi adresa koje koriste 32-bitne brojeve. Adresa je sastavljena od mrežnog dijela i dijela hosta, koji zavisi o klasi adrese.

Slijedi prikaz propisanih polja u IPv4 paketu:

| + | Bitovi 0 - 3 | 4 - 7 | 8 - 15 | 16 - 18 | 19 - 31 |
|---|---|---|---|---|---|
| 0 | Verzija | Dužina zaglavlja | Tip servisa - ToS (ponekad DiffServ i ECN) | Ukupna dužina | |
| 32 | Identifikacija | | | Zastavice | Ofset fragmenta |
| 64 | *TTL* vrijeme | | Protokol | *checksum* zaglavlja | |
| 96 | Izvorišna adresa | | | | |
| 128 | Odredišna adresa | | | | |
| 160 | Opcionalno | | | | |
| 192 | Podaci | | | | |

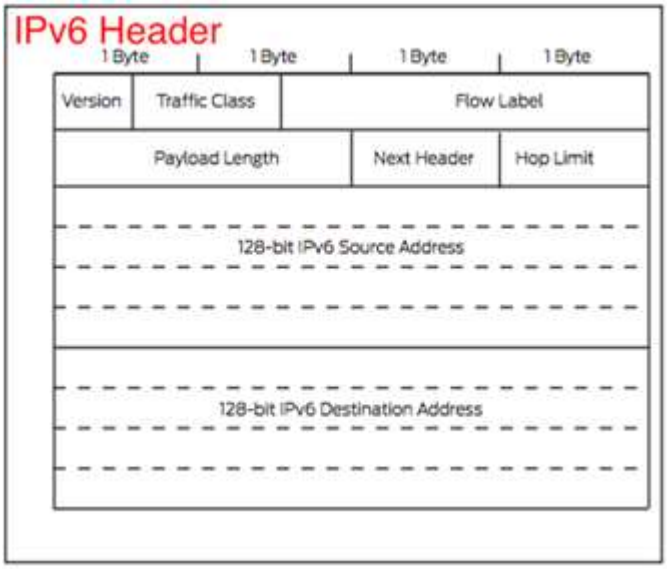
Definicija pojedinih polja:

| Ime polja | Opis |
|---|---|
| **Verzija** | Verzija IP paketa. |
| **IHL** | Dužina zaglavlja IP paketa. |
| **Tip usluge** | Prioritet kojim se paket treba tretirati prilikom prosljeđivanja. |
| **Dužina** | Ukupna dužina datagrama. |
| **Identifikacija** | Koristi se primarno za identifikaciju datagrama prilikom fragmentiranja. |
| **Zastavice** | Zauzimaju 3 bita, a koriste se za kontrolu ili identifikaciju fragmenata. |
| **Pomak fragmentacije** | Pomak fragmentiranog datagrama u oktetima. |
| **TTL** | Broj skokova koliko će dugo živjeti datagram. |

| | |
|---|---|
| **Protokol** | Opisuje koji se protokol prenosi u podacima. |
| **Provjera** | Polje koje služi za provjeru ispravnosti zaglavlja. |
| **Izvorišna adresa** | IP adresa izvora. |
| **Odred. adr.** | IP adresa odredišta |
| **Opcije** | Ako slijede dodatne opcije vezane za zaglavlje. |
| **Podaci** | Podaci koji se prenose u IP datagramu. |

## IPv6

IPv6 je šesta revizija Internet Protokola i nasljednik IPv4. Funkcioniše slično kao IPv4, takođe generiše unikatne, numeričke IP adrese neophodne za komunikaciju uređaja putem Interneta. Međutim, donosi nam i jednu veliku razliku: 128-bitne adrese.
Zaglavlje IPv6 je, u osnovi, pojednostavljeno zaglavlje verzije četiri ovog protokola. Dio polja i formata je zadržan, međutim izbačena su nepotrebna, slabo korištena i zastarjela polja, a dodana su polja za bolju podršku prometa u realnom vremenu. To je omogućuje vrlo jednostavnu implementaciju dodatne funkcionalnosti protokola, pogotovo za pojedine "end-to-end" opcije.
Dok je IPv4 zaglavlje bilo varijabilne dužine, **zaglavlje IPv6 ima fiksnu dužinu od 40 okteta, od čega čak 32 okteta otpada na adrese**. Osim toga, minimalno IPv6 zaglavlje ima samo sedam polja, za razliku od trinaest polja zaglavlja verzije 4. Smanjenjem broja obaveznih polja postignuta je brža obrada IPv6 paketa u ruterima-usmjernicima na mreži, jer je potrebno analizirati manji broj (jednostavnijih) polja.




Polja IPv6 zaglavlja su: **polje verzije protokola** (Version), **polje tipa prometa** (TrafficClass), **polje oznake toka** (FlowLabel), **polje dužine korisnog tereta** (PayloadLen), **polje sljedećeg**

**zaglavlja (**NextHeader), **polje ograničenja broja skokova** (HopLimit) i **polja odredišne i izvorišne adrese** (SourceAddress i DestinationAddress).

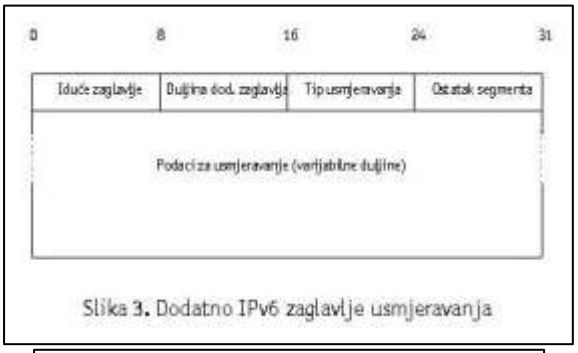
Novost u IPv6 je i način dodavanja opcionih polja u zaglavlje. Dok je u IPv4 zaglavlju polje opcija smješteno u osnovno IPv4 zaglavlje, i ono je varijabilne dužine, kod IPv6 zaglavlja sve opcije su izbačene iz osnovnog zaglavlja, a uvedena su dodatna zaglavlja koja definišu naprednije funkcije, te se nalaze nakon osnovnog zaglavlja. Ovakvim dizajnom protokola, ruterima u mreži ušteđeno je vrijeme obrade, jer ne troše procesorsko vrijeme na obradu polja koje se ne odnose na njih.

Optimizacija obrade paketa ostvarena je i nizanjem dodatnih polja zaglavlja u paketu: nakon osnovnog zaglavlja prvo se dodaju tzv. "hop-by-hop" opcije (one koje trebaju obrađivati ruteri-usmjerivači putem do odredišta), a na samom kraju zaglavlja tzv. "end-to-end" opcije (koje procesiraju samo krajnji čvorovi, npr. podaci za enkripciju).

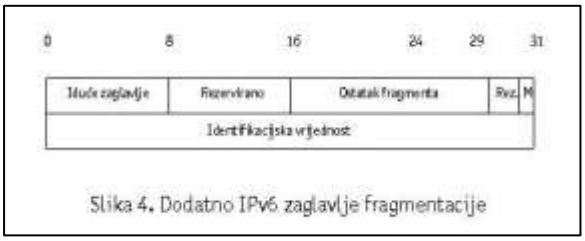
- Verzija (Version) – polje dužine 4 bita, označava verziju (6).
- Klasa prometa (Traffic Class) – odgovara polju "vrsta usluge" u IPv4. Omogućuje postavljanje željenog prioriteta pri uručivanju paketa. Dužina je 4 bita za postavljanje 16 različitih vrsta prometa. Neke od oznaka su već predefinisane, a neke ostavljene za buduće potrebe. Pravilo je da su brojevima od 0 do 7 označeni paketi kojima nije toliko bitno kašnjenje koliko pouzdana isporuka, dok su brojevima od 8 do 15 označeni paketi koji bi trebali stići u realnom vremenu. Ti paketi ne moraju putovati pretjerano pouzdano, ali ne smiju kasniti.
- Oznaka toka (Flow Label) – polje dužine 24 bita. S ishodišnom adresom čini jedinstveni broj koji označava pakete koji traže posebno rukovanje kod IPv6 usmjernika. Uvedeno je radi određivanja slijeda paketa određene vrste usluge (VoIP).
- Dužina podataka (payload length) – dužina korisnog sadržaja (u broju okteta). Polje slično polju ukupne dužine u IPv4 (total length).
- Slijedeće zaglavlje (next header) – označava koji tip zaglavlja slijedi odmah nakon osnovnog IPv6 zaglavlja (npr. TCP ili UDP zaglavlje na transportnom sloju ili zaglavlje proširenja (extension header).
- Zaglavlja proširenja može se dodati zbog autentikacije, enkriptiranja podataka, ICMPv6 poruka i dr.
- Maksimalni broj čvorova (hop limit) – broj koji definira koliko usmjernika paket može proći prije nego bude uništen. To je broj od osam bitova koji se smanjuje za jedan kod svakog prolaska kroz usmjernik. Paket se uništava ako vrijednost polja dođe na nulu. To je polje slično polju TTL u IPv4 verziji. U IPv6 izbačena je provjera ispravnosti podataka na mrežnom sloju kako bi se povećala efikasnost prosljeđivanja paketa. Prema tome IPv6 nema polje sažetak zaglavlja (checksum). Ta je provjera izbačena jer se već ionako radi na podatkovnom i transportnom sloju.
- Ishodišna adresa (source address) – adresa ishodišta paketa (128 bita)
- Odredišna adresa (destination address) – adresa odredišta paketa (128 bita)
- Dodatna zaglavlja Internet prokola verzije 6 su: čvor po čvor dodatno zaglavlje (Hop-by-Hop Options Header), dodatno zaglavlje usmjeravanja (Routing Header), dodatno zaglavlje fragmentacije (Fragment Header), dodatno zaglavlje odredišta (Destination Options Header), dodatno zaglavlje autentifikacije (Authentication Header) i dodatno zaglavlje sigurnosti enkapsulacije korisnog tereta (Encapsulating Security Payload Header).


Slika 1. Osnovno zaglavlje IPv6 Internet protkola

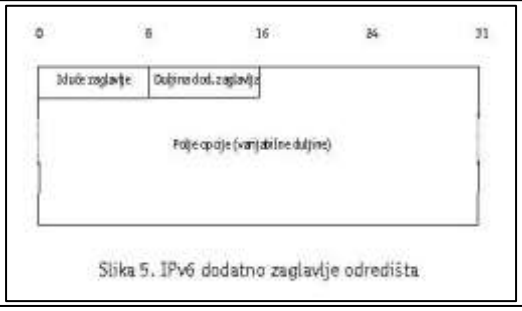

Slika 2. Čvor po čvor dodatno IPv6 zaglavlje



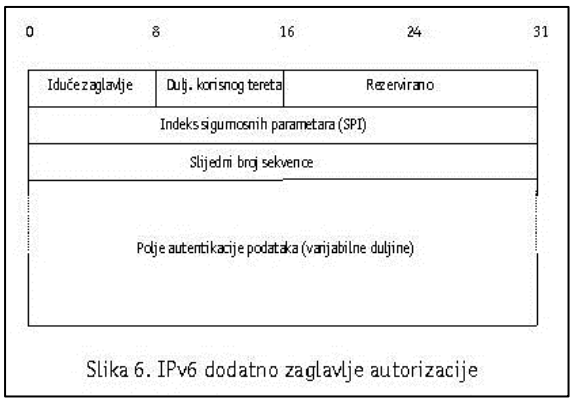

Slika 3. Dodatno IPv6 zaglavlje usmjeravanja



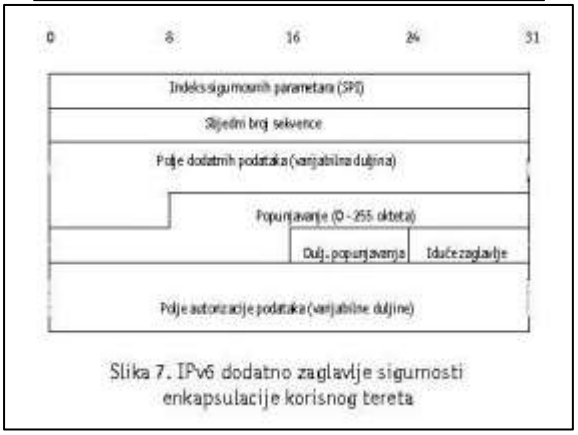

Slika 4. Dodatno IPv6 zaglavlje fragmentacije




Slika 5. IPv6 dodatno zaglavlje odredišta




Slika 6. IPv6 dodatno zaglavlje autorizacije



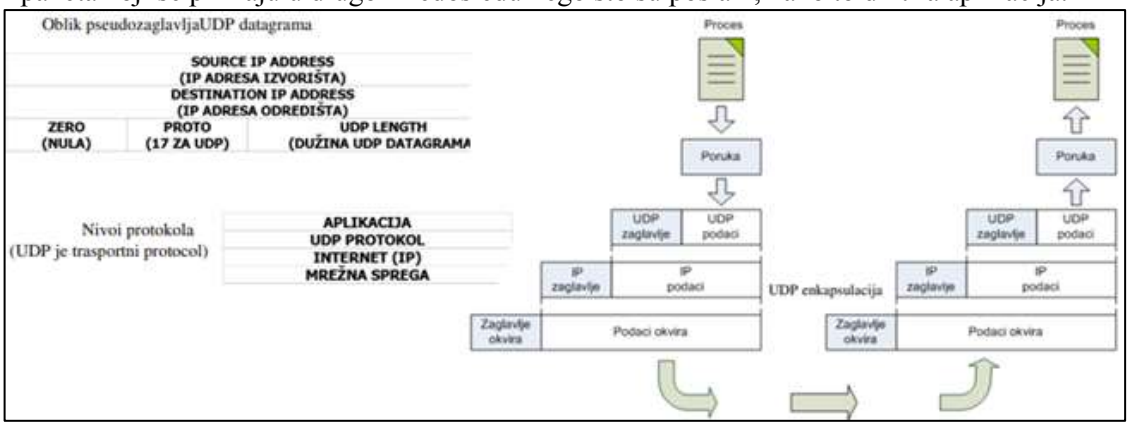

Slika 7. IPv6 dodatno zaglavlje sigurnosti enkapsulacije korisnog tereta

Nestanak IPv4 adresa je predviđen prije par godina i **prebacivanje je u toku već 10ak godina**. Process se razvija veoma sporo. Danas, uglavnom IPv4 i IPv6 mogu da rade paralelno – razmjena podataka između ovih protokola zahtijeva specijalni gateway (vidi).

*Većina operatvnih sistema već podržavaju i IPv6 i IPv4.*

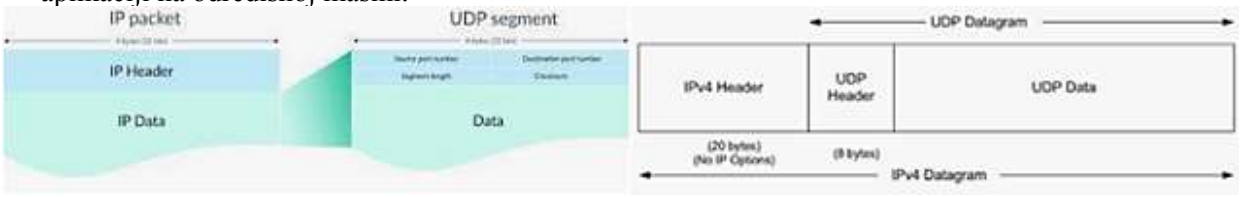
# UDP: Protokol korisničkih datagrama

Protokol korisničkih datagrama (*Protokol User Datagram*) je uveden 1980. godine i jedan je od najstarijih mrežnih protokola koji postoje.
UDP je jednostavan **protokol OSI transportnog sloja** za aplikacije aplikacija klijent/server, zasnovan je na Internet protokolu (IP) i predstavlja glavnu **alternativu TCP-u**. UDP (ponekad pod nazivom **UDP/IP**) često se koristi u aplikacijama za video konferencije ili računarskim igrama koje su napravljene specifično za performanse u realnom vremenu. Da bi postigli veće performanse, protokol dozvoljava pada pojedinačnih paketa (bez ponovnih pokušaja) i UDP paketa koji se primaju u drugom redosledu nego što su poslani, kako to diktira aplikacija.




*UDP poruka se smešta u IP datagram, a on u fizički okvir*

Konceptualno, jedina bitna razlika između UDP datagrama i IP datagrama je u tome što UDP **sadrži brojeve portova,** što omogućava predajnoj aplikaciji da se obrati tačno određenoj aplikaciji na odredišnoj mašini.

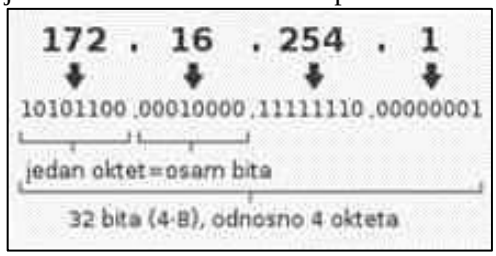



UDP portovi zavise od UDP/IP protokola. UDP portovi uključuju DNS port (53), port Dynamic Host Configuration Protocol (68) i Kerberos port (88), koji koriste servisi za igre.


Za razliku od TCP portova, UDP portovi ne moraju uspostavljati veze prije prenosa podataka. Pošto nema potvrde uspostavljanja konekcije to ga čini nepouzdanim za razliku od TCP protoklola.

# Klase mreža (Adresni razredi) kod Ipv4

Već je rečeno da Internet Protocol zahtijeva da svaki uređaj na mreži ima dodijeljenu adresu, koja omogućava njegovu jedinstvenu identifikaciju.
Svaki računar (uređaj-mrežni entitet) osim svoje adrese, posredno ima podatak i o adresi svoje mreže. IP adrese kategorizira u pet glavnih klasa: klase A, B, C, D i E. Do podatka o klasi se dolazi binarnim maskiranjem mrežnom maskom.
Numerička adresa ima dva dijela, koja nisu baš očita ako je promatrate samo kao niz od četiri broja. **Dio adrese predstavlja broj mreže** na koje je priključen računar, a da **drugi dio adrese predstavlja broj računara u toj mreži**.
Naravno, postavlja se pitanje "šta je šta" ako imate adresu od četiri broja: postoje barem tri mogućnosti.
Svaki od tih brojeva je u rasponu 0-255, što je upravo raspon brojeva koji se mogu prikazati u jednom 8-bitnom binarnom prikazu.




Svaki od ovih okteta definiše jedinstvenu adresu, s dijelom adrese koji predstavlja mrežu (neobavezno i podmrežu) i s drugim dijelom koji predstavlja određeni čvor na mreži.

Kada se razmišljalo o načinu realizacije IP adresiranja, pretpostavilo se da će postojati:
• mali broj samostalnih mreža s jako velikim brojem računara; klasa A,
• određen broj mreža koje imaju srednji broj računara: klasa B,
• vrlo veliki broj mreža koje povezuju manji broj računara klasa C.

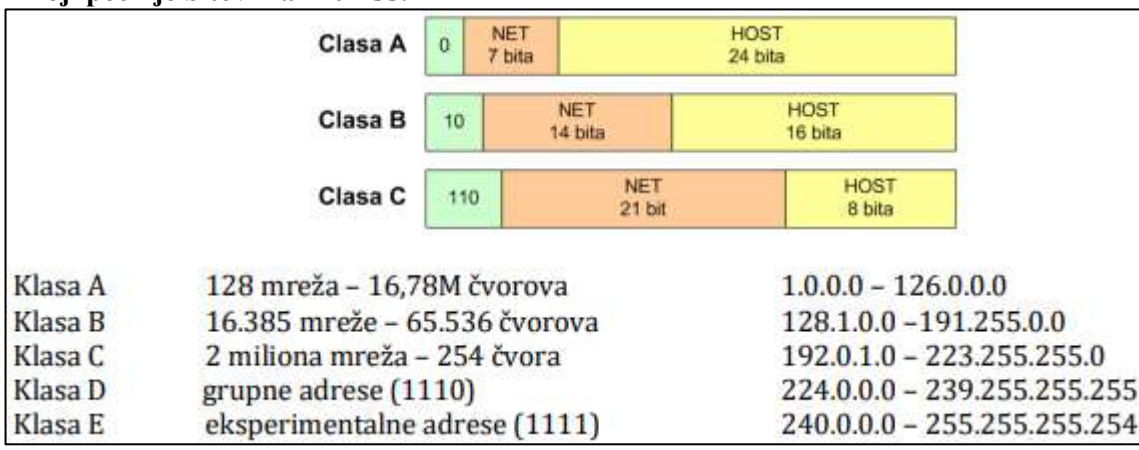
Ako opšti format adrese napišemo kao **aaa.bbb.ccc.ddd**
**U Klasi A** dio aaa adresa mreže, a ostali brojevi adresa računara. Tako može postojati samo nešto više od 120 takvih mreža, ali svaka može imati preko 16 miliona računara (jer posljednja tri broja označavaju samo računar).
**U klasi B**, dio aaa.bbb predstavlja adresu mreže. Budući da su brojevi do 126 već zauzeti za klasu A, u klasi B prvi broj je veći od 128. Tako može postojati 16 hiljada mreža u toj klasi, a

svaka od njih ima do 65 hiljada računara (jer računar predstavljaju posljednja dva broja).
**U klasi C**, prva tri broja, aaa.bbb.ccc, označavaju mrežu i zato je moguće imati oko 1 miliona mreža u toj klasi. Broj aaa mora biti veći od 192. Samo zadnji broj, ddd, koristi se za oznaku računara, pa mreža klase C može u sebi imati 254 računara.

| Razred | Vrijednost prvog okteta | ID mreže | ID računara | broj mreža u ovom razredu | broj računara u mreži |
|---|---|---|---|---|---|
| A | 0 - 127 | a | b.c.d | 128 = $(2^7)$ | 16 777 214 = $(2^{24} - 2)$ |
| B | 128 - 191 | a.b | c.d | 16 384 = $(2^{14})$ | 65 534 = $(2^{16} - 2)$ |
| C | 192 - 223 | a.b.c | d | 2 097 152 = $(2^{21})$ | 254 = $(2^8 - 2)$ |

*Podjelu IPv4 adresa na klase-razrede. Slova u tablici označavaju oktete adrese a.b.c.d.*

Postoje i **posebna klasa D za multicast koja počinje bitovima 224-229**, te **rezervisana klasa E koji počinje bitovima 240-255.**



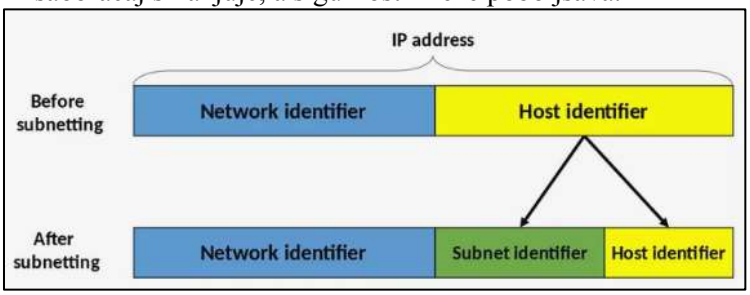

| | | |
|---|---|---|
| Klasa A | 128 mreža – 16,78M čvorova | 1.0.0.0 – 126.0.0.0 |
| Klasa B | 16.385 mreže – 65.536 čvorova | 128.1.0.0 –191.255.0.0 |
| Klasa C | 2 miliona mreža – 254 čvora | 192.0.1.0 – 223.255.255.0 |
| Klasa D | grupne adrese (1110) | 224.0.0.0 – 239.255.255.255 |
| Klasa E | eksperimentalne adrese (1111) | 240.0.0.0 – 255.255.255.254 |

Pojam klase veže se uz pojam klasna mreža (*Classful network*) koja je definisana iPv4 protokolom. Ovakav način adresiranja i određivanja mrežnih klasa (koje se ponekad nazivaju i adresni razredi) mreža se naziva i **klasično adresiranje**.

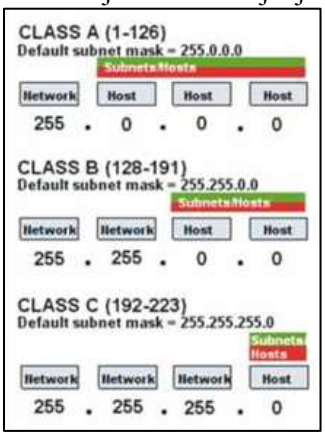
Danas (sa pojavom iPv6 protokola) se koristi **i** tzv. besklasno adresiranje (vidi poglavlje koje se odnosi na iPv6).

# Mrežna maska

Kad je riječ o većoj mreži, poželjno je njeno dijeljenje u više podmreža, jer se manje mreže lakše održavaju, mrežni saobraćaj smanjuje, a sigurnost mreže poboljšava.




Primjenom mrežnih maski (**subnet mask**) omogućeno je formiranje podklasa i podmreža unutar jedne dodjeljene mrežne klase. Na taj način se povećava broj mreža na račun broja računara.
Mrežna maska kod IPv4[17] je 32-bitni broj koji kaže koje bitove originalne IP adrese treba promatrati kao bitove mrežnog broja. Ako je bit mrežne maske postavljen u 1 smatra se da taj bit pripada adresi mreže, svi ostali bitovi (koji su u 0) definišu broj računara. Prema van se mreža još uvijek ponaša kao jedna iako je podijeljena.
Upotrebom maske usmjerivačke tablice rutera se mijenjaju jer moraju sadržavati podatke o podmrežama. Router u podmreži mora znati kako doći do ostalih podmreža i računara u svojoj podmreži. Svaki router mora napraviti logičku operaciju AND sa mrežnom maskom, kako bi dobio mrežni broj i potražio u tablici tu adresu.
**Mrežna maska je broj kojim se definiše opseg IP adresa koje pripadaju mreži.** To je specijalan 32-bitni broj koji, gledan u binarnom sistemu sadrži niz logičkih jedinica za kojima slijede logičke nule. Taj broju stvari predstavlja masku koja se primjenjuje na IP adresu logičkom operacijom AND. Logičke jedinice određuju dio IP adrese koji je nepromjenljiv a logičke nule predstavljaju dio IP adrese koji se može mijenjati.




Mrežna maska ne mora imati 24 bita. Ona može imati i više i manje bitova, zavisno od veličine mreže. Više bitova znači manje adresa u mreži i obrnuto.

[17] Kod Ipv6 se ovakvo maskiranje ne koristi, jer postoji dovoljno rezervisanog prostora, što je objašnjeno u poglavlju *Besklasno adresiranje*

Veličinu mrežne maske određuje onaj ko projektuje mrežu.
**Mreža ima određenu podmrežnu masku čak i ako nema podmreža.**
Naprimjer, maska za adrese iz klase A je 255.0.0.0, za klasu B 255.255.0.0, a za klasu C 255.255.0.
Generalno, koristi se statičko adresiranje da podesite malu kućnu mrežu i dinamičko adresiranje kada se povezujete na Internet.

Pogledajmo to na primjeru.
Uzmimo da je adresa mreže 10.10.10.0,
binarno 00001010.00001010.00001010.00000000.
Uzmimo da je mrežna maska mreže 255.255.255.0
(binarno 11111111.11111111.11111111.00000000).
Kada primenimo logičko AND između ova dva broja dobićemo:
00001010.00001010.00001010.00000000
11111111.11111111.11111111.00000000
---
00001010.00001010.00001010.00000000

Broj 00001010.00001010.00001010.00000000 pretvoren u decimalni sistem je 10.10.10.0, odnosno adresa mreže koju smo izabrali.
Primjetite da su posljednjih osam bitova u mrežnoj masci logičke nule.
**To znači da se u mreži 10.10.10.0 sa maskom 255.255.255.0 adrese računara dobijaju tako što se uzimaju različite vrijednosti posljednjih osam bitova.**
Mreži u našem primjeru pripadaju svi brojevi od 10.10.10.0 do 10.10.10.255, ukupno 256 adresa.
I zaista, ako uzmemo bilo koju adresu iz ovog opsega, na primjer 10.10.10.32 (binarno 00001010.00001010.00001010.00100000) i primenimo na nju masku dobićemo:
00001010.00001010.00001010.00100000
11111111.11111111.11111111.00000000
---
00001010.00001010.00001010.00000000

Rezultat je ponovo adresa mreže 10.10.10.0, što znači da 10.10.10.32 zaista pripada mreži 10.10.10.0 sa mrežnom maskom 255.255.255.0. Tako će biti sa bilo kojom drugom adresom iz ovog opsega.

U IP opsegu pored adrese mreže, postoji još jedna adresa koja se ne koristi za dodjelu nekom mrežnom uređaju već ima specijalnu namjenu.
To je **adresa za objave** (*broadcast*). To je u stvari **posljednja adresa u opsegu**. U našem primjeru, prva adresa, 10.10.10.0 je adresa mreže, a posljednja adresa 10.10.10.255 je broadcast adresa. Ova adresa ima namjenu da kada neki od uređaja u mreži treba da pošalje paket određenom servisu u mreži a ne zna na kojoj adresi se taj servis nalazi, on može paket poslati na broadcast adresu. Taj paket će primiti svi uređaji u mreži, a na njega će da odgovori samo onaj na kome se traženi servis nalazi.

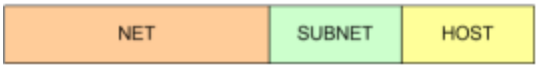
## Rezervisane IP adrese

Čitajući prvi oktet, možemo odrediti klasu adrese kojoj pripada.
Neke IP adrese ne smiju se koristiti za označavanje broja mreže ili računara.
Broj računara ili mreže ne smije biti **0**, zato jer nula označava "ovu mrežu". Naprimjer, ako napišete adresu 161.53.0.0, to označava mrežu čija je adresa 161.53.
Broj **255** koristi se za slanje nekih podataka na sve računara. Naprimjer, adresa 161.53.255.255 odnosi se na sve računare u mreži 161.53. Ako pošaljete neke podatke na tu adresu, oni će doći do svih računara u mreži 161.53.
Oznaka mreže **127** također je rezervirana (nema je u tablici). Adrese koje počinju sa 127 imaju posebnu primjenu; radi se o tzv. **loopback** adresama (povratnim adresama) koje se koriste za testiranje rada mreže. Mrežne poruke i paketi koji su adresirani na mrežu 127 nikada neće otići dalje u mrežu, već će se vratiti nazad. Posebno je zanimljiva adresa 127. 0. 0. 1, jer ona uvijek označava taj isti računar.
**Zadnji broj** u IP adresi ne smije biti 0 ili 255 (osim u gornja dva posebna slučaja).
**Prvi broj** također ne smije biti veći od 223; brojevi 224 i 225 rezervidane su za neke posebne slučajeve i najčešće se uopšte ne sreću.
Ova su ograničenja ujedno razlog zašto su brojevi mogućih računara i mreža u tablici takvi kakvi jesu.

## Besklasno adresiranje - classless addressing-

*Klasično adresiranje je metoda alokacije IP adrese koja dodjeljuje IP adrese prema pet glavnih klasa: A,B, C, D, E. Besklasno adresiranje je jedna od klasifikacija IP adresa.*

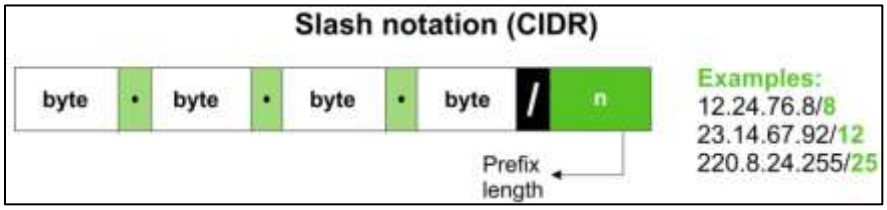
1996. godine uvedeno je besklasno adresiranje i danas gotovo u potpunosti potisnulo klasično, klasno adresiranje. Besklasno adresiranje je metoda raspodjele IP adresa koja je zamišljena kao zamjena za klasično adresiranje kako bi se smanjilo brzo iscrpljivanje IP adresa (prisutno kod iPv4 protokola).




Kod besklasnog adresiranja opsezi adresa koji se dodeljuju organizacijama su blokovi promenljive dužine koji ne pripadaju klasama. Blokovi mogu imati 2 adrese, 4 adresa, 128 adresa itd.

Kod besklasnog adresiranja, adresni prostor ($2^{32}$ adresa) je podeljen na blokove različitih veličina Organizaciji se dodeljuje blok veličine koja najbolje odgovara njenim potrebama.

Pored bitova za adresiranje mreže i čvorova, postoje i bitovi za adresiranje podmreže, tako da je stara podjela na klase je zamjenjena mrežnim prefiksom (**CIDR** *Classless Inter Domain Routing* **notacija** ili notacija sa kosom crtom) – proširenju standardne decimalne notacije gdje se s desne strane dodaje kosa crta i dužina prefiksa izražena kao decimalni broj.




Besklasno adresiranje dozvoljava različite dužine prefiksa. Moguće su dužine prefiksa koje variraju od 0 do 32. Dužina prefiksa ima inverzni odnos sa veličinom mreže. Manja mreža ima veliki prefiks; veći ima mali prefiks.

**Besklasna IP adresa je** sada **uređeni par (A,M).**

IP adresa A se dijeli na sufiks i prefiks pomoću adresne maske M.

Adresna maska M je dodatni 32-bitni broj, koji počinje nizom uzastopnih jedinica a završava nizom uzastopnih nula. Jedinice u M označavaju mjesta u A koja pripadaju prefiksu, a nule u M označavaju mjesta u A koja čine sufiks.

Da bi zapamtili besklasnu adresu, pamti se ukupno 64 bita umjesto dosadašnjih 32. Prefiks mreže se računa po sljedećoj formuli, gdje znak & označava operaciju „logičko i“ po bitovima.

PR = (A & M).

Besklasne adrese zapisuju se u ljudima čitljivijem formatu pomoću takozvane CIDR notacije.

| CIDR Block Size | Exponential Notation | Number of Addresses |
|---|---|---|
| /24 | $2^8$ | 256 |
| /23 | $2^9$ | 512 |
| /22 | $2^{10}$ | 1,024 |
| /21 | $2^{11}$ | 2,048 |
| /20 | $2^{12}$ | 4,096 |
| /19 | $2^{13}$ | 8,192 |
| /18 | $2^{14}$ | 16,384 |
| /17 | $2^{15}$ | 32,768 |
| /16 | $2^{16}$ | 65,536 |

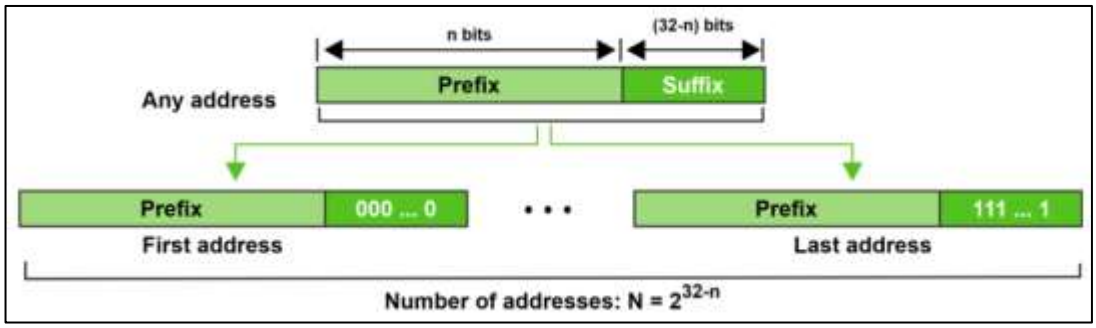
Glavnu ulogu u podjeli na podmreže ima parametar interfejsa mrežna maska (netmask). Svaki njen bit odgovara odgovarajućem bitu u IP adresi.

Vrijednost bita, 1, znači da odgovarajući bit IP adrese predstavlja bit adrese mreže.

Vrijednost bita, 0, znači da odgovarajući bit IP adrese predstavlja adresu hosta u toj mreži.

Uređeni par IP adrese i adresne maske se zapisuje u CIDR notaciji **kao na primjer 128.10.2.3/16**.

U ovom primjeru maska se sastoji od 16 jedinica i 16 nula, u decimalnoj notaciji ta maska bi bila 255.255.0.0 pa bi za zadanu IP adresu dala prefiks 128.10.0.0.




S obzirom na bilo koju adresu u bloku, obično želimo da znamo tri stvari: broj adresa u bloku, početnu adresu u bloku i posljednju adresu. Ove tri informacije, koje su prikazane na donjoj slici, lako je locirati jer je poznata dužina prefiksa n.

- Blok ima N = $2^{32-n}$ adresa, prema proračunu.
- „Najlijevih" n bitova se čuvaju, a (32 - n) krajnjih desnih bitova se postavljaju na nule da bi se odredila prva adresa.
- „Najlijevih" n bitova se čuvaju, dok su (32 - n) krajnji desni bitovi postavljeni na 1 da bi se odredila posljednja adresa.

| **IP adresa i mrežna maska** | | | | |
|---|---|---|---|---|
| 212.62.48.34 | 11010100. | 00111110. | 00110000. | 00100010 |
| 255.255.255.192 | 11111111. | 11111111. | 11111111. | 11000000 |
| AND | | | | |
| Subnet | Adresa | | | |
| 212.62.48.0 | 11010100. | 00111110. | 00110000. | 00000000 |
| Broadcast | Adresa | | | |
| 212.62.48.63 | 11010100. | 00111110. | 00110000. | 00111111 |
| prefiks /26 | | | | |

| **IP adresa i mrežna maska** | | | | |
|---|---|---|---|---|
| 131.108.2.2 | 10000011. | 01101100. | 00000010. | 00000010 |
| 255.255.255.0 | 11111111. | 11111111. | 11111111. | 00000000 |
| AND | | | | |
| Subnet | adresa | | | |
| 131.108.2.0 | 10000011. | 01101100. | 00000010. | 00000000 |
| Broadcast | adresa | | | |
| 131.108.2.255 | 10000011. | 01101100. | 00000010. | 11111111 |
| prefiks /24 | | | | |

*Dva primjera korištenja mrežne maske za određivanje CIDR prefiksa*

| IP Addresses | Bits | Prefix | Subnet Mask |
|---|---|---|---|
| 1 | 0 | /32 | 255.255.255.255 |
| 2 | 1 | /31 | 255.255.255.254 |
| 4 | 2 | /30 | 255.255.255.252 |
| 8 | 3 | /29 | 255.255.255.248 |
| 16 | 4 | /28 | 255.255.255.240 |
| 32 | 5 | /27 | 255.255.255.224 |
| 64 | 6 | /26 | 255.255.255.192 |
| 128 | 7 | /25 | 255.255.255.128 |
| 256 | 8 | /24 | 255.255.255.0 |
| 512 | 9 | /23 | 255.255.254.0 |
| 1 K | 10 | /22 | 255.255.252.0 |
| 2 K | 11 | /21 | 255.255.248.0 |
| 4 K | 12 | /20 | 255.255.240.0 |
| 8 K | 13 | /19 | 255.255.224.0 |
| 16 K | 14 | /18 | 255.255.192.0 |
| 32 K | 15 | /17 | 255.255.128.0 |
| 64 K | 16 | /16 | 255.255.0.0 |
| 128 K | 17 | /15 | 255.254.0.0 |
| 256 K | 18 | /14 | 255.252.0.0 |
| 512 K | 19 | /13 | 255.248.0.0 |
| 1 M | 20 | /12 | 255.240.0.0 |
| 2 M | 21 | /11 | 255.224.0.0 |
| 4 M | 22 | /10 | 255.192.0.0 |
| 8 M | 23 | /9 | 255.128.0.0 |
| 16 M | 24 | /8 | 255.0.0.0 |
| 32 M | 25 | /7 | 254.0.0.0 |
| 64 M | 26 | /6 | 252.0.0.0 |
| 128 M | 27 | /5 | 248.0.0.0 |
| 256 M | 28 | /4 | 240.0.0.0 |
| 512 M | 29 | /3 | 224.0.0.0 |
| 1024 M | 30 | /2 | 192.0.0.0 |
| 2048 M | 31 | /1 | 128.0.0.0 |
| 4096 M | 32 | /0 | 0.0.0.0 |

Za dobijanje adrese mreže vrši se operacija AND nad bitima IP adrese i mrežne maske, a za dobijanje adrese hosta u mreži vrši se operacija AND nad bitima IP adrese i invertovanim bitima mrežne maske, s tim da se vodeći bajtovi sa vrijednošću nula ne pišu.

# Adresiranje

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

Mrežni sloj ima ulogu da nadzire isporuku paketa od izvora do odredišta koji se mogu nalaziti i u različitim mrežama (odnosno nisu povezani na isti link). U slučaju kad su dva uređaja odnosno sistema povezana na isti link, ne postoji potreba za mrežnim slojem. Ali kad su uređaji povezana na različite mreže (linkove), sa uređajem za međumrežno povezivanje između njih, mrežni nivo je neophodan, a njegov zadatak je regulacija protoka paketa između dva sistema.
Kada peketi prelaze granice podmreža, mogu nastati brojni problemi. Fizičko adresiranje koje se koristi u drugoj mreži se može razlikovati od onoga koje važi u prvoj. Paket koji stiže iz jedne podmreže može biti previše veliki da bi se u drugoj mreži prenio jednim okvirom. Mogu se razlikovati protokoli nižeg nivoa. Na sloju mreže je da riješi sve ove probleme.

Radi jednostavnijeg rada adresiranje se provodi preko tri nivoa (tipa):

1. Fizičko na hardverskom nivou (preko hardverskog interfejsa i MAC adresiranja)
2. Logičko na nivou mrežnog i međumrežnog povezivanja (korištnjem IP adrese). Logičke adrese izvora i odredišta, sadržane su u zaglavlju sloja mreže.
3. Korisničko – simboličko

Primjeri adresa:

1. MAC jednoznačne adrese uređaja, koji prepoznaju drugi uređaji u mreži (hardversko adresiranje uređaja, Primjer. 00-B0-D0-86-BB-F7
2. IP adresa prilagođena računarima (numerička adresiranje primjer: 168.247.192.02)
3. DNS/FQDN adrese prilagođene ljudima (simboličko adresiranje primjer www.sveznadar.info)

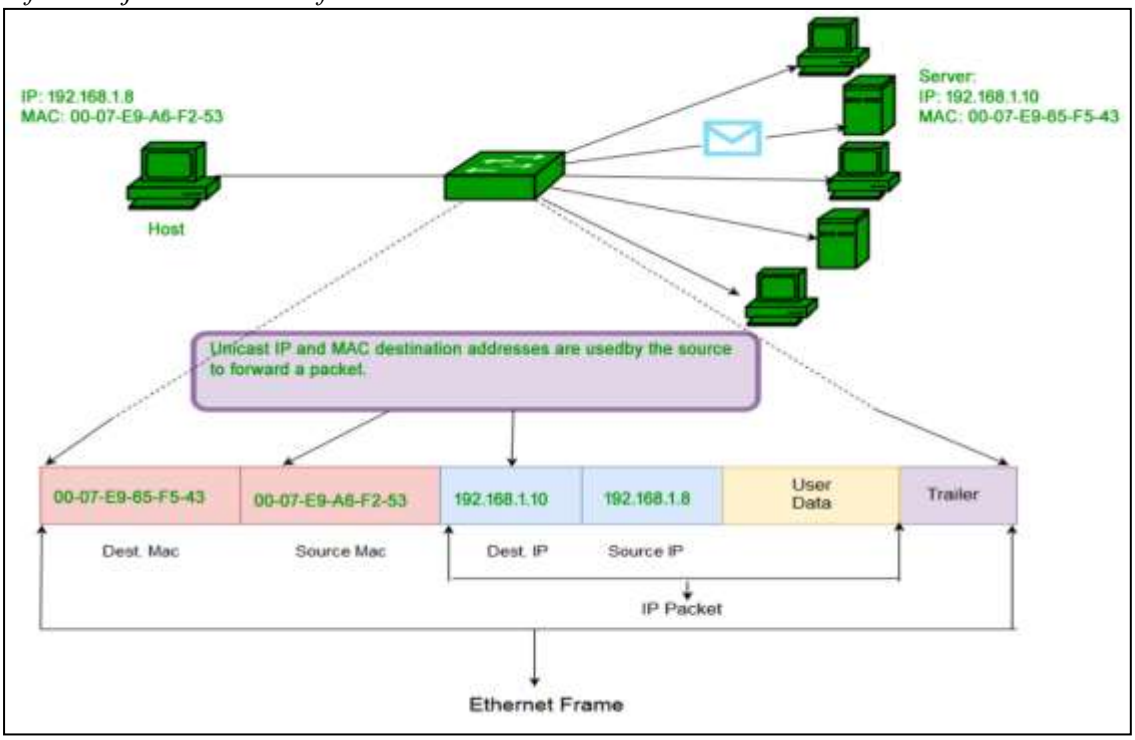
Fizičko adresiranje koje se realizuje na nivou sloja veze, rješava problem adresiranja lokano, na nivou zajedničkog linka. Složena mreža, formirana povezivanjem više, moguće različitih podmreža, koje koriste različite šeme fizičkog adresiranja, zahtijeva uvođenje logičkih (ili mrežnih) adresa, koje će biti jedinstvene na nivou cjelokupne mreže.

Na velikoj mreži kakav je Internet, **najveći je problem bio osmisliti sistem obilježavanja i imenovanja računara**, koji će koristiti svi protokoli, usluge. Ranije su djelomično objašneni MAC i IP adresiranje. To ćemo dodatno razjasniti uz objašnjenje korisničkog nivoa koji koristi ARP protokol i FQDN i DNS sistem adresiranja.

# Hardversko MAC adresiranje

U većini LAN-ova paketi putuju kroz zajednički medij te su vidljivi svim spojenim računarima. Javlja se problem: kako ostvariti prenos okvira od pošiljatelja *tačno određenom* primatelju? Rješenje se zasniva na dodjeljivanju takozvanih *hardverskih (fizičkih) adresa* računarima.

Mada je to objašnjeno (Adresa kontrole pristupa medijima -MAC-) zbog važnosti da još jednom naglasimo:
*Eternet predstavlja skup tehnologija i protokola primjenjenih unutar LAN mreža.*
*Na fizičkom nivou Eternet definiše raspored ožičenja, te vrste i nivoe signala za prenos podataka.*
*Na logičkom (nivou podataka) Eternet definiše način pristupa mediju za prenos podataka i definiše zajednički adresni format.*

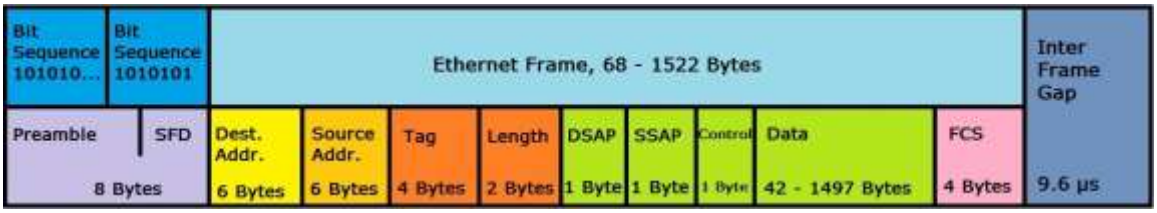



*Ilustracija korištenje MAC adrese kod slanja poruke u Ethernet okviru*

Jedinstveni identifikator – MAC adresa (*hardwar-eska* adresa, *ethernet* adresa) je sadržana u svim mrežnim karticama i svim ugrađenim mrežnim adapterima u mrežnim uređajima (*router, switch*).

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 orjentisan je prema fizičkom sloju i ima zadaću upravljati pristupom mediju.
Svaki okvir uz ostale podatke mora sadržavati adresu pošiljatelja te adresu primatelja. Prilikom slanja okvira, pošiljatelj upisuje u okvir svoju vlastitu adresu, te adresu računara kojem se okvir šalje.

Računar spojen na LAN ispituje adrese unutar svakog okvira koji prolazi mrežom, prihvaća (kopira) one gdje se adresa primatelja poklapa s njegovom vlastitom adresom, te ignoriše ostale. To znači da format okvira u stvarnim LAN tehnologijama, osim samih podataka koji čine koristan teret, takođe mora predvidjeti i dodatne informacije. Dobar primjer za to je Ethernet-ov okvir, gdje se uz same podatke i CRC zaista nalaze i obje adrese, te informacija o tipu sadržaja okvira. **Posao praćenja okvira koji u LAN-u prolaze zajedničkim medijem** prilično je zahtjevan.
Postoji više verzija Ethernet okvira, a verziju prilagođenu za VLAN možete pogledati na slici ispod:




*Struktura okvira Ethernet 802.3 sa oznakama (tag).*
*Polje oznake sadrži važne informacije za VLAN integraciju.*

Prilikom slanja podataka, CPU šalje okvir svojoj mrežnoj kartici (LAN interfejsu) i zahtijeva slanje. Nakon toga CPU može nastaviti s izvršavanjem aplikacijskog programa, a LAN interfejs čeka na pristup zajedničkom mediju i šalje okvir.
Primanje podataka odvija se tako da mrežna karta prati sve okvire koji putuju zajedničkim medijem, filtrira one s ispravnom i odgovarajućom adresom primatelja, te ih prosljeđuje CPU jedinici.

Svaki *Ethernet* okvir sadrži: zaglavlje, podatke koje prenosi i kontrolne podatke.

*Ethernet* okvir je maksimalne dužine 1522 bajta (ranije verzije 1518 bajtova). Preambula je karakterističan niz 101010101010.... koji označava početak okvira. Svaki Ethernet okvir sadrži (MAC) – fizičke adrese izvorišta i odredišta.
Polje rezervisano za adresu odredišta sadrži adresu primaoca; koja može biti i takozvana *multicast* adresa kada se podaci šalju za grupu računara ili *broadcast* adresa koja se koristi kada je potrebno da se paket prenese svim ostalim *Ethernet* stanicama u lokalnoj mreži.

U normalnom radu *Ethernet* adapter prima samo pakete koji u polju adrese primaoca imaju njegovu vlastitu adresu ili adresu koja predstavlja *broadcast* ili *multicast* adresu. Sve ostale *Ethernet* pakete kartica osluškuje ali ih ne prima jer su namjenjeni nekom drugom računaru koji se nalazi u istoj lokalnoj mreži.

*Ethernet* adapter može biti setovan da prima sve pakete koji se pojavljuju u medijumu. Moguće je snimati saobraćaj u mreži i kasnije analizirati događaje sa ciljem da se utvrdi nepravilnost u radu neke kartice ili računara. Ova osobina može da se koristi i za prisluškivanje saobraćaja na mreži što treba uzeti u obzir kada je važna sigurnost podataka koji se prenose kroz mrežu.

Dva bajta nakon MAC adresa određuju dužinu podataka koji se prenose u *Ethernet* okviru ili to može biti tip protokola na višim slojevima.

Maksimalna dužina podataka koji se prenose u *Ethernet* paketu je 1500 bajtova a sam sadržaj je prepušten mrežnom sloju.

Na kraju *Ethernet* paketa su kontrolni podaci - CRC (*Cyclical Redundancy Check*). Kontrolni podaci služe za detekciju greške koja može da se javi u toku prenosa *Ethernet* paketa preko fizičkog sloja. Princip detekcije greške je zasnovan na matematičkoj operaciji koja se izvodi nad celim *Ethernet* paketom. Rezultat matematičke operacije predstavlja kontrolni podatak (CRC).

Kada paket stigne na odredište, ista matematička operacija se izvrši ponovo pa ako rezultat nije identičan sa CRC podatkom upisanim na kraju *Ethernet* paketa - detektovana je greška u prenosu *Ethernet* paketa. *Ethernet* stanica koja primi paket i detektuje grešku u prenosu odbacuje paket. Problem izgubljenih podataka u mrežnom saobraćaju rešava transportni sloj (četvrti sloj po OSI modelu) ili sama aplikacija koja prima paket.

## Dodjeljivanje LAN adresa i utvrđivanje sadržaja

Postoje tri metode za dodjeljivanje adresa računaru unutar jednog LAN-a:


• *Statičko dodjeljivanje.* Koristi se adresa koji je proizvođač LAN interfejsa[18] ugradio u svoj uređaj i koja je jedinstvena na cijelom svijetu. Osobina statičkog dodjeljivanja je da je adresa računara stalna, čak i onda kad ga selimo iz mreže u mrežu, sve dok mu ne promijenimo mrežnu karticu. Takođe, uređaji raznih proizvođača mogu se odmah bez podešavanja adresa uključiti u istu mrežu.

• *Dinamičko dodjeljivanje.* Svojstvo dinamičkog dodjeljivanja je da eliminiše potrebu da proizvođači hardvera koordiniraju svoje adrese. Takođe, dinamičke adrese mogu biti znatno kraće od statičkih. Računar automatski bira adresu svaki puta kad se upali. Obično je riječ o biranju slučajnih brojeva, sve dok se ne pogodi slobodna adresa.

• *Konfigurabilno dodjeljivanje.* Konfigurabilne adrese su kompromis između statičkih i dinamičkih. Slično kao statičke, one su relativno stalne. Slično kao dinamičke, one mogu biti kratke. Administrator mreže svakom računaru postavlja adresu koju je sam izabrao. Postavljanje adrese se obavlja pomoću sklopki na LAN interfejsu ili upisivanjem u EPROM interfejsa.

Ranije je objašnjeno da je broadcasting prenos podataka gdje jedan računar šalje iste podatke svim drugim računarima u mreži. Kod LAN tehnologija ovakav prenos se može jednostavno i efikasno izvesti zato što podaci ionako putuju zajedničkim medijem i "vidljivi" su svim računarima. Uz postojeće adrese računara u LAN-u, uvodi se i dodatna (rezervirana) "broadcast" adresa.

[18] Ranije je djelimično objašnjena uloga i komponente mrežna kartica kao praktične implementacije LAN interfejsa

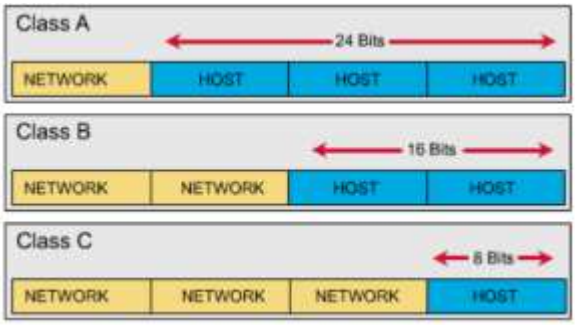
LAN interfejs u svakom računaru se konfiguriše i "prepravlja" se tako da filtrira takođe i okvire čija adresa primatelja je jednaka broadcast adresi. Dakle kada okvir pošaljemo na broadcast adresu, svaki računalo u mreži primit će kopiju tog okvira.
Slično je i kod multicasting prenosa podataka. Jednan računar šalje iste podatke grupi "pretplaćenih" računara. Uvode se dodatne "multicast" adrese. Svaka od tih adresa odgovara jednoj grupi računara. LAN interfejs računara koje je uključeno u grupu podešava se tako da osim vlastite i broadcast adrese "prepoznaje" i dotičnu multicast adresu.

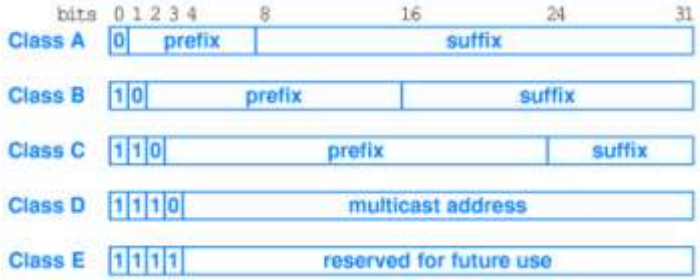
Iz samog sadržaja okvira teško je zaključiti koja vrsta podataka se nalazi u tom okviru.
Npr okviri koji nose e-mail poruke, tekstualne datoteke ili web stranice svi sadrže ASCII znakove.
Da bi primatelj mogao odrediti vrstu nekog okvira, potrebna je dodatna informacija u samom okviru.
Postoje dvije metode za utvrđivanje sadržaja.
• *Eksplicitno navođenje tipa okvira*. Sama mrežna tehnologija predviđa da se u formatu okvira nalazi posebno polje za tip okvira. Također, sama tehnologija svojim standardima definiše identifikatore za neke tipove okvira.
• *Implicitno navođenje tipa okvira.* Korištena mrežna tehnologija u svom formatu okvira ne predviđa polje za tip. Pošiljatelj i primatelj dogovaraju se da će razmjenjivati samo jednu vrstu sadržaja. Ili se dogovaraju da će polje za tip okvira sami uključiti na određeno mjesto u dio okvira koji je inače predviđen za podatke.
Obje metode imaju prednosti i mane. Eksplicitno navođenje je pouzdanije, no obuhvaća samo one tipove okvira koji su prepoznati i standardizirani na razini dotične mrežne tehnologije.
Implicitno navođenje je fleksibilnije no lako može dovesti do nesporazuma.

Vidljivo da podaci koji putuju LAN-om nisu zaštićeni od neovlaštenog čitanja. Svaki korisnik s računarom spojenim na LAN u pravilu vrlo lako može čitati tuđe poruke. Da bi zaštitili podatke, moramo se služiti metodama kao što je kriptovanje.

# IP adrese Internet protokola

Da bi mogli izvršiti generalizaciju koja dopušta dizajniranje i projektovanje mreža različitih konfiguracija ovdje ćemo koristiti virtuelne mreže. Pod tim pojmom podrazumjevaćemo bilo kakvu mrežu koja ima osobine LAN mreže.
Virtuelnu mrežu možemo realizirati isključivo ukoliko svi čvorovi koriste jedinstven sistem adresiranja. U takvoj virtuelnoj mreži **sistem adresiranja mora biti nezavisan o fizičkim adresama.**
Rezultat je da dva aplikacijska programa ili dva korisnika izmjenjuju poruke bez znanja fizičkih adresa. Informaciju o fizičkim adresama trebaju samo niži slojevi protokola. IP adresiranje stvara dojam velike homogene mreže s jedinstvenom uslugom. Adresiranje u stogu protokola TCP/IP je određeno i*nternet protokolom* - IP.
Svaki čvor u mreži ima 32-bitni[19] broj koji se naziva ***internet protocol address*** ili skraćeno ***IP adresa***.
Svaki paket koji se šalje kroz virtuelnu mrežu u zaglavlju ima IP adresu polaznog i dolaznog čvora. Sva komunikacija se odvija jedino korištenjem IP adresa.



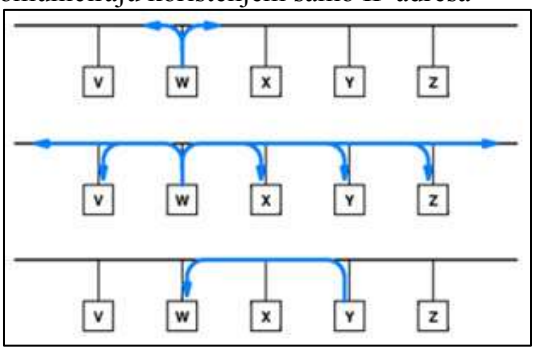

*Adresa mreže* (prefiks) jednoznačno određuje i identifikuje fizičku mrežu u kojoj se čvor nalazi.
*Adresa čvora* (sufiks) označava pojedinačni čvor u mreži.
Svaki čvor ima jedinstvenu IP adresu koja je uređeni par (prefiks, sufiks).

Ovakva hijerarhijska struktura Internet adresa olakšava usmjeravanje-rutiranje, kao i administriranje Interneta. Naime, administriranje mrežnih adresa je globalno, a sufiksa lokalno.

[19] Za objašnjenje adresiranja koristiće se iPv4 protokol, a gotovo identični principi važe i za iPv6

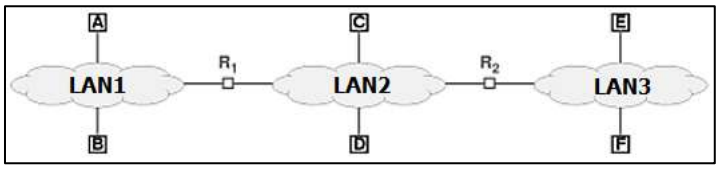
# Pretvaranje IP-adrese u hardversku
# ARP Protokol za rješavanje adresa

Pošto su realizovane softverski može se reći da su IP adrese virtuelne.
Koriste ih viši slojevi protokola. Hardverski sloj ne razumije virtualne IP adrese. Okviri koji nemaju korektnu fizičku adresu ne mogu biti preneseni kroz fizičku mrežu.
To nameće potrebu potreba za prevođenjem virtuelne (IP) u fizičku adresu (MAC) i obrnuto.
Preslikavanje između virtualne IP adrese i fizičke adrese se zove rješavanje adresa (*address resolution*). Dio TCP/IP stoga koji rješava ove probleme se zove *ARP* (Adress Resolution Protocol) **Protokol za rješavanje adresa ARP**. ARP standard specificira slanje ARP poruka kroz mrežu, a ARP zahtjev se šalje svima kao difuzija (broadcast). Odgovor se šalje u okviru koji je namjenjen samo čvoru koji je poslao difuzijsku poruku.
U hijerarhiji stoga protokola ARP protokol razdvaja (otuda ono resolution u imenu) više i niže slojeve protokola. ARP softver sakriva detalje fizičke mreže tako što omogućava višim slojevima protokola da komuniciraju korištenjem samo IP adresa




*Ilustracija slanja poruka u skladu s ARP protokolom (poruka svima odgovor onome ko je poslao)*

ARP protokol se najčešće koristi za prevođenje 32-bitnih IP adresa u 48-bitne Ehternet adrese. Standard određuje samo generalni oblik ARP poruke. Posebno, određeno je da se cijela ARP poruka transportuje unutar fizičkog okvira kao njen korisni sadržaj. Dakle riječ je o *enkapsulaciji* poruka. Više puta objašnjena tehnika enkapsulacije predviđa da se u zaglavlju okvira specificira tip poruke koja je u okviru. Razlikovanje među različitim ARP porukama moguće je tek analizom ARP poruke.




**Primjer 1.**
Ako host "A" koji zahtijeva slanje IP paketa hostu "B", ne zna Ethernet adresu koju domaćin "B" ima, tada šalje ARP zahtjev putem emitiranja.
Host "B" će, ako ima vlastitu IP adresu, zapamtiti IP adresu podnositelja zahtjeva, a zatim odgovoriti na zahtjev. Kada zahtjev stigne na host „B", ono što se čini je da se zapamti navedeni zahtjev u lokalnu tablicu pod nazivom ARP predmemorija.

**Primjer 2.**
Ako imate dva hosta u različitim mrežama, koji se zovu "1" i "2", kada "1" treba prenijeti paket na "3", ovaj element mora doći iz mreže "1".

Stoga, budući da je u različitim mrežama, "1" će prenijeti ono što je potrebno na fizičku adresu usmjerivača, na njegovom izlazu. Ova fizička adresa može se dobiti s IP -a uređaja, sve dok se koristi ARP tablica.

Što bi se dogodilo da se unos ne nađe u tablici? Budući da se paket prenosi svima ruter će prvo provjeriti vlastitu tablicu kako bi pronašao mjesto na koje će poslati svoj paket i poslati ga putem odgovarajućeg interfejsa.

Ponavlja se sa svim srednjim čvorovima dok ne dođe do rutera mreže u kojoj je "C".

Adresa iz daleke fizičke mreže se nikada ne prevodi.

Na slici gore možete vidjeti ilustraciju gdje računar A (iz mreže LAN1) šalje paket -datagram- računru F (u mrežu LAN3). Tada ruter $R_1$ **ne** prevodi IP adresu od F, nego cijeli datagram prosljeđuje kroz srednju mrežu (m2) prema ruteru $R_2$.

Postoje sljedeće tri osnovne tehnike prevođenja adresa:

- pretvaranje adrese *korištenjem tablice* (table lookup),
- pretvaranje adrese *direktnim računanjem* (closed-form computation),
- pretvaranje adresa *izmjenom poruka* (message exchange).

TCP/IP stog protokola može koristiti sva tri navedena tipa prevođenja virtualnih adresa.

Tablice se najčešće koriste za prevođenje adresa u WAN-u.

Prevođenje izračunavanjem se koristi za mreže koje podržavaju konfigurisanje fizičkih adresa.

Prevođenje izmjenom poruka se koristi u LAN-ovima.


*Okvir, te zaglavlje okvira koji nosi ARP poruku*

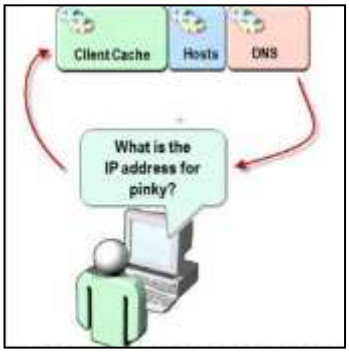

*Format poruka u ARP protokolu*

Napomenimo:

1. IP adresa ne označava računar (host), nego spoj (intrefejs) između računara i mreže.
2. Računari, kao i ruteri, mogu imati vezu s nekoliko mreža. To je tzv multi-homed host princip koji povećava robustnost i performanse mreže.
3. Ruter je čvor u dvije mreže, a protokoli za usmjeravanje ga tretiraju kao i bilo koji drugi čvor u mreži. Zbog toga svaki ruter po TCP/IP protokolu ima svoju IP adresu. **Svaki ruter ima barem dvije pridružene IP adrese**, budući da je:
   - ruter je čvor u više fizičkih mreža,
   - svaka IP adresa ima prefiks koji označava fizičku mrežu.

# DNS sistem

DNS sistem vrši preslikavanje domenskog imena (FQDN) u jednu ili više IP adresa te obrnuto, preslikavanje jedne ili više IP adrese u jedno domensko ime.




Da bi se izbeglo pamćenje IP adresa izmišljen je alternativni sistem imenovanja, tzv. DNS. **DNS je adresna šema koja obezbjeđuje bazu podataka sa imenima računara i odgovarajućim preslikavanjem u jedinstvene IP adrese.**
**DNS (Domain Name System)** je strogo hijerarhijski distribuirani sistem u kojem se mogu nalaziti različite informacije, no prvenstveno one o IP adresama i slovnim nazivima za računare.
Većina operativnih sistema koristi DNS sistem implicitno, pa je moguće nekom računaru na Internetu pristupiti i preko IP adresu i kroz domensko ime - ako ono postoji.

**DNS je sistem distribuirane baze podataka**, koji obezbjeđuje protokol za razrješavanje (resolution) imena krajnjeg računara. Dakle, ako je dato ime računara, DNS može da ga razrješi (tj. preslika, kopira) u njemu odgovarajuću IP adresu.
DNS radi i u drugom smjeru, ako je data IP adresa, DNS može da izvede ime u koje se preslikava ta IP adresa.

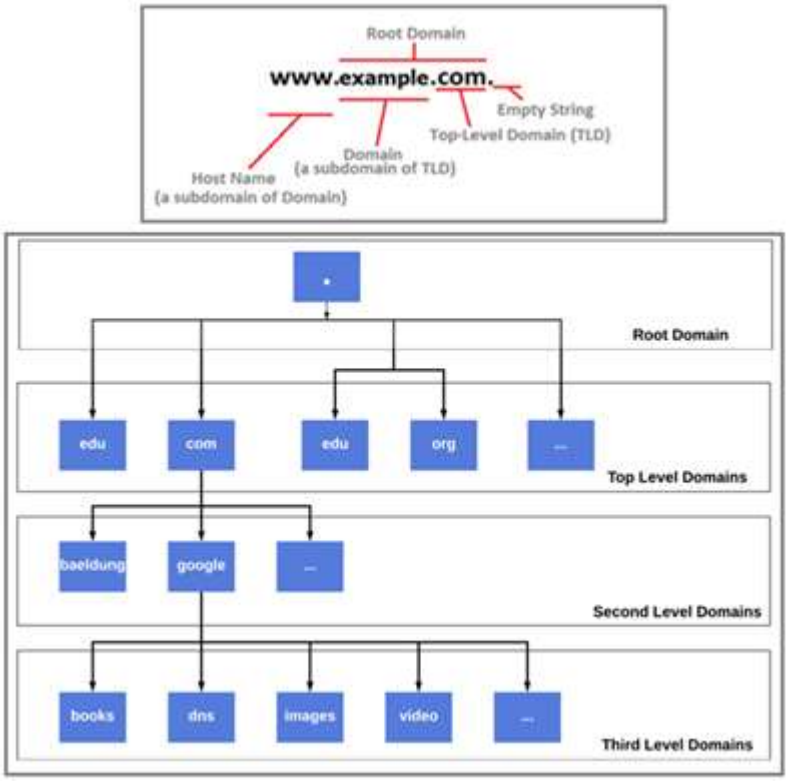
Prethodnik Interneta ARPAnet imao je tekstualna datoteku "hosts.txt". Ona je sadržavala naziv i IP adresu za svako računar, koji se nalazio u mreži.
Kako su mreža i broj korisnika rasli, bilo je sve teže pamtiti IP brojeve. Zbog toga je 1984. godine razvijen prvi Domain Name System (DNS), tj. distributivna baza podataka koja u osnovi sadrži sva imena svih računara i opreme koja su spojena na Internet, čime su Internet adrese dobile današnji oblik.
1998. je formiran ICANN (International Corporation for Assigned Names and Numbers - www.icann.org) - neprofitna, privatna korporacija, koja koordinira tehničkim upravljanjem Internet Domain Name Sistema, raspodjelom IP adresa, parametara Internet protokola i brojeva portova. ICANN je objedinio veliki broj kompanija - registranata širom svijeta koje Internet korisnicima omogućavaju registraciju domena i tako je nastao Shared Registration System koji se i danas primjenjuje.

Slovni nazivračunara (engl. hostname) je jedinstveno simboličko ime unutar pojedine mreže kojim se koriste neki protokoli (SMTP, NNTP) za elektroničku identifikaciju nekog računara. Takvi slovni nazivi mogu biti samo jedna riječ, ako se recimo radi o lokalnoj mreži; ili nekoliko riječi odvojenih tačkama. Klijentima DNS informacije pružaju DNS serveri (DNS servers), koristeći DNS protokol za komunikaciju kako sa klijentima tako i međusobno.

*Kod interneta: DNS je glavni indeks interneta koji usmjerava promet za upite širom weba. Najjednostavnija analogija je ona sa listom kontakata na vašem telefonu: kontakti se sortiraju po imenu, ali onda sadrže određene telefonske brojeve ili adrese.*

# Domensko ime i potpuno kvalificirano ime domena FQDN

Domensko ime je simboličko ime računara na Internetu koje ga jednoznačno[20] određuje.
DNS sistem vrši preslikavanje domenskog imena u jednu ili više IP adresa te obrnuto, preslikavanje jedne, ili više IP adrese u jedno domensko ime.
Potpuno kvalificirano ime domene (FQDN[21]), koje se ponekad naziva i apsolutno ime domena, je ime domena koje specificira njegovu tačnu lokaciju u hijerarhiji stabla sistema imena domena. On specificira sve nivoe domena, uključujući domen najvišeg nivoa i korijensku zonu. Potpuno kvalificirano ime domene odlikuje se nedostatkom dvosmislenosti: može se tumačiti samo na jedan način.




*Ilustracija DNS hijerarhijske strukture koja određuje FQDN ime*

**Labela** (label) je alfanumerički niz znakova dug maksimalno 63 znaka. Više takvih labela se međusobno odvajenih tačkama čine domensko ime, **koje se u potpunoj formi kada su navedene sve labele zove i FQDN** (Fully Qualified Domain Name).
Svaka labela mora se sastojati od 1 do 63 znaka (*ne mogu se koristiti dvije uzastopne tačke*), a ukupni FQDN ne smije premašiti ukupno 255 znakova.

[20] Postoji mogućnost da više računara dijeli jedno domensko ime, ali su izuzetci kojima se ovdje nećemo baviti
[21] Termin – "Potpuno kvalifikovano ime domene" definiše konvenciju imenovanja, ali termin FQDN se odnosi na "Puno ime hosta" u odnosu na termin – "Host" daje samo ime hosta bez protokola.

Labele se sastoje od isključivo alfanumeričkih znakova i znaka "-" (dakle ASCII znakovi od A do Z i znak "-"), pri čemu se labele ne razlikuju po velikim i malim slovima[22]. Svaka labela na početku mora imati slovo ili broj.

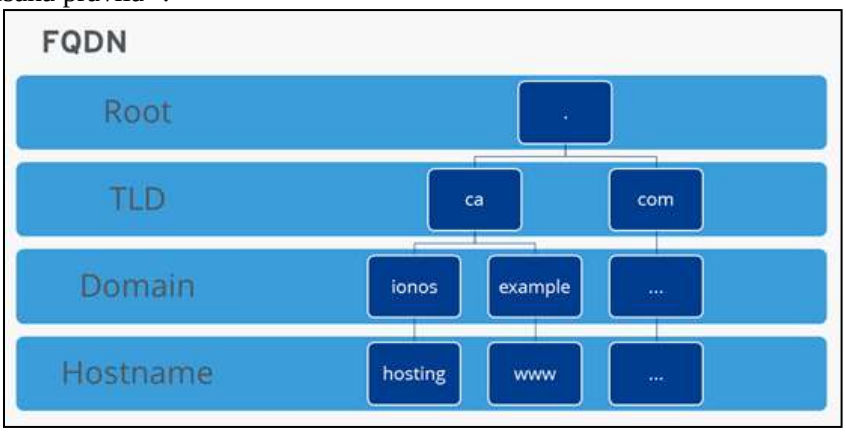
Da bi se FQDN dodatno razlikovao od labela odnosno standardnih (ne nužno potpunih) domenskih imena, česta je konvencija dodavanja dodatne tačke (znaka ".") na kraj domenskog imena.

**U** pojedinom domenu, odnosno **domenskom prostoru ne mogu postojati dvije iste labele** - što znači niti dvije poddomena niti dva računara istog imena.

Na većini modernih operativnih sistema se DNS sistem koristi implicitno, pa je moguće nekom računaru na Internetu pristupiti kako kroz odgovarajuću IP adresu, ali i kroz domensko ime - ako ono postoji.

## Vršne domene TLD i domenski registri

Domenska imena su obično grupisana i završavaju pojedinom grupom labela za koje postoje tačno definisana pravila[23].




*Šematski prikaz strukture hijerarhije potpuno kvalificiranih imena domena*

Takve vršne-završne labele se nazivaju TLD (Top-Level Domain) imena, kojih postoje dva[24] tipa:

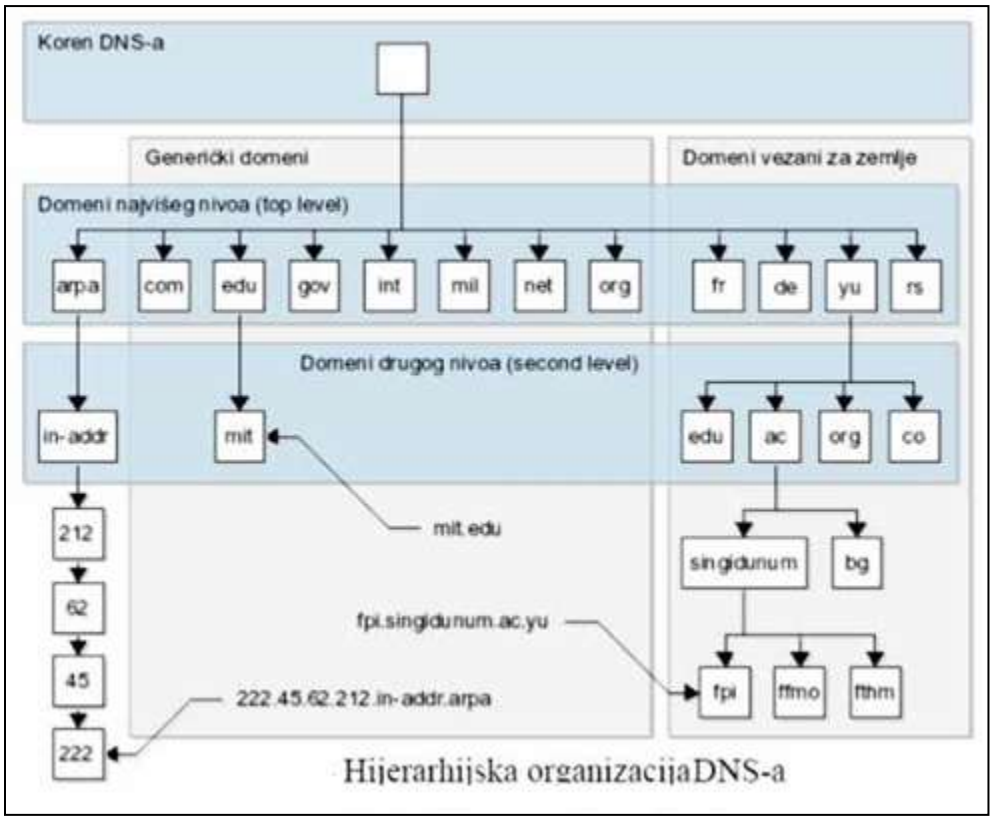
- **geografski bazirane domene**, tzv. **ccTLD** (*country code TLD*) domene koje predstavljaju državni dvoslovni kod baziran na ISO-3166 standardu, a danas ih ima preko 240 u upotrebi

[22] Ipak je preporuka da koristite mala slova

[23] Ovdje data hijerahijska struktura propisana je od strane ICANN. Postoje i različite organizacije koje nude alternativne vršne DNS servere, nudeći najčešće i vlastiti skup TLD-eva, nekompatibilan sa ICANN-ovom listom, npr. ORSC (Open Root Server Confederation), OpenNIC, Pacific Root, New.Net; i najorganiziraniji ORSN (Open Root Server Network) koji ima direktnu kompatibilnost sa ICANN-ovom bazom.

[24] *Spomenimo da postoji i **infrastrukturni top-level** domeni: **jedini** u ovoj grupi je **arpa** domen, ali on se najčešće svrstava u domene.*

- **generičke domene**, tzv. **gTLD** (*generic TLD*) domene koje se obično sastoje od 3 ili više slova.




Krajnje desna labela je TLD (Top-Level Domain), a svaka druga labela lijevo je poddomena - domena koja je hijerarhijski ispod prethodne. Ukupno maksimalno podjela može biti 127, dok se držimo zadane granice od 255 znakova za FQDN. Na kraju, **labela koja je krajnje lijeva je kratko ime računara** (već spomenuti slovni naziv računara -**hostname**, dakle bez domene).

Slično kao i za IP adrese, postoje **domenski registri**, baze podataka o domenama i odgovarajućim IP adresama, po jedan za svaku TLD.
Domenske registre dodjeljuju i održavaju specijalne ustanove poznate kao NIC (Network Information Centre), to su najčešće neprofitne ili državne organizacije.
Informacije o registracijama su dostupne kroz **Whois sistem,** pa je tako za Evropu nadležan whois.ripe.net server.
Za ccTLD-ove su obično nadležne vlade pojedine države, dok je za gTLD nadležan isključivo ICANN.
Zadnja oznaka u ccTLD imenu najčešće je oznaka države[25] (ba za Bosnu i Hercegovinu, rs za Srbiju, hr za Hrvatsku, si za Sloveniju, de za Njemačku, uk za Veliku Britaniju, fr za Francusku, au za Australiju itd. No, u slučaju računara lociranih u SAD (najčešće) nema oznake us, već na tom mjestu stoji oznaka tipa mreže u kojoj se nalazi računar.

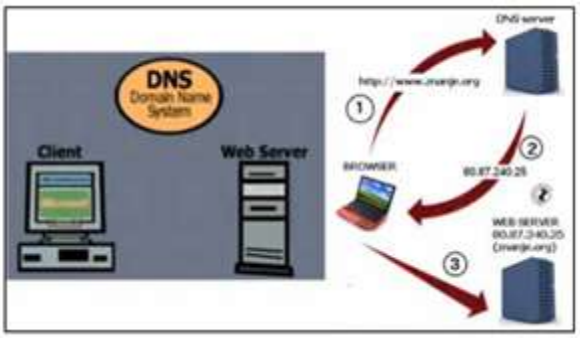
[25] državni domen koji je identičan dvoslovnoj oznaci države prema ISO 3166 standardu.

Tako **edu** označava obrazovnu ustanovu, **com** komercijalnu organizaciju, **gov** vladinu ustanovu, **mil** vojni računar, **org** neku međunarodnu organizaciju, **net** neku mrežu koja se prostire na većem području ili pruža mrežne usluge itd.

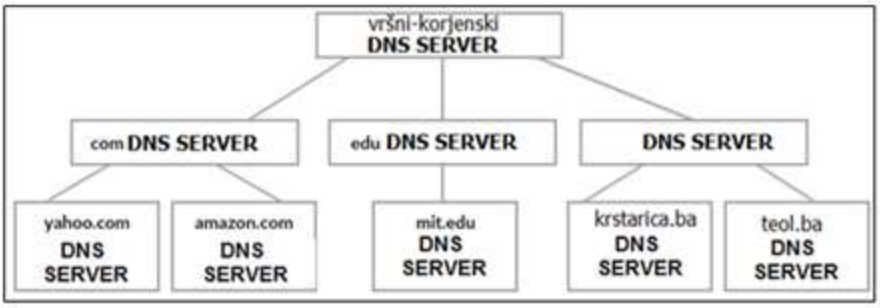
IANA (The Internet Assigned Numbers Authority) je nezavisna organizacija sa sjedištem u Sjedinjenim Američkim Državama koja upravlja globalnim domenskim internetskim prostorom, kao i sistemom središnjih (root) servera koji osiguravaju funkcioniranje DNS sistema.
ICANN (Internet Corporation for Assigned Names and Numbers) je neprofitna internetska korporacija sa sjedištem u Marina Del Rey-u (Kalifornija, Sjedinjene Američke Države) za dodjeljivanje imena i brojeva, a upravlja sistemom imenovanja domena najvišeg nivoa na Internetu.
NIC.BA/Registrator je web aplikacija na kojoj se vrši rezervacija naziva .ba domena i koja sadrži sve podatke o registrantima registriranih naziva domena. Sadržaj aplikacije je javan i može mu se pristupiti na web stranici http://www.nic.ba. Registar je administrator državnog top level domaina TLD Bosne i Hercegovine .ba, ovlašten od relevantnih institucija, koji je odgovoran za upravljanje i dodjelu naziva domena ispod .ba naziva domena. Registrar je pravno lice koje ispunjava opšte i tehničke uslove za podršku registru naziva .ba domena, a ovlašten je od registra. Registrant-korisnik naziva domena je pravno ili fizičko lice koje u skladu sa Pravilnikom registrira i na određeni vremenski period koristi dodijeljeni naziv domena. RFC (Requests for Comments) je serija zabilješki (vođenih od 1969. godine), a u vezi sa Internetom (prethodno ARPANET).
Aktivacija traženog naziva .ba domena podrazumijeva da je korisnik registru dostavio sve potrebne podatke, uključujući podatke o name serverima i njihovim pripadajućim IP adresama.

## DNS rezolucija i DNS serveri

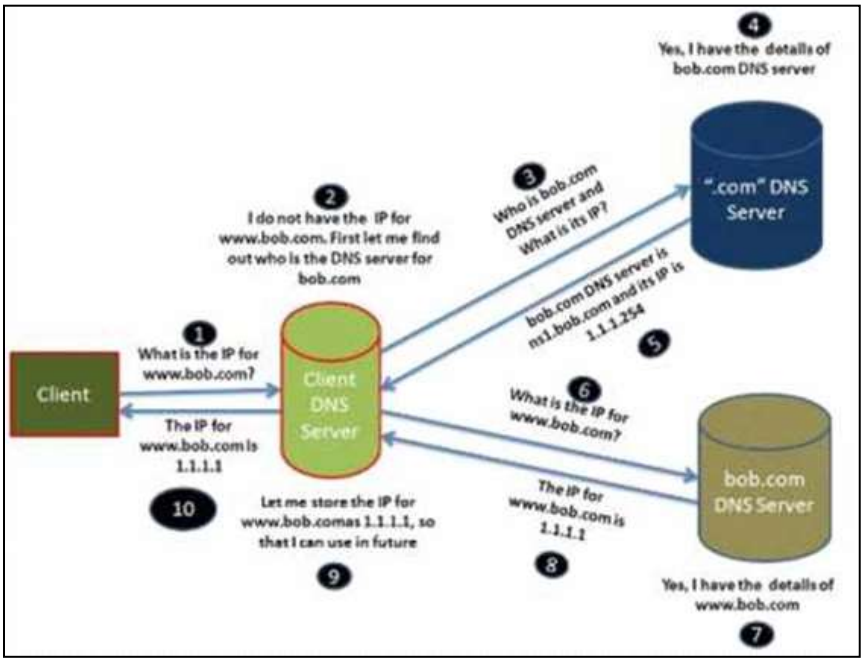
Svaki se funkcionalni DNS sistem nužno sastoji se od tri dijela:




• DNS klijent (resolver), program koji se izvršava na klijentskom računaru i koji formira određeni DNS zahtjev. Takav program je najčešće ugrađen u standardnoj biblioteci u formi sistemskih poziva koje pozivaju različiti korisnički programi
• Rekurzivni (recursive) DNS server, koji nakon dobijenih upita za klijenta obavlja pretraživanje kroz DNS stablo i vraća nazad odgovore klijentima
• Autoritativni (authoritative) DNS server, koji odgovara na upite rekurzivnih servera te vraća ili završni odgovor ili zbog delegiranja vraća referencu na neki drugi autoritativni DNS server.




Proces primanja zahtjeva i njihove obrade te vraćanja odgovora se naziva DNS rezolucija (***name resolution***). Osnovna rezolucija je proces pretvaranja domenskog imena u IP adresu: prvo se traži DNS server, a zatim mu šaljemo upit za adresom, na koji on odgovara sa traženom adresom. Budući da je DNS strogo distribuirana baza, ona je raspodijeljena po mnogo različitih servera.

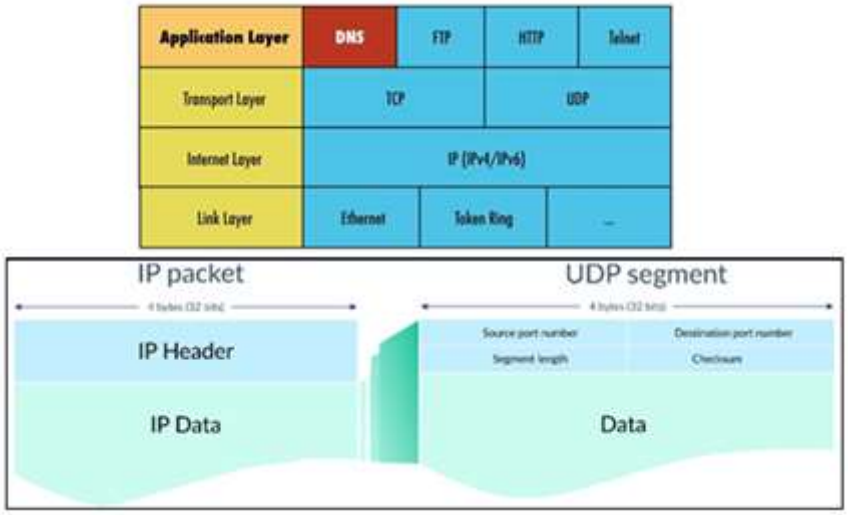



*Ilustracija koja pokazuje kako DNS server traži i pronalazi IP adresu*

No, očigledno je da zbog raspodijeljenosti rezolucija obično ne može biti obavljena kroz samo jedan upit i odgovor, već najčešće zahtijeva dužu komunikaciju i niz upita i odgovora. Najčešća je situacija da klijent šalje zahtjeve lokalnom DNS serveru (koji je direktno nadležan za klijentski računar), koji predstavlja rekurzivni server i obavlja upite te zatim vraća odgovor klijentu. Očigledno, najveći i najkomplikovaniji dio procedure predstavlja traženje autoritativnog servera u složenoj DNS hijerarhiji.

**DNS protokol** se nalazi na najvišem aplikacijskom sloju TCP/IP modela, te je preko interfejsa vezan sa sa TCP protokolom i UDP protokolom nižeg prenosnog nivoa.

DNS serveri koristi standardne portove dodijeljene od IANA-e: TCP/53 i UDP/53. Na njima osluškuje zahtjeve, te može bilo sa dotičnih bilo sa nekog visokog porta (port veći od 1024, zavisno o konfiguraciji servera) poslati odgovor u vidu traženih zapisa odnosno RR-ova (resource record).




*Pozicija UDP-a u OSI modelu i IP paketu*

Standardno se uvijek koristi UDP za upite, a komunikacija se uglavnom svodi na jedan UDP upit i jedan UDP odgovor.
TCP komunikacije se koristi jedino kad veličina odgovora prelazi 512 bajtova ili za grupne prenose DNS informacija, tzv. prenos zone (zone transfer).
Prilikom slanja paketa koristeći UDP preko IP-a, dio podataka svakog IP paketa je formatiran kao UDP segment. Svaki UDP segment sadrži 8-bajtno zaglavlje i podatke promjenjive dužine.
Resolver šalje UDP paket lokalnom DNS serveru koji pronalazi odgovarajuću IP adresu i vraća je resolveru, a on programu koji ga je pozvao.
Taj program sada ima IP adresu te može uspostaviti TCP vezu sa odredištem ili slati UDP pakete.

Svaki od DNS servera brine se o održavanju baze podataka -tablice, s IP i FQDN adresama za svoju domenu, a za ostale domene zna kojem drugom DNS serveru treba proslijediti zahtjev.
Na primjer, ako neko računar želi znati IP adresu računara ftp.teol.ba i pošalje zahtjev DNS serveru, moguća su tri rezultata:

Pri slanju DNS upita moguća su dva scenarija:

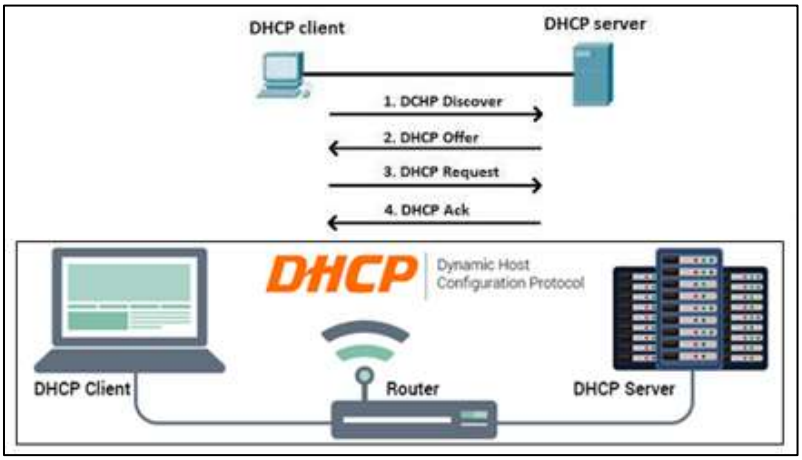
- DNS server odmah **zna** odgovor, jer ga pronalazi u svojoj bazi podataka o računarima te domene.
- DNS server **ne zna** koja je IP adresa i mora pitati drugog servera.

DNS server zna odgovor jer je neko ranije tražio adresu tog računara, pa ju je on sačuvao nakon što ju je saznao od drugog servera (obično se kaže ima je **u kešu**).

Standardni DNS upit je vrlo jednostavan, sadrži uglavnom samo adresu koja se želi razriješiti - no odgovori su vrlo komplikovani jer sadrže sve adrese i zamjenske adrese koje su rezultat upita. Stoga se odgovori obično sažimaju posebnim algoritmima, eliminirajući nepotrebne podatke i smanjujući samu veličinu UDP datagrama. U slučaju da i dalje veličina paketa prelazi 512 bajtova, šalje se parcijalna poruka u obliku UDP paketa sa posebnim bitom postavljenim (TC=1), koji označuje da se upit mora ponoviti koristeći TCP.

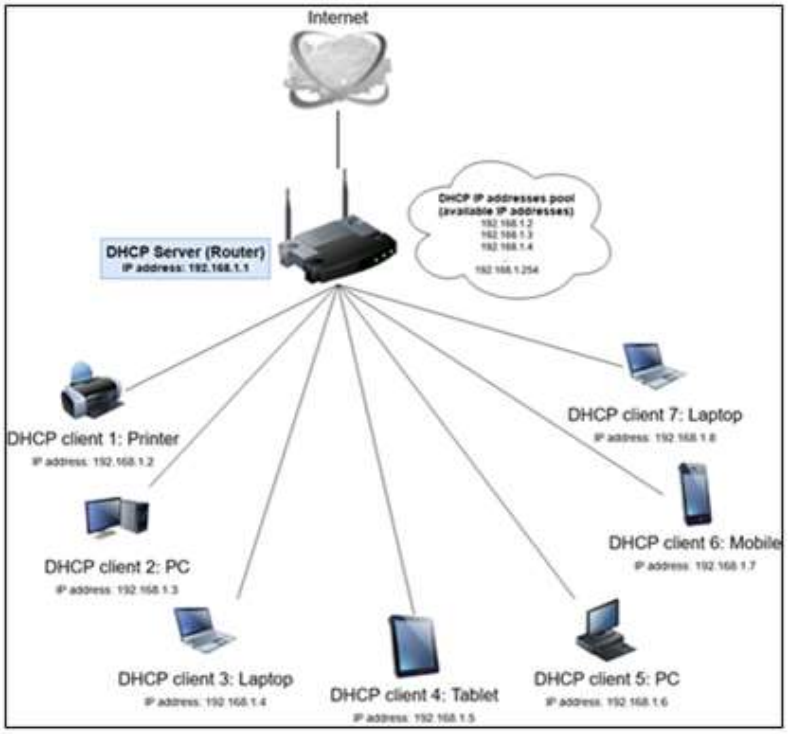
# DHCP: Dinamički protokol konfiguracije hosta

Dinamički konfiguracijski protokol za host (*Dynamic Host Configuration Protocol*) je protokol koji se koristi za pružanje brzog, automatskog i centralnog upravljanja za distribuciju IP adresa unutar mreže.




DHCP se također koristi za konfiguriranje odgovarajuće maske podmreže, zadanog pristupnika i DNS servera na uređaju. Olakšava konfigurisanje mreže jer eliminiše ručno dodavanje osnovnih postavki za jednu računarsku mrežu.

DHCP je prihvaćen kao standardni protokol u oktobru 1993. godine. Posljednja definicija DHCPv6 koja opisuje prilagođenja u novom IPv6 okruženju je predstavljena 2003. godine.




DHCP server osigurava da su dodijeljene IP adrese posebne (jedinstvene za datu mrežu), i brine se da u mreži nema sukoba.

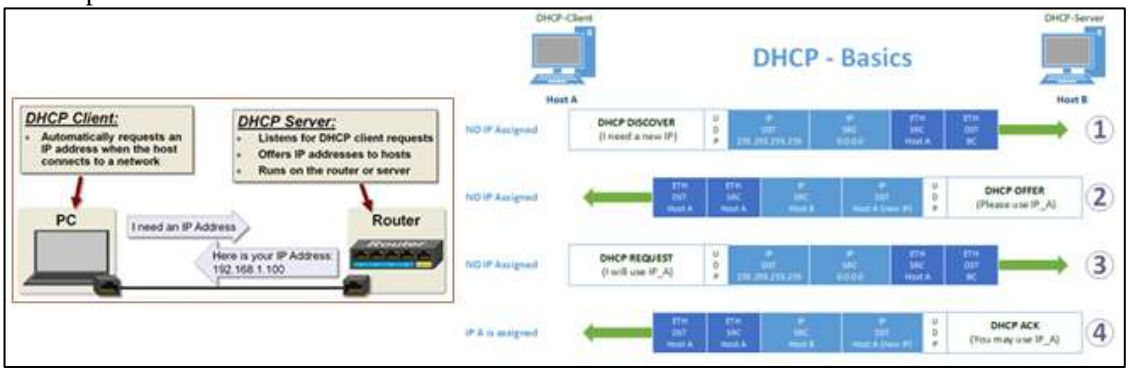
Budući da DHCP dopušta konfiguraciju da se automatski dogodi, koristi se u gotovo svim uređajima koji se povezuju s mrežom, uključujući računare, svičeve, pametne telefone, igraće konzole itd. S administrativne tačke, svaki uređaj na mreži može dobiti IP adresu s ništa više od zadanih mrežnih postavki, koja je postavljena da automatski dobije adresu. Jedina druga alternativa je ručno dodjeljivanje adresa svakom uređaju na mreži.

DHCP server definiše opseg ili raspon IP adresa koje koristi za posluživanje uređaja s adresom. Ovaj skup adresa je jedini način na koji uređaj može dobiti važeću mrežnu vezu.

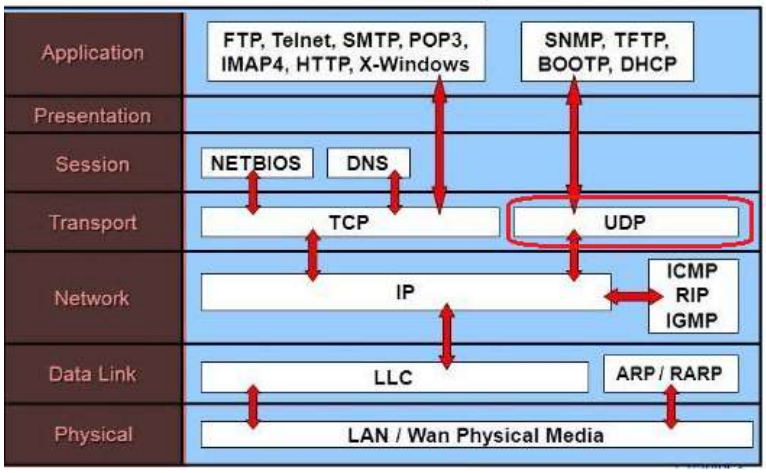
Ovo je još jedan od razloga što je DHCP toliko koristan jer omogućuje puno uređaja da se povezuju s mrežom tokom određenog vremenskog razdoblja bez potrebe za masovne rezervacije dostupnih adresa.

Na primjer, čak i kad DHCP server defiše samo 20 adresa, 30, 50, ili više uređaja mogu se povezati s mrežom sve dok ne više od 20 koriste istovremeno jednu od dostupnih IP adresa.

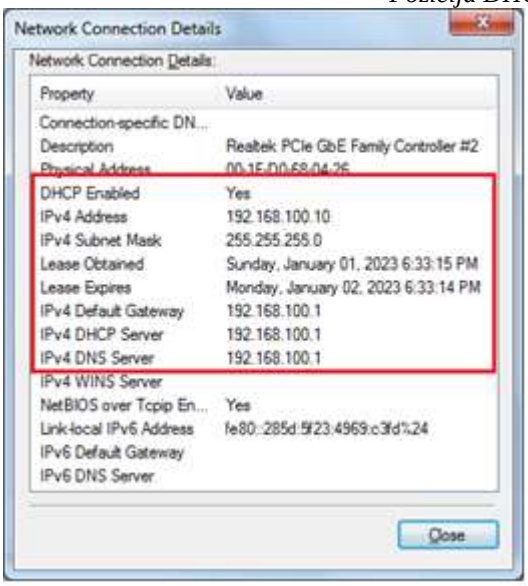
DHCP klijent emituje DHCP otkrivenu poruku na mreži koja sadrži njegovu MAC adresu namenjenu za UDP port broj 68. Ovaj datagram je poznat kao DHCPDISCOVER poruka, koja je zahtjev za bilo koji DHCP server koji prima datagram za informacije o konfiguraciji. Kao što naziv implicira, svrha DHCPDISCOVER poruke je otkrivanje DHCP servera. Klijenti DHCP bi trebali ponovo prenijeti poruku kada se ne primi odgovor od DHCP servera. Na primjer, ako nijedan DHCP server ne odgovori na DHCPREQUEST, klijent nastavlja s emitiranjem do četiri puta u 2, 4, 8 i 16 sekundi. Ako odgovor ne dobije za to vrijeme, klijent nastavlja sa emitovanjem svakih pet minuta.




*Koraci DHCP protokola*



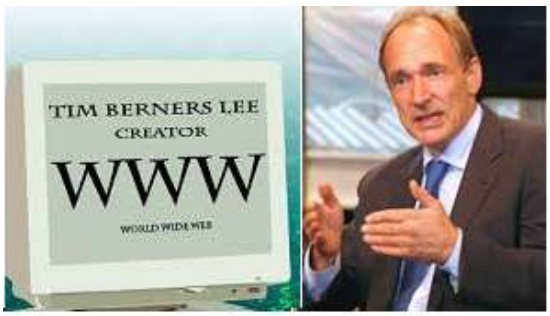
*Pozicija DHCP kod OSI modela*



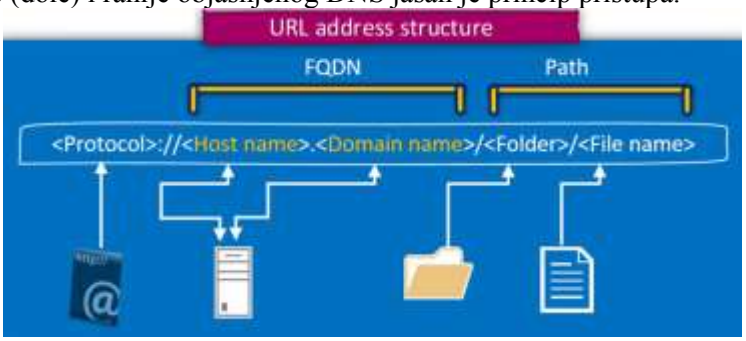

Kod Windows operativnog sistema, se koristi Automatsko privatno IP adresiranje (APIPA, *Automatic Private IP Addressing*) koje dodjeljuje posebnu privremenu IP adresu kada DHCP server ne isporučuje funkcionalni uređaj na uređaj i koristi tu adresu dok ne dobije onaj koji funkcioniše.

## Web adresa ili Jedinstvena adresa mrežnog resursa URL

-*Uniform Resource Locator*- -**jedinstvena Web adresa mrežnog resursa**-
URL se može shvatiti kao **mrežno proširenje standardne organizacije podataka** (fajlova-datoteka).




URL adresnu sintaksu prvi put je definisao Tim Berners-Lee za primjenu na Webu, a standardi su definisani standardom RFC 1738.
Za adresiranje i pristup koristi DNS sistem, odnosno FQDN jedinstveno domensko ime prošireno putanjom do resursa kojem se želi pristupiti. Resurs na koji pokazuje URL adresa može biti HTML dokument (web stranica), slika, ili bilo koja datoteka koja nalazi na određenom web serveru.
Na osnovu slike (dole) i ranije objašnjenog DNS jasan je princip pristupa.



Sintaksa (opšti oblik pisanja) URL adrese je:

**protokol://imeServisa.imeDomena:port/lokacija web datoteke (path-putanja)**

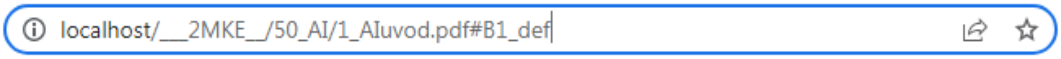
Pisanje URL-a započinje navođenjem protokola koji će se koristiti za pristup dokumentu navedenom na kraju URL-a. Kao separator koji označava kraj naziva protokola dolazi dvotačka, a zatim dvije obične kose crte.
Nakon toga se kao Host name navodi ime servisa. Ako se ne navede podrazumjevano je www. Iza druge kose crte slijedi **ime domene,** kome servis pristupa. Ono može biti pisano ili **u obliku numeričke IP adrese** računara na kome se domena nalazi (gdje je hostovana), ili kao uobičajeno slovno ime (FQDN adresa). Dakle IP adresa je dio URL-a.
Poslije imena računara se opciono nalazi port preko koga se pristupa, Ako nema porta, pristup se obavlja preko registrovanog porta protokola. Kao separator imena računara i porta koristi se dvotačka.
**Nakon separatora slijedi lokacija datoteke kojoj se pristupa,** gdje se hijerarhijski navodi imena direktorija do datoteke kojoj se pristupa.
To čak i ne mora da bude klasična datoteka već recimo upit (SQL ili drugi) dokument u bazi, rezultat finger ili archi komande i slično. Npr. To može biti i fragment. Ovo je interna referenca stranice, koja se odnosi na dio unutar web stranice. Pojavljuje se na kraju URL-a i počinje hashtagom (#), kao u primjeru na slici ispod.

Primjer URL adrese:

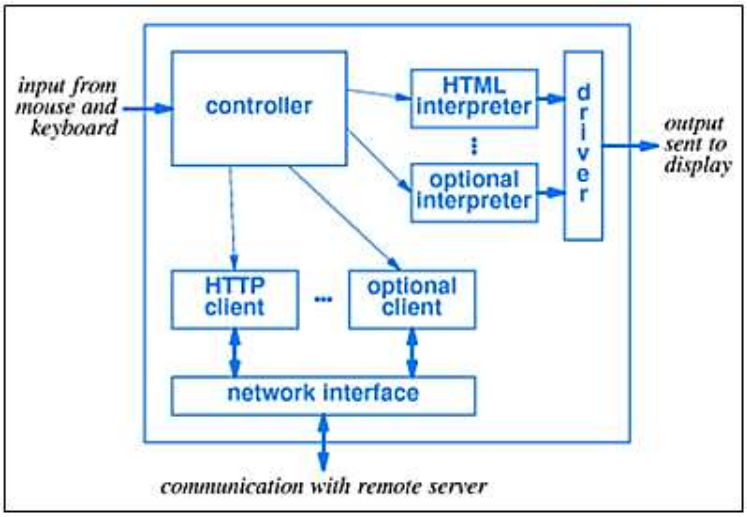

Ovo je URL adresa koja određuje gdje se na Webu nalazi resurs – PDF dokument 1_AIuvod.pdf (tačnije bukmark #c_cilj koji je označen unutar tog dokumenta).
Prvi dio URL-a (https://) govori da se tom resursu može pristupiti preko HTTPS protokola[26], te da se resurs nalazi na web serveru (hostu) s nazivom domene "mke.sveznadar.info", a nakon toga prikazuje /50_AI/1_AIuvod.pdf#c_cilj putanju kroz strukturu direktorija (podirektorij 50_AI) na disku toga servera.

Kod modela klijent-server WWWserver i klijent "razgovaraju" koristeći HTTP (preporučeno sigurnosnu verziju tog protokola, HTTPS) protokol. Klijent šalje zahtjev serveru.
1. Korisnik upisuje URL adresu u klijentski program[27]
2. Klijent obrađuje primljene podatke
3. Server prima zahtjev i šalje podatke klijentu

[26] Postoji izuzetak od pravila da se obavezno navede protokol, a to su lokalni URL-ovi koji se koriste za pristup datotekama što se nalaze na hard disku računara na kojem radite - lokalni URL. U tom slučaju se umjesto protokola navodi ime servera: localhost




[27] URL adresa može se pisati velikim i malim slovima, ali se preporučuje se korištenje isključivo malih slova (da bi se smanjila mogućnost greške za slučaj da korisnik ručno upisuje URL adresu.). Iako URL-ovi mogu da sadrže blanko znakove između karaktera, obično ih nemaju.

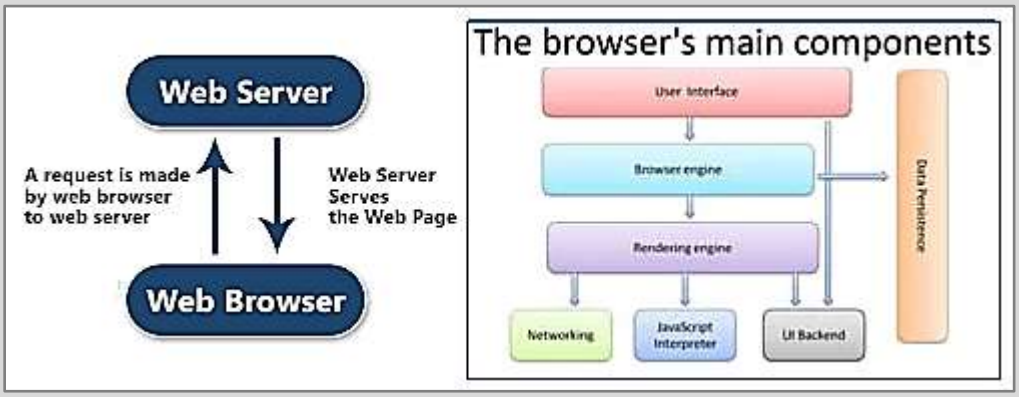



*Komponente web pregledača koji je standarna klijentska aplikaija kojom se pristupa nekom udaljenom mrežnom resursu koristeći http protokol*

HTTP protokol je relativno jednostavan. Sastoji se od svega nekoliko komandi.

- GET: zahtjeva određeni podatak od servera.
- HEAD: traži informaciju o statusu dokumenta
- PUT: šalje podatke serveru, koje server koristi da bi zamjenio određeni dokument.
- POST: šalje podatke serveru, koje server dodaje danom dokumentu.

Osim HTTP postoje i drugi protokoli za komunikaciju web klijenata i servera, na primjer HTTPS koji se koristi za kriptiranu komunikaciju, ili FTP za trensfer fajlova, ili e-mail za razmjenu elektronske pošte.
Takođe, osim HTML postoje i drugi jezici za zapisivanje dokumenata - takozvani *markup* jezici - na primjer XML, VXML. Sve su to razlozi zašto današnji web pregledači (web browser) imaju prilično složenu građu. Slika ispod prikazuje glavne komponente i ulogu web pregledača.

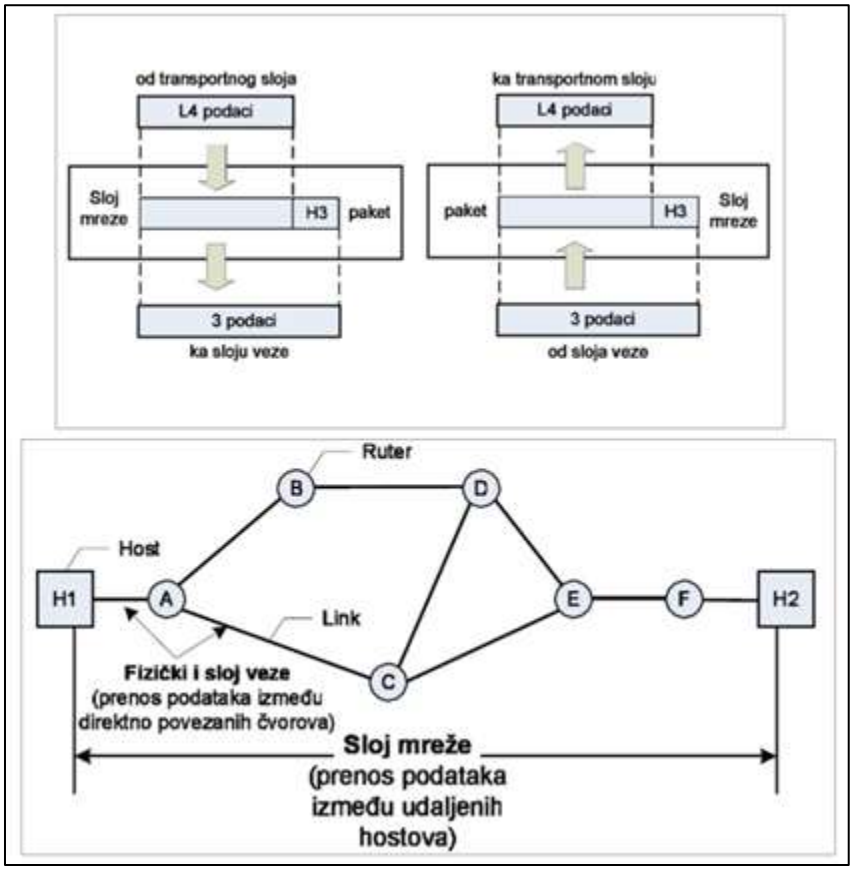



U posljednjih 15-tak godina WWW se intenzivno razvijao te su se u njega uklopile brojne dodatne tehnologije. Zahvaljujući takvom razvoju, današnji web dokumenti ne moraju isključivo biti tekstovi u HTML-u ili nekom sličnom markup jeziku, već mogu poprimiti složenije oblike.

URL adrese domena izazivaju **probleme jer se često mijenjaju**, npr. zbog promjena servera na kome se čuvaju Web stranice, promjene strukture direktorija, položaja datoteka sa sadržajem Web stranica i sl. Te promjene izazivaju poteškoće kod održavanja Web stranica jer one u pravilu pozivaju veći broj URL adresa i zato je potrebno često ispitivati jesu li se URL adrese promijenile, pronaći važeće URL adrese i ažurirati stare adrese. Ukoliko se to ne radi dovoljno često, tada adresa postaje nepristupačna.

## Pregled adresiranja po slojevima

1.SLOJ VEZE radi sa fizičkim adresama(MAC)
2.MREŽNI SLOJ radi sa IP adresama
3.TRANSPORTNI SLOJ radi sa logičkim portovima (preko portova procesi izlaze na NET, na primjer SMTP ima izlaz preko porta 25, a POP3 preko porta 110).

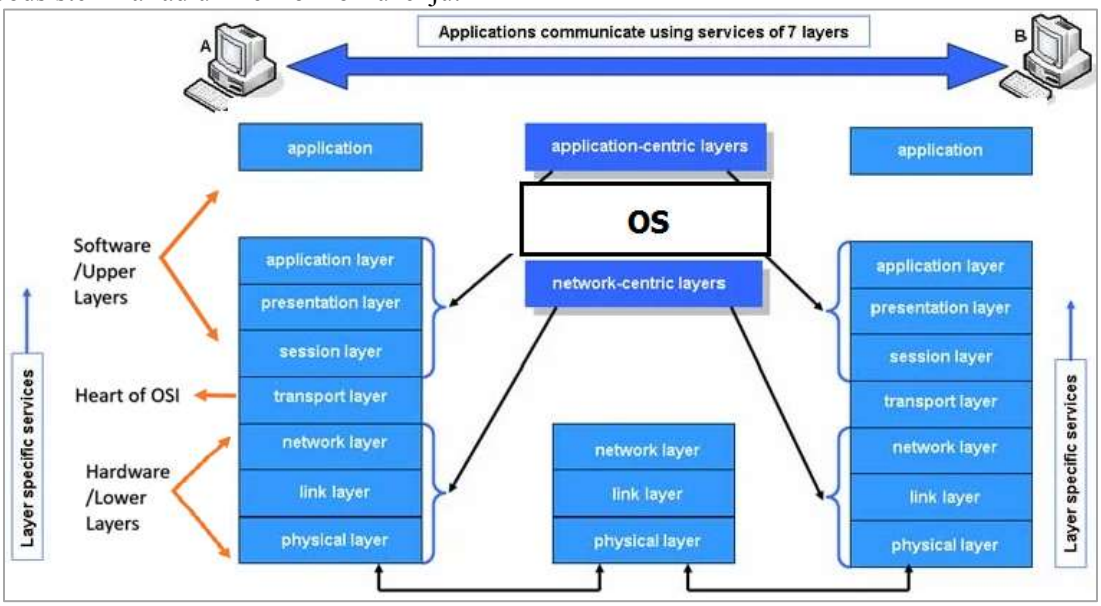



Ilustracija sfesiranja u sloju mreže OSI modela

**Fizičko adresiranje**, koje se realizuje na nivou sloja veze, rješava problem adresiranja lokano, na nivou zajedničkog linka. Složena mreža, formirana povezivanjem više, moguće različitih podmreža, koje koriste različite šeme fizičkog adresiranja, zahtijeva uvođenje logičkih (ili mrežnih) adresa, koje će biti jedinstvene na nivou cjelokupne mreže. **Logičke adrese** izvora i odredišta, sadržane su u zaglavlju sloja mreže.

# Operativni sistemi računara i podrška za mreže

Iako se pod osnovne funkcije operativnog sistema ubrajaju upravljanje centralnim procesorom, memorijom i periferijskim uređajima, savremeni operativni sistemi posjeduju i kompletan podsistem za rad u mrežnom okruženju.




*Pristup operativnog sistema pojedinim slojevima OSI modela*

Osnovni nivo mrežne podrške jeste podrška za hardver koji služi za fizički pristup mreži (mrežna kartica, modem i sl.). Mrežni podsistem (mrežna podrška) u operativnim sistemima se najčešće realizuje kroz podršku za mrežni hardver (1. i 2. sloj *OSI* modela) i podršku za mrežne protokole (3. i 4. sloj *OSI* modela), dok se podrška višim slojevima *OSI* modela uglavnom prepušta korisničkom softveru koji se izvršava na operativnom sistemu. Postoje i situacije u kojima se podrška za transportni pa čak i mrežni sloj prepušta korisničkom softveru kao i situacije u kojima operativni sistem ima ugrađenu podršku za protokole aplikativnog sloja.

Podrška za hardver računara se kod operativnih sistema realizuje u vidu modula jezgra operativnog sistema. Ovi moduli se nazivaju drajverima (engl. *driver*) i operativni sistemi se najčešće isporučuju sa već sadržanim drajverima za popularni mrežni hardver. U slučajevima kada podrška za hardver nije već uključena u operativni sistem od strane proizvođača operativnog sistema, drajveri se preuzimaju od proizvođača hardvera.

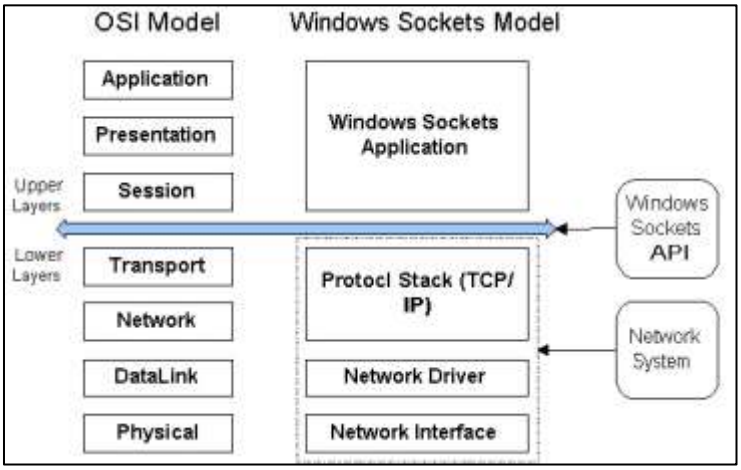
Osim podrške za mrežni hardver (fizički sloj) operativni sistem mora imati podršku za protokole sloja veze, mrežnog i transportnog sloja koji se koriste u mreži na koju je računar priključen.

Ukoliko operativni sistem ne posjeduje podršku za bilo koji od ovih slojeva, vertikalna komunikacija (komunikacija između slojeva unutar računara) će biti prekinuta i pristup mreži onemogućen.

Na primjer, ukoliko računar posjeduje odgovarajući mrežni hardver, podršku za *IP* protokol mrežnog sloja i podršku za *TCP* protokol transportnog sloja ipriključen na Eternet mrežu koja radi pod *TCP* i *IP* protokolima, ali ne posjeduje podršku za sam Eternet protokol, pristup mreži će biti onemogućen usljed prekida vertikalne komunikacije na sloju veze.

## Koncept Windows socketa

Windows Sockets[28] (***WinSock***, Windos utičnica) definiše raspodjelu poslova između mrežne aplikacije i steka mrežnih protokola: aplikacija obezbjeđuje sadržaj, dok stog mrežnih protokola obezbjeđuje isporuku.
WinSock API je programski priključak na mrežu. Možete uključiti bilo koji uređaj ili aplikaciju u električnu utičnicu ((socket). Drugim riječima, možete pokrenuti bilo koji TCP /IP mrežna aplikacija na bilo kojoj WinSock implementaciji, bez obzira na to preko kojeg medija radi – Ethernet, Token Ring, serijska linija – ili koja kompanija obezbjeđuje stek TCP/IP protokola.



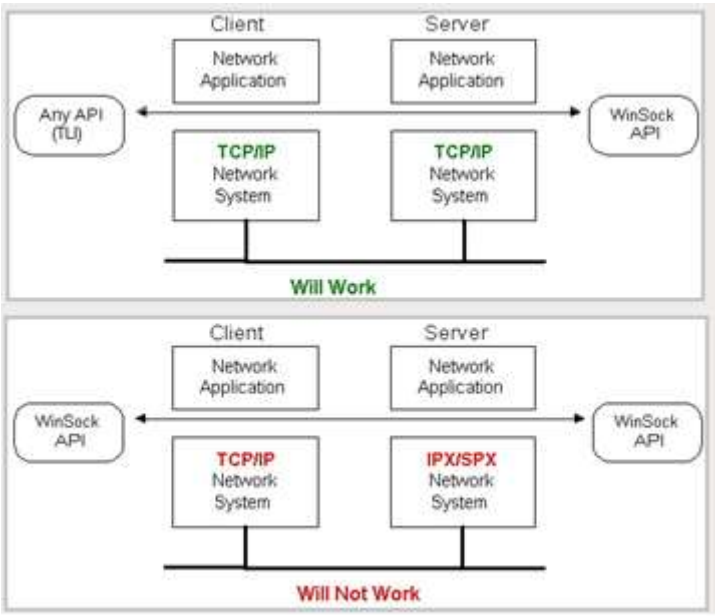

*WinSock aplikacija ima modularnu slojevitu arhitekturu*

WinSock, takođe, obezbjeđuje binarnu kompatibilnost. Izvršni fajl ne zahtjeva promjene kada se premjesti sa jednog provajdera mrežnog sistema na drugog, ili između platformi operativnog sistema.
Windows Sockets API WSA sastoji se od zbirke funkcija, struktura podataka i konvencija. WSA pruža standardni pristup mrežnim uslugama osnovnog steka protokola bilo kojoj Windows aplikaciji.
Datoteka WINSOCK.DLL je uključena u sve verzije Windowsa nakon Windows 3.1.[29] Od 2012. i Windowsa 8 koriste se RIO API *("RIO" (Registered IO), "RIO" registrovani IO*) ekstenzije (dodaci i proširenja) za Winsock.
**WinSock mrežni model je pojednostavljena verzija OSI modela**. Međutim, individualna OSI funkcionalnost i dalje postoji u WinSock mrežnom modelu na konceptualnom nivou.
Slojevi se mogu kombinovati. Mnogi stekovi protokola kombinuju transportni i mrežni sloj i kao rezultat toga mrežni sloj nema standardni API.
Neki slojevi su opcioni. Mnogim aplikacijama nije potreban sloj za prezentaciju. WinSock API (WSA) je uniforman čak i ako API za osnovni stek nije. WinSock je nezavisan od protokola. WinSock je nezavisan od mrežne kartice.

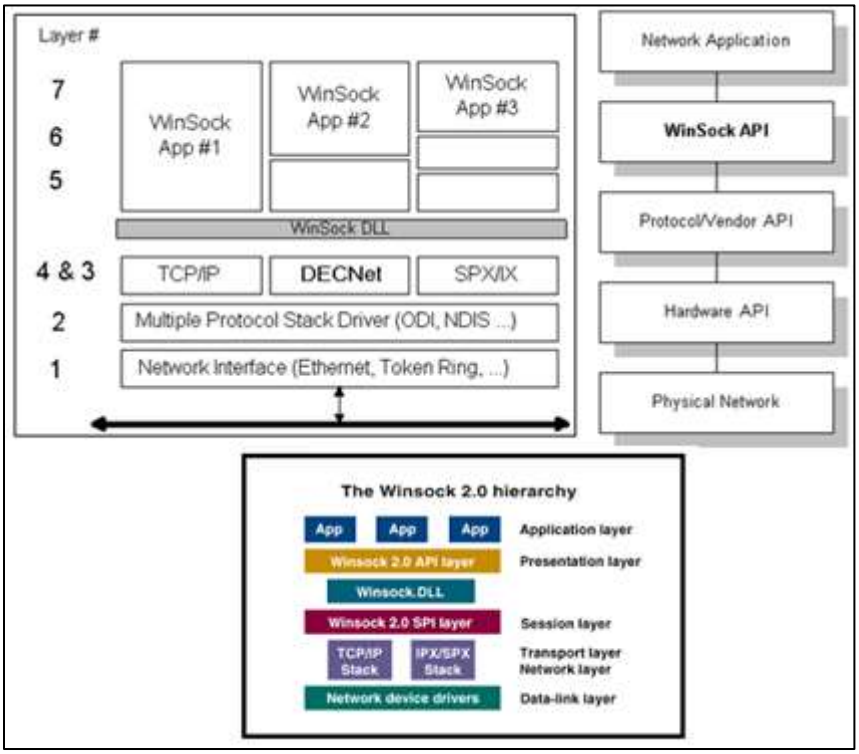
Windows Sockets API je nezavisan od protokola. API omogućava pristup uslugama u paketu protokola. Različiti protokoli pružaju iste usluge. Ako imate dva umrežena računara i želite da

[28] Windows Sockets API (WSA), kasnije skraćen na Winsock
[29] Rane internet aplikacije su često instalirale DLL kako bi osigurale njegovo postojanje

komuniciraju jedan s drugim, jedini put kada trebate koristiti isti API je ako planirate koristiti isti izvorni kod. Uvijek je potreban isti paket protokola na oba računara.



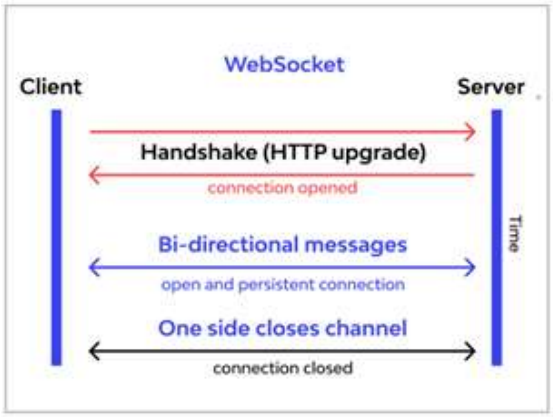

*Da bi dva umrežena računara komunicirala, API-ji ne moraju biti isti, ali protokoli moraju biti*

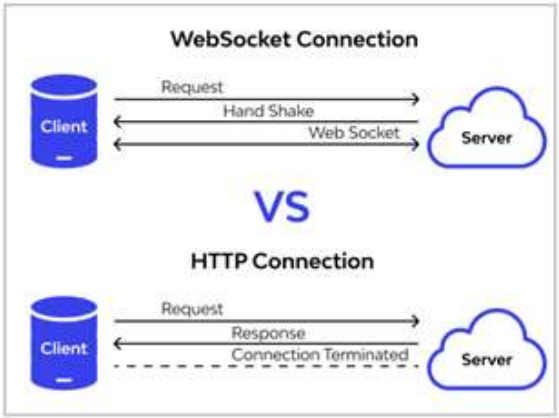



*Odnos WinSok i OSI modela*

# WebSocket, protokol koji definiše priključak na web

WebSocket je komunikacioni protokol, koji pruža full-duplex komunikacione kanale preko jedne TCP veze klijenta i servera. Veza, ostvarena WebSocket protokolom traje sve dok je bilo koji od učesnika prekine. Jednom kada jedna strana prekine vezu, druga strana neće moći komunicirati jer se veza automatski prekida na njenom prednjem dijelu. Koristi ga većina modernih web aplikacija kada je riječ o nesmetanom strimingu podataka i različitom nesinhronizovanom prometu.
WebSocket protokol verzija 13, koji je standardizirao IETF kao RFC 6455, 2011. godine, predstavlja zvanični i standard.
API specifikacija koja dozvoljava web aplikacijama da koriste ovaj protokol poznata je kao **WebSockets**. Većina pretraživača podržava ovaj protokol, uključujući Google Chrome, Firefox, Microsoft Edge, Safari i Opera.

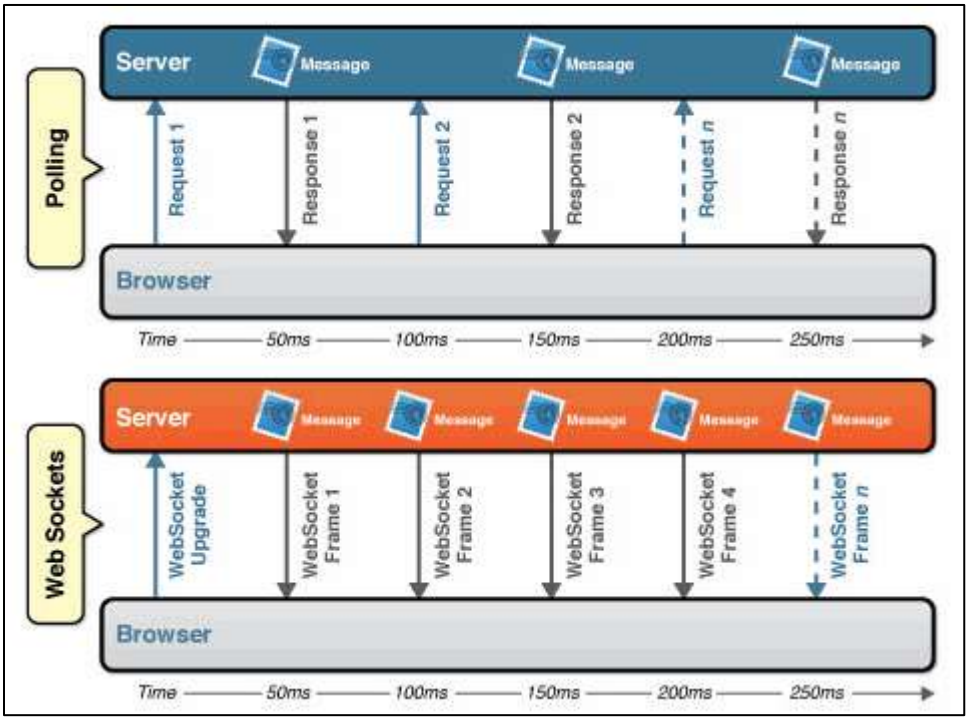



WebSocket se razlikuje od HTTP-a. Oba protokola se nalaze na sloju 7 u OSI modelu i zavise od TCP-a na sloju 4. WebSocketu je potrebna podrška od HTTP-a za pokretanje veze.
RFC 6455 navodi da je WebSocket "dizajniran da radi preko HTTP portova 443 i 80, kao i da podržava HTTP proxy i posrednike" , što ga čini kompatibilnim sa HTTP-om.

Detalnija analiza webSocket protokola bi zahtjevala daleko viši nivo nego što ga nudi ovaj priručnik, pa ćemo razmotriti samo početak procedure korištenja ovog protokola i njegov cilj.
Proces uspostavljanja WebSocket veze počinje sa WebSocket rukovanjem koje uključuje korištenje nove šeme ws ili wss, nadogradnjom HTTP zahtjeva koji sadrži nekoliko zaglavlja kao što su Connection: Upgrade, Upgrade: WebSocket, Sec-WebSocket-Key, i tako dalje.
Zaglavlje odgovora, Sec-WebSocket-Accept, sadrži vrhunsku vrijednost dostavljenu u zaglavlju zahtjeva Sec-WebSocket-Key. Ovo je povezano sa specifikacijom protokola koja se koristi da zadrži pogrešne informacije. Drugim riječima, poboljšava sigurnost API-ja i sprječava loše konfigurisane servere da stvaraju greške u razvoju aplikacije.
Ovo je omogućeno obezbjeđivanjem standardizovanog načina da server šalje sadržaj klijentu, a da ga klijent nije prethodno zahtjevao, i omogućavanjem da se poruke prosljeđuju napred-nazad, dok je veza otvorena. Na ovaj način se može odvijati dvosmjerni tekući razgovor između klijenta i servera. Komunikacija se obično obavlja preko TCP porta broj 443 (ili 80 u slučaju nebezbjednih veza), što je korisno za okruženja koja blokiraju ne-web internetske veze pomoću fajervola.

Funkcije koje nudi server klijentima jesu prijava, odjava i slanje tekstualnih poruka. Komunikacija se obavlja u jednoj grupi, ali moguće je jednostavno ponuditi podršku sa više "soba" (*chat rooms*). Sa svakim klijentom se uspostavlja konekcija pomoću posebne sesije i moguće je pamtiti podatke klijenta u njegovoj sesiji, kao što su njegovo korisničko ime, vrijeme prijave ili odabrana (tema) soba. Pomoću seta
sinhronizovanih sesija server prosljeđuje poruke svima, ili prema svima koji pripadaju istoj sobi.




*Ilustracija koja pokazuje osnovnu prednost Winsocket protokola:*
*neprekidnu komunikaciju dok god je veza "živa"*
*ukidanjem višestrukih konekcija Websocket je aktivan sve dok se korisnik ne odjavi*

Bez obzira što je WebSockets neformalni standard za rad sa mrežnim aplikacijama u realnom vremenu, postoji niz operativnih problema, posebno kako se aplikacija mijenja, povećava i dograđuje, a korisnička baza uključuje i koristi promjenu tehnologije kao što su: zaštitni zidovi, topologija mreže, testiranje opterećenja i sigurnost.

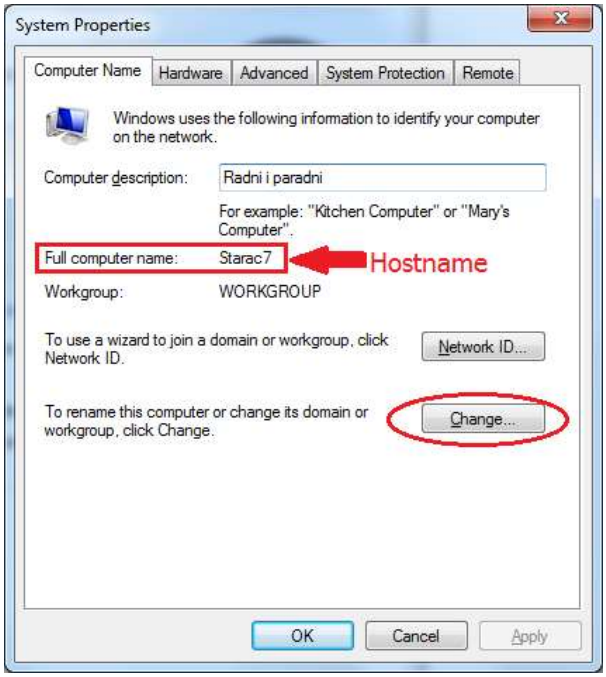
# Osnovni alati za provjeru rada mreže

Postoje razni mrežni programi i komande koje možete koristiti. Neki su pogodni za dijagnozu i ovdje ćemo objasniti neke od komandi koje se univerzalno koriste za dijagnostiku. Za to se standardno koristi ICMP protokol, koji je dio TCP/IP protokola (što je ranije objašnjeno).
U objašnjenjima koja slijede korišteno je Windows okruženje, mada postoje slične (ili iste) opcije i za druge OS.

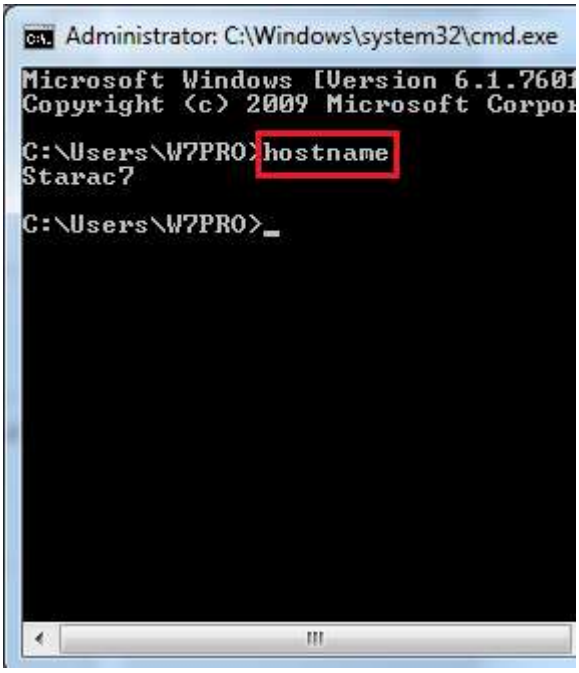
## Kako saznati ime računara: Hostname

1. Svaki računar ima svoje ime računarskoj mreži. To se može proveriti preko npr. ***Control Panel \ System \ Computer Name*** putanje.

1. Pozivom kartice System properties direktno se dobije ime računara: *Full computer name*




2. Naredbom **hostname** (iz cmd panela kod Windows-a) se dobija ime računara.




*Napomena: Ime koje jedinstveno određuje (identifikuje) svaki računar na Internetu ili lokalnoj računarskoj mreži jeste njegova IP (Internet Protocol) adresa. To **NIJE** ime računara.*
*Čestu zabunu izaziva to što se u ime hosta: hostname zamjeni sa imenom računara: computername, a pogotovo to što komandom hostname dobijamo ime računara koje odgovara korisničkom imenu računara. Glavna razlika između IP adrese i imena hosta je u tome što je IP adresa numerička oznaka koja se dodjeljuje svakom uređaju spojenom na računarsku mrežu koji koristi Internet protokol za komunikaciju, dok je ime hosta oznaka koja se dodjeljuje mreži koja korisnika šalje na određenu web stranicu ili web stranicu.*

# Pingovanje

**Packet Internet Grouper** (**ping**[30]) je osnovni administrativni alat za testiranje mreže koji se najčešće koristi za ispitivanje postojanja konekcije između dva entiteta i otkrivanja problema u računarskim mrežama. Izraz ping se ponekad prevodi i kao *latencija*. Da se naglasi da je to vrijeme čekanja, odnosno vrijeme koje protekne od trenutka zahtjeva za podatcima do trenutka dok se ti podatci ne pojave.


*Pingovanje je slanje podataka sa jednog kompjutera na određenu IP adresu i određeni port* sa ciljem da se ti paketi vrate sa te IP adrese i pri tom se izmjeri brzina ping-a, odnosno vrijeme za koje su paket stigli i vratili se do određenog računara u mrezi.

Ping podrazumjeva slanje ICMP (*Internet Control Message Protocol*) poruke -*echo request* (zahtjev za eho) do odredišnog čvora. Ako je konekcija ispravna (funkcionalna), odredišni čvor prima ICMP zahteve i na njih odgovara porukom *echo response* (eho odgovor). Ping paket obično sadrži 32, 56 ili 64 bajtova podataka. Ako host koji šalje zahtev primi odgovor u određenom roku, smatra se da je veza stabilna, što znači da su svi mrežni uređaji između krajnjeg čvora i stanice koja šalje ping ispravno podešeni za prenos podataka.

Ping daje sljedeće informacije:

- Svakom paketu ping dodjeljuje jedinstven broj u nizu i obavještava o brojevima paketa koje primi, kao i o njihovom redosljedu. Na taj način moguće je utvrditi da li su paketi izgubljeni, duplirani ili im je redoslijed izmenjen.
- Ping provjerava kontrolni zbir (*checksum*) svakog poslatog i primljenog paketa pa se mogu otkriti neki oblici oštećenja.
- Ping dodjeljuje vremenski pečat (*timestamp*) svakom paketu, a odredišni čvor ga vrada, pa se može izračunati koliko je trajala razmjena paketa RTT (*Round Trip Time)* –vrijeme potrebno da paket stigne do odredišta i vrati se nazad
- Omogućava testiranje funkcionalnosti mrežne kartice (neke funkcije slojeva 1 i 2, npr. brzina prenosa, kontrola prenosa, detekcija greške), kao i mogućnost računara da razmjenjuje podatke preko mreže. Ovo se ostvaruje pingovanjem bilo koje adrese iz opsega 127.0.0.1-127.255.255.254.

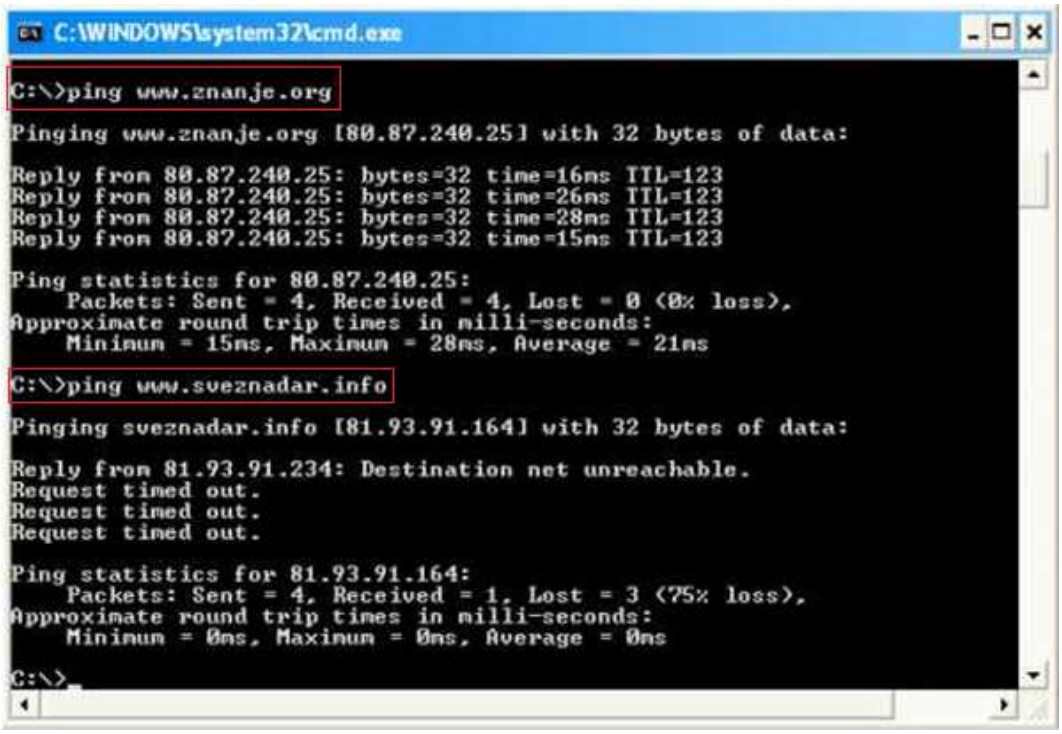
Ukoliko ping ne uspije, javiće grešku poput *Destination host unreachable*, što znači da je problem u TCP/IP komunikaciji (*Odredište hosta-domaćina nedostupno*).

[30] Za nastanak termina ”ping” postoje (bar) dvije teorije. Prva kaže da je to akronim “*Packet Internet Inter-Network Groper*”, što se prevodi kao Paketni internet međumrežni groper (gdje groper ima višestruko značenje a u sebi uključuje ostvarivanje kontakta). Drugo se veže za nautički termin otkrivanja podmornice sonarima gdje sonari ispuštaju zvukove koji se zove ”ping” ne bi li se na taj način odredilo gdje se koja podmornica nalazi. Drugo objašnjenje se čini vjerovatnijim jer je se koristi slična teknika, pa je prvo obješnjenje termina vjerovatno bakronim koji se ustalio u mrežnom okruženju.

Ovo još uvijek ne znači da je problem kod Vas, možda je "pao" *pingani* server ili veza vašeg Internet providera sa svijetom. Probajte *pingovati* još nekoliko adresa i tek ako na svima dobjete grešku možete biti sigurni da je problem baš s vaše strane mreže.

**Kako se vrši pingovanje kod Windowsa?**
Pingovanje kod Windowsa se provodi u cmd modu komandom ping i navođenjem komade ping te naziva Url adrese: PING URL

Ukoliko ping "prođe" do zadane destinacije i natrag, ispisaće za to potrebno vri|eme što znači da veza između vas i te adrese postoji te da grešku treba potražiti negdje drugdje.




*Primjeri pingovanja URL-ova znanje.org i sveznadar.info*

Naredba ping ima sintaksu:
**Ping [-t] [-a] [-n] [-l] [-f] [-i] [-v] [-r] [-s] [-w] [-j] naziv cilja** (URL koji pingujemo)

Parametri koji se koriste opciono i imaju sljedeće značenje:

t- Nastavite slati na željenu adresu dok ne prestane odgovarati, a ako želimo prekinuti i prikazati statistiku, pritisnemo CTRL+prekid, i bojkotiratiping I da ga dovršimo koristimo CTRL + C.

a- Prikažite identifikacijski broj date adrese.

n - Broj poslanih poruka zahtjeva za eho (poslanih paketa podataka), a zadana vrijednost je 4.

Odgovorite ili zatražite ... itd

l - Veličina prenesenog paketa podataka, navedena je u bajtima, zadana veličina paketa je 32, a maksimalna 65.527.

f- Nemojte fragmentirati paket koji su ruteri poslali na putu do predviđenog odredišta.

i - Vrijeme između svakog snopa i drugog, mjereno u milisekundama.

v - Zadana vrsta usluge je 0 i navedena je kao decimalna vrijednost u rasponu 0 do 255.

r- Broj prenosnih točaka ili skokova u liniji komunikacije s adresom i pri korištenju ovog kriterija korišten je Snimite rutu Ovo je za bilježenje puta koji je prošla poruka zahtjeva do odgovarajuće poruke odgovora na zahtjev.

s- Vrijeme zabilježeno po dolasku svakog skoka ili njegovoj transformaciji (vrijeme dolaska poruke zahtjeva za eho i odgovarajuće poruke odgovora).

w- Vrijeme čekanja na odgovor s adrese u milisekundama, a ako poruka odgovora nije primljena, prikazuje se poruka o grešci "Zahtjev je istekao" "Zahtjev je istekao" Zadano vrijeme čekanja je 4000 (4 sekunde).

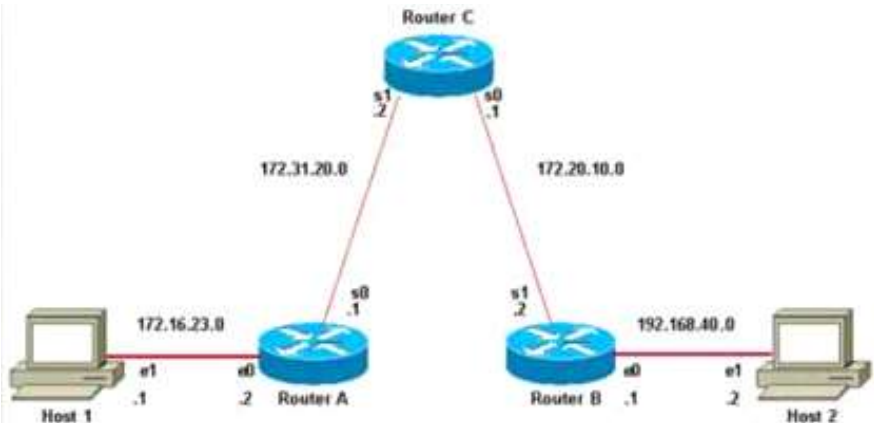
j - Određuje broj i najveći broj odredišta koja paket podataka prolazi kroz svoju putanju do odredišta

Naredba **ping** se može koristiti i u maliciozne svrhe, pa se neki sajtovi štite od takvih napada zabranjivanjem slanja ICMP eho odgovora.

## Komanda tracert/traceroute

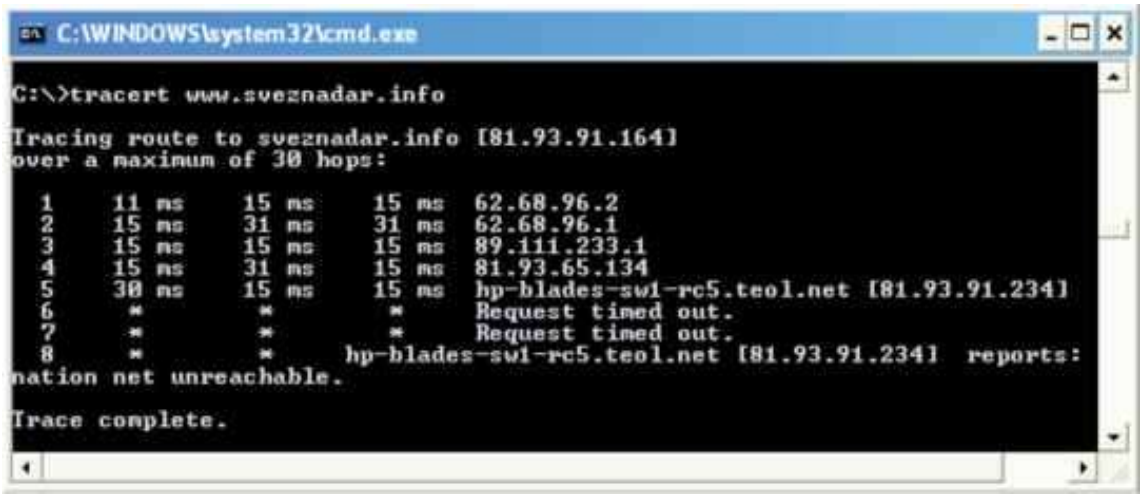
Traceroute je dijagnostička alatka za praćenje puta IP paketa od jednog do drugog računara u mreži. Kod Windowsa je to komanda koja se piše tracert, ali se uobičajeno koristi termin traceroute[31]. Ova komanda je slična komandi ping po tome što takođe koristi ICMP pakete.

Traceroute je veoma korisna mrežna alatka za dijagnostiku. traceroute prikazuje svakog domaćina kroz kojeg paket putuje dok pokušava da stigne do svoje destinacije. Putujući ka svom odredištu navedenom u IP adresi, ovi paketi prolaze kroz seriju rutera. Iz izveštaja ovog programa moguće je videti kašnjenja na pojedinim ruterima.



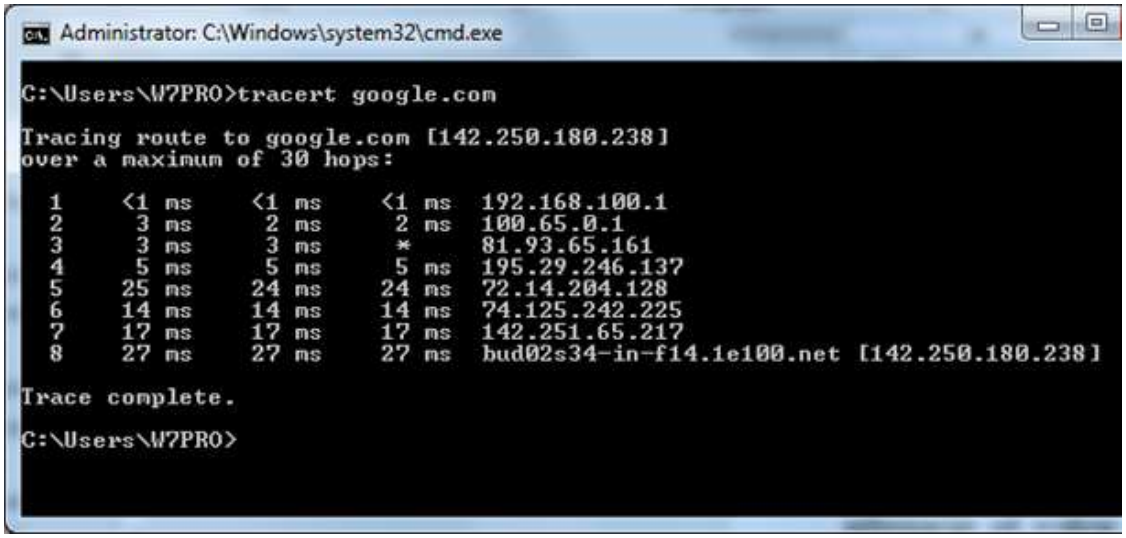

[31] Sem razlikr u kucanju postoje i neke razlike u sintaksi. Ovdje je dat prikaz opcija za tracert: Windows komandu

Možete vidjeti koliko "skokova" ima do sajta sveznadar.info ima od Vas pomoću komande:
*tracert* www.sveznadar.info
Prikazan je svaki domaćin (host), zajedno sa vremenima odgovora za svakog domaćina.
Trace Route koristi isti tip eho-poruke kao i Ping, ali te poruke koristi na drugačiji način.Trace Route koristi TTL parametre u eho-poruci da mapira putanju određenu od strane poruke koja se pomjera kroz mreže. Ova poruka je prvo poslata sa TTL vrijednošću 1. Ovo će isteći kod prvog rutera (ili gateway-a). Zatim se TTL povećava za jedan svaki put kad je poruka poslata izvan, sve dok ne stigne do destinacije.




Svaki put kad se TTL poruka vrati od strane nekog rutera dobijaju se dvije značajne informacije: IP adresa gateway-a gdje je istekla poruka, i vrijeme koje je potrebno da poruka napravi pun krug do tog gateway-a i nazad do pošiljaoca. Ova informacija je obično prikazana u praćenju putanje. Ovo omogućava da se napravi označena putanja napravljena od strane paketa, korak po korak, od izvora do destinacije.
Ako je cilj nedostupan, Trace Route će obično prikazati svaki korak putanje do tačke gde je poruka vraćena.
Obično je omogućeno maksimalno 30 skokova pre nego se prekine proces. Ovaj maksimum može biti promjenjen od strane korisnika.
Većina programa za praćenje putanje će poslati najmanje tri poruke na svaki korak putanje, vraćajući informacije od svakog od ovih pokušaja. Ako poruka nije vraćena, nedostajuća poruka je obično identifikovana kao zvjezdica (*) umjesto odgovarajućeg vremena potrebnog da se napravi cijeli krug.

**tracert** će prihvatiti destinaciju datu ili u formi numeričke IP adrese ili kao DNS ime domena. Ako je data IP adresa, program će obično vratiti i ime koje je povezano sa tom adresom. Ako je zadato DNS ime sistem će vratiti IP adrese.
Kako program prikazuje svaki skok putanje, obično će prikazati IP adresu i bilo koje ime domena koje je povezano sa tom adresom.
Program traceroute koristi opciju vremena preživljavanja paketa (time-to-live , TTL) da bi sa svakog mrežnog usmjerivača (rutera) izazvao slanje ICMP poruke TIME_EXCEEDED. Svaki usmjerivač koji obrađuje paket istovremeno umanjuje vrijednost TTL polja za jedinicu, pa TTL polje postaje svojevrstan brojač skokova.




*Prikaz rute do google.com računara (vidite da nije obavezno unijeti kompletnu simboličku adresu - izostavljeno je www. , ali isti rezultat ćete dobiti i ako je unesete)*

Program traceroute možemo upotrijebiti da bismo utvrdili tačnu putanju paketa. Kao što smo pomenuli, traceroute pomaže da otkrijete topologiju ciljne mreže, i identifikuje mehanizme za kontrolu pristupa (programski izvedenu zaštitnu barijeru ili usmjerivač za filtriranje paketa) koji možda filtriraju saobraćaj.

Sintakse ove komande je:
**tracert [-d] [-h maksimalan_broj skokova] [-j lista racunara] [-w tajmaut] ciljni računar**
Opcije komande tracert su:
- d Nalaze da se adrese ne prevode u imena računara.
- h maksimalan_broj skokova Određuje maksimalan broj skokova do ciljnog računara.
- j lista_racunara Odreduje grubu putanju duž liste računara iz argumenta lista_racunara.
- w tajmaut Za svaki odgovor čeka broj milisekundi zadatih argumentom tajmaut.

Ping i Trace Route se koriste kod otklanjanja problema sa TCP/IP komunikacijama. Oni dozvoljavaju mrežnom administratoru da testira da li udaljeni sistem dostižan, i ako nije gdje su veze u prekidu.

*Traceroute **samo pomaže** da otkrijete topologiju mreže, i identifikuje mehanizme za kontrolu pristupa (programski izvedenu zaštitnu barijeru ili ruter-usmerivač za filtriranje paketa) koji možda filtriraju saobraćaj.*
U realnom - složenom okruženju može da bude više putanja, odnosno uređaja za usmjeravanje s više mrežnih veza.
Svaka veza može da ima drugačiju listu za kontrolu pristupa (access control list ACL). Mnoge veze će propustiti zahtjev programa traceroute, ali će ga druge odbiti zato što imaju drugačiju ACL listu. Zbog toga je neophodno da programom traceroute ispitate cijelu mrežu. Pošto traceroute primjenite na sve sisteme u mreži, počnite da sastavljate dijagram mreže koji treba da odslika arhitekturu mrežnog prolaza na Internet i lokaciju mehanizama pomoću kojih se kontroliše pristup. Taj dijagram se naziva dijagram putanja za pristup (*access path diagram*).

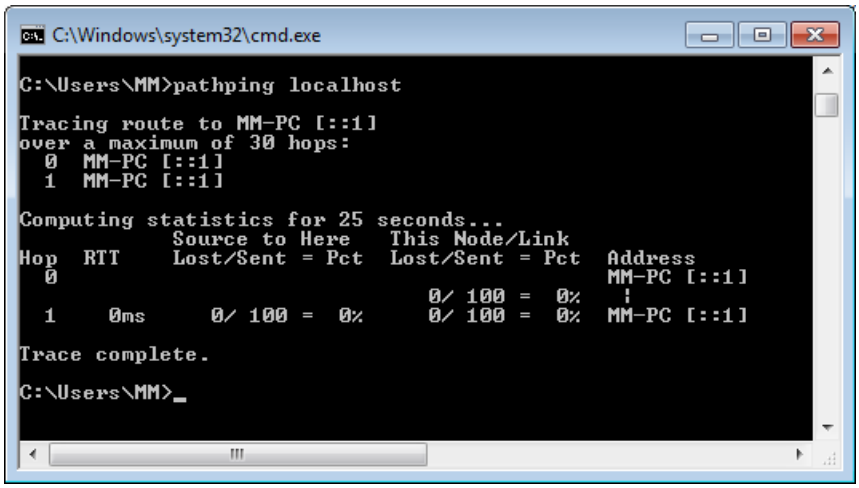
| Hop # | RTT 1 | RTT 2 | RTT 3 | Name/IP Address |
|---|---|---|---|---|
| 10 | 81 ms | 74 ms | 74 ms | 205.134.225.38 |

*Ilustracija rezultata komande tracert*

Objašnjenje stavki rezultata komande:
Broj skoka, Hop Number – Ovo je prva kolona i jednostavno je broj skoka duž rute. U ilustraciji, to je deseti skok.
RTT kolone – Sljedeće tri kolone prikazuju povratno vrijeme (RTT) za vaš paket da stigne do te tačke i vrati se na vaš računar. Ovo je navedeno u milisekundama. Postoje tri kolone jer traceroute šalje tri odvojena signalna paketa. Ovo je da bi se prikazala konzistentnost ili nedostatak iste na ruti.
Domena/IP kolona – posljednja kolona ima IP adresu rutera. Ako je dostupno, ime domene će također biti navedeno.

## Pathping

Program **PATHPING.EXE** je kombinacija PING i TRACERT programa. Budući da naredba prikazuje stepen gubitka paketa na mrežnim uređajima, administrator može odrediti ko uzrokuje mrežne probleme:
**sintaksa: pathping -n [target]**
gdje je target IP adresa (koja se obično navodi kao simboličko ime), a opciono kada koristite '/n', naredba pathping ne rješava IP adrese uključenih rutera.

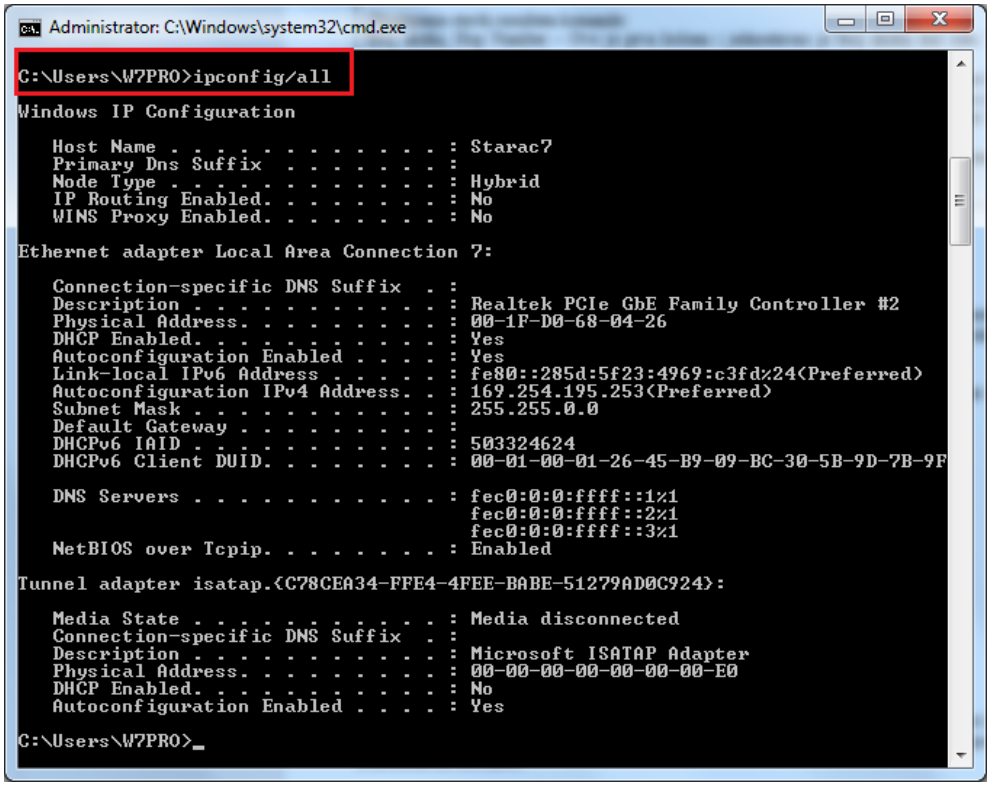



Npr. u slučaju da ispitujete status lokalnog računara umjesto IP adrese unijećete localhost (što je njegovo predefinisano ime, koje odgovara rezervisanoj adresi 127.0.0.1). a mogući odgovor je pokazan na slici gore.

# Komanda IPCONFIG

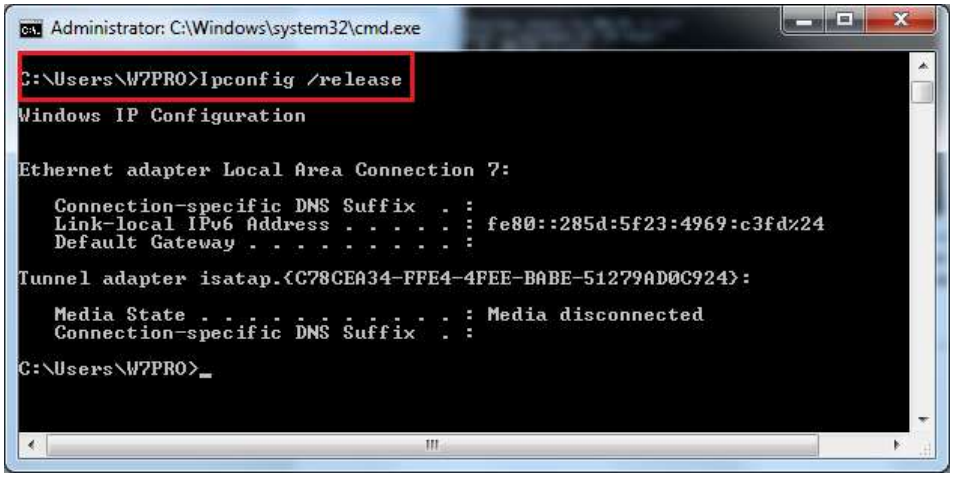
IPCONFIG (što znači "konfiguracija internetskog protokola"- "Internet Protocol configuration") je konzolni aplikacijski program koji prikazuje sve trenutne vrijednosti TCP/IP mrežne konfiguracije i osvježava postavke Dynamic Host Configuration Protocol (DHCP) i Domain Name System (DNS).

Puna sintaksa**: ipconfig [/all , /renew [adapter] ,/release [adapter]]**




Ako se navede bez parametara, ispisaće osnovne IP adrese za sve mrežne adaptere odnosno za sve konekcije.
Sa **ipconfig /?** se dobijaju sve moguće opcije i prikaz rada sa njima.
**Ako naredba koristi argument /all**, dobija se prikaz cijele TCP/IP konfiguracije za sve fizičke i logičke mrežne interfejse.
Sadržaj DNS keš memorije na lokalnom računaru se vidi narednom **ipconfig /displaydns**.
Ime zapisa o resursu je navedeno pod poljem Record name. Vrijednost predstavlja (najčešće) IP adresu u koju se prevodi ime a navedeno je pod zadnjim poljem u svakom zapisu gde inače piše i tip polja. Tip polja može biti A, NS, CNAME, MX, PTR itd. TTL (Time To Live) predstavlja vremenski period za koji zapis je validan odnosno za koji ostaje u lokalnom DNS kešu.

Komanda ipconfig ne samo da prikazuje informacije o mrežnim postavkama, već se može koristiti i za resetovanje ili osvježavanje mrežnih postavki.




Ako više ne želimo koristiti dodijeljenu IP adresu možemo koristiti naredbu: **Ipconfig /release.** Ako ste restovali (oslobodili se dodjeljene IP adrese) moraćete da zatražite novu od DHCP servera. To možemo učiniti pomoću naredbe **Ipconfig /renew**.

```
ipconfig /renew
```

Kada obnova (renew) bude uspješna vidjet ćete isti izlaz kao ipconfig komanda, sa pregled nove IP adrese, maske podmreže i gatewaya.
Računar čuva lokalnu keš memoriju svih DNS zapisa koje je posjetio. Ova keš memorija se koristi za brzo prevođenje imena domena na ispravnu IP adresu. Na ovaj način vaš računar ne mora kontaktirati DNS server svaki put kada posjetite Google.com, na primjer.

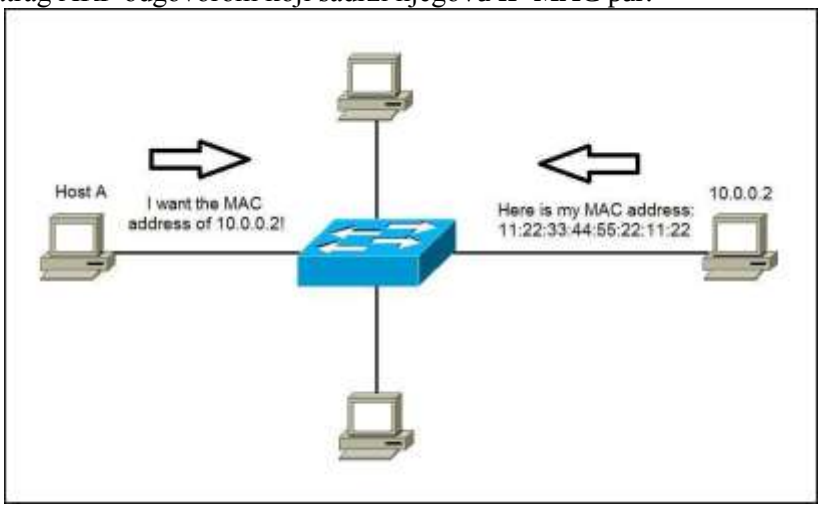
Za pregled sadržaja DNS keša možete koristiti parametar displaydns (kao naredbu ipconfig /displaydns)

**Parametar /flushdns** naredbe ipconfig će sadržaj lokalne DNS keš memorije obrisati (resetovati).

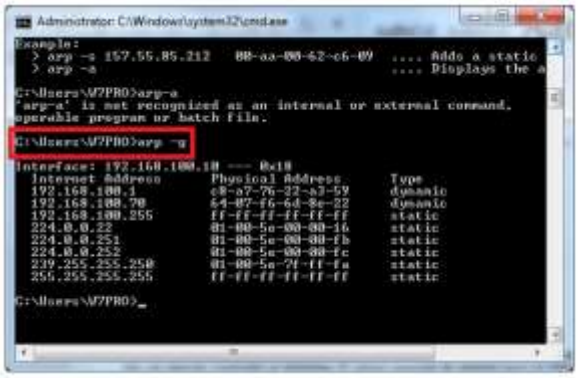
**ipconfig / showclassid, ipconfig / setclassid**
Ove opcije upravljaju identifikatorima klase DHCP-a. Klase DHCP mogu administratorima da definišu na DHCP serveru kako bi primjenili različite mrežne postavke na različite tipove klijenata. Ovo je napredna karakteristika DHCP-a koja se obično koristi u poslovnim mrežama, a ne na kućnim mrežama.

# Komanda ARP

ARP (*Address Resolution Protocol*) je komunikacijski protokol kojim se dobiva fizička adresa na lokalnoj mreži iz poznate mrežne adrese. Najrašireniji njegova primjena danas je na Ethernetu gdje se IP adrese povezuju s MAC adresama. ARP omogućuje povezivanje računara po fizičkom sloju odnosno razrješava veze između IP adresa i adresa koje koristi drugi sloj.
Program-komanda ARP.EXE omogućava pregled i uređivanja ARP tabele. Arp naredba omogućava mapiranje fizičke adrese poznate kao IPv4 adrese. Ova metoda uključuje slanje ARP requesta. Uređaj za koji su potrebni podatci upućuje ARP zahtjev na mrežu, a lokalni uređaji odgovarju natrag ARP odgovorom koji sadrži njegovu IP-MAC par.




*Primjer razmjene ARP poruka*





U cmd prozoru ukucajte **arp –a** i pritisnite **Enter**.
Ne budite iznenađeni ako je tabela prazna. Poruka koja de biti prikazana će vjerovatno biti, '*No ARP Entries Found'*. Windows računari uklanjaju bilo koje adrese koje nisu korištene nakon par minuta.
Pokušajte ping par lokalnih adresa i websajtova URL. Onda opet pokrenite komandu. Slika ispod prikazuje moguće rezultate **arp –a** komande.

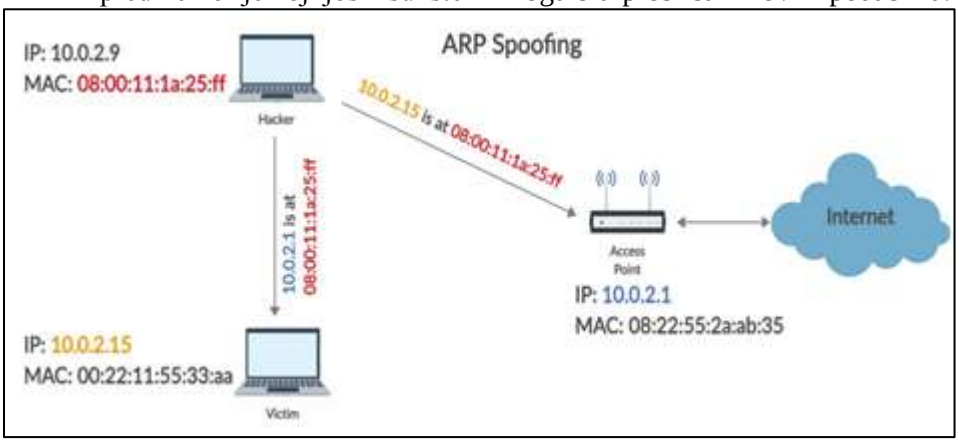
# Rad i opasnosti korištenja ARP protokola

Da malo analiziramo i sam ARP protokol i opasnosti koje on krije. ARP protokol povezuje MAC i IP adrese. Evo pojednostavljenog opisa kako on radi:

- Novi računar prilikom pridruživanja u LAN dobije jedinstvenu IP adresu.
- Paketi podataka stižu do LAN gateway-a i namijenjeni su određenom računaru.
- Gateway zahtjeva od ARP-a da pronađe MAC adresu koja odgovara IP adresi iz paketa.
- Šalje se poruka ARP zahtjeva („tko je X.X.X.X reci Y.Y.Y.Y“, gdje su X.X.X.X i Y.Y.Y.Y IP adrese) koristeći Ethernet adresu za emitiranje, a tu poruku prime svi u LAN-u. Samo uređaj koji ima traženu adresu odgovori, dok ostali odbace poruku.
- Ciljni uređaj formira odgovor „X.X.X.X je hh:hh:hh:hh:hh:hh“, gdje je hh:hh:hh:hh:hh:hh MAC adresa računara s IP adresom X.X.X.X.
- Y.Y.Y.Y primi taj odgovor i pohrani par IP – MAC adresa u svoju ARP predmemoriju (*ARP cache*).
- Svaki put kada dođe do zahtjeva za nekom MAC adresom prvo se provjeri je li pohranjena u predmemoriji, ako je koristi je, a ako nije šalje ARP zahtjev da je sazna i pohrani.

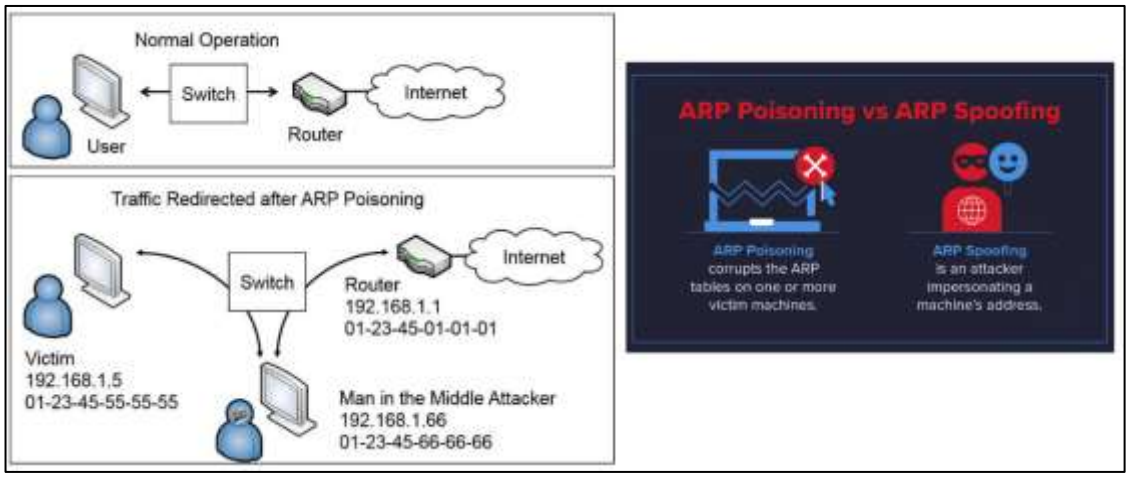
Iz perspektive sigurnosti i računarske forenzike ARP je jedan od faktora rizika. Često se zaboravlja uspostaviti bolju sigurnost drugom sloju OSI modela (sloju podataka gdje je smješten i ARP). Na taj način mreža ostaje otvorena za razne napade.

Nedostaci i ranjivosti ARP-a
Nema mehanizama za provjeru autentičnosti dolaznih paketa što znači da bilo ko može krivotvoriti ARP poruku koja sadrži zlonamjerne informacije za oštećenje ARP predmemorije ciljnog uređaja.
Podaci iz ARP predmemorije koji još nisu istekli mogu biti prebrisani novim podacima.




ARP je „stateless“ protokol i zbog toga će se smjestiti i pohraniti u predmemoriju bilo koji podaci pristigli s ARP odgovorom bez obzira na to jesu li ili nisu zatraženi.
Upravo te ranjivosti mogu dovesti do ARP lažiranja (eng. **ARP spoofing**) koje može učiniti komunikaciju nesigurnom i podložnom za ostale napade kao što je čovjek u sredini (MITM), uskraćivanje usluge (DOS), napad kloniranja, otmica sesije i mnogi drugi.

ARP lažiranje ima još nekoliko naziva i varijacija, a oni glase „*ARP poison routing*“ i „*ARP cache poisoning*“. U ovom napadu napadač šalje lažne ARP poruke ciljnoj lokalnoj mreži kako bi se u predmemoriji napadnutog uređaja smjestio i zapamtio par MAC i IP adrese koje se mogu dalje koristiti za zlonamjerne radnje. Taj par adresa najčešće predstavlja MAC adresu napadača i IP adresu nekog legitimnog uređaja ili servera unutar mreže.



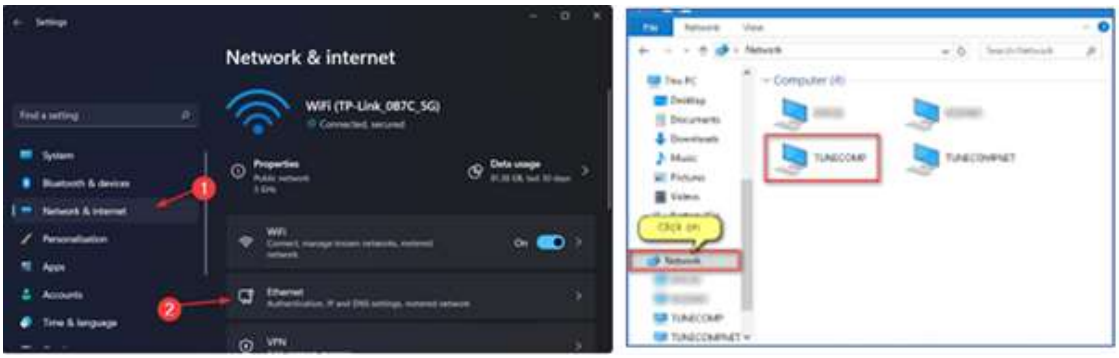

**Uskraćivanje usluge (DOS** napad *Denial-of-service attack***)** iskorištavanje je ARP lažiranja predmemorije. Napadač može dati žrtvi lažni zadani pristupnik koji ne postoji na mreži i na taj način žrtva gubi vezu s mrežom.
**MAC poplava** (*MAC flooding*) tehnika je kojom se preopterete „switch“ uređaji u mreži i time često prelaze u „hub“ način rada. Tako preopterećen uređaj prestaje održavati sigurnost na portovima i šalje sav promet svim računarima u toj mreži. Na taj način napadač može “njuškati” pakete u mreži.

Lažni podaci u ARP keš predmemoriji mogu rezultirati slanjem podataka s računara žrtve na računar napadača umjesto na stvarno odredište.
Slanje lažnih ARP poruka može se izvoditi s kompromitiranog uređaja u LAN-u, ali i direktno s napadačevog računara koje je izravno povezano na ciljni LAN. Kada je ARP lažiranje uspješno provedeno tada napadač može raditi neke ostale zlonamjerne radnje kao što su:

- Pregledavanje paketa i prosljeđivanje prometa na originalno odredište (presretanje: i*nterception*)
- Izmjenjivanje podataka prije prosljeđivanja (napad čovjeka u sredini: *Man-in-the-middle attack*)
- Pokretanje napada uskraćivanja usluge

# Otkrivanje mreže- Network discovery- kod Windowsa

Kod Windowsa *Otkrivanje mreže* je mrežna postavka koja utiče na to da li vaš računar može pronaći druge računare i uređaje na mreži i da li drugi računari na mreži mogu pronaći vaš računar.



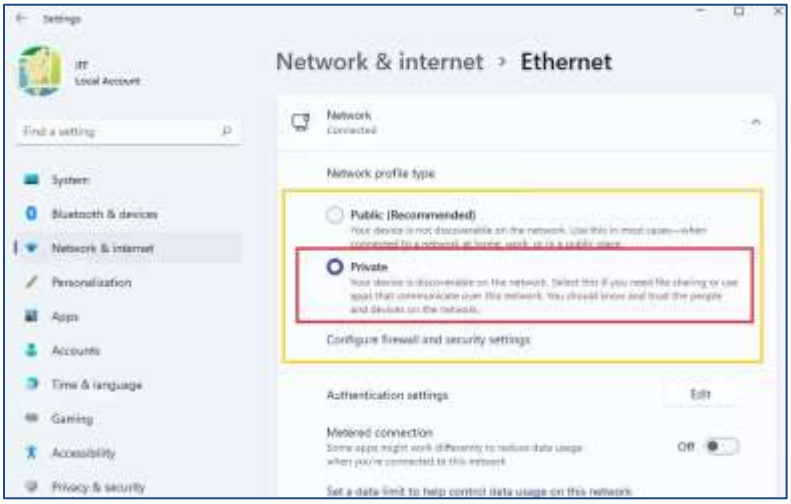

*Otključivanje - otkrivanja mreže kod Win 11 i Win 10*

Otkrivanje mreže zahtijeva da se pokrenu usluge DNS klijent, Function Discovery Resource Publication, SSDP Discovery i UPnP Device Host, da je otkrivanju mreže dozvoljeno komunicirati preko Microsoft Defender-a (Windows Firewall zaštitnog zida) i da drugi zaštitni zidovi ne ometaju otkrivanje mreže. Ethernet mreže nazivaju se "Network", dok se bežične mreže nazivaju prema SSID-u hotspota.

U operativnom sistemu Windows[32] postoje dva profila (poznata i kao mrežna lokacija ili tip mreže) za Ethernet i Wi-Fi mreže.
*Javna mreža* -**Public**- ovaj mrežni profil se dodjeljuje novostvorenim vezama. To čini da vaš računar nije vidljiv za druge uređaje na istoj mreži. Smatra se da javna mreža nije bezbjedna, npr. da se dijeli sa trećom stranom bez jake zaštite. Windows primjenjuje određena restriktivna pravila zaštitnog zida gdje su deljenje datoteka, otkrivanje mreže, prebacivanje medija i automatsko podešavanje štampača onemogućeni. NAPOMENA: uključivanje u javnu mrežu trebalo bi da znači da vi predefinisano **niste vidljivi** drugim u mreži, niste dostupni trećoj strani.
*Privatna mreža* -**Private network**- ovaj profil mrežne veze je primjenjiv na kućne mreže. Manje je restriktivan i omogućava dijeljenje vaših datoteka i foldera. Vi ste u ovom profilu **vidljivi** drugim računarima na mreži. Ako vjerujete povezanoj mreži, možete postaviti ovaj profil za nju. Ustvari postoji i treći profil: *Mreža domena* - **Domain network** - profil koji se automatski primjenjuje kada se vaš PC pridruži Active Directory-ju[33], a vi se autentifikujete na kontroleru domena.

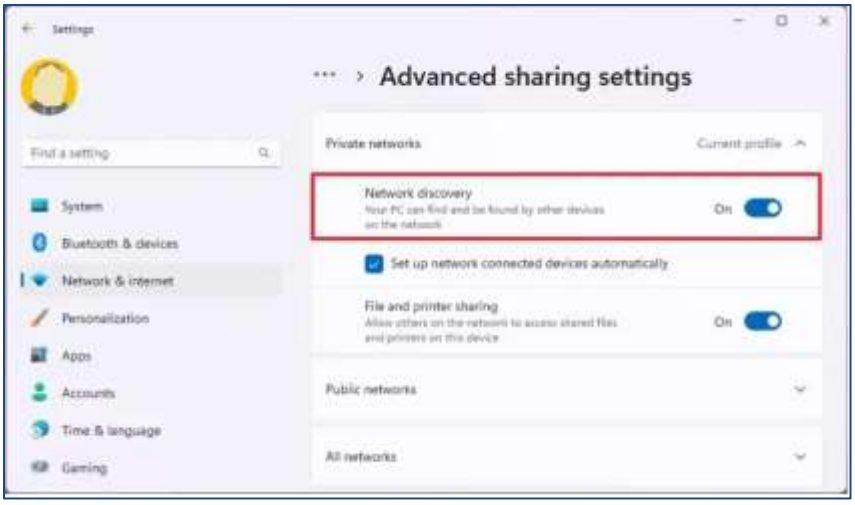
[32] U ranijim vertijama postojale su četiri mrežne lokacije: kuća, posao, javna i domena; privatna mreža u Windows 10 je ista kao kućna mreža u prethodnim verzijama OS-a,
[33] Active Directory domena je kolekcija objekata unutar mreže Microsoft Active Directory. Objekt može biti jedan korisnik ili grupa ili može biti hardverska komponenta, kao što je računar ili štampač. Svaka domena sadrži bazu podataka koja sadrži informacije o identitetu objekta.

Za podešavanje Eternet postavki: 1.Otvorite Postavke- Settings/ 2. Kliknite na Mreža i internet- Network & internet/ Kliknite na Ethernet stranicu na desnoj strani/ U odjeljku „Vrsta mrežnog profila“ – “*Network profile type*” odaberite vrstu profila koji želite.




Slično možete izvršiti podešavanje za WiFI uređaj (samo u koraku 2. Umjesto Ethernet birate WiFi.

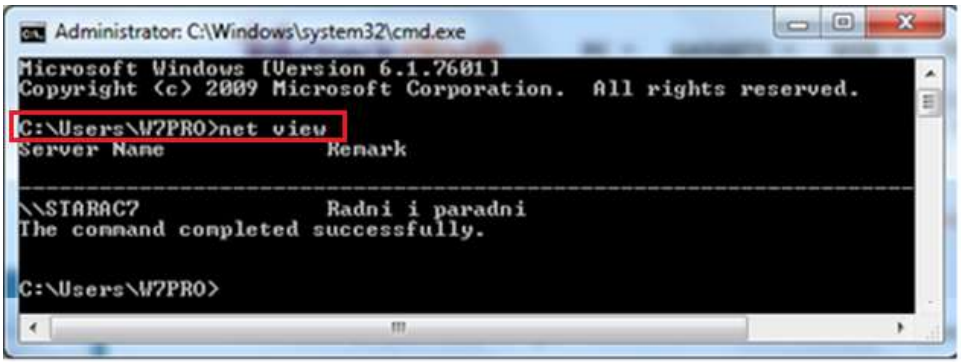
Predefinisano postavkama, kada se prvi put povežete na novu mrežu (žičnu ili bežičnu), od vas će biti zatraženo "Želite li dozvoliti da vaš PC mogu otkriti drugi računari i uređaji na ovoj mreži?" pomoću čarobnjaka za mrežnu lokaciju. Uključivanje ove postavke priprema vaš računar za dijeljenje datoteka i uređaja na mreži. Na osnovu mrežne lokacije koju odaberete, Windows će mreži automatski dodijeliti stanje otkrivanja mreže i automatski postaviti odgovarajuće Windows zaštitni zid i sigurnosne postavke za tip mreže na koju ste se povezali.




Poslije toga Mrežnu lokaciju možete promijeniti bilo kada. Takođe se nude opcije naprednog podešavanja, ali to je područje Windows operativnog sistema, pa ih ovdje nećemo komentarisati. Pogotovo kreiranje sopstvenog mrežnog prfila koje zahtjeva korištenje *Registry Editor*-a.

Otkrivanje mreže je proces koji omogućava računarima i uređajima da pronađu jedni druge kada su na istoj mreži. To je početni korak koji sistem administratori poduzimaju kada žele mapirati i nadgledati svoju mrežnu infrastrukturu. Ovaj proces se ponekad naziva i otkrivanjem topologije.
Da biste pronašli računare u mreži na Windows 11, koristite ove korake:
1. Otvorite File Explorer.
2. Kliknite na Mreža-Network u lijevom prozoru.
3. Pogledajte računare dostupne na mreži (otkrivanje može potrajati i malo duže u zavisnosti od okruženja).
4. Dvaput kliknite na uređaj da pristupite njegovim zajedničkim resursima, kao što su dijeljeni folderi ili dijeljeni štampači.


Može se koristiti i komandna liniju da vidite listu svih uređaja i računara povezanih na vašu mrežu. Da biste to mogli učiniti, morate se prijaviti na svoj PC koristeći administratorski nalog i unijeti komandu ***net view***.



# Promjena TCP/IP postavki kod Windowsa – Majkrosoft uputstvo:


TCP/IP definiše način na koji računar komunicira sa drugim računarima.
Da biste olakšali upravljanje TCP/IP postavkama, preporučujemo da koristite automatizovani Dynamic Host Configuration Protocol (DHCP).
DHCP automatski dodjeljuje adrese Internet protokola (IP) računarima na mreži ako mreža to podržava. Ako koristite DHCP, ne morate da promjenite TCP/IP postavke ako premjestite računar na drugu lokaciju, a DHCP ne zahtijeva da ručno konfigurišete TCP/IP postavke kao što su Domain Name System (DNS) i Windows Internet Name Service (WINS).

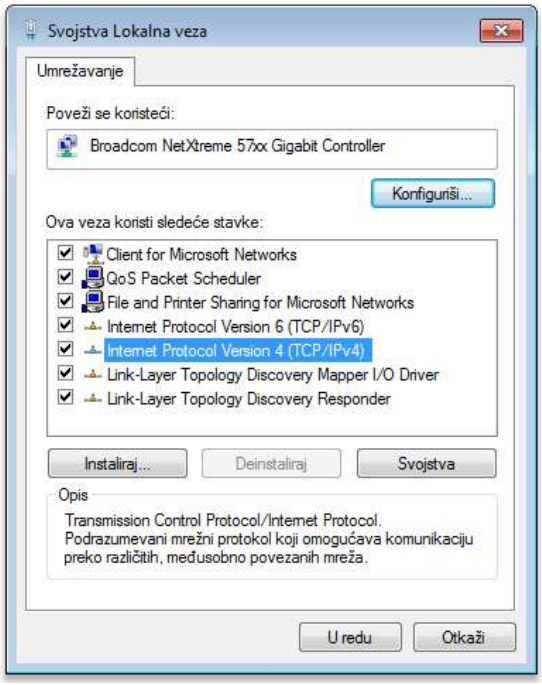
Da biste omogućili DHCP ili promjenili druge TCP/IP postavke, slijedite ove korake:

1. Otvorite opciju „Mrežne veze“ tako što ćete kliknuti na dugme Start , a zatim izabrati stavku Kontrolna tabla. U polju za pretragu otkucajte termin adapter, a zatim u odjeljku „Centar za mrežu i dijeljenje“ izaberite stavku Prikaz mrežnih veza.
2. Kliknite desnim tasterom miša na Internet vezu koju želite da promijenite, a zatim izaberite stavku Svojstva. Ako vam bude zatražena administratorska lozinka ili njena potvrda, otkucajte lozinku ili je potvrdite.
3. Izaberite karticu Umrežavanje. U okviru Ova veza koristi sledeće stavke izaberite stavku Internet Protokol Verzija 4 (TCP/IPv4) ili Internet Protokol Verzija 6 (TCP/IPv6), a zatim izaberite stavku Svojstva.
4. Da biste naveli postavke IPv4 IP adrese, izvršite neku od sljedećih radnji:
   - Da biste automatski pribavili IP postavke koristeći DHCP protokol za dinamičko konfigurisanje računara je skup pravila koji omogućava uređajima na računarskoj mreži da traže i dobiju IP adresu od DHCP servera, dakle da pribavi automatski dijeljenu adresu i sazna dodatne informacije kao što je adresa njegovog rutera za prvi skok i adresa njegovog DNS servera. DHCP je u stanju da automatizuje mrežne aspekte, otuda je i nazvan plug-and-play protokolom.)

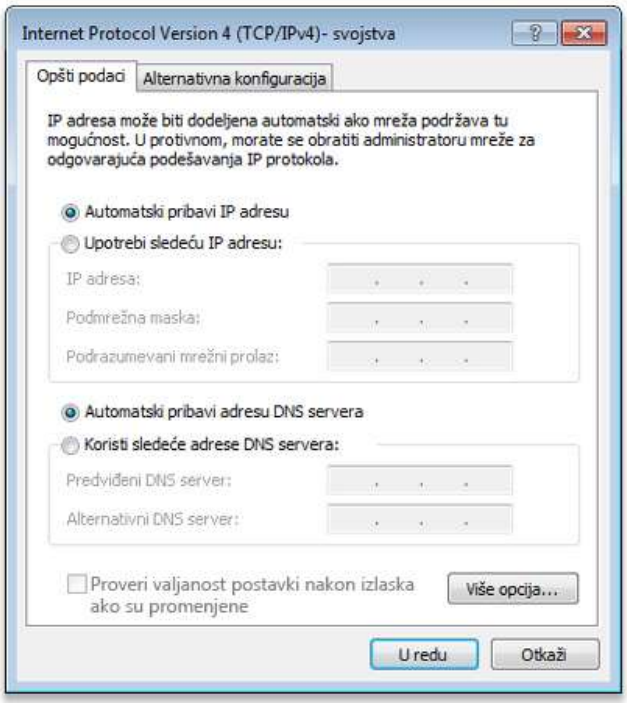
Izaberite stavku Automatski pribavi IP adresu, a zatim kliknite na dugme OK.

- Da biste naveli IP adresu, izaberite stavku Koristi sljedeću IP adresu, a zatim u poljima IP adresa, Podmrežna maska i Podrazumjevani mrežni prolaz otkucajte postavke IP adrese.

5. Da biste naveli postavke IPv6 IP adrese, izvršite neku od sledećih radnji:
   - Da biste automatski pribavili IP postavke koristeći DHCP, izaberite stavku Automatski pribavi IPv6 adresu, a zatim kliknite na dugme OK.
   - Da biste naveli IP adresu, izaberite stavku Koristi sledeću IPv6 adresu, a zatim u poljima IPv6 adresa, Dužina podmrežnog prefiksa i Podrazumjevani mrežni prolaz otkucajte postavke IP adrese.




*Dijalog „Svojstva mrežne veze“*




*Dijalog „Svojstva Internet Protocol verzije 4 (TCP/IPv4)“*

6. Da biste naveli postavke adrese DNS servera, izvršite neku od sledećih radnji:
   - Da biste automatski pribavili adresu DNS servera koristeći DHCP, izaberite stavku Automatski pribavi adresu DNS servera, a zatim kliknite na dugme U redu.
   - Da biste naveli adresu DNS servera, izaberite stavku Koristi sledeće adrese DNS servera, a zatim u poljima Predviđeni DNS server i Alternativni DNS server otkucajte adrese primarnih i sekundarnih DNS servera.

7. Da biste promjenili napredne DNS, WINS i IP postavke, kliknite na dugme Više opcija.

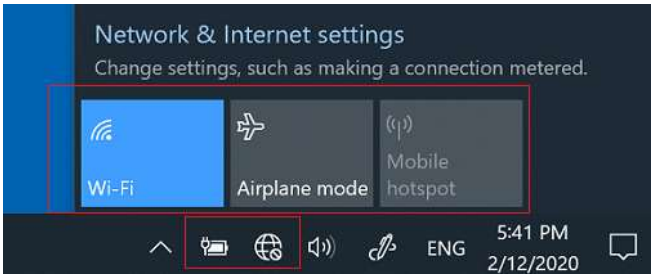
# Popravite probleme sa mrežnom vezom u Windowsu

Standardna rutina za pokretanje automatskog rješavanja mrežnih problema:

Select **Start** > **Settings** > **System** > **Troubleshoot** > **Other troubleshooters**.

Under **Other**, select **Network Adapter** > **Run**.

Ili iz starne linije pristup mrežnom adapteru:




*Windows 11 Windows 10*

Isprobajte ove mogućnosti da biste riješili probleme sa mrežnom vezom.

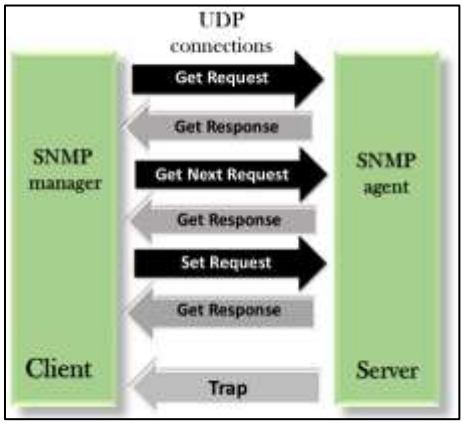
Evo šta Microsoft kaže:

- Provjerite je li Wi-Fi uključen. Odaberite Start > Postavke > Mreža i internet, a zatim uključite Wi-Fi. Zatim odaberite Više opcija (>) pored Wi-Fi, a zatim odaberite Prikaži dostupne mreže. Ako se mreža koju očekujete da vidite pojavi na listi, odaberite je, a zatim odaberite Poveži. Otvorite Wi-Fi postavke
- Provjerite možete li koristiti Wi-Fi mrežu za pristup web stranicama s drugog uređaja. Ako ne možete, ponovo pokrenite modem, ruter i uređaj i ponovo se povežite na Wi-Fi.
- Pokušajte uključiti i isključiti Wi-Fi. Ovo može riješiti probleme ponovnim pokretanjem vaše veze.
- Ako se vaš Surface još uvijek ne povezuje, isprobajte korake na Surface ne može pronaći moju bežičnu mrežu.

*I ovdje Majkrosoft koristi svoje čuveno uputstvao: Isključi pa ponovo uključi,* ***možda*** *proradi.*

# Softver za upravljanje mrežama

Da bi mrežni administrator mogao efikasno obavljati svoj posao, potreban mu je odgovarajući *softver za upravljanje mrežama*. Već je rečeno da je upravljanje mrežom je u internetu implementirano na najvišem, dakle aplikacijskom, sloju OSI protokola.

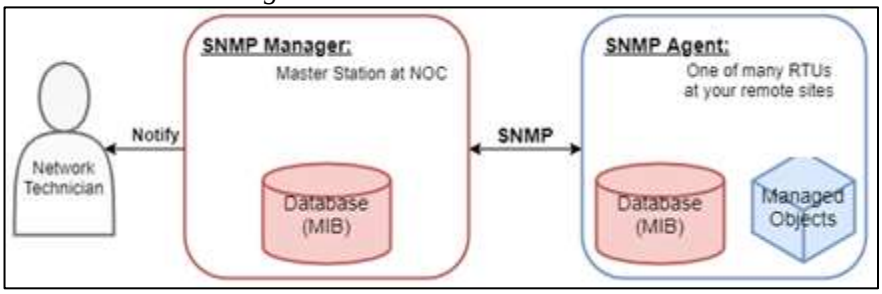



Glavne funkcije softvera za upravljanja mrežom su sljedeće.

• Softver dozvoljava administratoru da "na daljinu" ispituje uređaje poput računara, rutera, svičeva…, te da odredi njihovo stanje ili dobije statistiku o dijelovima mreže na koje su oni spojeni.

• Softver dozvoljava administratoru da "na daljinu" upravlja takvim uređajima, na primjer da mijenja njihove tablice rutiranja ili da konfiguriše njihov mrežni interfejs.

Da bi se naglasila razlika između aplikacija za "obične" korisnike i onih za mrežne administratore, kod sistema za upravljanje mrežama izbjegavaju se termini "klijent" i server". Aplikacijski program na administratorovom računaru naziva se *manager*, a aplikacijski program na mrežnom računaru zove se *agent*.

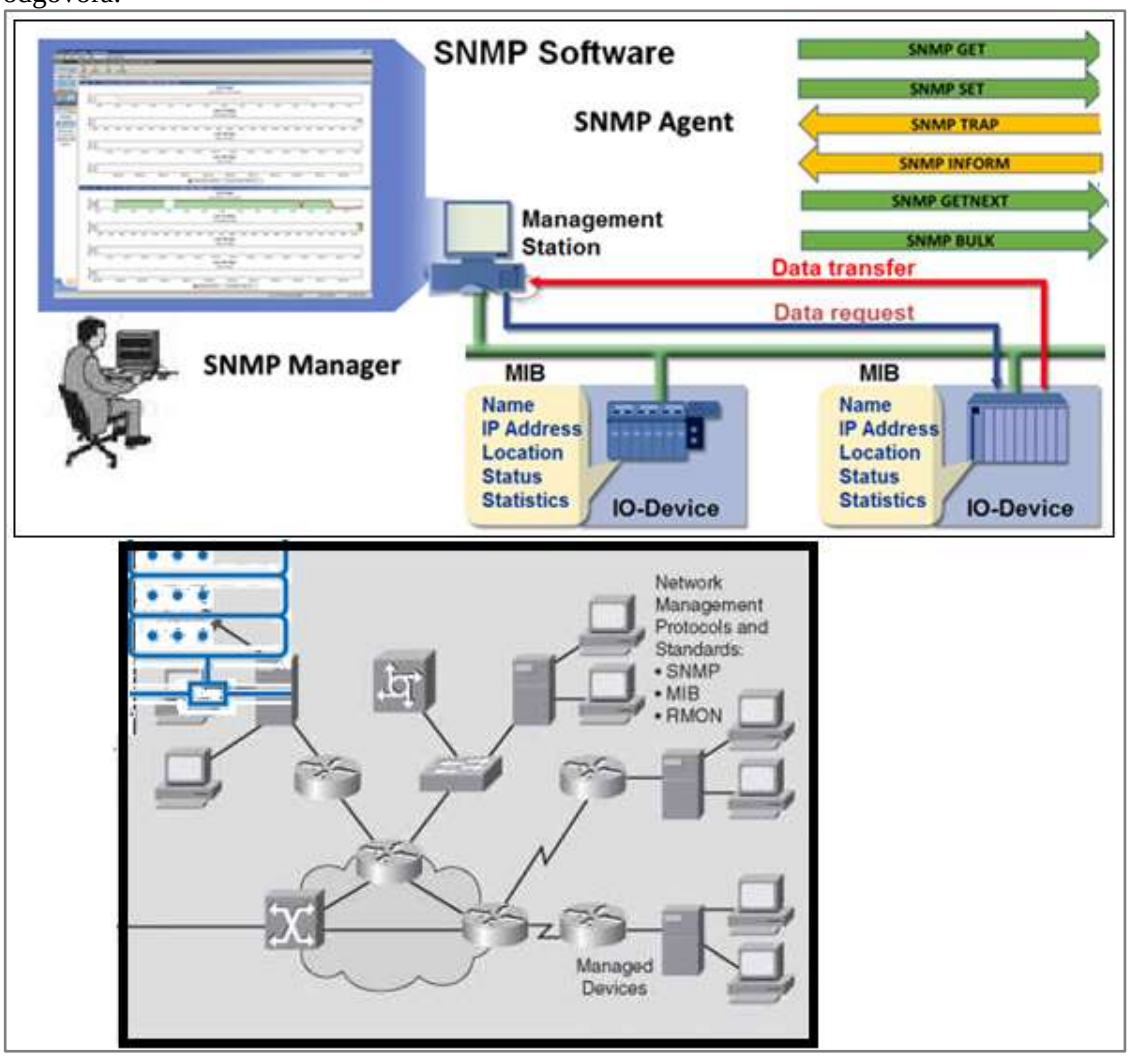



Kad administrator treba stupiti u interakciju s određenim hardverskim uređajem, on pokreće odgovarajući aplikacijski program koji se ponaša kao klijent. Na samom hardverskom uređaju radi drugi aplikacijski program koji se ponaša kao server. Klijent i server koriste uobičajene transportne protokole kao što su TCP ili UDP.

Postoje dva osnovna protokola za upravljanje mrežom, a to su komunikacijski protokol za kontrolu poruka ICMP, (čijim komandama kao što je ping smo se dijelom upoznali ranije) i jednostavni mrežni protokol za nadzor i upravljane, poznat kao SNMP o kome ćemo reći nešto više.

# Jednostavni protokol za upravljanje mrežom – SNMP

Jednostavni protokol za upravljanje internetom zove se *Simple*[34] *Network Management Protocol*. (SNMP). Trenutna verzija je SNMPv3. SNMP definiše način kako manager komunicira s agentom. Dakle, SNMP definiše format i značenje managerovih zahtjeva odnosno agentovih odgovora.




Protokol SNMP je dio sistema za upravljanje mrežom (*Network Management System*), sačinjenog od nekoliko dijelova. To su:

- Jedna ili više upravljačkih stanica (*network management station*) na kojima se izvršavaju upravljačke aplikacije (management application)

[34] Ponekad (rjeđe) se umjesto jednostavan-simple koristi opis standardni-standard

- Jedan ili više upravljanih čvorova (*managed node)* na kojima se izvršavaju upravljački agenti (managed elements)
- Upravljačke informacije (*management information*)
- Protokol SNMP po kojem se upravljačke informacije prenose između upravljačkih aplikacija i agenata

SNMP omogućava prikupljanje većeg broja podataka s uređaja. Praktično svaki mrežni uređaj, mnogi serveri i aplikacije su kreirani da raspoznaju i reagiraju na SNMP protokol, poslan od strane upravljačke mrežne centrale. Upravljačka stanica, često zvana SNMP manager, je program koji nadgleda ili upravlja elementima na upravljanim čvorovima mreže u skladu s politikom upravljanja, koja je određena od strane mrežnog administratora/upravitelja.
Upravljani čvor je mrežni uređaj čijim se stanjima upravlja ili ih se nadgleda te se može izvesti akcija na uređaju ili zabraniti. Kod upravljanog čvora se koristi naziv SNMP agent. Upravljačke informacije, koje su fizički smještene u SNMP agentima, SNMP upravitelji vide ih kao skup upravljanih objekata, a taj skup objekata je objedinjen u jednu bazu upravljačkih informacija (engl. Management Information Base, MIB)

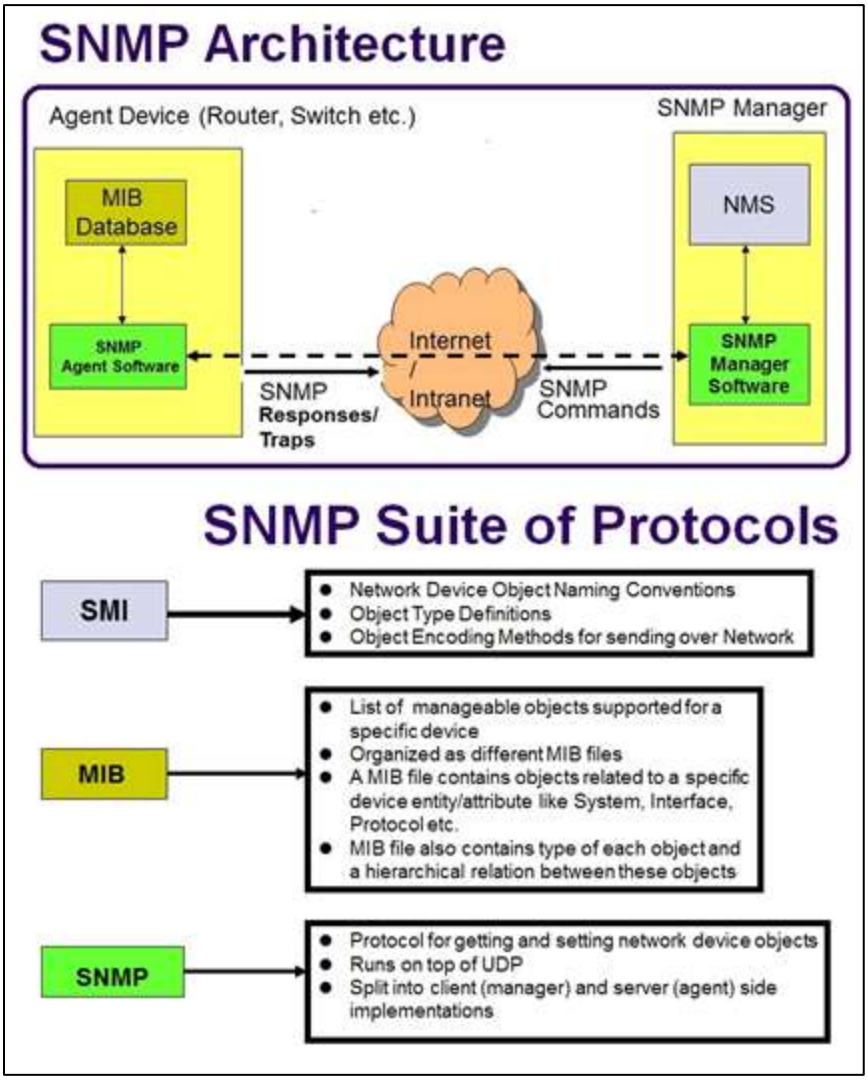
SNMP koristi *paradigmu dohvaćanja i spremanja* (fetch and store paradigm).
Osnovne operacijekoje podržava SNAP protokol su:
• fetch za dohvaćanje vrijednosti nekog virtualnog objekta unutar nekog uređaja,
• store za spremanje vrijednosti u objekt unutar uređaja.
Objekt koji može biti dohvaćen ili spremljen ima jedinstveno ime. Naredba fetch ili store sadrži ime objekta.

Nadgledanje udaljenog uređaja postiže se dohvatom vrijednosti. Definišu se objekti koji opisuju status uređaja. Definišu se imena tih objekata. Da bi saznao status uređaja, administrator naredbom fetch dohvaća vrijednost odgovarajućeg objekta
Upravljanje udaljenim uređajem postiže se kao „nusprodukt“ (side-effect) dobijenih vrijednosti. Definišu se objekti koji odgovaraju pojedinim operacijama kao što su reset brojača, pražnjenje međuregistara (buffera), ponovni start uređaja (reboot) i slično.

SNMP je razvijen 1998. na osnovu RFC 1052 standarda. Taj RFC je kompleksna specifikacija za mrežno upravljanje. Prva verzija protokola opisana je u dokumentu RFC 1157 (IETF standard) 1991. godine. Ovim dokumentom su definisani formati poruka i komunikacioni protokol, poruke koje se mogu razmjenjivati između upravljačkih entiteta i upravljačke stanice koje omogućavaju čitanje i ažuriranje vrednosti, poruke za upozoravanje (tj. alarmiranje – trap). Trenutno je preporučena SNMPv3 koja ima poboljšane sigurnosne mehanizme, kao što je mehanizam za autentifikaciju i zaštitno kodiranje SNMP poruka, tj. enkripciju.

# Baza upravljačkih informacija – MIB

S obzirom na raznolikost opreme kreiran je formalni jezik apstraktnih zapisa koji opisuje pravila i strukture za zastupanje, kodiranje i prenos podataka (*Abstract Syntax Notation One*, ASN.1), kako bi se mogla omogućiti komunikacija između opreme različitih proizvođača. Ovim se standardom postiže definisanje tipova podataka korištenih za konstrukciju SNMP poruke, tako da SNMP agenti i upravljači mogu biti pisani u bilo kojem programskom jeziku.
Standard za izgradnju MIB baze, definicije MIB varijabli te značenje odgovarajućih fetch i store operacija se zove SMI (Structure of Management Information) i on je zapravo podskup od standarda ASN.1.




MIB je logička baza upravljačkih informacija (tj. definicija), napravljena na osnovu konfiguracije i statističkih informacija uskladištenih na uređaju.

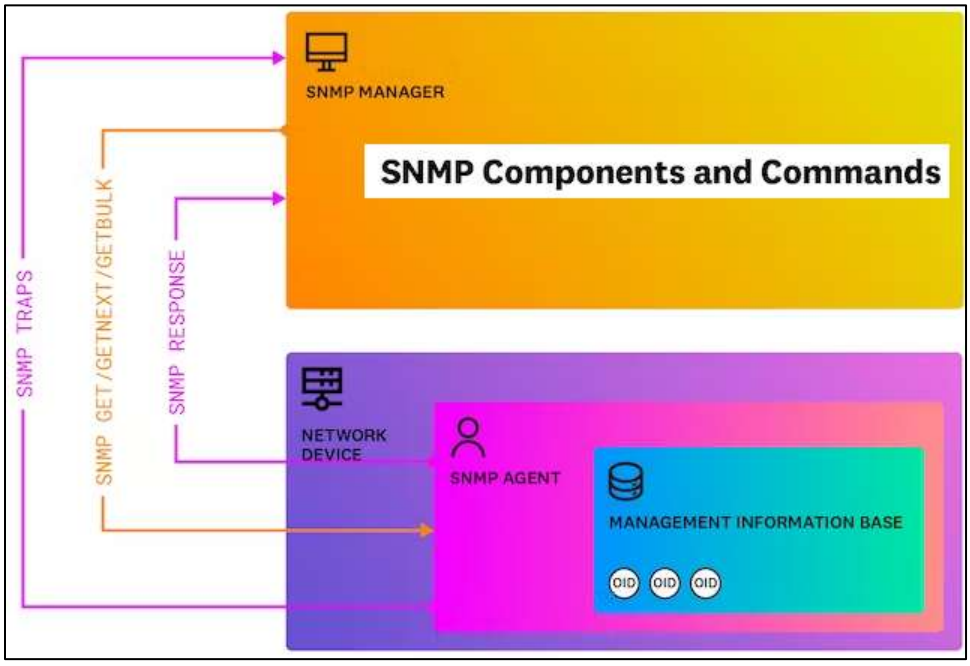
MIB hijerarhija se može prikazati kao stablo. Djeca i roditelji ne mogu imati iste cjelobrojne vrijednosti. Djeca mogu dalje biti roditelji, čineći tako podstablo.
Svaki SNMP agent sadrži popis svih svojih upravljanih objekata i moraju sadržavati sljedeće zapise:

- Ime,
- OID (engl. object identifier),
- Tip podataka,
- Dozvole čitanja i pisanja te
- Kratki opis za svaki objekt SNMP agenta.

Skup svih objekata unutar uređaja kojima SNMP može pristupiti zove se *Baza upravljačkih informacija* (**Management Information Base** - MIB). SNMP zapravo ne definiše MIB. SNMP standard samo definiše format poruke i način kako se poruke kodiraju.
Manager i agent moraju se usaglasiti u pogledu imena objekta te značenja odgovarajućih fetch i store operacija.

## SNMP komande

SNMP može obavljati mnoštvo funkcija, koristeći mješavinu push i pull komunikacija između mrežnih uređaja i sistema upravljanja.

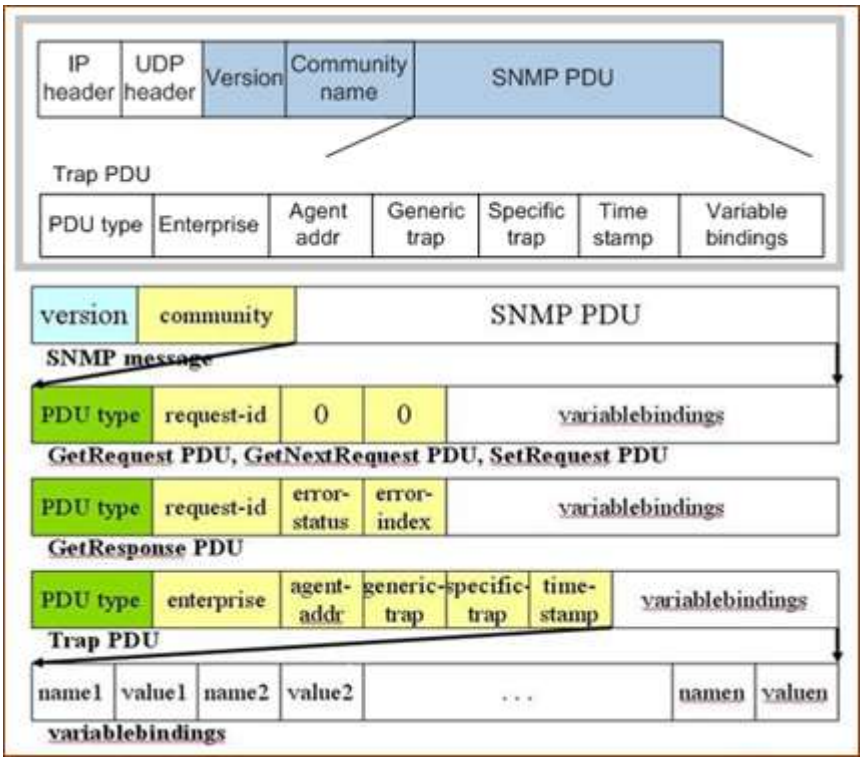



Može izdati naredbe za čitanje ili pisanje, kao što je resetovanje lozinke ili promjena konfiguracijske postavke. Takođe može izvestiti o tome koliko je propusnog opsega, CPU-a i memorije u upotrebi, a neki SNMP menadžeri automatski šalju administratoru e-mail ili tekstualnu poruku ako je unapred definisani prag premašen.

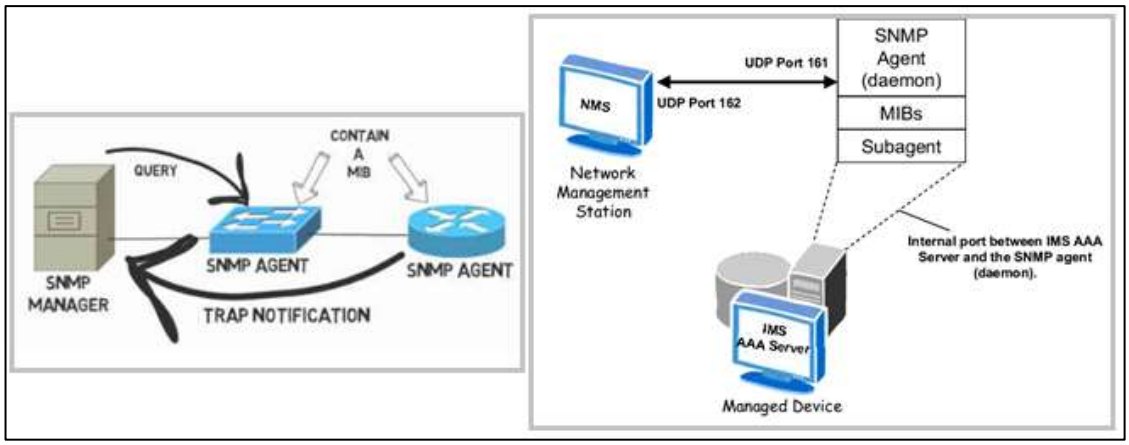
Većinu vremena, SNMP funkcioniše sinhrono, s komunikacijom koju pokreće SNMP menadžer i agent koji šalje odgovor. Naredbe i poruke (koje se prenose preko UDP-a unutar TCP/IP protokola), poznate su kao jedinice podataka protokola (protocol data units, PDU).

Najčešće korištene SNMP naredbe:

- GET zahtjev **GET Request**: generiše SNMP menadžer i šalje agentu da dobije vrijednost varijable, identifikovane njenim OID-om, u MIB-u.
- **GETBULK** zahtjev: SNMP menadžer šalje agentu da efikasno dobije potencijalno veliku količinu podataka, posebno velike tabele.
- **GETNEXT** zahtjev: SNMP menadžer šalje agentu da dohvati vrijednosti sljedećeg OID-a u MIB-ovoj hijerarhiji.
- **INFORM** Request: Asinhrono upozorenje slično TRAP-u, ali zahtjeva potvrdu prijema od strane SNMP menadžera.
- **RESPONSE** ODGOVOR: Agent šalje SNMP menadžeru, izdaje kao odgovor na GET zahtjev, GETNEXT zahtjev, GETBULK zahtjev i SET zahtjev. Sadrži vrijednosti traženih varijabli.
- **SET** zahtjev: SNMP menadžer šalje agentu za izdavanje konfiguracija ili naredbi.
- **TRAP**: Asinhrono upozorenje koje agent šalje SNMP menadžeru da ukaže na značajan događaj, kao što je greška ili neuspjeh, da se dogodio.

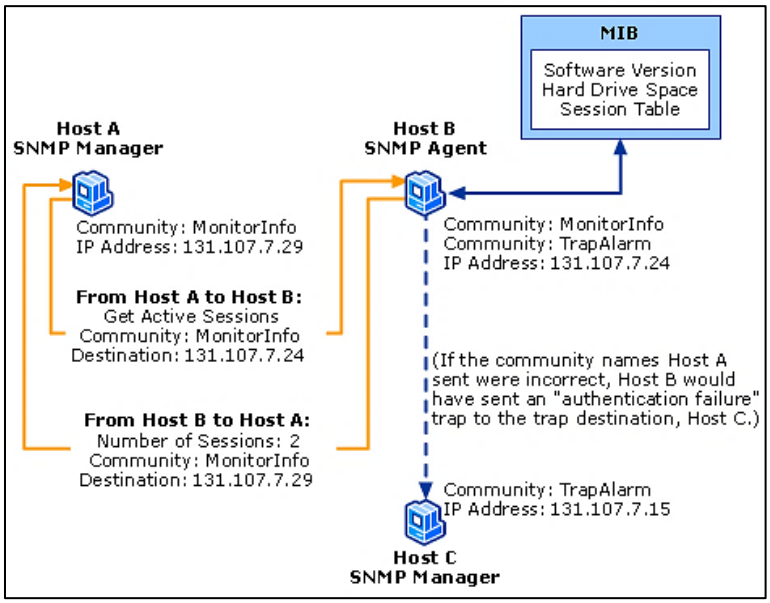


## Opis rada protokola SNMP




SNMP proširuje UDP protokol i može se pojednostavljeno predstaviti koracima:

- agent sluša na UDP portu 161,
- odgovori se šalju na NMS port (1961),
- maksimalna veličina SNMP poruke ograničena je maksimalnom veličinom UDP poruke,
- sve SNMP implementacije moraju primiti pakete najmanje dužine 484 bajta,
- ako dođe do greške prilikom prenosa, prima se poruka na NMS portu 162




*Primjer koji ilustruje korake pri korištenju SNMP protokola*

Host A - SNMP menadžer, šalje poruke sa zahtjevom za informacijama o broju aktivnih sesija, imena zajednice kojima SNMP menadžer pripada, Host B - SNMP agentu (131,107.3.24). Koristi se SNMP Management API biblioteka za izvođenje ovog koraka.

- Host B - SNMP agent, prima poruke i provjerava naziv zajednice (MonitorInfo) sadržan u paketu. Lista imena zajednica se prima i procjenjuje za dozvole pristupa za tu zajednicu i provjerava izvornu IP adresu.
- Ako naziv zajednice ili pristupne dozvole nisu tačni,
- Sa SNMP usluge konfigurisane za slanje trap-zamki za autentifikaciju, Host B - Agent šalje poruke "Neuspjeh autentifikacije" na odredište za trap-zarobljavanje koje je odredio Host C. Hostovi B i C pripadaju zajednici TrapAlarm.
- SNMP Agent Master komponenta
- Imenujte odgovarajućeg ekstenzija da dohvati tražene informacije o sesiji iz MIB-a.
- Koristeći informacije o sesiji preuzete od proširenja, SNMP servis rekonstruiše SNMP poruku koja sadrži broj aktivnih sesija i odredište - IP adresu (131.107.7.29) SNMP menadžera, Host A.
- Host B šalje odgovor Hostu A

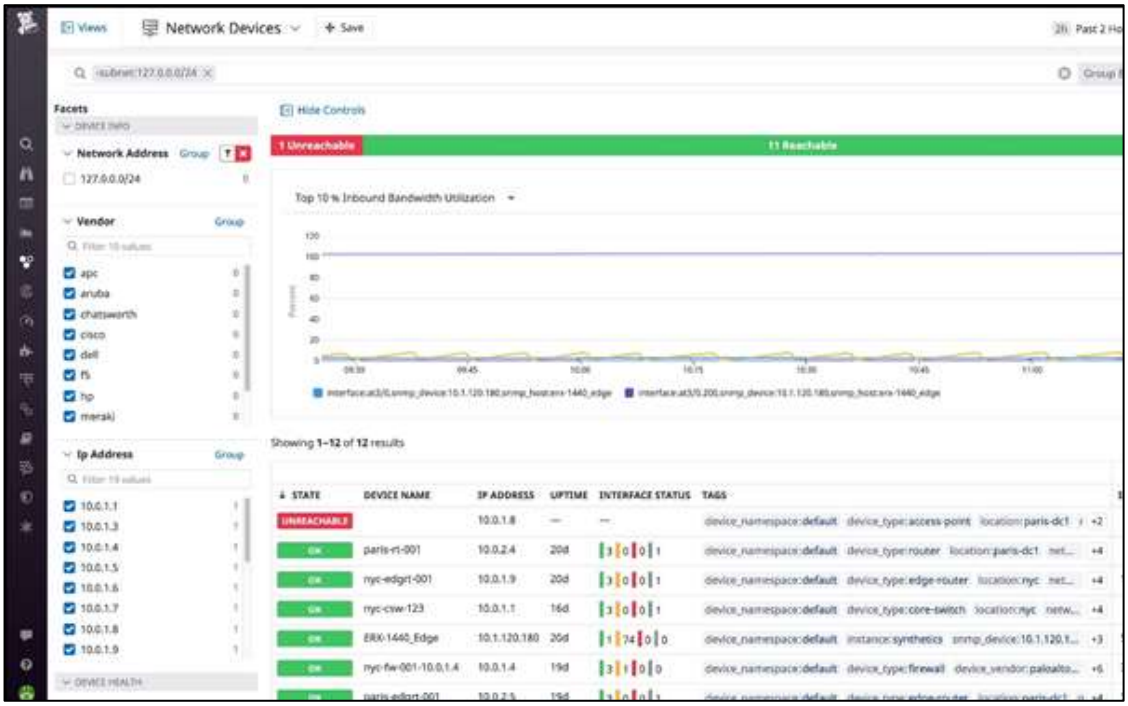
## Programske implementacije koje koriste SNMB

Kod upravljanja mrežama kad postoji potreba za realizacijom složenijeg i funkcionalnijeg mrežnog sistema obično se koriste namjenski softverski paketi.


Ovdje ćemo samo spomenuti nekoliko najčešće korištenih paketa.

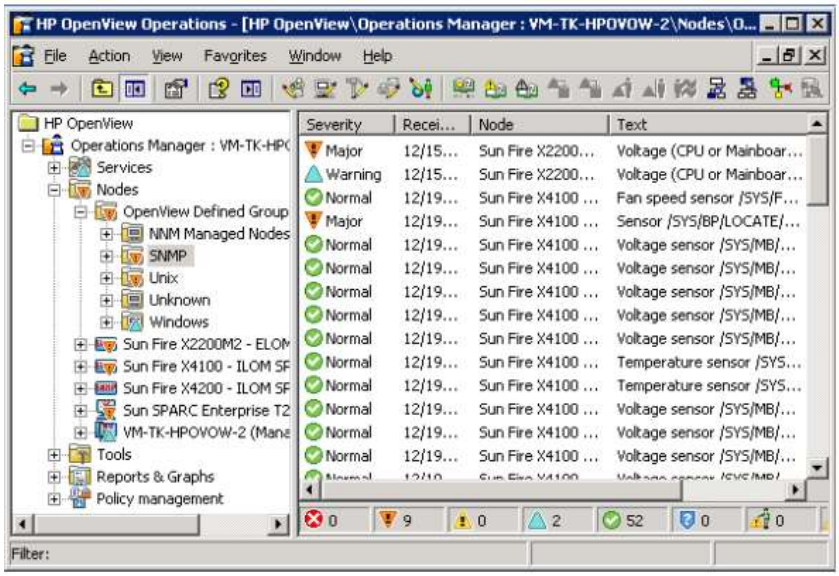
**Datadog Network Device Monitoring**, usluga zasnovana na oblaku prati statuse vaših mrežnih uređaja i izdvaja podatke o prometu koristeći SNMP. Pruža uvid u vaše lokalne i virtuelne mrežne uređaje, kao što su ruteri, prekidači i zaštitni zidovi. Automatski otkriva uređaje na bilo kojoj mreži i prikazuje prikupljati metriku kao što su iskorištenost propusnog opsega, količina poslanih bajtova i određuje da li su mrežni uređaji aktivno.

Ranije je bio vrlo popularan **HP BTO** (prvobitno HP OpenView), proizvod firme Hewlett Packard. Ovaj alat, između ostalog, je omogućavao automatsko otkrivanje mrežne topologije, administriranje korisnika, konfiguriranje intervala prozivanja i druge napredne funkcionalnosti.



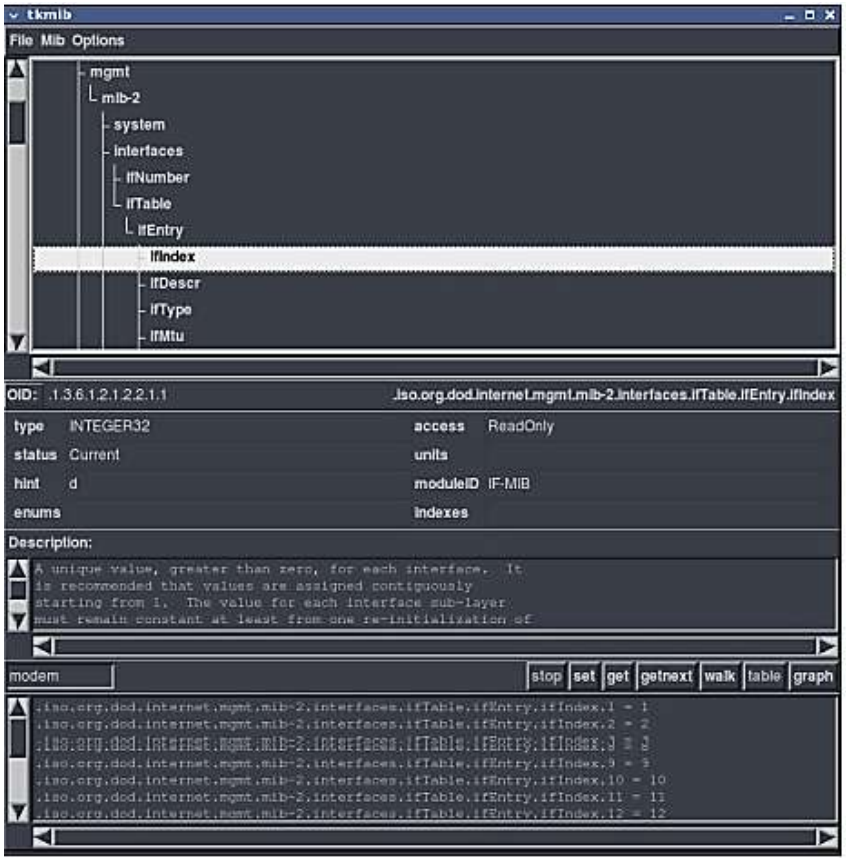

*Datadog pruža vidljivost vašeg cjelokupnog inventara uređaja kojima upravlja SNMP; preuzeto sa: https://www.datadoghq.com/knowledge-center/network-monitoring/snmp-monitoring*

Iako je HP BTO izdan i održavan od strane HP-a, namijenjen je i podržan i za uređaje drugih proizvođača. Proizvodi su danas dostupni kao različiti HP-ovi proizvodi koji se prodaju kroz HP Software Division.




*Neke od operacija i funkcionalnosti HP OpenView-a primjenjene na Windows; Izvor:Hp OpenView*

Postoje i besplatne programske implementacije a među popularnijim je **Net-SNMP** koji podržava sve tri verzije SNMP v1, SNMP v2C i SNMP v3. Moguće ga je jednostavno "skinuti" s Interneta. Podržava IPv4 i IPv6, radi na većini operativnih sistema, sadrži generičku klijentsku biblioteku, paket aplikacija komandne linije, predstavlja visoko proširiv SNMP agent, koji sadrži Perl i Python module.

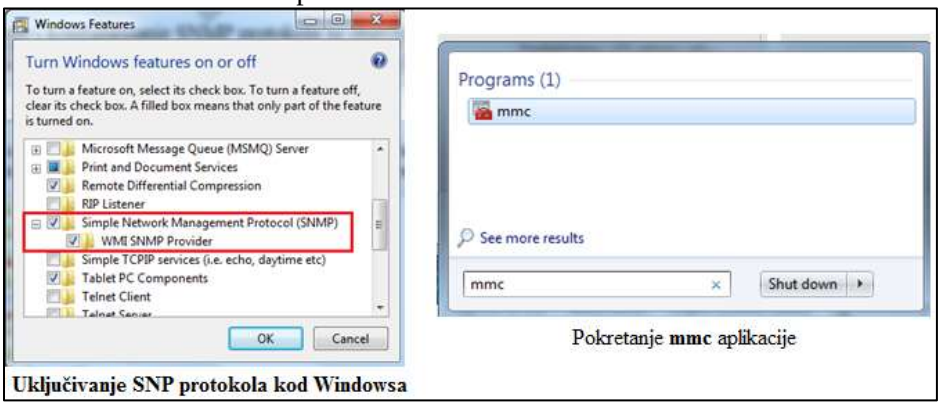


v

*NET-SNMP GUI Izvor: net-snmp.sourceforge.net*

# Instalacija i korištenje SNMP protokola kod Windowsa

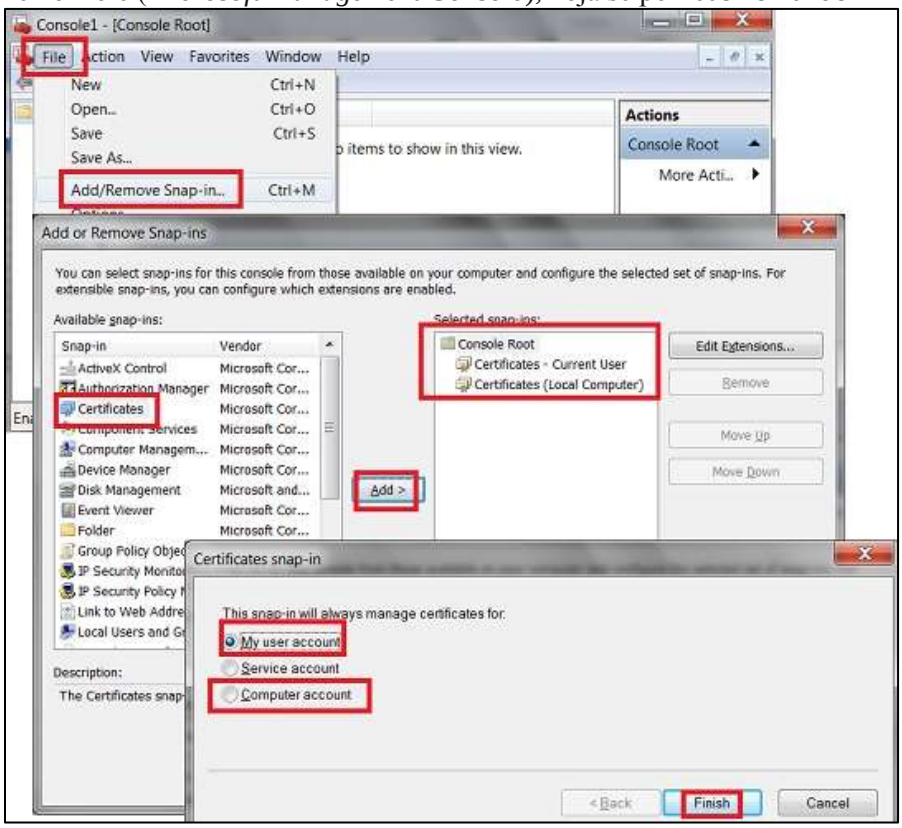
SNMP provajder i protokol **nije** instalisan predefinisano i treba ga naknadno instalisati (čekiranjem). Windows koriste Windows Management Instrumentation (WMI). Podešavanje i konfigurisanje SNMP protokola se obavlja iz Control panela izborom opcije Turn Windows features on or off iz ponude Programs and Features




Uključivanje SNP protokola kod Windowsa

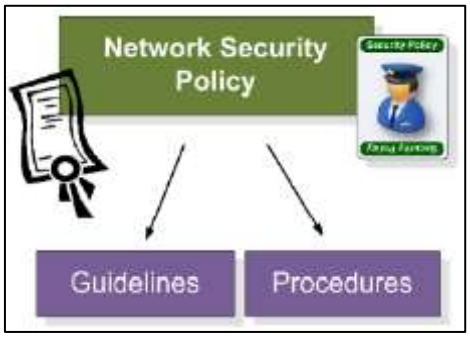
Pokretanje **mmc** aplikacije

Monitor performansi (*Performance Monitor*) se može pokrenuti naredbom *perfmon* ili iz upravljačke konzole (*Microsoft Management Console*), koja se pokreće komandom **mmc**.



# Sigurna mreža i sigurnosna politika

Postoje razne definicije sigurne mreže, na primjer:
• To je mreža koja ne dopušta osobama izvana da pristupe računarima unutar naše organizacije.
• To je mreža koja sprečava osobama izvana da mijenjaju informacije na web stranicama naše organizacije.
• To je mreža koja osigurava povjerljivost komuniciranja, na primjer da e-mail poruku ne može čitati nitko osim pošiljatelja i primatelja.
Budući da nema jednoznačne definicije sigurne mreže, svaka organizacija mora definisati svoju *sigurnosnu politiku* (security policy) gdje određuje *šta* treba dozvoliti, šta treba spriječiti. Kod definisanja sigurnosne politike potrebno je naći kompromis između sigurnosti, jednostavnosti i cijene korištenja mreže. Treba odlučiti koji aspekti sigurnosti su za dotičnu organizaciju najvažniji, a koji se eventualno mogu zanemariti.




Politika mrežne sigurnosti (Network security policy, NSP) je okvirni **dokument** koji opisuje **pravila i procedure** za pristup računarskoj mreži.
NSP određuje kako se politike primjenjuju i izlaže neke od osnovne arhitekture okruženja sigurnosti kompanije/mrežne sigurnosti. NSP politike bi se mogle izraziti kao skup instrukcija koje razumije mrežni hardver posebne namjene namijenjen za osiguranje mreže.

**Aspekti sigurnosti**
Postoje razni aspekti sigurnosti. Nabrojat ćemo nekoliko najvažnijih.
• *Integritet podataka*. Da li primatelj zaista dobiva podatke koje je poslao pošiljatelj, ili ih je neko putem promijenio?
• *Dostupnost podataka*. Da li ovlašteni korisnici mogu doći do podataka, ili ih neko u tome ometa?
• *Povjerljivost podataka*. Da li su podaci koji putuju mrežom zaštićeni od neovlaštenog čitanja?
• *Autentičnost podataka*. Da li podaci koje je dobio primatelj zaista potječu od navedenog pošiljatelja?
**Čuvanje integriteta pomoću kriptovanja**
Tehnike za zaštitu podataka od slučajnog oštećenja (na primjer kontrolni zbirovi) ne osiguravaju integritet. Naime, ako napadač namjerno mijenja podatke koji prolaze mrežom, on će također promijeniti i kontrolni zbroj.
Stvarna zaštita od zlonamjernog mijenjanja podataka zasniva se na *kriptografskoj hash funkciji* i tajnom ključu koji je poznat samo pošiljatelju i primatelju.
Postupak je sljedeći:
• Pošiljatelj na osnovu sadržaja poruke i ključa računa vrijednost H hash funkcije i šalje je uz poruku.
• Primatelj ponavlja isti račun i provjerava da li je dobio istu vrijednost H.
Napadač koji pokušava promijeniti poruku ne može na ispravan način promijeniti i H jer ne zna ključ.

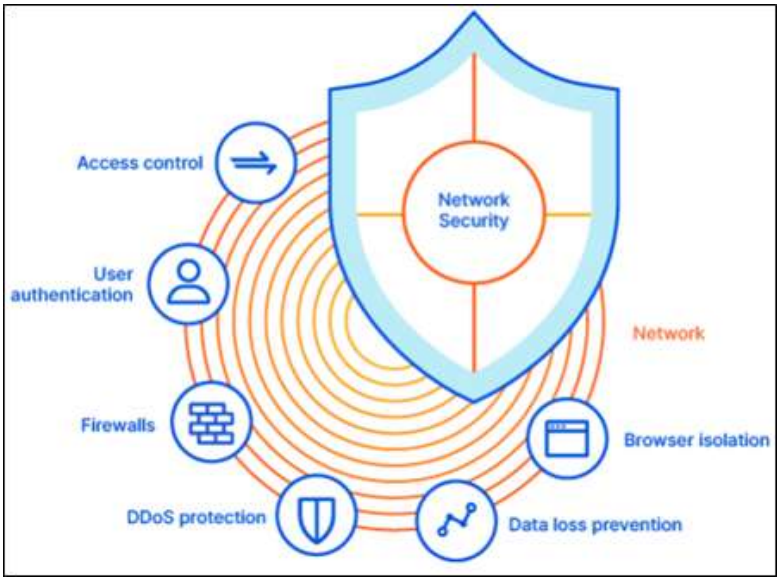
**Čuvanje dostupnosti pomoću lozinki**

Dostupnost podataka osigurava se tako da se neovlaštenim korisnicima spriječi nepotrebno zauzimanje računarnih ili mrežnih resursa. Jedan način zaustavljanja neovlaštenih korisnika je uvođenje lozinki za pristup resursima. Ako uvedemo lozinke, onda moramo paziti da se one ne šalju po mreži u nezaštićenom obliku, pogotovo ako je riječ o bežičnoj mreži.

Na primjer, ako se korisnik prijavljuje za rad na drugom računaru pomoću Telnet, tada svako ko prisluškuje promet na mreži može doznati njegovu lozinku. Danas postoje protokoli koji prenose lozinke u kriptiranom obliku, a primjer ssh umjesto Telnet.

## Tehnologije za sigurnost

Gotovo sve računarske mreže su povezane i čine dio Internet infrastrukture. Pošto je internet javno dostupan prenos informacije i podataka je izložen mnogobrojnim sigurnosnim problemima. Metode za sigurnost poput kriptiranja prilično su složene. Zato su razvijene neke standardne tehnologije, koje se kao gotova rješenja mogu uključiti u rad pojedinih mreža ili ugraditi u druge aplikacije.




Evo nekoliko takvih standardnih tehnologija za sigurnost koje se intenzivno koriste na Internetu.

• *Intrusion Detection System* (IDS). Sistem koji prati sve pakete koji stižu u lokalnu mrežu i upozorava administratora ako se pojavila neka sumnjiva radnja, kao na primjer sistematsko ispitivanje TCP portova u potrazi za aktivnim poslužiteljem (TCP port scanning) ili uspostavljanje beskorisnih TCP veza u svrhu namjernog zagušenja servera (SYN flood).

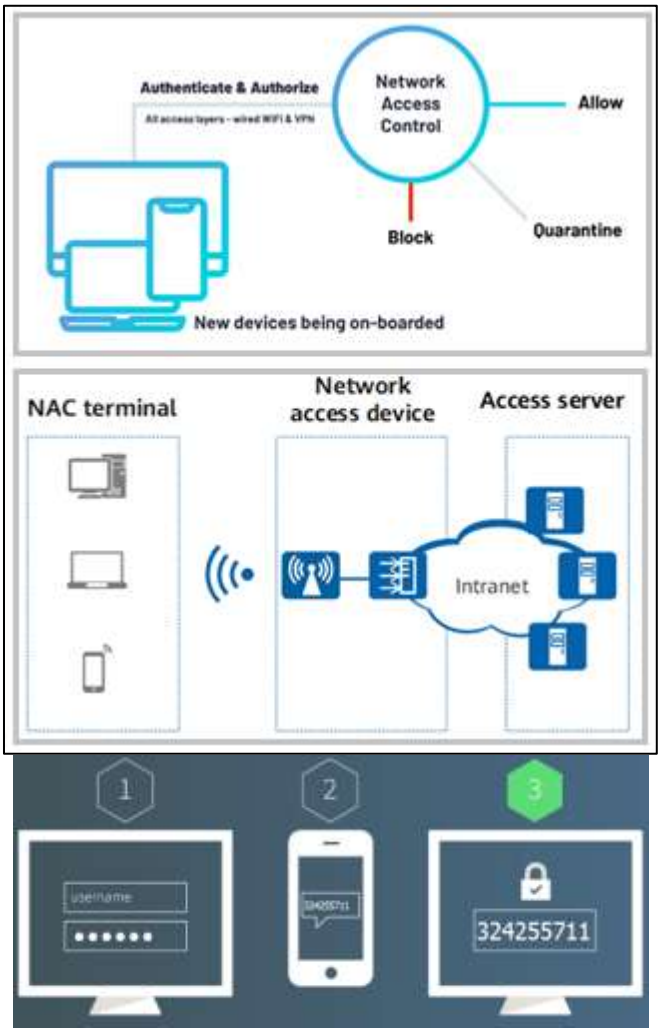
• *Pretty Good Privacy* (PGP). Kriptografski sistem koji se može uključiti u razne aplikacije u svrhu kriptiranja podataka prije slanja na mrežu. Razvijen na MIT, popularan u akademskoj zajednici.

• *Secure Shell* (ssh). Aplikacijski protokol sličan Telnet-u, s time da se svi podaci između klijenta i servera prenose u kriptiranom obliku. Koristi se unutar programa Putty za sigurno prijavljivanje na udaljeno računar.

• *Secure Socket Layer* (SSL). Softver koji se umeće između aplikacijskog programa i Socket API i koji kriptira podatke prije slanja kroz Internet. Koristi se na web stranicama koje uključuju financijske transakcije.

• *Remote Authentication Dial-In User Service* (RADIUS). Protokol koji omogućuje centraliziranu autentikaciju, autorizaciju i obračunavanje usluga za grupu korisnika. Popularno rješenje za ISP-ove koji imaju dial-up korisnike, te za VPN-ove koji dozvoljavaju zaposlenicima da se spajaju na zaštićenu mrežu od kuće.

• *Wi-Fi Protected Access* (WPA). Dio standarda za Wi-FI bežični LAN. Služi se kriptiranjem, omogućuje povjerljivost komuniciranja i autentičnost korisnika koji se spajaju na LAN.



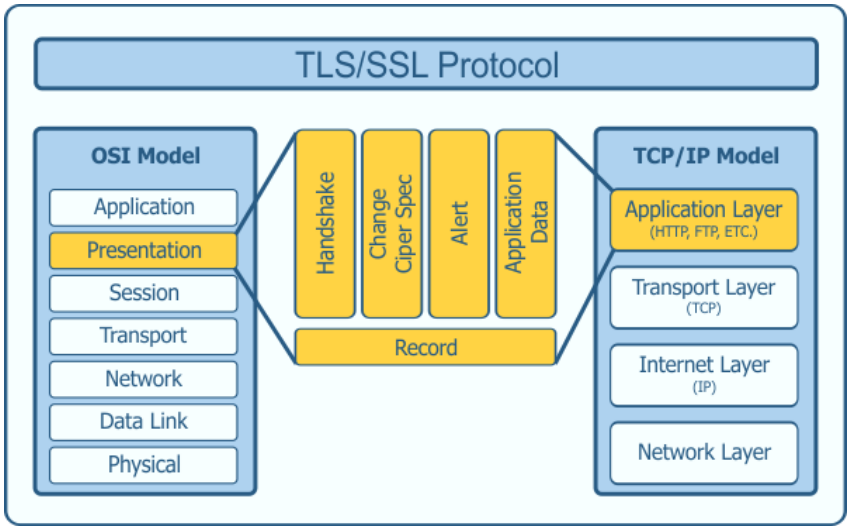

*Primjer korištenja dvo-faktorske autentifikacije*

**Kontrola pristupa** (*Access control*) ograničava pristup podacima i softveru koji se koristi za manipulaciju tim podacima. To je ključno za sprječavanje neovlaštenog pristupa i smanjenje rizika od insajderskih prijetnji. Rješenja za upravljanje identitetom i pristupom (IAM) mogu pomoći u ovoj oblasti.

**Autentifikacija** (*User authentication*), ili verifikacija identiteta korisnika, ključna je komponenta kontrole pristupa. Korištenje dvofaktorske autentifikacije (2FA- *two-factor authentication*) umjesto jednostavnih lozinki važan je korak ka tome da mreže budu sigurnije.
Autentifikacija je proces određivanja identiteta nekog subjekta. Najčešće se odnosi na neku fizičku osobu. Ali to se može odnositi na provjeru bilo kog entiteta. U praksi subjekt daje određene podatke po kojima druga strana može utvrditi radi li se baš o tom subjektu za kojeg se on predstavlja. Primjer upotrebe autentifikacije je upisivanje korisničkog imena i lozinke.
Dvo-faktorska autentifikacija je nadogradnja jedno-faktorske autentifikacije koja se u pravilu odnosi na unos korisničkog imena i lozinke. Da bi se dobila dvo-faktorska autentifikacija potrebno je dodati još jedan korak u prijavi, (npr. unos koda koji je poslan u sms-poruci na određeni telefonski broj) koji omogućuje veću zaštitu podataka.

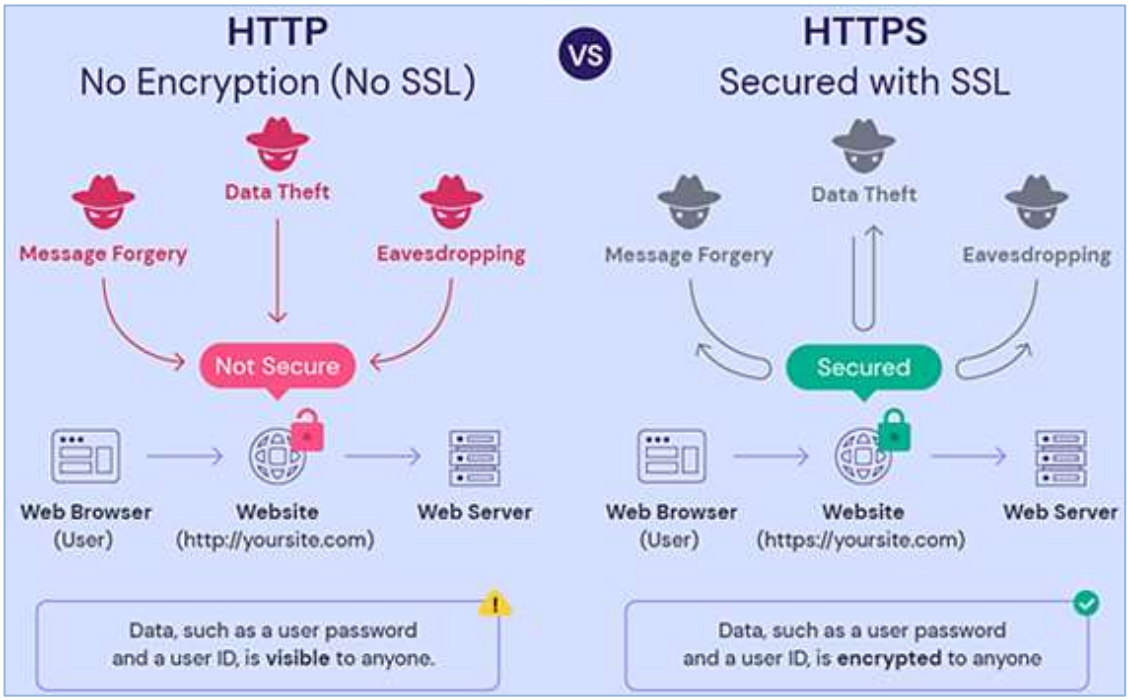
## SSL/TLS protokol


Krajem prošlog vijeka predstavljeni su protokoli pomoću kojih su, kod prenosa podataka unutar mreža (a naročito interneta), propisane procedure koje garantuju sigurnost prenosa. Radi se o *Secure Sockets Layer/Transport Layer Security* (SSL/TLS) protokolu[35], kao i *Secure Electronic Transactions* (SET) protokolu. Svaka verzija SSL i TLS protokola ima svoj paket šifara, a svaka nova verzija ima paket šifara koji je na višem nivou bezbjednosti i ima bolje performanse od prethodnih. TLS je novijeg datuma i danas je u upotrebi. SSL protokol je uglavnom napušten.



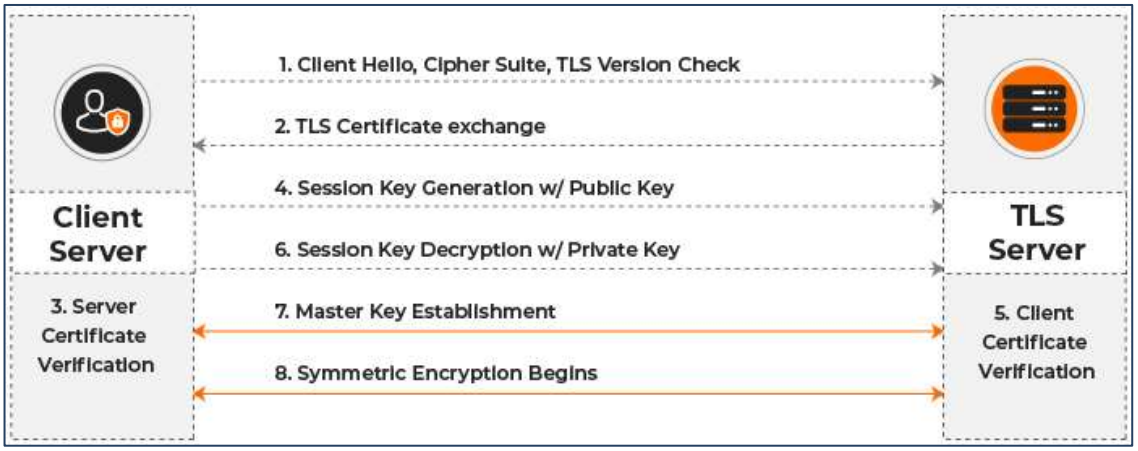

Sigurnosni protokoli se nalazi između aplikacionog i transportog nivoa. Na predajnoj strani TLS prima podatke (recimo HTTP), šifruje ih i šifrovane šalje na TCP soket.

[35] Postoje razlike između SSL i TLS, ali u osnovi protokol je isti. SSL i TLS se razlikuju prema načinu na koji uspostavljaju konekciju. SSL pravi eksplicitnu konekciju putem porta, dok TLS uspostavlja implicitnu konekciju putem protokola.




*HTTP ne koristi sigurnosne mehanizme za razliku od HTTPS što ga čini sigurnijim*

Kada dva sistema koji koriste TLS pokušaju da se povežu, svaki sistem će se potruditi da potvrdi da drugi podržava TLS. Ovaj proces se naziva TLS rukovanje (*TLS handshake)*, i tu obje strane odlučuju o TLS verziji, algoritmu šifriranja, paketu šifri itd. koji će se koristiti u proceduri. Kada se TLS rukovanje uspješno izvrši, oba sistema počinju razmjenjivati podatke na sigurnoj liniji. Šifriranje i dešifriranje provode uz pomoć kriptografskih mehanizama koji se nazivaju ključevi. U kriptografiji javnog ključa, javni ključevi se koriste za šifriranje informacija, dok se tajni privatni ključevi mogu koristiti za dešifriranje tih informacija. Budući da su uključena dva različita ključa, ova tehnika se naziva "asimetrična kriptografija", za razliku od "simetrične kriptografije", gdje jedan ključ može izvršiti i enkripciju i dešifriranje.



Svako TLS rukovanje prati iste osnovne korake. Pretpostavimo da se pretraživač (klijent) pokušava povezati sa serverom na kojem se nalazi web stranica:

- Klijent traži od servera da otvori I uspostavi bezbjednu liniju, a server odgovara tako što prikazuje listu verzija TLS-a i paketa šifrovanja sa kojima je kompatibilan. Kada se dogovore oko onih koje će koristiti u transakciji, započinju rukovanje.
- Server šalje kopiju svog javnog ključa, priloženu njegovom digitalnom sertifikatu, klijentu. Klijent provjerava sertifikat kako bi potvrdio da je server legitiman, i ako jeste, nastavlja s transakcijom.
- Klijent koristi javni ključ servera i njegov privatni ključ za šifriranje 'ključa sesije' (*'session key'*) koji je ključ koji će obje strane koristiti za šifriranje i dešifriranje informacija u ovoj konkretnoj sesiji. Ključ sesije postaje nevažeći čim se veza prekine.
- Obje strane testiraju vezu tako što jedna drugoj šalju šifrovane poruke. Ako ih drugi može dešifrirati pomoću ključa sesije, veza je uspješno osigurana.

Kod ovdje opisanog i ilustrovanog primjera korištena je i asimetrična i simetrična enkripcija korištena za osiguranje veze. Za kreiranje ključa sesije korištena je asimetrična enkripcija. Ali od tog trenutka nadalje, ključ sesije se koristio za bilateralno šifriranje i dešifriranje cjelokupnog protoka informacija između obje strane. Evo zašto:

Asimetrična enkripcija je matematički zahtjevna za resurse. Operacije enkripcije-dešifriranja koje uključuju dva ključa s obje strane bitno opterećuju procesorsku jedinicu koja pokreće ovaj proces. Ako je sistem konfigurisan da upravlja cijelom vezom na ovaj način – korištenjem javnog ključa za šifriranje i privatnog ključa za dešifriranje – vjerojatno bi brzo došlo do preopterećenja i prekioda veze već u prvih nekoliko minuta. Mnogo je sigurniji od svog simetričnog pandana, ali se ne može efikasano primjeniti.

Međutim, simetrična enkripcija, koja koristi jedan zajednički ključ za šifriranje i dešifriranje, nije toliko zahtjevna za resurse. Upravo zbog toga se asimetrična enkripcija koristi za uspostavljanje sigurne veze između dvije strane i koristi se za generiranje ključa sesije za koji, u teoriji, samo te dvije strane mogu znati. Sada se simetrična enkripcija može koristiti za osiguranje veze, s obzirom na dodatni sloj sigurnosti koji joj je dodat prvim korakom.

# SSL/TLS digitalni serifikat

Generalno, digitalni sertifikati su digitalni dokumenti koje su 'potpisali' pouzdani autoriteti i djeluju kao dokumenti o vlasništvu nad javnim ključem. Kao proširenje, oni služe za potvrđivanje legitimnosti servera ili klijenta.
Digitalni sertifikati su važni dijelovi u domenu kriptografije javnog ključa. Oni su vezani uz javne ključeve i dokaz su da je vlasnik javnog ključa zapravo legitimni vlasnik.

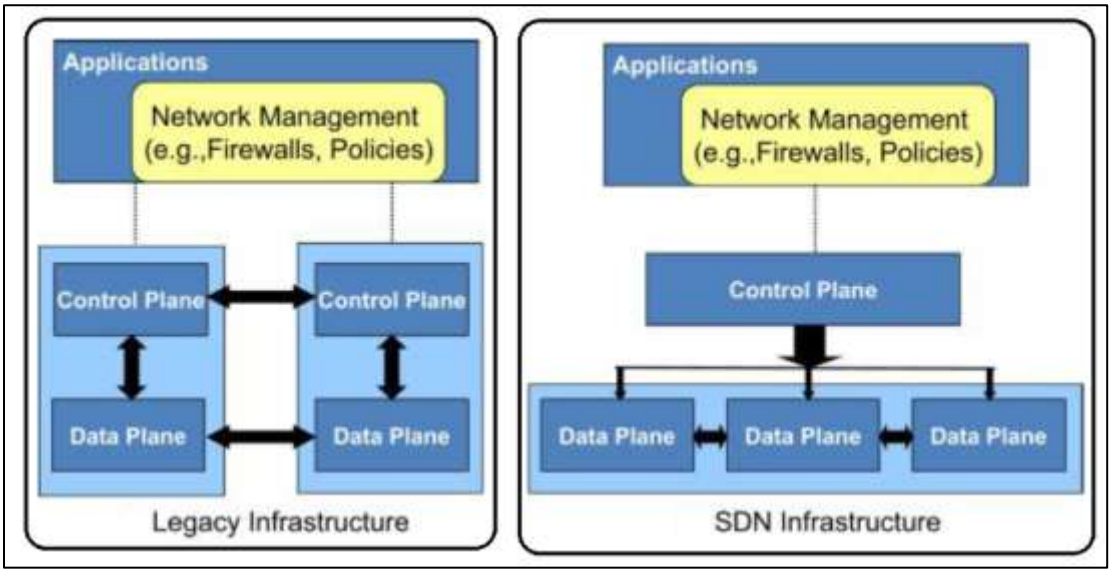
Digitalne sertifikate potpisuju, prodaju i izdaju tijela koja se zovu *'*Ovlašteni sertifikatori*'* - *'Certificate Authorities'* (ili CA,uobičajeno), a koja su tijela od povjerenja odgovorna za provjeru autentičnosti svakoga ko zatraži sertifikat. Budući da glavni operativni sistemi i pretraživači imaju ugrađene 'prodavnice povjerenja' - 'trust stores' koje se sastoje od ovih CA-a, pretraživači će automatski vjerovati sertifikatima koje izdaju glavni CA-ovi.

Izraz 'x.509 sertifikati' se koristi za razlikovanje SSL/TLS sertifikata od drugih vrsta digitalnih sertifikata (na primjer, sertifikati za potpisivanje koda).


Sertifikati su ključni za to da web stranice budu lako prepoznatljive korisnicima kao pouzdana, sigurna stranica. Web stranice na kojima su instalirani važeći SSL/TLS sertifikati imat će 'https' ispred naziva web stranice u traci za pretraživanje, s obzirom da je sertifikat ispravno instaliran. U nekim pretraživačima, upotreba važećih sertifikata proširene validacije (vrsta TLS sertifikata) će uzrokovati da HTTPS katanac postane zelen, pružajući posjetiteljima dodatnu (ne baš opravdanu) sigurnost da se nalaze na legitimnoj web stranici.

# SDN Softverski definisane mreže

U prethodnim poglavljima bavili smo se uobičajenom i standardnom arhitekturom "klasičnih" računarskih mreža.
Softverski definisane mreže (SDN) kreirane su kao rješenje za sljedeću generaciju mrežnih arhitektura. Ovaj koncept nudi centralizovanu kontrolu nad cijelom mrežom i unapređuje skalabilnost, pouzdanost i sigurnost. Sam pojam je relativno nov (datira iz 2009. godine) ali osnovna ideja je nastala u osamdesetim godinama prošlog stoljeća.
"Klasične" mreže funkcionišu na protokolima koji su nastajali, prilagođavali, unaprjeđivali i mijenjali se godinama i time postajali sve kompleksniji i detaljniji. Eventualni problemi i nedostaci se rješavaju zaobilaženjem, uvođenjem dodatnih protokola ili uvođenjem novih verzija postojećih protokola.
Za razliku od administratora mreža programeri ne moraju znati sve koncepte operativnih sistema na kojima se njihove aplikacije izvršavaju nego razvijaju aplikacije s ograničenom količinom pravila i koncepata mogu biti kreativni i dobiti relativno brze i dovoljno dobre rezultate. Kod dizajniranja mreža nedostajala je takva apstrakcija koju imamo u programiranju.
Uvođenjem apstrakcije i kod računarskih mreže smanjila se kompleksnost, izdvajanjem samo onih komponenti koje su bitne za dato okruženje.

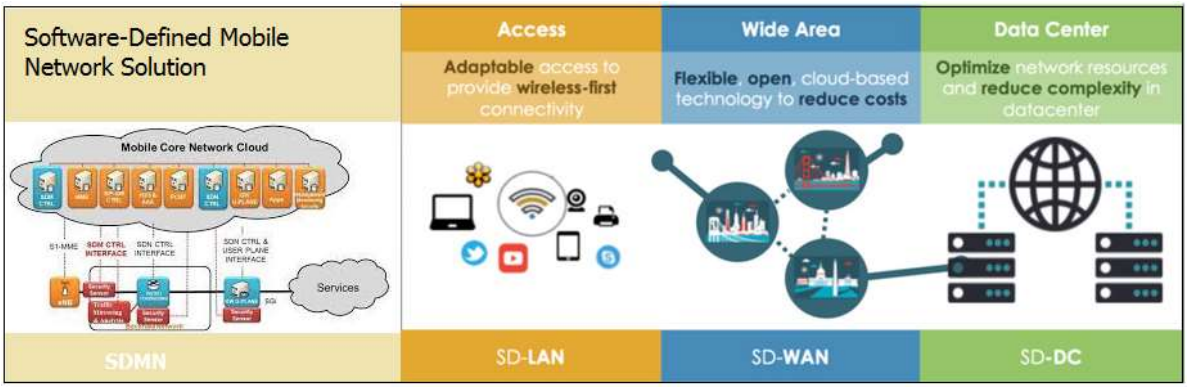



*Razlika između "klasične"(na slici označene kao zastarjela (Legacy) i SDN infrastrukture, Izvor: http://flowgrammable.org/sdn/openflow/*

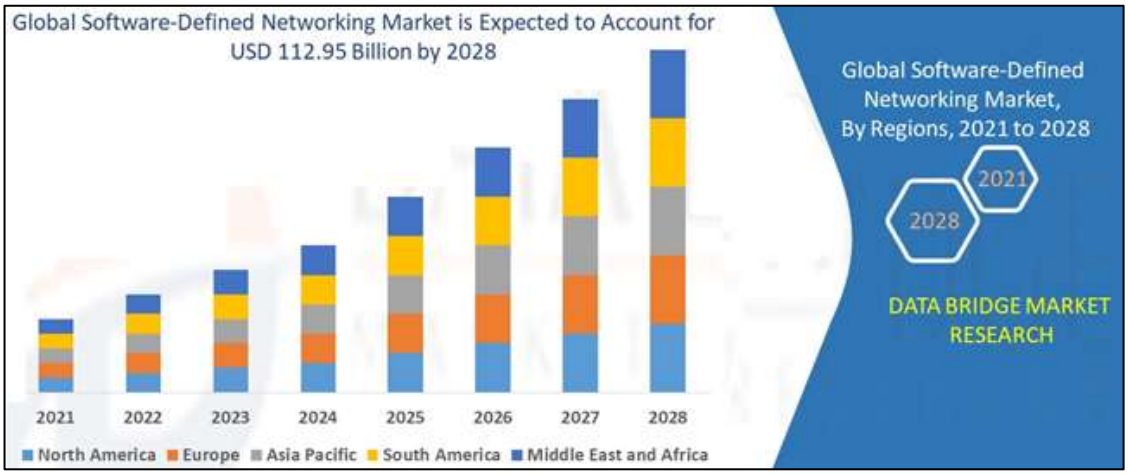
U tradicionalnim mrežama ravan podataka i kontrolna ravan implementirani su na svakom uređaju. SDN kontrolna ravan je razdvojena od ravni podataka i logički centralizovana. (nije potrebno nadzirati i prolaziti kroz sve slojeve).
Nasuprot klasičnog mrežnog okruženja (gdje svaki mrežni uređaj ima upravljačke i kontrolne cjeline koje nadziru podatke), SDN definiše izdvajanje kontrolne cjeline na **jednu komponentu koja konstantno komunicira sa svim uređajima** i dinamički određuje svim uređajima kako će i na koji način slati podatke.

U modernim rješenjima računarstva u oblaku, potrebama za trenutnim i privremenim promjenama prioriteta prometa te zahtjevnim potrebama za resursima sistema softverski definisana mreža pruža puno agilnije adaptacije i promjene unaprijed programiranim konfiguracijama baziranim na otvorenim standardima.
Softverski definisano umrežavanje izvorno je definisalo pristup projektovanju, izgradnji i upravljanju mrežama na način da se razdvoji mrežno upravljanje i prosljeđivanje.
Uobičajeno se ove aplikacije klasiraju i nazivaju prema mrežama gdje se koriste:

- **SDMN** Softverski definisano mobilno umrežavanje
- **SD-WAN** je WAN kojim se upravlja korištenjem principa softverski definisanog umrežavanja.
- **SD-LAN** je lokalna mreža (LAN) izgrađena na principima softverski definisanog umrežavanja. SD-LAN-ove karakteriše njihova upotreba sistema upravljanja oblakom i bežično povezivanje bez prisustva fizičkog kontrolera.
- **SD-DC** je marketinški termin koji se koristi za promociju velikih (obično korporacijskih) računskih centara koji koriste SDN koncepte virtuelizacije kao što su apstrakcija, udruživanje i automatizacija na sve resurse i usluge centra.



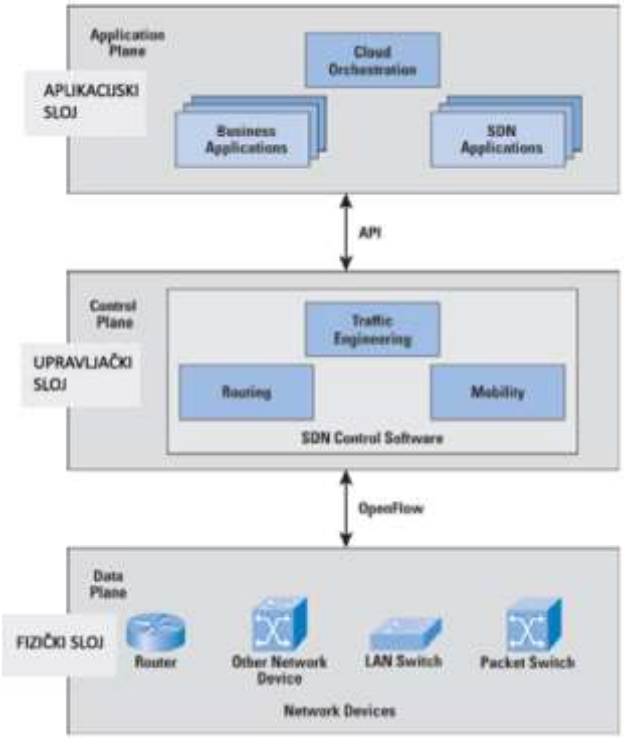

Predviđa se da će ovakav pristup u potpunosti zamjeniti tradicionalne mreže i da je koncept softverski definisanih mreža budućnost umrežavanja. U toku su velika infrastrukturna ulaganja što se može vidjeti i iz grafikona:




*Preuzeto sa: https://www.databridgemarketresearch.com/reports/global-sdn-market*

# SDN arhitektura

SDN provajderi mrežnih usluga nude širok izbor konkurentskih arhitektura, ali najzastupljenija je metoda umrežavanja putem centralne upravljačke jedinice, razdvajanjem upravljačke logike na računarske resurse izvan uređaja.




Arhitektura SDN mreže sastoji se od tri sloja.

Ideja je razdvajanja vertikalne mrežne infrastrukture na zaseban upravljački sloj i sloj podataka te otvaranje mogućnosti progamabilnosti mreža je osnov SDN mreža.
SDN pokušava centralizirati mrežnu inteligenciju u jednoj mrežnoj komponenti **odvajanjem procesa prosljeđivanja mrežnih paketa** (tzv. data plane) **od procesa usmjeravanja** (tzv. control plane [kontrolni dio].

Ključnu ulogu ima centralna upravljačka jedinica, odgovorna za upravljanje uređajima pod svojom domenom, koji u tom slučaju čine fizičku mrežnu infrastrukturu.

Kontrolni dio (*control plane*) se sastoji od jednog ili više kontrolera, koji se smatraju centrom ili *mozgom* SDN mreže u koju je ugrađena cjelokupna inteligencija.

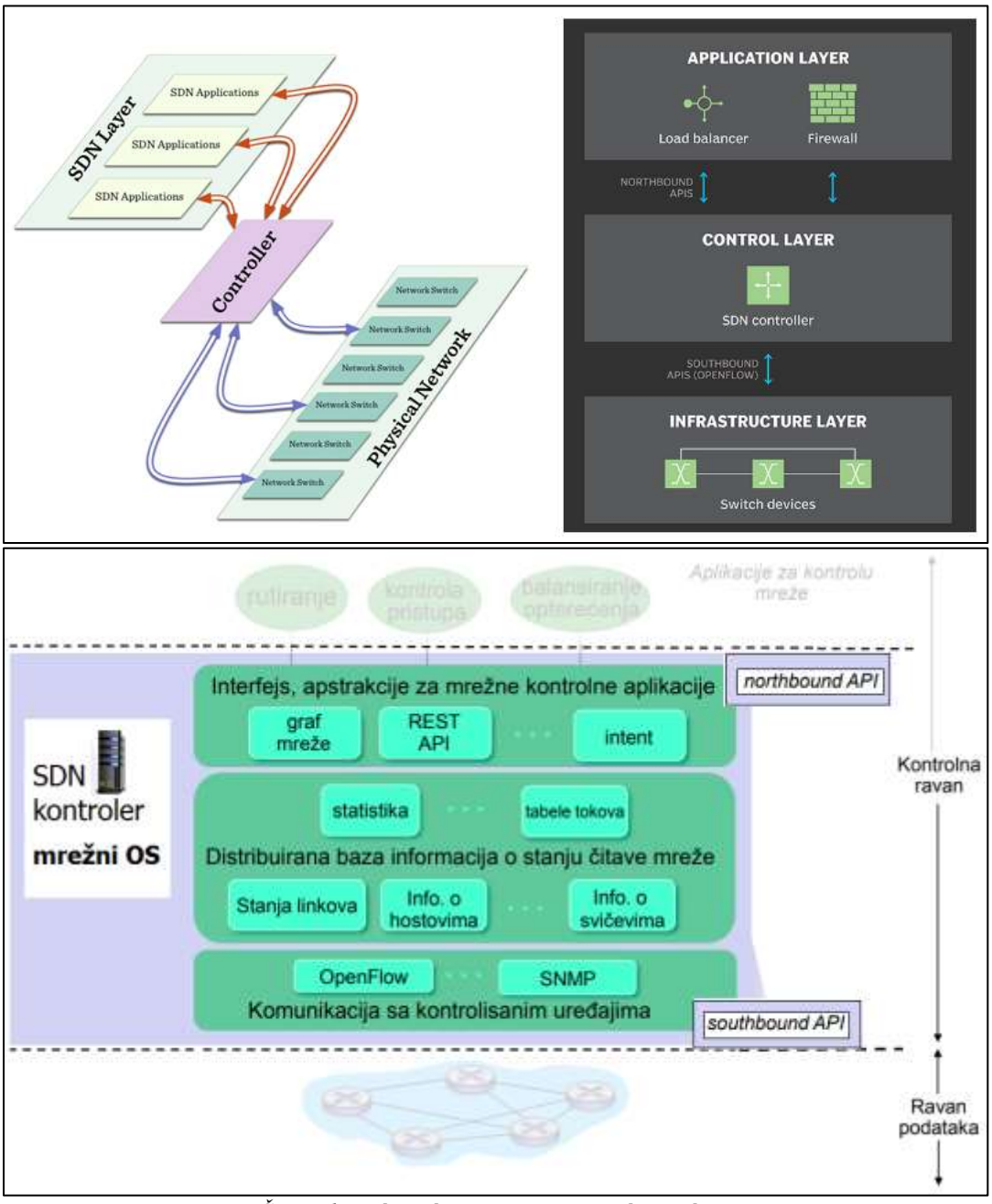
SDN kontroleri nude centralizovani prikaz cjelokupne mreže i omogućuju mrežnim administratorima upravljanje osnovnim sistemima.

# SDN kontroler

SDN kontroler je jezgro softverski definisane mreže. Nalazi se između mrežnih uređaja na jednom kraju mreže i aplikacija na drugom kraju. Svaka komunikacija između aplikacija i mrežnih uređaja mora ići preko kontrolera. SDN kontroler se nalazi između sloja aplikacije i sloja infrastrukture.
SDN kontroler ima zadataka da:
- Održava informacije o stanju mreže
- obavlja interakcija sa mrežnim kontrolnim aplikacijama putem northbound API-ja
- Interakcija sa mrežnim svičevima preko southbound API-ja

Kontrolna ravan (***control plane***) je inteligentna logika u mrežnoj opremi koja kontroliše kako se upravlja prometom podataka i kako se njime rukuje. S druge strane, ravan podataka je ravan prosljeđivanja koja upravlja prosljeđivanjem/manipuliranjem/ispuštanjem mrežnog prometa podataka. Ovakvim razdvajanjem, osnovna inteligencija mrežnih elemenata (tj. kontrolna

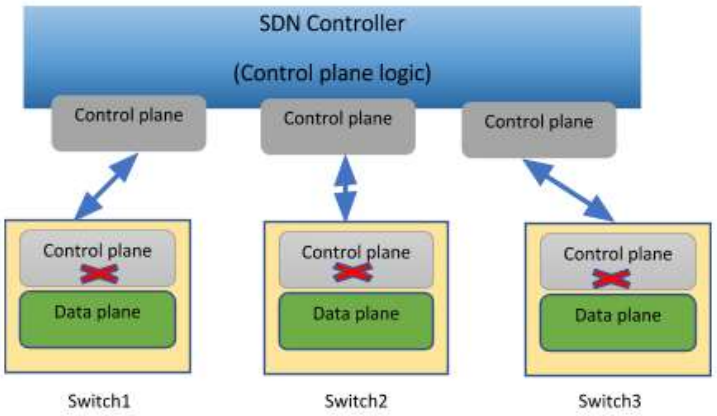
ravan) može se premjestiti na centralno mjesto koje obično nosi bilo koji od sljedećih naziva: 'kontrolni sistem', 'kontroler' ili 'mrežni operativni sistem'. SDN kontroler služi kao neka vrsta operativnog sistema (OS) za mrežu.




*Šematski prikaz uloge i pozicije SDN kontrolera*

SDN kontroleri usmjeravaju promet prema politikama prosljeđivanja koje postavlja mrežni operater, čime se minimiziraju ručne konfiguracije za pojedinačne mrežne uređaje.

Uklanjanjem kontrolne ravni sa mrežnog hardvera i pokretanjem umjesto softvera, centralizovani kontroler olakšava automatizovano upravljanje mrežom i olakšava integraciju i administriranje poslovnih aplikacija.




Kontrolno razdvajanje ima mnoge prednosti kao što su:

• Centralno upravljanje: Možete da konfigurišete, nadgledate i rešavate probleme sa mrežom i takođe možete da dobijete potpuni uvid u nju (mrežnu topologiju) od kontrolera.

• Pojednostavljenje - Lagana (Light-weighted) mrežna oprema: Mrežni elementi kao što su svičevi i ruteri mogu se pojednostaviti, što zauzvrat može pomoći da s vremenom postanu jeftiniji. Inteligencija bi bila na kontroleru gdje bi se nalazila kontrolna ravnina (tj. kontrolna logika), omogućavajući kontrolu osnovnih elemenata mreže guranjem pravila preko njih kroz zajednički kanal (tj. protokole).

• Virtuelizacija mreže: Virtuelizacija mreže dovodi do višestanarstva (arhitektura u kojoj jedna instanca softvera radi na serveru i opslužuje više zakupaca), što zauzvrat pomaže da se iskoristi puni potencijal mrežnih elemenata. SDN kontroler može apstrahovati osnovnu fizičku mrežu i omogućiti mrežnim administratorima da programiraju virtuelne mreže koje odgovaraju svakom zakupcu. Primer iz stvarnog života mesta gde se koristi virtuelizacija mreže su data centri – arhitektura se koristi za deljenje zajedničke fizičke mreže među mnogim korisnicima.

Sva softverska rješenja definisana mrežnim rješenjima imaju neku verziju SDN kontrolera, kao i programskih interfejsa, Southbound[36] API (Application Programming Interface) i Northbound API.

SDN kontroleri se prodaju na tržištu od strane mnogih velikih dobavljača/kompanija za umrežavanje. Neki primjeri ovih kontrolera su Cisco Open SDN kontroler, Juniper Contrail, Brocade SDN kontroler i PFC SDN kontroler iz NEC-a.

Mnogi open source SDN kontroleri poput Opendaylight, Floodlight, Beacon, Ryu itd. su takođe prisutni na tržištu.

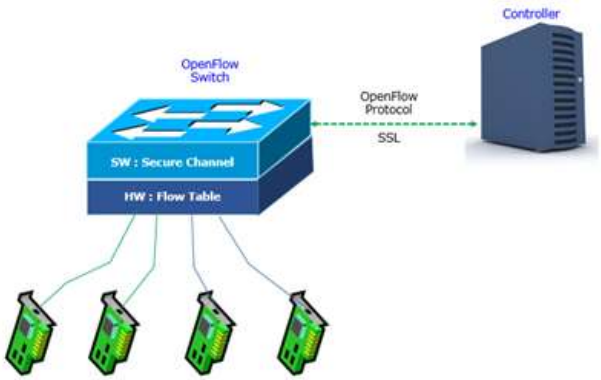
Većina mrežnih provajdera i zajednica otvorenog koda prihvatila je Openflow kao komunikacijski protokol između kontrolne ravni i ravni podataka.

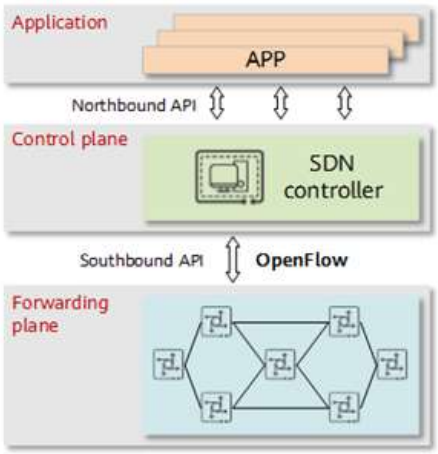
SDN rješenje sa OpenFlow zahtijeva implementaciju protokola i u kontroleru i u mrežnim elementima.

[36] Termin "*southbound*" u arhitekturi računarskih mreža predstavlja interfejs određenog sloja prema nižem sloju, suprotno od pojma "*northbound*" koji značio interfejs određenog sloja prema višem sloju.

# OpenFlow

OpenFlow je komunikacijski protokol koji daje pristup mehanizmima prosljeđivanja (forwarding plane) mrežnih paketa. SDN kontroler komunicira sa pojedinačnim mrežnim uređajima koristeći Soutbound API, standardno preko OpenFlow protokola konfigurišući mrežne uređaje i birajući optimalnu mrežnu putanju za promet aplikacije.
OpenFlow (OF) se smatra prvim standardom u SDN-u. Ovaj protokol su prvi razvili istraživači na Univerzitetu Stanford 2008. godine, a prvi ga je usvojio Google u svojoj osnovnoj mreži 2011-2012. Njime sada upravlja Open Networking Foundation (ONF). Najnovija verzija koja se koristi u industriji je V1.5.



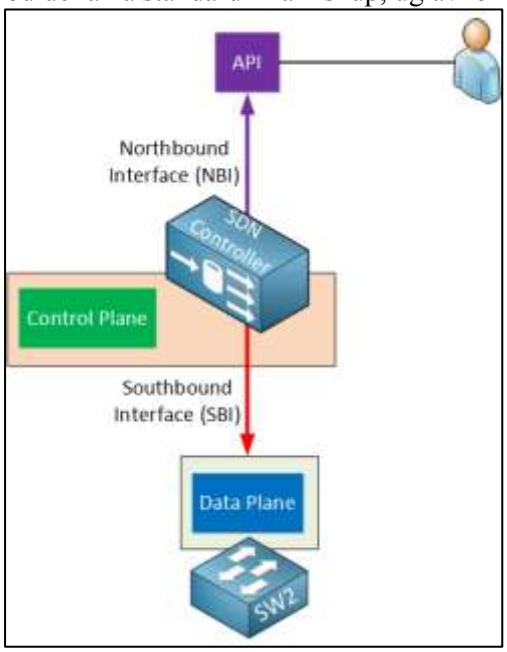




OpenFlow omogućuje mrežnim kontrolerima određivanje putanje mrežnih paketa kroz mrežu svičeva. SDN kontroler preuzima informacije iz aplikacija i pretvara ih u pakete, koji se dovode do svičeva preko OF. Takođe se može koristiti za nadgledanje statistike svićeva i portova u upravljanju mrežom.
OpenFlow protokol se uspostavlja samo između kontrolera i svičeva. Ne utiče na ostatak mreže. Ako bi se „hvatanje“ paketa obavilo između dva sviča u mreži, oba povezana na kontroler preko drugog porta, hvatanje paketa ne bi otkrilo nijednu OF poruku između prekidača. Namijenjen je isključivo između sviča i kontrolera. Ostatak mreže nije pogođen.
OpenFlow omogućuje i daljinsko upravljanje svičevima različitih proizvođača – često svaki sa svojim vlastitim vlasničkim interfejsom i skriptnim jezicima – pomoću jednog, otvorenog protokola.
OpenFlow omogućuje udaljenu administraciju tablica prosljeđivanja paketa svičeva na OSI sloju tri (OSI 3), dodavanjem, modifikovanjem i uklanjanjem pravila i radnji za podudaranje paketa. Na taj način kontroler može povremeno ili ad hoc donositi odluke o usmjeravanju i prevesti ih u pravila i radnje s podesivim životnim vijekom, koji se zatim raspoređuju u tablicu toka rutera odnosno sviča, ostavljajući stvarno prosljeđivanje podudarnih paketa sviču, koje će se tada odraditi hardverskom brzinom (tzv. brzinom žice).

Protokol OpenFlow koristi TCP protokol i propisuje korištenje Transport Layer Security-a (TLS). OpenFlow kontroleri bi trebali koristiti TCP port 6653; kojeg slušaju i kontroler i svičevi.

## Northbound API

Northbound API čini informacije izgrađene iz SDN kontrolera (koji su kreirani u Soutbound API najčešće korištenjem OpenFlow protokola) dostupnim za aplikacije.
Tako je praktično OpenFlow protokol osnov i ovog interfejsa, pa se često OpenFlow koristi kao sinonim za SDN mreže.
Open Networking Foundation (ONF) je 2013. godine stvorila radnu grupu koja se posebno fokusirala na API-je za Northbound API i njihov razvoj. Industrija se, međutim, nikada nije odlučila na standardizirani skup, uglavnom zbog toga što zahtjevi za primjenom jako variraju.




Svaka aplikacija će razviti prikaz tabela toka za mrežne uređaje, a zatim će poslati zahtjeve kontroleru za distribuciju na mrežne uređaje.

Na primjer, aplikacija virtuelnog prebacivanja bi izgradila mrežni graf/bazu podataka svih tačaka u mreži fizičkih i virtuelnih svičeva.
U višeklijentskoj (*multi-tenant*) Ethernet mreži, aplikacija bi razvila skup pravila toka koja emuliraju Ethernet VLAN-ove uz održavanje pune izolacije za rutu svakog paketa. Pravila rutiranja bi se sastojala od vrijednosti zasnovanih na ulaznim i izlaznim portovima, plus izvorni i odredišni MAC (fizičke adrese uređaja).

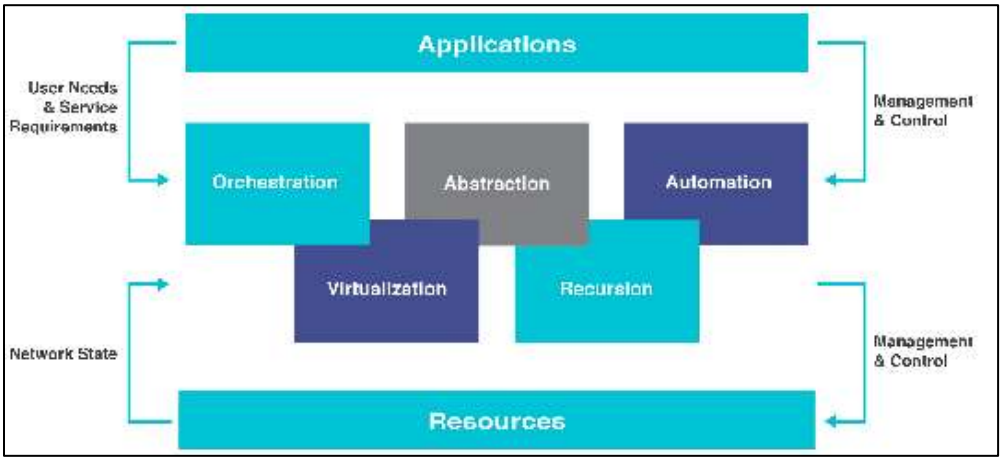
Northbound API se sastoji od sljedećih tipova API-ja:

- Sinhroni: Sinhroni API-ji su pokrenuti od strane klijenta, a informacije se prezentiraju preko servera kao odgovor na API. Sinhroni API-ji se mogu klasificirati u dvije kategorije:
  - Get/Fetch: Ovi API-ji dobijaju informacije o mreži bez uticaja na stanje mreže.
  - Push/Post/Modify: Ovi API-ji modificiraju stanje mreže.
- Asinhroni: Asinhroni API-ji obavještavaju aplikacije usmjerene na sjever o promjenama u mreži putem komunikacije između servera i klijenta.

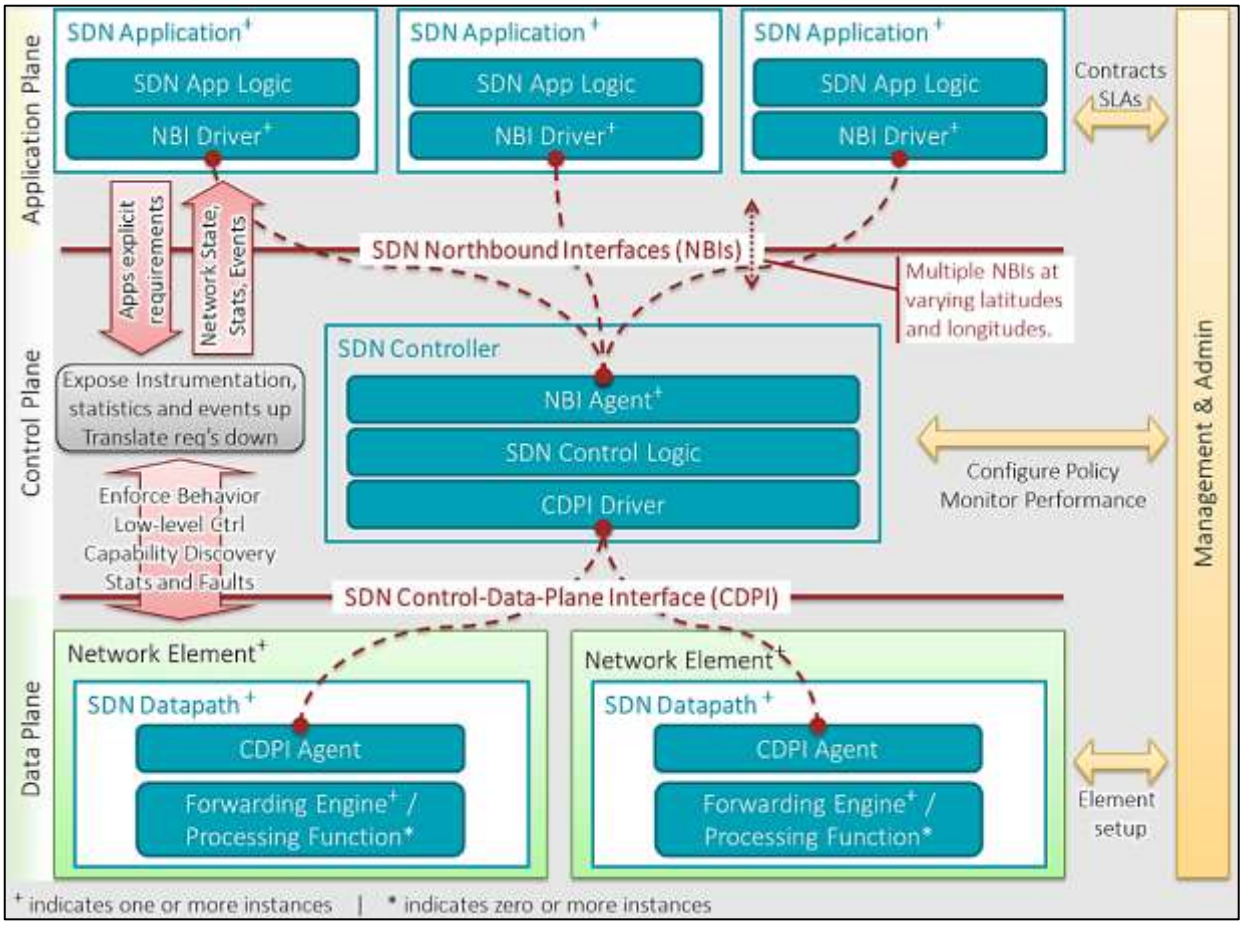
## SDN aplikacije

Da sumiramo ovaj uvod u SDN umrežavanje: SDN aplikacija je softverski program koji je dizajniran za obavljanje zadatka u softverski definisanom mrežnom okruženju.

SDN aplikacije su programi koji eksplicitno, direktno i programski postavljaju svoje mrežne zahtjeve i željeno mrežno ponašanje SDN kontroleru preko Nortbound API interfejsa (NBI). Ove aplikacije mogu koristiti apstraktan pogled na mrežu za svoje interne svrhe za donošenja odluka.




SDN aplikacija se sastoji od jedne SDN aplikacijske logike i jednog ili više NBI drajvera. SDN aplikacije mogu same izložiti drugi sloj apstrahovane mrežne kontrole, nudeći na taj način jedan ili više NBI višeg nivoa preko odgovarajućih NBI agenata.



# IoT, ili Internet stvari

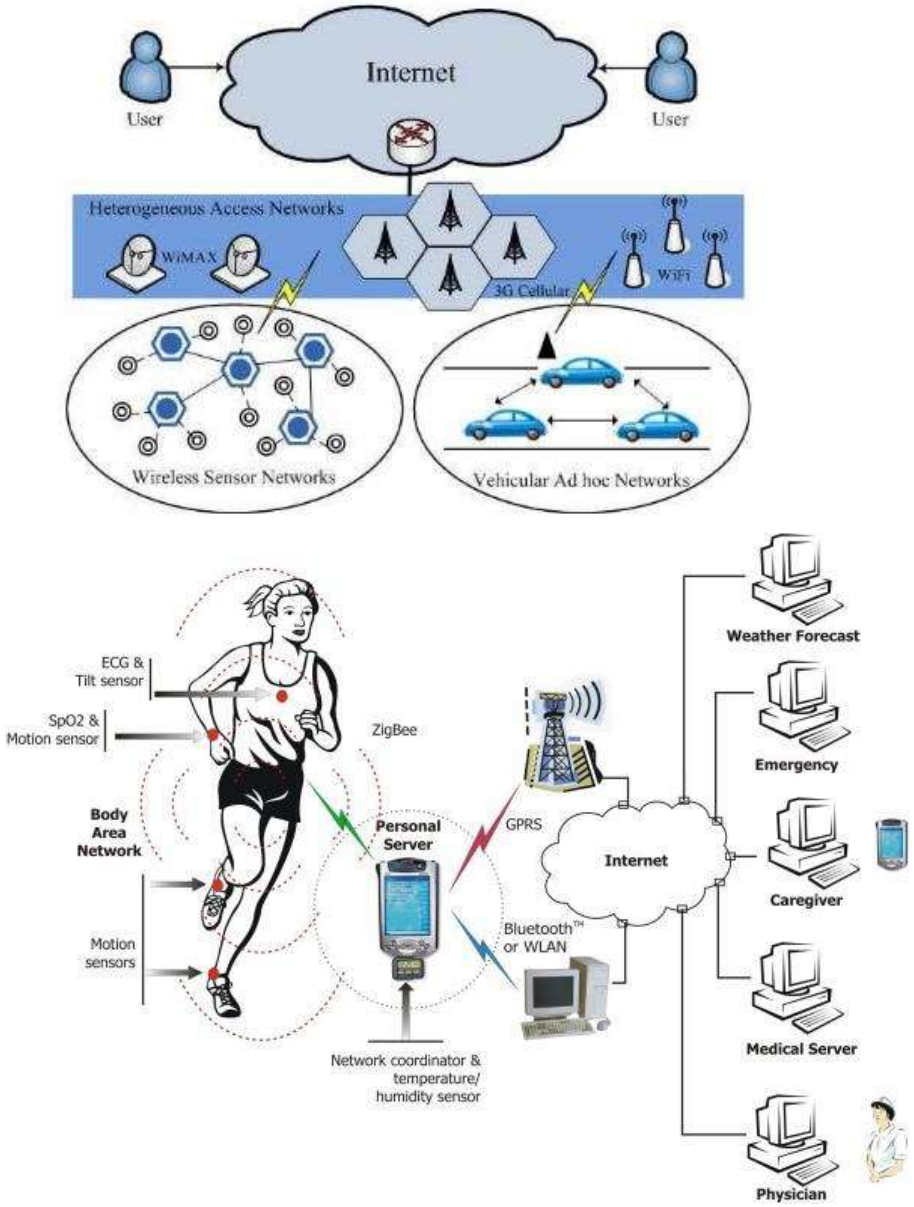

Termin IoT (***Internet of Things***), ili Internet stvari, odnosi se **na jedinstvenu** zajedničku **mrežu povezanih uređaja i tehnologiju koja olakšava komunikaciju između uređaja i oblaka, kao i između samih uređaja.** Predstavlja mrežnu infrastrukturu u kojoj fizičke i virtualne "stvari" svih vrsta komuniciraju i nevidljivo su integrirane**.** Internet stvari integriše svakodnevne „stvari“ sa internetom. Prve aplikacije ove vrste pojavile su se gotovo paralelno sa burnim razvojem interneta još 90-ih. Sada imamo (bez pretjerivanja) milijarde uređaja povezanih na internet.
Navešćemo samo nekoliko primjera gdje se koriste:

**IoT u proizvodnji** koristi prediktivno održavanje za smanjenje neplaniranih zastoja i nosivu tehnologiju za poboljšanje sigurnosti radnika. IoT aplikacije mogu predvidjeti kvar mašine prije nego što se dogodi, smanjujući vrijeme zastoja u proizvodnji. Nosivi šljemovi i narukvice, kao i kamere za kompjuterski vid, koriste se za upozoravanje radnika na potencijalne opasnosti. Tehnologija je posebno korisna za kontrolu temperature u rashladnim prostorijama i čuvanje kvarljive robe.

**IoT u automobilskoj industriji,** Analitika vođena senzorima i robotika povećavaju efikasnost u proizvodnji i održavanju automobila. Na primjer, industrijski senzori se koriste za pružanje 3D slika unutrašnjih komponenti vozila u realnom vremenu. Dijagnostika i rješavanje problema mogu se obaviti mnogo brže dok IoT sistem automatski naručuje zamjenske dijelove. Pametan automobil (**smart car**) uključuje funkcije kao što su senzori sudara za upozorenje vozača, GPS i kontrola okoliša, usluge upozorenja koje kontaktiraju kompaniju za proizvodnju automobila kada automobil zahtijeva pregled.

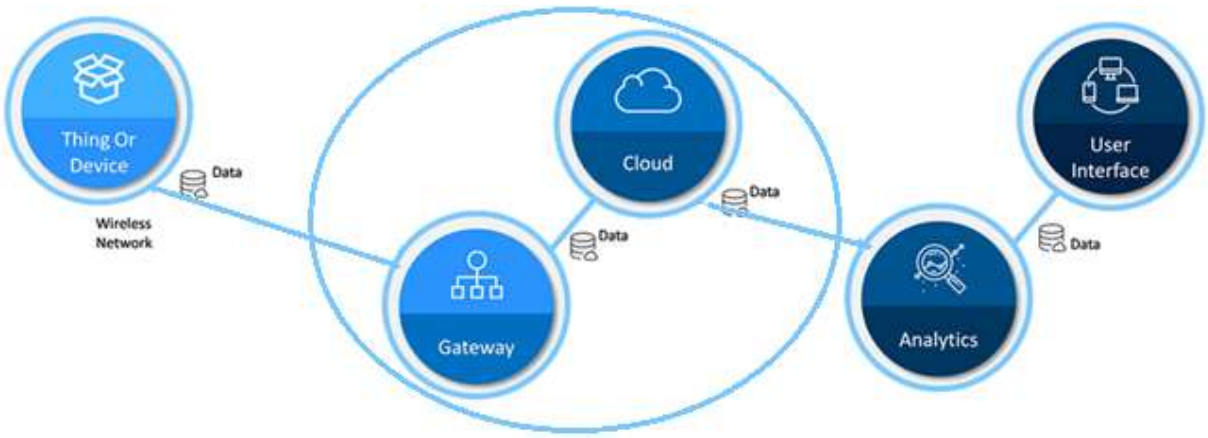
**IoT kod logistike i trensporta,** Špedicije koriste industrijske IoT aplikacije kako bi pratile vozila i optimizirale potrošnju goriva na rutama..

**IoT u prodaji,** Komercijalni i industrijski IoT uređaji mogu pomoći u upravljanju lancem nabavke, uključujući upravljanje zalihama, odnose s dobavljačima, upravljanje voznim parkom i planirano održavanje. Menadžeri lanca nabavke prave informirana predviđanja putem pametnih algoritama usmjeravanja i preusmjeravanja. Amazon je pokrenuo inovacije u automatizaciji i saradnji ljudi i mašina u maloprodaji. Amazonovi objekti koriste robote povezane s internetom za praćenje, lociranje, sortiranje i premještanje proizvoda.




U ovom poglavlju nećemo ni pokušati da razjasnimo konkretne načine i mogućnosti umrežavanja "internet stvari". Daće se samo **prikaz koji je uvod u budućnost umrežavanja**. Stručnjaci (Cisco Systems) procjenjuju da je 2020. godine bilo preko 20 milijardi uređaja (stvari) spojeno na Internet, sa tendencijom daljeg porasta što će znatno promijeniti ne samo način poslovanja već i kompletan život.

# Osnovne komponente i način rada IoT




Tipičan IoT sistem radi kroz prikupljanje i razmjenu podataka u realnom vremenu. IoT sistem ima četiri komponente:

1. Pametni uređaj

Pametni uređaj predstavlja osnov IoT sistema, pa se ponekad koristi i kao sinonim za kompletnu tehnologiju „internet stvari". *Thing* (ili *Device*), IoT uređaji imaju senzore ugrađene u njih. Prikupljaju podatke iz svog okruženja, korisničkih unosa ili obrazaca korištenja i prenosi podatke preko interneta do i iz svoje IoT aplikacije.

2. Povezivanje

Cloud serveri obrađuju podatke koje prikupljaju senzori. Ali, da bi to učinili, potrebne su im platforme i veze između njih. Povezivost je veza između svih IoT uređaja u bilo kojem Iot sistemu uključujući senzore, rutere, gatewaye, korisničke aplikacije i platforme.


3. IoT aplikacija

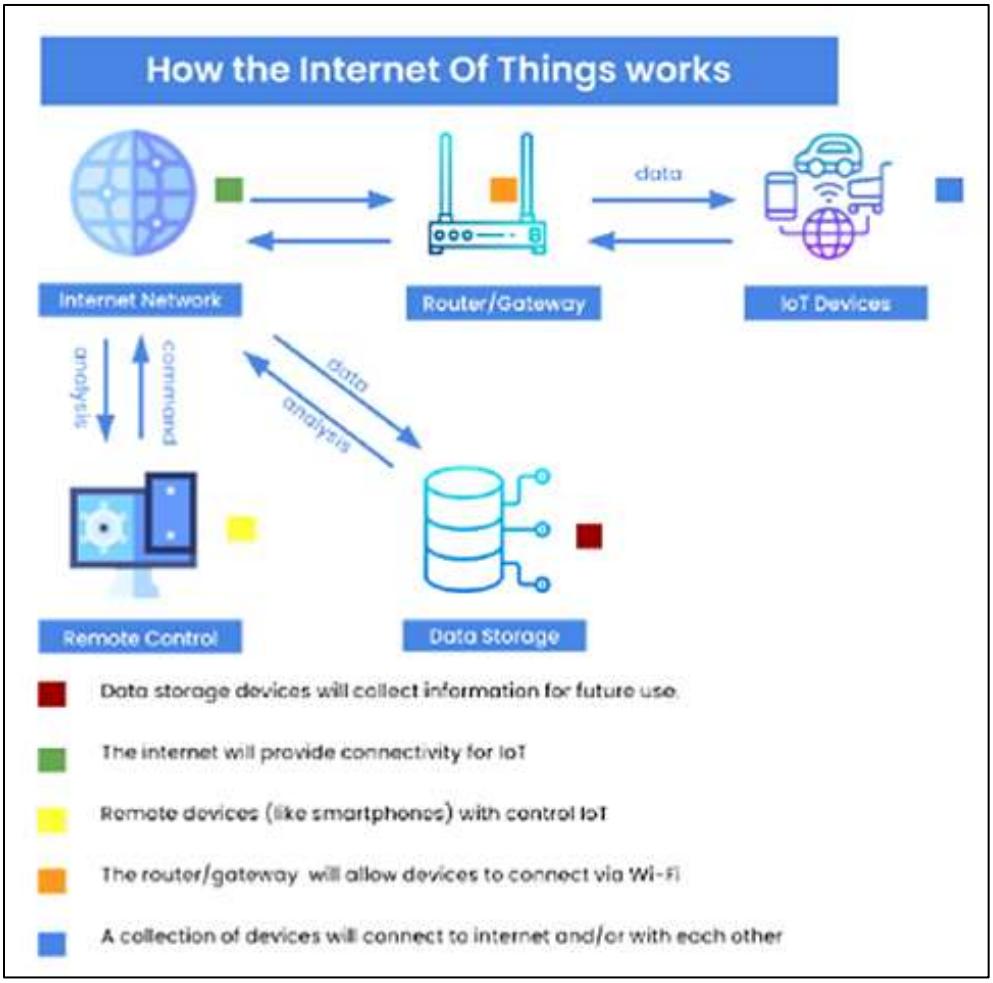
IoT aplikacija je skup usluga i softvera koji integrira podatke primljene s različitih IoT uređaja. Koristi mašinsko učenje ili tehnologiju umjetne inteligencije (AI) za analizu (Analitic) podataka i donošenje odluka.

Ove odluke se saopštavaju nazad IoT uređaju i IoT uređaj zatim inteligentno reaguje na unose.

4. Korisnički interfejs

IoT uređajem (ili sa više IoT uređaja objedinjenih u funkcionalnu cjelinu) obično se upravlja putem grafičkog korisničkog interfejsa. Uobičajeni primjeri uključuju mobilnu aplikaciju ili web stranicu koja se može koristiti za registraciju i kontrolu pametnih uređaja. Za razliku od

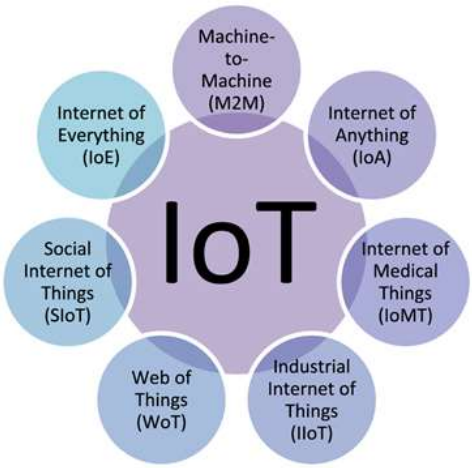
standardnih web ili mobilnih aplikacija, IoT rješenja uključuju dodatne slojeve. Nestandardni pristupi dizajnu interfejsa moraju kreirati jedinstvena rješenja za specifične IoT platforme, što često rade putem pokušaja i grešaka. Ovo uključuje umjetnu inteligenciju (AI), ulazno-izlazne tokove podataka, distribuciju korisničkih prava, specijalizovane platforme i još mnogo toga. Dizajneri moraju biti upoznati sa svakom komponentom IoT mreže kako bi sistem učinili besprekornim i lakim za krajnje korisnike.

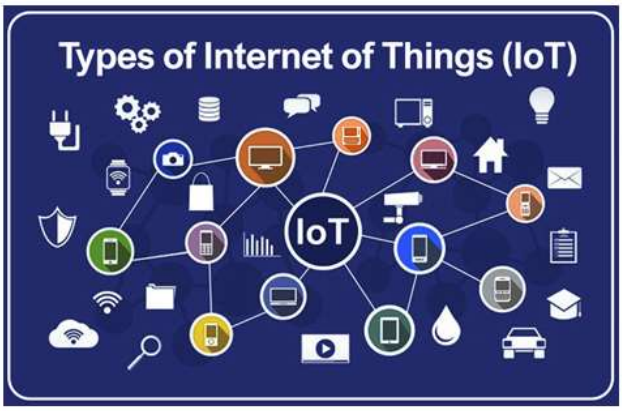



Rad IoT-a je različit za različite IoT sisteme/arhitekture. Međutim, ključni koncepti rada su slični. Osnov svakog IoT uređaja je bežični čip koji mu omogućava povezivanje na WiFi. IoT uređaji prikupljaju podatke sa svojih senzora i koriste softver kako bi odredili šta dalje. U većini slučajeva, IoT uređaj će:

- Povezati se sa centralnim serverom, obično u vlasništvu kompanije koja proizvodi uređaj, kako biste dobili više informacija
- Po potrebi uporediti i poslati podatke na druge web stranice i servere radi prikupljanja dodatnih informacija

- Povezati se na server za razmjenu poruka kako bi vas mogao e-mailom, SMS-om ili zvati da se povežete se s drugim IoT uređajima na istoj WiFi mreži kako biste im rekli da nešto urade.



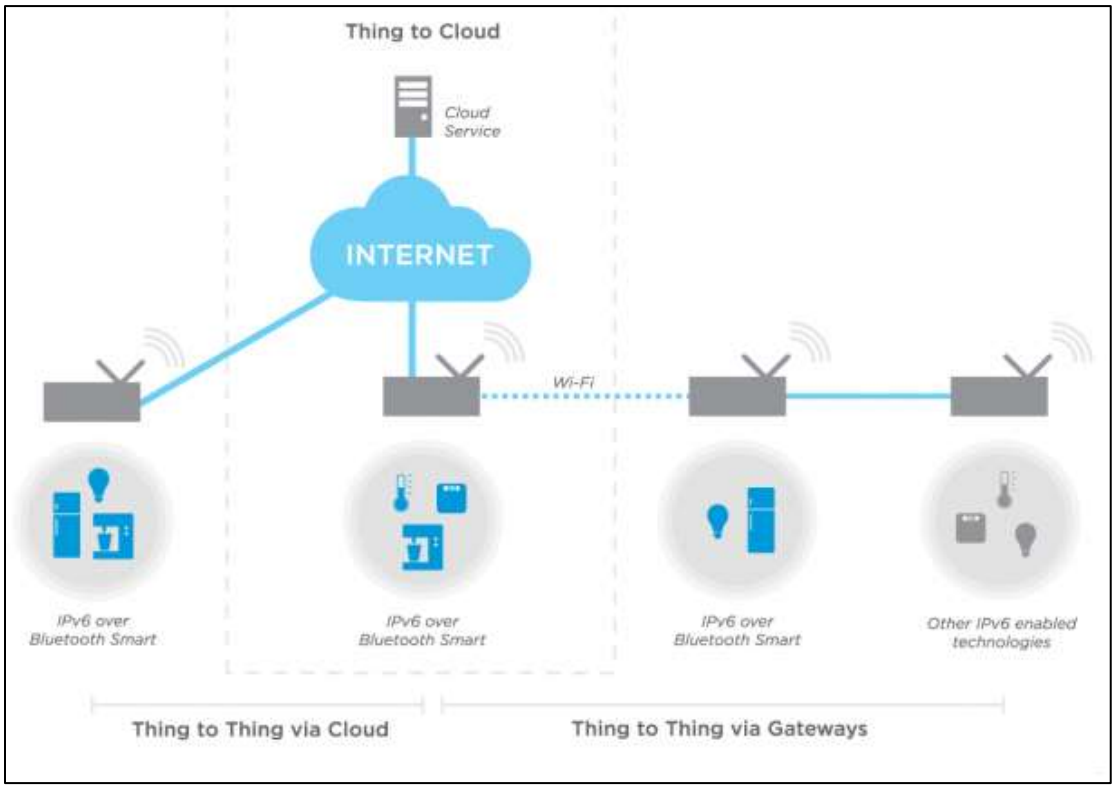

Lista tipova IoT uređaja kontinuirano raste iz dana u dan. Nabrojaćemo neke uobičajene vrste IoT uređaja:

- Senzori: Ovi senzori su inteligentni i mogu prikupljati informacije kako bismo donijeli odluku. Optički senzori za automatska ulična svjetla, senzori temperature za pametne termostate i unutrašnji senzori ugrađeni u industrijske mašine su primjeri senzora
- Sigurnosni uređaji: IoT senzori pokreta su dio naprednih IoT sigurnosnih sistema. Sigurnosne kamere za pametne kuće i uređaji za snimanje zvuka već su uobičajeni poslovnim i industrijskim prostorima.
- Pametni nosivi uređaji: Nosivi uređaji su jedni od najprepoznatljivijih IoT uređaja. Slušalice i pametni satovi su najčešći među njima. Međutim, u ovoj kategoriji ima još uređaja kao pametne naočale, uređaji proširene stvarnosti itd.
- Inteligentni uređaji: Inteligentni šporeti i frižideri, povezani televizori prikupljaju informacije o okolini putem IoT uređaja i u skladu s tim vrše odgovarajuća prilagođavanja.
- Aktuatori: Većina IoT uređaja prikuplja podatke o okolišu, dok aktuatori primaju podatke od drugih IoT uređaja i opremljeni su mehanikom potrebnom za fizičke promjene na osnovu primljenih podataka.

Da bi ove uređaje umrežili bilo bi potrebno protokole i tehnologije koje ih definišu.

# Mrežne tehnologije kod IoT

U IoT mreži koriste se različite mrežne tehnologije npr.:
WPAN (*Wireless Personal Area Network*) ili WLAN koja uključuje Wi-Fi.
Podržane su mobilne komunikacijske tehnologije poput 2G, 3G, 4G, LTE. Koriste se pametni telefoni i mobilni komunikacijski sistem koji će se povezivati na bazne stanice, a bazne stanice omogućavaju povezanost sa WAN, odnosno Internetom.
Najčešća kontrola topologije je WPAN koji je bluetooth ili NFC (*Near Feild Communication*). WPAN je često povezan sa pametnim telefonom i pametni telefon može dovesti signal preko 3G, 4G, LTE preko bazne stanice i bazna stanica će to povezati na WAN.

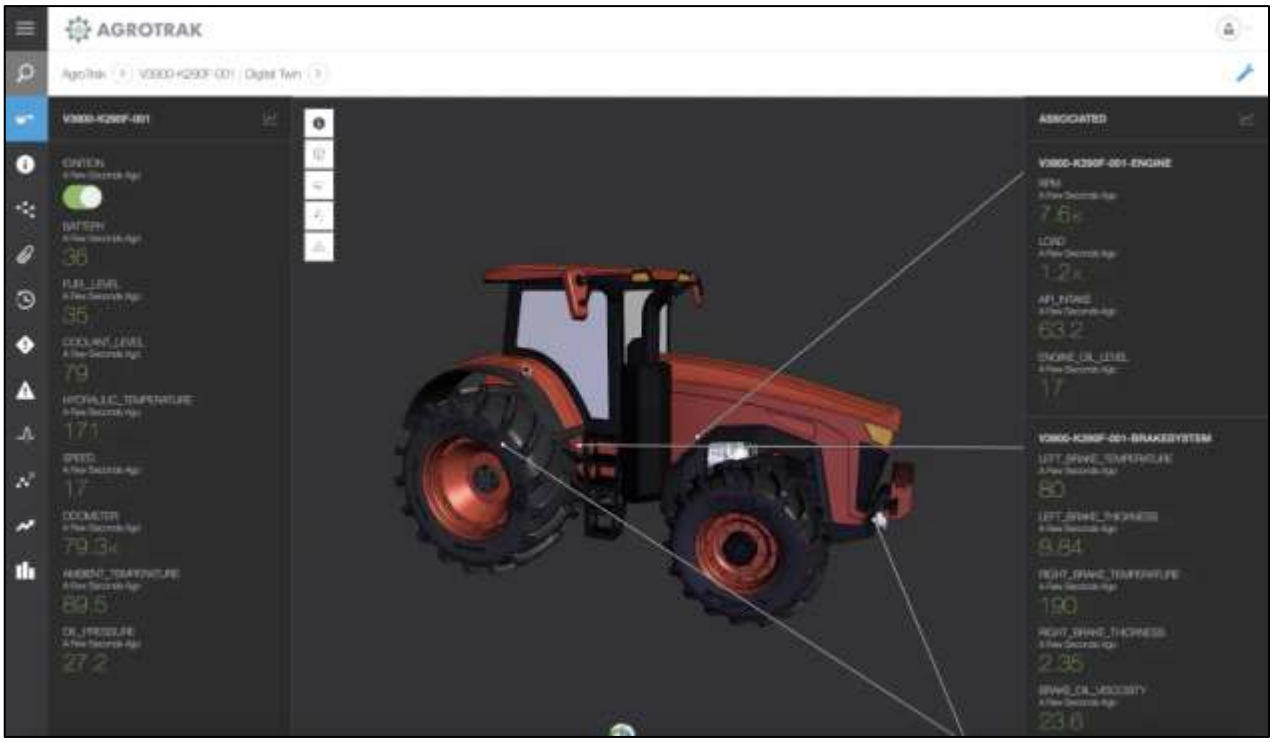



*Bluetooth IoT mreža*

Bluetooth Smart uređaji mogu se povezati na internet preko Bluetooth Smarta pomoću graničnog rutera. Granični ruter djeluje kao uređaj koji je povezan s internetom i omogućava pristup čvorovima interneta.

# IIoT, industrijski IoT

Industrijski IoT (IIoT) odnosi se na primjenu IoT tehnologije u industrijskim okruženjima, posebno u pogledu instrumentacije i kontrole senzora i uređaja koji koriste tehnologije oblaka. Donedavno se u industriji koristila samo komunikaciju mašina-mašina (M2M) za postizanje bežične automatizacije i kontrole. Pojavom oblaka i srodnih tehnologija (kao što su analitika i mašinsko učenje), može se postići novi nivo automatizacije i s njim stvoriti i nove poslovne modele.
IIoT se ponekad naziva četvrtim talasom industrijske revolucije ili industrijom 4 (Industry 4.0).




Traktor kao mrežni čvor i "Industrijaka internet stvar": *Primjer dizajniranja i konfigurisanja aplikacije IIoT-a*
*Mašine se mogu kontinuirano nadzirati i analizirati kako bi se osiguralo da rade u okviru dozvoljenih tolerancija*

# Standardi, referentna tijela i organizacije

Jednom prilikom je upitan da objasni šta je Internet Tim Berners-Li[37] je odgovorio:
*Protokoli, protokoli i protokoli.*
A protokole definišu referentna tijela za standardizaciju.

Internet je nesumnjivo najznačajnija mreža, a World Wide Web Consortium poznat po svom akronimu W3C je organizacija koja se bavi standardizacijom tehnologija korištenih na webu, koji je najznačajniji servis interneta. Osnovana je 1994. godine u saradnji između Massachusetts Institute of Technology (MIT) i Evropske organizacije za nuklearna istraživanja (CERN).


W3C djeluje kroz radne grupe te kreira i održava WWW standarde koji se nazivaju W3C preporuke (**W3C Recommendations**). W3C preporuke objavljuju se na W3C web stranicama. Osim toga W3C koordinira rad drugih organizacija za standardizaciju koje djeluju na istom području kao što su Internet Engineering Task Force, Wireless Application Protocols (WAP) Forum i Unicode Consortium. Na svojoj zvaničnoj stranici

W3C kaže da njegova misija uključuje "izradu protokola i smjernica koje osiguravaju dugoročni rast weba." Glavni standardi sem web protokola propisani od w3c su CGI, CSS, DOM, HTML, HTTP, XHTML i XML (očigledno sve ono što je vezano za veb).

Počevši od 1997. godine, W3C je stvorio regionalne kancelarije širom svijeta. Od septembra 2009. godine imala je osamnaest glavnih svjetskih kancelarija koje su bile zadužena za Australiju, zemlje Beneluksa (Belgija, Holandija i Luksemburg), Brazil, Kinu, Finsku, Njemačku, Austriju, Grčku, Hong Kong, Mađarsku, Indiju, Izrael, Italiju, Južnu Koreju, Maroko, Južnu Afriku, Španiju, Švedska i od 2016. Veliku Britaniju.

W3C ima stalno zaposleni tim od stotinjak ljudi zaposlenih širom svijeta na čelu sa izvršnim direktorom. Većinu poslova standardizacije obavljaju vanjski-eksterno angažovani stručnjaci u različitim radnim grupama W3C-a.

Prema podacima iz 2022. W3C organizaciju čini 459 članova. Zahtjeve za članstvo odobrava W3C. Mnoge smjernice i zahtjevi su detaljno navedeni, ali ne postoje konačne smjernice o procesu ili standardima prema kojima bi članstvo moglo biti konačno odobreno ili odbijeno. Članovi mogu biti vladine i nevladine organizacije i korporacije. Članstvo se plaća. Troškovi članstva su navedeni na kliznoj skali, u zavisnosti od karaktera organizacije koja se prijavljuje i zemlje u kojoj se nalazi. Zemlje su kategorizirane prema pokazateljima i mjerilima Svjetske banke prema bruto nacionalnom dohotku po glavi stanovnika. Dakle: *ako hoćete da propisujete pravila morate imati novca* za to.

Internet korporacija za dodeljivanje naziva i brojeva (*Internet Corporation for Assigned Names and Numbers,* **ICANN**) zadužena je za upravljanje adresama na Internetu, određivanje

[37] Timothy Berners-Lee, britanski naučnik koji je najzaslužniji za razvoj World Wide Web (WWW) 1989. kog je osmislio, dok je radio u CERN-u.

autonomnih sistema, administraciju korenog sistema domenskih imena, određivanje brojeva za protokole i sl. Prije formiranja ove korporacije pri američkom ministarstvu trgovine, njene funkcije su vršene na Institutu za informacione nauke pri Univerzitetu Južna Kalifornija, na osnovu ugovora sa američkim ministarstvom odbrane. Pri ovoj korporaciji funkcioniše i *IANA (Internet Assigned Numbers Authority*).


**IETF**, Specijalna komisija za razvoj Interneta (*Internet Engineering Task Force*) zadužena je za razvoj i promovisanje Internet standarda. Učesnici ove organizacije su volonteri, s tim da je njihov rad plaćen od strane njihovih poslodavaca ili sponzora (trenutnog predsedavajućeg ove organizacije sponzorišu kompanija *VeriSign* i američka Nacionalna bezbjednosna agencija).


**ITU**, Međunarodna telekomunikaciona unija (*International Telecommunication Union)* je agencija pri Ujedinjenim nacijama, sa sedištem u Ženevi. Osnovni cilj ove agencije je razvoj telekomunikacione infrastrukture i uspostavljanje međunarodnih standarda.

Evropski institut za telekomunikacione standarde (engl. *European Telecommunications Standards Institute, ETSI*) je nezavisna, neprofitna organizacija, priznata od strane evropske komisije, a osnovana 1988. godine od strane evropske konferencije za poštansku i telekomunikacionu administraciju. Osnovni doprinos ove organizacije je u razvoju standarda za mobilnu komunikaciju.

Dominantnu ulogu na polju računarske bezbjednosti i njene standardizacije imaju SAD. Vodeće organizacije na polju standardizacije bezbjednosnih sistema funkcionišu kao agencije vlade SAD.

Američki Nacionalni institut za standardizaciju i tehnologiju (*National Institute of Standards and Technology, NIST*), ranije poznat pod imenom Nacionalni biro za standardizaciju (*National Bureau of Standards, NBS*), osnovan je 1901. godine kao agencija departmana za trgovinu vlade SAD. Kao zvanična misija instituta navedena je promocija inovativnosti i industrijske kompetitivnosti SAD putem unapređivanja nauke, standarda i tehnologije.

Jedna od najznačajnijih organizacija za standardizaciju na polju računarske bezbjednosti je američka Nacionalna bezbjednosna agencija (*National Security Agency, NSA*). Ova agencija je osnovana 1952. godine sa ciljem da pruži usluge nadgledanja komunikacija stranih obavještajnih službi i zaštitu komunikacija vlade SAD. Od 2008. godine ova agencija je zadužena i za zaštitu vladinih računarskih sistema i mreža.

# Reference

Pisko akademija
https://sveznadar.info/20-WINTipsTricks/01-StartPiskoMreze.html

Računarske mreže: Mladen Veinović, Aleksandar Jevremović
http://www.racunarskemreze.com/Knjiga.

Sabah Al-Fedaghi, A Conceptual Foundation for the Shannon-Weaver Model of Communication https://www.researchgate.net/publication/272964534_A_Conceptual_Foundation_for_the_Shannon-Weaver_Model_of_Communication

SNMP protokol, NCERT-PUBDOC-2010-09-313
https://www.cis.hr/www.edicija/LinkedDocuments/NCERT-PUBDOC-2010-09-313.pdf

Dragan Pleskonjic, Nadzor računarskih mreža,
https://dragan-pleskonjic.com/wp-content/uploads/2017/01/SRM_Predavanje_13.pdf

Mreže računara, skripta; Luka Grubišić, Robert Manger
https://web.math.pmf.unizg.hr/~luka/publ/MR-skripta.pdf

http://www.phy.pmf.unizg.hr/~dandroic/nastava/rm/dns.pdf

https://www.cisco.com/c/en/us/solutions/enterprise-networks/what-is-networking-software.html

https://www.fastcabling.com/2022/03/07/media-conversion-ethernet-to-fiber/

https://www.spiceworks.com/tech/networking/articles/what-is-network-software/

https://support.microsoft.com/en-us/windows/fix-network-connection-issues-in-windows-166a28c4-14c1-bdb1-473c-09c1571455d8

https://www.ibm.com/docs/hr/i/7.1?topic=service-network-hardware-software

https://www.javatpoint.com/classful-vs-classless-addressing

Softverski definirana mreža; B. Valić, T. Gligora, Veleučilište Velika Gorica,
https://www.bib.irb.hr/

https://opentechdiary.wordpress.com/2015/07/18/part-4-a-walk-through-internet-of-things-iot-basics/

Pregled i analiza performansi softverski definiranih mreža, Vlajčić, Marija;
https://repozitorij.fpz.unizg.hr/islandora/object/fpz:1421

https://www.educba.com/my-courses/free/

https://www.cloudflare.com/learning/network-layer/network-security/