

## 17. MAC adresa

- Adresiranje obavezno na deljenim vezama
- **Fizička adresa** Ethernet protokola – **MAC (Media Access Control) adresa**
- Jedinstveni identifikator čvora
- Upisuje se u frejm (**odredišna i polazna adresa**)
- Na **osnovu odredišne adrese** čvor zna da li je frejm koji je stigao namenjen njemu i da li da ga procesira
- Dužina: 48 bits – 6 bytes
- Zapisuje se u **heksadecimalnom formatu** sa 12 heksadecimalnih cifri odvojene sa : ili –ili .
- Jedan adresni prostor, **nema hijerarhije**
- Adresu **dodeljuje proizvođač** mrežnog uređaja
- Burned-in address (BIA) – **upisana u ROM** mrežnog uređaja
- Jedinstvene na **globalnom nivou**
- Proizvođači se registruju kod IEEE da bi dobili jedinstveni broj (3 bytes)
- Taj broj ugrađuju u adresu
- **Prvih 24 bita jedinstvena oznaka proizvođača uređaja** (Organizationally Unique Identifier)
- Ostalih 24 bita jedinstven broj koji dodeljuje proizvođač

### **3 vrste MAC adresa:**

- **Unicast** -jedinstvena adresa uređaja koja se koristi kada se frejm šalje tačno jednom uređaju
- **Multicast** - za adresiranje grupe uređaja, frejmove adresirane na multicast adresu čitaju svi uređaji iz te multicast grupe - **Prva tri bajta - 01-00-5E**
- **Broadcast** - specijalna adresa sa svim bitima 1 (FF-FF-FF-FF-FF-FF) – ovaj frejm na toj adresi čitaju svi uređaji na mreži.

### **Broadcast domen**

- Dva čvora pripadaju jednom **broadcast domenu** ako jedan čvor može da primi frejm poslat da broadcast adresu od strane drugog čvora

## 18. Protokoli prenosnog nivoa

- Nisu standardizovani ni opisani uz pomoć RFC dokumenata kao viši nivoi.
- Zbog povezanosti sa **fizičkim** nivoom standardizovani su od strane **inženjerskih organizacija za standardizaciju**(IEEE, ISO..)
- **Protokoli** implementirani **na hardveru i drajverima** mrežnih uređaja.

### TCP/IP

- Prenosni nivo uporediv sa **mrežnim** nivoom TCP/IP protokol stacka
- Na mrežnom nivou imamo **različite protokole** u odnosu na **topologiju** i **fizički nivo mreže**
- Svi oni komuniciraju na **višem nivou** sa **IP protokolom**.
- Obezbeđuju **IP protokolu nezavisnost** od **fizičke implementacije mreže**

### **Neki od protokola**

- Ethernet
- Wireless LAN Protocol
- Token Ring
- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)
- Frame Relay → Asynchronous Transfer Mode (ATM)

## 19. Ethernet frejm

- Ethernet kao familija protokola i tehnologija definisanih standardima IEEE 802.2 i 802.3
- Obuhvata i **protokole OSI prenosnog nivoa** i *tehnologije OSI fizičkog nivoa*.
- Najčešće korišćena LAN tehnologija

IEEE 802.2 – Funkcije llc podnivoa - Logical link kontrol

IEEE 802.3 – Funkcije MAC podnivoa – Media access control

PDU – Ethernet frejm koji **enkapsulira** IP paket

Sadrži : **zaglavlje**, podatke, **trailer**

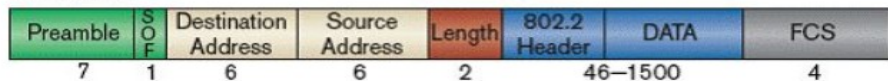
**Dva tipa ethernet frejma:**

1. **Ethernet II(DIX Ethernet standard)**
2. **Ethernet 802.3 standard**

Ethernet II



IEEE 802.3



1. **Preamble i SOF**(Start of Frame) delimiter - niz bitova za **sinhronizaciju čvorova**( ne sadrže info koje se tiču Ethernet protokola i ne smatraju se delom frejma) – **8B**

2. **Destination Address** – odredišna adresa čvora na koju se šalje frejm – **6 bytes**

3. **Source Address** – polazna adresa **čvora koji šalje frejm** – **6 bytes**

4. **Type** – oznaka **protokola višeg nivoa** koji je enkapsuliran u frejm – **2 bytes**

4.1. **Lenght** – dužina podataka koji se prenose u bajtima – **2 bytes**

- **802.2 Header** – kontoloni podaci 802.2 podnivoa (SSAP, DSAP, Ctrl) – **3 bytes**

5. **Data** – enkapsulirani podaci – **46 (43) -1500 (1497) bytes**

6. **FCS** – Frame Check Sequence, kontrolna suma (**CRC vrednost**) – **4 bytes**

**Razlika između ova dva tipa:**

- Frejm ima **maksimalnu dužinu** – **1518 bytes**
- **Type/Length < 1500** onda je to polje dužina i **Ethernet II tip** frejm
- **Type/Length > 1500** onda je to polje **oznaka protokola** i **Ethernet 802.3 tip** frejm

Oznake protokola moraju biti definsane vrednostima većim od 1500 da bi to funkcionisalo

## 20. Hab

### - **Mrežni uređaj**

- Povezuje radne stanice na druge habove

### - **Portovi RJ45**

- Fizička **topologija zvezda** (može da ima do 3 nivoa)

- **Signal** koji primi na jednom portu **prosledi na sve ostale** (eventualno ga pojača pre toga)

Radi na fizičkom nivou (**ne gleda frejmove**)

### - **Logička topologija magistrala**

- Svi čvorovi pripadaju jednom kolizionom domenu i jednom broadcast domenu

- Ethernet sa habovima – Deljeni Ethernet.

- Veći broj čvorova – veća verovatnoća da se desi kolizija

### - **Loša skalabilnost mreže**

U **jednom momentu samo jedan čvor koristi medijum** – svi čvorovi dele propusni opseg

- Svi podaci dolaze do svih čvorova na mreži

- Povećanjem broja čvorova lošiji odziv mreže

- Rešenje – upotreba svičeva

## 21. Svič

Povezuje radne stanice i druge habove i svičeve

### - **Fizička topologija zvezda kao i kod haba**

Izgleda isto kao hab, ali drugačije funkcioniše

- **Svič analizira frejmove**, pa kažemo da radi na drugom nivou i da je **uređaj drugog nivoa**

- **Frejm primljen** na jednom portu šalje na **tačno određen drugi port (selective forwarding)**

- Na osnovu odredišne adrese u frejmu zna kom portu da prosledi

### Svič tabela (MAC tabela)

- **Parovi:** MAC adresa – ogovarajući port

- Svič čita odredišnu adresu iz **zaglavlja frejma**

- U svič tabeli se nalazi informacija na kom portu se nalazi uređaj sa tom adresom

- Frejm prosleđuje na taj port

### **Kako se popunjava tabela**

#### **Svič može da je nauči**

- **Analizira zaglavlja frejmova** i na osnovu **polaznih adresa** zaključuje na kom portu se nalazi koja adresa

- Ako za odgovarajuću adresu nema informaciju u tabeli upisuje je

- Vremenom nauči adrese svih povezanih uređaja

#### - **Inicijalno tabela prazna**

- Ako **svič ne zna na koji port** treba da prosledi frejm (nema informaciju u svič tabeli) **šalje ga na sve portove (flooding)**

- Inicijalno svič se ponaša kao hab

- Vremenom nauči tabelu

- **Red u tabeli ima vremensko trajanje**, nakon nekog vremena ako **adresa nije korišćena red se izbacuje** iz tabele da bi tabela bila manja i lakše pretraživa

- Tabela može i **ručno da se popuniti**

## FLOODING

-Svič šalje frejm na sve portove u 2 slučaja:

1. Ako je upućen na **broadcast adresu**

2. Ako u svič **tabeli nema informaciju** na kom se portu nalazi ta adresa (tabela još uvek nije naučena)

- **Svi čvorovi** povezani na svič pripadaju **jednom broadcast domenu**

- Svič **deli kolizioni domen** - Svaki port na sviču kreira poseban kolizioni domen

- **Smanjen broj kolizija**

- Za slanje frejma svič kreira **logičku full-duplex point-to-point konekciju** između dva čvora

- **Full-duplex konekcija** - čvor u isto vreme može i da **prima** i da **šalje podatke**

- Takvih konekcija može da bude više u isto vreme

- **Čvorovi koriste ceo propusni opseg**

- **Primer: 100 Mbps LAN, 10 čvorova**

→ Povezani habom – dele propusni opseg, prosečno svaki čvor će da ima **10 Mbps propusni opseg**

→ Povezani svičem – svaki čvor koristi ceo propusni opseg, svaki čvor ima **100 Mbps propusni opseg**

## Upravljivi i neupravljivi

→ **Neupravljivi** – vrše osnovnu funkcionalnost, ne postoji mogućnost nikakve konfiguracije

→ **Upravljivi** – mogu se konfigurisati (ručno popunjavanje svič tabele, uključivanje/isključivanje portova, kreiranje VLAN-ova,...)

**Modularni** – mogu se stavljati različiti portovi (moduli) u zavisnosti od potrebe

## 22. VLAN

- Struktuiranim kabliranjem korisnici grupisani u odnosu na fizičku lokaciju, Potrebno logičko grupisanje korisnika

- Potrebno razdvojiti grupe da nemaju komunikaciju preko drugog nivoa jer je kontrola saobraćaja između grupa na 3. nivou

- Jedna grupa treba da bude jedan broadcast domen - Jedna grupa treba da bude jedna IP mreža

- Svi uređaji **povezani na svič** pripadaju **jednom broadcast domenu** i imaju komunikaciju preko drugog nivoa

- **Frejm poslat na broadcast adresu svič prosleđuje na sve portove.**

**Rešenje** – svaka grupa korisnika ima svoj svič

**Loše rešenje** (broj korisnika, broj portova na sviču...)

**Bolje rešenje** – svič ima mogućnost da se to softverski uradi

## **Virtual LAN**

- Portovi na sviču se **podele u grupe**

- **Svaka grupa** jedan **broadcast domen**

- **Frejm poslat na broadcast adresu svič prosleđuje samo na portove koji pripadaju istoj grupi kao i port sa kog je došao frejm**

- Grupa - VLAN

- **Jednostavno realizovati na jednom sviču**

**Ako je povezano više svičeva kako portove sa različitim svičeva staviti u jednu VLAN grupu?**

- IEEE 802.1Q – **VLAN tagovanje**
- U **zaglavlju frejma** (iza polja **source address**) dodaje se **VLAN tag (4 bytes)** koji nosi informaciju kojoj VLAN grupi pripada frejm, odnosno kojoj VLAN grupi pripada port sa kog je došao frejm.
- Tag potrebno dodavati samo kada se frejm šalje na drugi svič
- **Trunk port** – port preko kog su svičevi povezani i koji vrši tagovanje
- **Svaki VLAN zaseban broadcast domen**
- Između VLAN-ova **nema komunikacije na drugom nivou**
- **Komunikacija preko trećeg nivoua – potreban uređaj koji radi na trećem nivou – ruter, L3 svič**
- Dobili smo **logičko grupisanje** korisnika
- Dobili smo kontrolu saobraćaja između grupa

## **23.WLAN**

**LAN mreže na bežičnom medijumu(deljeni je medijum)**

- Protokol definisan standardom **IEEE 802.11**
- Koristi 48-bitne MAC adrese
- Standardom IEEE 802.2 definisane funkcije LLC podnivoa kao i kod Ethernet-a
- **MAC podnivo se razlikuje**
- Problemi pristupa medijumu, adresiranja i detekcije grešaka

Za pristup medijumu se koristi **CSMA/CA algoritam**

- **Ideja - izbeći kolizije jer se teško detektuju**  
(opisati CSMA/CA)

Postoji **povratna informacija o isporuci frejma**, za svaki poslati frejm dobija se obaveštenje da je stigao

- Ako obaveštenje izostane znak da je došlo do kolizije ili da iz nekog drugog razloga frejm nije isporučen i da ga treba ponovo poslati

Frejm mnogo komplikovaniji od Ethernet frejma → Mnogo više kontrolnih podataka

Wireless mrežna kartica – na korisničkim uređajima

- **Wireless access point** – komunicira sa korisničkim uređajima i obično je **povezan žičnim medijumom na neku mrežu**

- Zbog prirode medijuma funkcionalnost **slična habu** – sve što se pošalje od strane jednog čvora dolazi do svih drugih čvorova

## **WLAN standardi**

WLAN standardi

Postoje različiti standardi u odnosu na frekvencije i protok podatka koji se postiže

- IEEE 802.11a i IEEE 802.11b prvi koji su bili u upotrebi
- Nasledio ih je 802.11g sa protokom od **54Mbps**
- 802.11n radi na 2.4 Ghz ili 5 GHz, protok do **600 Mbps, WiFi 4**
- 802.11ac radi na 2.4 Ghz ili 5 GHz, protok do **6 Gbps, WiFi 5**
- 802.11ax sledeća generacija - **WiFi 6**
- WiFi uređaji obično podržavaju sve verzije unazad od trenutno aktuelne
- Protok koji se postiže zavisi od same implementacije na uređaju

## Bezbednost

- Nije fizički ograničen medijum
- Svako ima pristup
- Bezbednost podataka veliki problem
- Protokoli za enkripciju (šifrovanje) podataka i autentifikaciju
  - WEP - prvi napravljen, vrlo loša zaštita
  - WPA - napravljen da zameni WEP, i dalje ranjiv
  - WPA2 - poboljšana enkripcija, ima sigurnosne propuste
  - WPA3 - najnoviji

## 24. Zadaci mrežnog nivoa

- Opisuje komunikaciju između različitih skupova čvorova gde je jedan skup čvorova ustvari mreža gde su svi čvorovi povezani na isti prenosni medijum sto je jedan broadcast domen.
- Ne može se proširiti na globalni nivo – velik broj čvorova, nema hijerarhije imena i **različite arhitekture mreže**.
- Za komunikaciju unutar jedne mreže dovoljan je samo prenosni al imeđu više mreža onda mrežni jer čvorovi nemaju direktnu konekciju.
- **Različite mreže mogu imati različite protokole prenosnog nivoa i da imaju različite fizičke izvedbe.**
- Čvor na mrežnom nivou je **host**.

### Konkretni zadaci

- Da bi se omogućila komunikacija između različitih mreža potrebno je obezbediti:

**Adresiranje** – jedinstveno adresiranje mreže i hostova unutar nje

**Rutiranje** – pronalaženje putanje između dva hosta – paket u svom putu prolazi kroz više mreža

Ruteri – uređaji za usmeravanje paketa ka odredištu.

### PDU – paket

#### Delovi paketa:

1. **Zaglavlje** – kontrolni podaci bitni za mrežni nivo
2. **Data, payload** – podaci dobijeni od protokola višeg nivoa

OSI mrežni nivo je uporediv sa Internet nivoom TCP/IP protocol stack-a

Najznačajniji protokoli Internet nivoa su IP i ICMP protokoli

**IP protokol** se koristi za **transport podataka**

**ICMP protokol** se koristi za **dektciju grešaka u komunikaciji**

## 25. IP protokol (uopšteno)

- **Osnovni zadatak** – prenos podataka od jednog hosta do drugog na **osnovu njihovih adresa**

PDU – IP paket

- **Connectionless** – ne kreira konekciju između dva hosta koji razmenjuju podatke (kada jedan šalje paket ovaj drugi nema zna da treba da mu stigne)
- Paketi **nezavisni** jedan od drugog i mogu do odredišta da putuju različitim putanjama i da stižu proizvoljnim redosledom.
- Nema garancije isporuke tako da nema ni povratne informacije da li je paket stigao na odredište.
- Pouzdanost komunikacije rešena na **transportnom nivou**.
- Jednostavan protokol, razmenjuje malu količinu podataka vezanu za sam protokol.

- **Nezavisan od fizičke arhitekture**(koja vrsta medijuma, topologija...) to mu je obezbedio prenosni nivo.
- IP protokol je isti za sve vrste mreža.
- Fizička arhitektura određuje samo veličinu paketa koja može da se prenese.
- **MTU(Maximal Transmission Unit)** – maksimalna veličina IP paketa koja se može preneti preko protokola nižeg nivoa.
- Različite mreže imaju različiti MTU – Ethernet protokol MTU-1500B
- Aktuelna verzija je IPv4 – 32bitna adresa- problem mali adresni prostor potrosila se
- Standardizovana verzija Ipv6 128b adresa u fazi implementacije

## **26. IP paket**

### **- Zaglavlje i podaci**

Prikazana u formatu 32-bitnih reči i enkapsulira se u frejm.

#### **Prva 32-bitna reč:**

1. **Version** – verzija IP protokola – 4b
2. **IHL** – Internet header length dužina zaglavlja IP paketa u 32-bitnim rečima(nema fiksnu dužinu)4b
3. **Type of Service** – prioritet paketa u transportu – 8b
4. **Total length** – **dužina paketa** bajtovima (uključujući i zaglavlje i podatke) – 16b

#### **Druga 32bitna reč** – polja vezana za proces fragmetacije

1. **Identification** – 16 bits
2. **Flags** - 3 bits
3. **Fragment Offset** – 13 bits

#### **Treća 32-bitna reč**

1. **TTL** – **Time To Live** – trajanje IP paketa u transportu – **8 bits**
2. **Protocol** – oznaka protokola višeg nivoa koji je enkapsuliran u paket – **8 bits**
3. **Header Checksum** – kontrolna suma zaglavlja paketa – **16 bits**

#### **Četvrta 32-bitna reč**

1. **Source IP address** – IP adresa hosta koji šalje paket – **32 bits**

#### **Peta 32-bitna reč**

1. **Destination IP address** – IP adresa hosta kome je paket upućen – **32 bits**

Prvih pet reči su obavezna polja

#### **Od šeste do dvadesete 32-bitne reči:**

1. **IP Options** – **opciona polja** – retko se koriste i može da se upiše striktna putanja paketa ili tačke kroz koje je paket prošao kao i vreme prolaska

Max dužina zaglavlja je 20 32-bitnih reči

Data – Enkapsulirani podaci dobijeni iz protokola višeg nivoa – kao poslednja rel

## 27. TTL mehanizam i fragmentacija

Time to live – 8bit

- **Maksimalna granica** trajanja IP paketa u transportu

- Paket putuje hop-by-hop od rutera do rutera tako da je TTL **hop count** – broj rutera kroz koje paket može proći

Kada prođe kroz ruter hop count se smanji za 1, a kada postane 0 onda se izbacuje paket iz saobraćaja.

- Ovo sprečava da se paketi beskonačno vrte u petlji.

Max vrednost 8 bita što je  $2^8 = 256 - 1$  kao max vrednost polja što znači da paketi mogu proći maksimalno 255 rutera (obično ih nema preko 30)

**Fragmentacija** – podela paketa na više paketa ako im je paket već od MTU (pojava kada ruter prebacuje paket sa jedne vrste mreže na drugu).

-Maksimalna veličina paketa je  $2^{16} - 1$  a veličina MTU za npr Ethernet 1500

-Ako je paket veći onda se podeli na više manjih gde svaki ima svoje zaglavlje i podatke i manji je od MTU.

-Na odredištu se od fragmenata rekonstruiše originalni IP paket, s tim da moraju svi fragmenti da stignu i isporučivanje podataka višem nivou.

-Ako viši nivo ne dobije podatke tražiće **retransmisiju** a onda će se ponovo slati **svi podaci originalnog paketa** a ne samo fragmenti koji nisu stigli što je loše.

Obično se **veličina podataka** u IP paketu (veličina **segmenta sa četvrtog nivoa**) uklopi da ne mora da se radi fragmentacija.

- **MSS - Maximum Segment Size** – maksimalna veličina segmenta na četvrtom nivou

$MSS = MTU - 20$

- Ne može se izbeći kada paket na putanji naiđe na mrežu sa manjim MTU

### Polja za fragmentaciju u IP paketu

1. **Identification** – identifikacija originalnog IP paketa koji je rastavljen na fragmente

2. **Flags** –

1. ■ **MF** – More Fragments – da li ima još fragmenata

2. ■ **DF** – Don't Fragment – da li sme da se radi fragmentacija

3. ■ Ne koristi se

3. **Fragment Offset** – lokacija fragmenta u originalnom IP paketu (udaljenost od početka paketa)

## 28. IP adrese i opsezi adresa

Adresa trećeg nivoa jer treba obezbediti adresiranje mreža i hostova unutar mreža

Svaki host = jedinstvena IP adresa

- Nosi Informaciju **kojoj mreži host pripada**, kao i **jedinstvenu oznaku** unutar mreže

- Adrese se koriste kao polazna i odredišna adresa u **zaglavlju** IP paketa

**Dužina** – 32 bita u decimalnom formatu kao četiri decimalna broja razdvojena tačkom -**Dotted decimal**

4 bajta svaki jedan decimalni broj

Sastoje se od dva dela koji nisu fiksne dužine

1. **Oznaka mreže – prvi deo**

2. **Oznaka hosta** unutar mreže – drugi deo

Prvobitno su se opsezi adresa delili po klasama (klasa A 7 bita, klasa B 14 C21- ako ima do 255 hostova) – vremenom je ponestalo mesta pa je osmišljen optimalniti način kreiranja opsega sa classless addressing.



## 29. Classful i classless šema adresiranja

- **Classfull**- prvobitna podjela adresnog prostora

**Klasa A** 0-networkID(8b) preostalih 24b za hostID – **Za velik broj hostova 2 na 24 -1**

**Klasa B** 10+14b za **network** preostalih 16 za host – 65535 hostova

**Klasa C** 110 + 21b za network id ostalih 8 za hostove znači 255 **hostova**

**Klasa D** 1110 multicast

Klasa E 1111 za eksperimente

### Classless

- Oznaka mreže promenljive dužine bez obzira na klasu kojoj pripada adresa

- Dužina oznake mreže definisana mrežnom maskom

- **Mrežna maska** -32-bitna adresa koja se sastoji od 1 i 0

**Broj jedinica** u masci određuje **broj bitova** u adresi koji **predstavljaju oznaku mreže**

Dva načina zapisa maske 255.255.255.0 ili /24

Classful addressing - maske imale predefinisane vrednosti /8, /16 ili /24

Classless addressing -maska proizvoljne dužine

Specifičnost mrežne maske - broj jedinica u masci

IP mreža jedinstveno određena adresom i mrežnom maskom

Na osnovu njih se određuje

1. **oznaka mreže**- kada se na host deo mreže stave sve 0(ili kada se pdradi and između bilo koje adrese i maske)
2. **opseg adresa koje se dodeljuju hostovima** - opseg adresa između oznake mreže i broadcast adrese
3. **broadcast adresa** -adresa na koju se šalje saobraćaj namenjen svima u mreži – dobije se kada se u host deo stave 1

## 30. Javne i privatne IP adrese

Sve IP adrese jedinstvene na internetu IANA vodi računa o podeli adresnog prostora, ip adrese, dns domene tcp/udp portove

- Adrese kojima **IANA** raspolaže su **javne IP adrese**.

- Host sa javnom IP adresom može da komunicira sa svim drugim hostovima sa javnim adresama na Internetu

- Hostovi u lokalnim mrežama nemaju uvek potrebu za komunikacijom na Internetu nego samo sa komunikacijom u lokalnoj mreži (ili imaju potrebu za ograničenom komunikacijom, e-mail, www...)

### **Ideja:**

Hostovi koji nemaju potrebu da komuniciraju na Internetu mogu koristiti IP adrese koje su jedinstvene na nivou lokalne mreže

**IANA** odredila privatne opsege IP adresa i njihovo korišćenje je slobodno ne kontroliše ih IANA

- Hostovi koji koriste prvatne komuniciraju unutar lokalne računarske mreže i **ne mogu da komuniciraju sa hostovima na Internetu**.

- Različite lokalne mreže mogu da koriste iste privatne opsege jer su te adrese jedinstvene samo na nivou lokalne mreže.

### **- Privatni opsezi**

1. 10.0.0.0/8

2. 172.16.0.0/12

3. 192.168.0.0 /16

Ove adrese se ne pojavljuju nigde kao javne adrese hostova koji komuniciraju na Internetu

Sve ostale adrese osim ovih (i nekih sa specijalnom namenom) su javne

## 31. NAT

- Hostovi u lokalnim mrežama imaju potrebu za ograničenom komunikacijom na Internetu tipa pristup www srvisima razmena e-mail poruka
- Ta **komunikacija** je inicirana od strane hosta u **lokalnoj mreži**, hostovi na netu nemaju potrebu da direktno – samoinicijativno da pristupaju hostovima u lokalnoj mreži
- **NAT** (Network Address Translation) – servis koji prevodi privatne adrese u javne i obrnuto.
- Implementiran na **ruteru** preko koga je privatna mreža povezana sa javnom **internetom**.
- Ruter ima **javnu IP** adresu na **portu** preko kog je **povezan na javnu mrežu**, a **privatnu** na portu preko kog je povezan na **privatnu mrežu**.
- Ruter kao posrednik u komunikaciji između hostova sa privatnim i hostova sa javnim adresama

### **Koraci:**

1. Host u privatnoj mreži šalje pakete ruteru sa svojom privatnom IP adresom
2. Ruter privatnu adresu zamenjuje sa svojom javnom, pamti od koga je dobio paket i dalje ga prosleđuje
3. **Povratak** Ruter na svoju javnu adresu dobija paket kao odgovor na poslati paket
4. U dobijenom paketu svoju javnu adresu zamenjuje sa privatnom adresom hosta i prosleđuje mu paket

**Svi paketi koji izlaze** izvan privatne mreže imaju **javnu** adresu **rutera**.

**Hostovi javne mreže** komuniciraju sa **ruterom** direktno, ne sa hostovima unutar privatne mreže (oni su sakriveni)

NAT za funkiconisanje koristi **IP adrese** trećeg nivoa i **portove** četvrtog

Ima više tipova NAT-a gde neki omogućavaju hostovima iz javne mreže direktan pristup hostovima u privatnoj (DNAT ili port forwarding)

**Upotrebom privatnih opsega za adresiranje** u lokalnim mrežama u **kombinaciji sa NAT** servisom za pristup javnoj mreži dobili smo:

→ **Racionalnije korišćenje javnog opsega** IP adresa

→ **Bezbednije okruženje** u lokalnim mrežama

## 32. Dodela IP adresa i DHCP

- IP adrese je potrebno dodeliti one nisu dodeljene kao mac adrese od strane proizvođača

### **Dodela adresa**

**1. Statička dodela** – administrator ručno konfiguriše parametre na hostovima (troši vreme) ali je dobro jer administrator tačno zna koji host ima koju adresu (**pogodno** za hostove koji trebaju da imaju stalnu adresu – štampač server...)

**2. Dinamička dodela** – Koristi se DHCP, radi se automatski i na mreži postoji DHCP server (štedi vreme administratorima, adrese se ne dodeljuju za stalno nego na određen period)

### **DHCP – Dynamic Host Config Protocol**

- Protokol aplikativnog nivoa

- Dodeljuje automatski mrežne parametre korisničkim uređajima na mreži od stran DHCP servera

- Mrežni parametri koji se dodeljuju:

1. IP adresa
2. Mrežna maska
3. Default gateway
4. DNS server...

Proces dodele parametara ima 4 koraka (razmenjuju se 4 paketa)

1. **DHCP discovery** - Kada se klijent konektuje na mrežu šalje **na broadcast adresu poruku** kojom traži mrežne parametre od DHCP servera - U poruci šalje svoju **MAC adresu**

2. **DHCP offer** - Kada server (jedan ili više njih) primi poruku rezerviša IP adresu koju vezuje za klijentovu **MAC adresu i šalje je sa ostalim mrežnim parametrima** kao **ponudu** klijentu - **Poruka se šalje se na broadcast adresu** jer klijent još uvek nema IP adresu
3. **DHCP request** - Klijent može da dobije više ponuda i **prihvata samo jednu** - Na **broadcast adresu** šalje **poruku o prihvatanju ponude**.
4. **DHCP acknowledgement** -DHCP server čija je ponuda prihvaćena šalje klijentu **potvrdu o prihvatanju** ponude i **vreme koliko klijent** može da koristi te parametre - Nakon isteka vremena klijent će ponovo da zahteva parametre

- DHCP server dodeljuje adrese iz definisanog skupa adresa - **address pool**

- Dodeljene **adrese vezuje za MAC adrese** klijenata i tako pamti kom klijentu je dodelio koju adresu

- Adrese se dodeljuju privremeno na određen period - **lease period**

-Nakon isteka lease perioda klijent ponovo šalje zahtev za mrežne parametre, odnosno za novi lease period sa istim parametrima

- Ako je **istekao lease period** i **klijent nije poslao** novi zahtev DHCP server adresu **vraća u address pool** i može da je dodeli nekom drugom klijentu.

- Za **hostove koji uvek treba da imaju istu adresu** (šampači, serveri...) administrator može u okviru DHCP servera da **rezerviša adrese**

- Rezervisana adresa se vezuje za MAC adresu host

### **33. ARP**

#### **Problem:**

IP paket ima polaznu i odredišnu IP adresu i enkapsulira se u **frejm** protokola drugog nivoa.

Da bi se poslao frejm potrebno je znati polaznu odredišnu MAC adresu tj adresu drugog nivoa

Host koji šalje IP paket zna svoje IP i MAC adrese al ne zna MAC adresu odredišta da bi poslao frejm

#### **ARP – Address Resolution Protokol**

- Koristi se da bi se saznala **fizička adresa** hosta čija je IP adresa poznata

- Implementiran za različite protokole drugog nivoa na LAN mrežama koji koriste deljenim medijum i adrese (Ethernet, IEEE 802.11, TokenRing...)

Mehanizam sa dva koraka:

1. **ARP Request** – Host koji treba da pošalje paket na određenu IP adresu, a nema odredišnu MAC adresu šalje arp request, on se enkapsulira u frejm koji se šalje na broadcast adresu. Poslaće IP adresu i zahtevati od hosta sa tom IP adresom da mu u odgovor pošalje svoju MAC adresu
2. **ARP Reply** – Host koji primi ARP request u kome se nalazi njegova IP adresa odgovara. ARP reply se enkapsulira u frejm koji se šalje na MAC adresu onog koji je poslao zahtev. **Odgovor** sadrži MAC adresu

Po prijemu ARP reply-a polazni host ima sve potrebne informacije za slanje IP paketa

- **Komunikacija** obično podrazumeva **slanje više paketa** na jednu adresu

- Bilo bi vrlo **neefikasno za svaki paket slati jedan ARP Request i ARP Reply**

- **Host čuva informacije koje dobije kroz ARP**

- **ARP tabela** - parovi MAC adresa i IP adresa

- Host kada šalje IP paket prvo će proveriti da li u ARP tabeli postoji odgovor IP adresa ako je tu uzmeće MAC adresu iz tabele. U suprotnom pokrene ARP mehanizam

- Red u tabeli traje određen period ako host nije slao pakete u tom periodu na tu adresu onda se red izbacuje.

**Cilj** : tabela mala i brzo pretraživa

Možemo ručno popunjavati tabelu

### **ARP je protokol DRUGOG nivoa**

- Koristi se kada se šalje paket hostu koji je u istoj mreži tj na istom broadcast domenu
- Omogućava enkapsulaciju IP paketa u frejm
- Kada se paket šalje hostu koji je u drugoj mreži paket putuje preko rutera (jednog ili više)
- Kada se paket šalje od hosta do rutera ili od rutera do rutera enkapsulira se u frejm (koristi se ARP)

### **34. Ruteri**

- Za komunikaciju između hostova u različitim mrežama.
- Mrežni uređaj **TREĆEG nivoa**
- Funkcije vrši na osnovu **informacija iz zaglavlja paketa**
- Povezuje različite mreže i prosleđuje pakete između njih
- Može da ima **različite interfejs** u odnosu na **vrstu mreže** na koju je povezan.
- Povezan na mreže preko svojih interfejsa gde je svaki interfejs povezan na različitu mrežu
- Svaki interfejs ima **IP adresu iz mreže** na koju je povezan – ruter nema ip adresu

#### **Osnovne f-je:**

1. Pronalaženje najbolje putanje za slanje paketa
2. Prosleđivanje paketa ka njegovoj destinaciji.

Kada ruter dobije IP paket, na osnovu **odredišne IP adrese** u paketu određuje **na koji interfejs** će da ga prosledi - rutiranje

#### **Odluku donosi na osnovu informacija u tabeli za rutiranje**

- Dobija **pakete enkapsulirane u frejm** protokola drugog nivoa koji se koristi na mreži na koju je povezan interfejs
- Ako je interfejs povezan na **Ethernet LAN** mrežu dobija paket enkapsuliran u **Ethernet frejm**
- Radi **dekapsulaciju**, odnosno raspakuje paket iz frejma
- Donosi **odluke o daljem slanju** paketa na osnovu **informacija u zaglavlju** paketa

**Ponovo enkapsulira paket u frejm** i to frejm protokola drugog nivoa mreže na koju se prosleđuje odnosno na koju je povezan interfejs preko koga se paket prosleđuje.

- Ako je to WAN mreža sa PPP protokolom onda u PPP frejm
- Šalje frejm

### **35. Rutiranje**

Svaki uređaj trećeg OSI nivoaa radi rutiranje i ima tabelu za rutiranje – ruter računar

- Paketi od odredišta do destinacije putuju **hop-by-hop** od rutera do rutera ili od hosta do rutera
- Ruter na osnovu informacija u svojoj ruting tabeli određuje kuda će dalje da proslediti paket.
- Paket se **uvek** prosleđuje nekom **susednom** ruteru
- **Susedni ruter** na osnovu svoje tabele za rutiranje određuje gde će dalje proslediti paket.

**Direktno konektovane mreže** – mreže na koje je ruter povezan preko svojih **interfejsa** (komunikacija preko drugog nivoa)

**Udaljene mreže** – mreže do kojih se može doći preko drugih rutera

## Susedni ruteri - ruteri na direktno konektovanim mrežama

Saobraćaj se šalje ili susednom ruteru (ako je namenjen nekoj udaljenoj mreži) ili hostu na direktno konektovanoj mreži (ako je namenjen tom hostu)

U tabeli za rutiranje se nalaze rute

Mogu biti

1. **Direktno konektovane** – rute za direktno konektovane mreže, automatski se dodaju u tabelu kao posledica dodele IP adrese i maske interfejsu rutera.
2. **Statičke rute** – rute za udaljene mreže
3. **Dinamičke mreže** – rute za udaljene mreže, dodaju ih protokoli za dinamičko rutiranje

Svaka ruta ima:

1. **Oznaku mreže i masku mreže na koju se odnosi**
2. **IP adresu susednog rutera** kome treba da prosledi paket kako bi on stigao do odredišne mreže (Next hop adresa)
3. **Oznaku interfejsa preko kog treba da prosledi paket na mrežu.**

- Direktno konektovane rute **nemaju NEXT hop** adresu i koristi se oznaka 0.0.0.0

- **Default ruta** – specijalna ruta koristi se za slanje saobraćaja namenjenog za mreže koje se ne nalaze u tabeli za rutiranje. Za oznaku mreže i masku koriste 0.0.0.0 i 0.0.0.0

- Na **korisničkim uređajima** default ruta se naziva i **default gateway**

- **Hostovi u lokalnoj mreži** obično komunikaciju sa svim **ostalim mrežama** ostvaruju **preko jednog rutera**

- Sav saobraćaj koji je namenjen drugim mrežama treba da šalju tom ruteru

- Za hostove u lokalnoj mreži taj ruter je default gateway

- **IP adresa default gateway-a** obično se na hostu podešava zajedno sa IP adresom hosta, to je **adresa interfejsa** na ruteru preko kog je ruter povezan sa lokalnom mrežom na kojoj se nalazi host.

- Dodeljivanjem IP adrese i maske hostu **automatski se u tabelu** za rutiranje hosta dodaje **direktno konektovana** ruta za mrežu kojoj host pripada.

- Dodeljivanjem adrese **default gateway-a** **automatski se u tabelu** za rutiranje hosta **dodaje default ruta**

- **Tabela za rutiranje hosta** koji je u nekoj **lokalnoj mreži** automatski se popuni kao posledica dodele **IP adrese, maske i default gateway-a** hosta.

- Dodelom **adresa interfejsima rutera** automatski se u tabelu za rutiranje **dodaju direktno konektovane rute**

- Rute za **udaljene mreže i default ruta** (ako je potrebna) dodaju se **ručno ili kroz protokole** za dinamičko rutiranje

### **36. Pronalaženje odgovarajuće rute**

- Ruter kada dobije paket na osnovu **odredišne adrese u paketu** i **informacija u tabeli** za rutiranje određuje kuda dalje da pošalje paket.

- **Za svaku rutu** u tabeli ruter radi logičku operaciju **AND** između **odredišne adrese** iz paketa i **maske iz tabele**, **razultat poredi sa oznakom mreže**.

- Ako se rezultat poklapa sa oznakom mreže ruta je kandidat za slanje paketa

**IP adresa AND maska rute = Net ID rute - ruta kandidat za slanje paket**

Može biti više kandidata - uzima se ona ruta čija maska ima veću specifičnost (veći broj jedinica)

- Kada se pronađe odgovarajuća ruta gleda se **Next Hop** i **interfejs**

- Ako je ruta direktno konektovana (Next Hop 0.0.0.0) paket se eknapuslira u frejm i šalje preko interfejsa definisanog u ruti.

- Ako ruta nije direktno konektovana (Next Hop je adresa nekog susednog rutera) paket treba proslediti tom ruteru

- Da bi se odredilo kuda treba proslediti paket da bi stigao do rutera ponavlja se proces traženja rute u tabeli za rutiranje, ali ovaj put za adresu rutera a ne za odredišnu adresu iz paketa

- **Default ruta** – uvek kandidat za slanje jer uvek važi  $0.0.0.0 \text{ AND IP adresa} = 0.0.0.0$

- Pošto je **specifičnost maske default rute 0** ona je uvek **poslednji izbor**, odnosno koristi se samo kada nema nijedna druga ruta koja je kandidat za slanje

- **Ako za paket ne postoji nijedna ruta** koja je kandidat za slanje paketa, paket se **izbacuje iz saobraćaja**

### **37. Statičko i dinamičko rutiranje**

#### ***Statičko rutiranje***

- U tabelu za rutiranje rute mogu da se dodaju ručno od strane administratora (statičke rute)

#### **Nedostaci:**

1. Dodavanje novih mreža i rutera zahteva ručne izmene tabela za rutiranje na svim drugim ruterima
2. Širenjem mreže tabele za rutiranje postaju teške za održavanje
3. Velika mogućnost greške prilikom konfiguracije

---

#### ***Dinamičko rutiranje***

- **Protokoli** za dinamičko rutiranje omogućavaju **automatsku razmenu informacija o rutama** između rutera

#### **Prednosti:**

1. Dodavanje novih mreža i izmene na mreži ne zahtevaju ručne izmene tabela za rutiranje od strane administratora, ruteri sami razmene informacije o izmenama
2. Administratori imaju manje posla oko održavanja

#### **Nedostaci:**

1. Troši se protok na mreži na razmenu informacija o rutiranju - kod statičkog rutiranja nema nikakve razmene informacija vezanih za rutiranje
2. Troše se resursi rutera na procesiranje dobijenih informacija da bi se izračunale rute kod statičkog rutiranja nema računanja ruta

Koriste se oba tipa rutiranja zavisno od veličine i tipa mreže i administratorovog izbora i znanja

#### **Osnovne komponente protokola za rutiranje:**

1. **Skup poruka** koje koriste ruteri u **svrhu razmene informacija o rutiranju**, kao i **način razmene tih poruka**
2. **Algoritam** koji se koristi za **računanje ruta** na osnovu dobijenih **informacija**

### Tipovi protokola za dinamičko rutiranje:

1. **Vektor udaljenosti (Distance vector)** – RIP EIGRP
2. **Stanje linka – Link state** – OSPF, ISIS
3. **Vektor putanje(Path vector)** - BGP

### 38. Distance vector protokoli

- Informacije o rutiranju razmenjuju tako što šalju rute iz tabela za rutiranje i razmenjuju se samo sa **susednim ruterima**.

- Za svaku rutu se definiše metrika – **cena rute**.

- Ako ruter dobije dve rute za istu mrežu koristi onu koja ima **manju metriku**.

- Kada ruter šalje rutu povećava joj metriku u odnosu na **vrstu linka** prema drugom ruteru.

#### **RIP – Routing information Protocol**

- Najstariji, postoje verzije 1 i 2 za IPv4 i RIPng za Ipv6

- **Metrike rute – hop count** – broj rutera kroz koje treba proći da bi se stiglo do mreže

- Ruta koja ima manju metriku je bolja

- **Informacije o rutiranju** se razmenjuju tako što ruter periodično na 30 sekundi šalje celu routing tabelu susednim ruterima

- Prilikom slanja **svakoju ruti** se **poveća metrika** za 1

- Prilikom slanja **direktno konektovane rute** dobijaju **metriku 1**

- Kada ruter dobije routing tabelu od **susednog rutera upoređuje rute sa svojim rutama**

- Ako je za jednu mrežu dobio rutu koja ima bolju metriku (manju) od postojeće rute, u routing tabelu će da stavi novu rutu a izbaci postojeću

- **Bolja metrika** znači da treba **proći kroz manji broj rutera** da bi se stiglo do određene mreže

#### **Nedostaci:**

1. Metrika je hop count, bez obzira na karakteristike linkova
2. Mreža sporo **konvergira** jer se **informacije** od rutera do rutera **propagiraju na 30 sekundi**
3. **Uvek se šalje cela tabela za rutiranje** - nepotreban saobraćaj
4. **Informacije** se šalju **periodično bez obzira** da li je bio nekih **promena** na mreži
5. Ruteri nemaju celu sliku mreže nego samo metrike pojedinačnih ruta

### 39. Link state protokoli

- Informacije o rutiranju razmenjuju tako što šalju **informacije o stanju svojih veza** (linkova) sa susednim ruterima.

- Veza ima metriku (cenu)

- Informacije se šalju **svim ruterima** ne samo susednim.

- Na osnovu tih informacija ruteri kreiraju sliku cele topologije mreže i na osnovu toga određuju najbolje putanje do pojedinačnih mreža (rute)

- Prevazilaze ograničenja i nedostatke distance vector protokola

- **Algoritmi za računanje ruta** kod link state protokola komplikovaniji pa zahtevaju **bolje performanse uređaja** nego distance vector protokoli

- Podržavaju ih bolji (skuplji) mrežni uređaji.

#### **OSPF - Open Shortest Path First**

- Najviše se koristi – Verzija 2 za IPv4 i verzija 3 za Ipv6

- Linkovima između rutera se dodeljuju metrike

- Metrika se računa na osnovu **bandwidth-a linka – što je veći bolja je metrika tj manja je**.

- Svaki ruter sa susednim ruterima uspostavlja i održava “susedske” odnose

- **Odnosi** se održavaju **periodičnim razmenjivanjem kratkih Hello paketa** sa susedima (na 10 sekundi)
- Na osnovu “**susedskih**” odnosa svaki ruter **zna ko su mu susedi** i kolike su **metrike linkova** sa susedima
- Te **informacije** se šalju **Link-state paketima** svim ostalim ruterima na mreži
- Ruter na osnovu **Link-state paketa** koje dobija od drugih rutera **kreira sliku cele topologije mreže** i na osnovu toga **računa rute za ruting tabelu**

- Link-state paketi se **ne šalju periodično**, nego samo kad dodje do neke promene (prekid linka, promena bandwidth-a linka,...)
- **Promene stanja linkova** se detektuju kroz “susedske” odnose, odnosno kroz razmenu Hello paketa
- Ruteri koji razmenjuju **Link-state pakete** pripadaju **jednoj mulitcast grupi** i paketi se razmenjuju samo **unutar te grupe**, a ne kroz broadcast

#### ***Prednosti u odnosu na RIP:***

- **Brža konvergencija** – kada ruter dobije informaciju o prekidu nekog linka, na osnovu slike mreže može da izračuna novu rutu
- **Metrika** – bandwidth
- **Informacije se šalju samo kada dodje do neke promene na mreži**, a ne periodično (periodično se šalju samo Hello paketi koji troše malo protoka)

## **40. ICMP i provera dostupnosti hosta**

- Pošto IP protokol nema garanciju isporuke tako da kad host pošalje IP paket nema info da li je on stigao.
- Garancija isporuke je na protokolu na četvrtom nivou.
- ICMP je protokol na trećem nivou i obezbeđuje povratne informacije o poslatom paketu(**to i dalje nije garancija isporuke**)

### **ICMP – Internet Control Message Protocol**

- I ako je protokol trećeg nivoa **enkapsulira se u IP paket**
- Služi za dijagnostikovanje problema na mreži.
- ICMP poruke se **generišu kao odgovor na poslato paket**, usled nekih problema ili stanja na mreži, a od strane rutera koji paket ne može da prosledi dalje

#### ***Format poruke:***

1. **Type** – tip poruke
2. **Code** – događaj u okviru tipa -podtip
3. **Checksum** – kontrolna suma cele poruke
4. **Contents** – sadržaj poruke – zavisi od tipa

Postoje različiti tipovi ICMP poruka

#### ***U odnosu na tip poruke obezbeđuju***

1. Proveru dostupnosti hosta
2. Informacije o nedostupnosti destinacije
3. Informacije o redirekciji rute
4. Informacije o isteku TTL paketa

### **Provera dostupnosti hosta**

- Koriste se dva tipa ICMP poruka
  1. Echo request(type 8, code 0)
  2. Echo Reply(type 0, code 0)

- Kada host dobije Echo Request poruku dužan je da odgovori sa Echo Reply, ako odgovori dostupan je.



- U sadržaju ovih tipova poruka šalju se identifikacija i redni brojevi poruka radi uparivanja odgovarajućih zahteva i odgovora

**Ping** – aplikacija koja koristi Echo request i echo reply za proveru dostupnosti konkretnog hosta

- Šalje određen broj zahteva i očekuje odgovore
- Na osnovu toga ispisuje informacije koliko odgovora je stiglo i koje vreme je proteklo između zahteva i odgovora
- Takođe vrlo jednostavan način da se host natera da radi nešto i da mu se troše mrežni resursi
- **Korišćen za razne vrste napada na mreže i viruse**
- Vrlo često ova vrsta saobraćaja zabranjena na hostovima (kroz firewall)

## **41. ICMP destination unreachable**

- Tip poruka koji se koristi za slanje informacije o nedostupnosti odgovarajuće destinacije

- Type 3
- Postoje različiti podtipovi u odnosu na destinaciju
- Generišu se od strane nekog rutera ili hosta na putanji paketa
- Generišu se kao odgovor na paket koji ruter ne može da isporuči na destinaciju

- Šalju se na polaznu adresu u zaglavlju IP paketa

- U **sadržaju poruke** se šalje **zaglavlje i 64 bita IP paketa** koji je izazvao generisanje ICMP poruke da bi host **identifikao koji paket nije isporučen**.

Korisne za utvrđivanje problema na mreži

- **Postoje različiti podtipovi poruka**
- Svaki podtip ima **istu oznaku za Type - 3, a različitu oznaku za Code**

1. **Network Unreachable - Type 3, Code 0** -Generiše se kada ruter za odgovarajući **paket nema rutu** ka **odredišnoj mreži** ili ima rutu ali je link neaktivan
2. **Host Unreachable - Type 3, Code 1** - Ganeriše se kada **paket stigne do rutera** kome je **odredišna mreža direktno konektovana**, a **host** kome treba proslediti paket nije aktivan - Ruter ne dobija odgovor na ARP Request
3. **Fragmentation required - Type 3, Code 4** - Kada paket stigne do linka gde je MTU manji od veličine paketa potrebno je izvršiti fragmentaciju .Ako je u zaglavlju paketa DF flag postavljen na 1 ruter će izbaciti paket iz saobraćaja i na polaznu adresu iz paketa poslati ICMP poruku type 3, code 4

## **42. ICMP time exceeded i Traceroute**

- Tip poruke koji se koristi za slanje informacije da je istekao TTL paketa u transportu
- Type 11, Code 0
- **TTL - Time To Live** - maksimalan broj rutera kroz koje paket može proći
- Svakim prolaskom se smanjuje za 1

- Kada padne na **0 paket se izbacuje iz saobraćaja** i na polaznu adresu iz paketa se šalje ICMP poruka type 11, code 0.

### ***Traceroute***

- Aplikacija koja koristi Echo Request, Echo Reply i Time Exceeded
- Koristi se za utvrđivanje putanje paketa od jednog hosta do drugog
- **Generiše listu hopova** kroz koje je paket prošao.
- Putanja se utvrđuje slanjem sekvence **Echo Request poruka**

- **Prva poruka** se pakuje u paket koji ima **TTL 1**
- Kada paket stigne do prvog rutera, ruter će TTL vrednost smanjiti na 0, izbaciti paket iz saobraćaja i vratiti Time Exceeded poruku
- Ruter koji je poslao Time Exceeded poruku je prvi hop na putanji
- Sledeća poruka se pakuje u paket koji ima TTL 2
- Drugi ruter na putanji će da izbaci taj paket iz saobraćaja i pošalje Time Exceeded poruku
- Na osnovu primljene Time Exceeded poruke se zna ko je drugi hop na putanji
- Postupak se ponavlja sa povećavanjem TTL vrednosti dok se ne dobije Echo Reply poruka od odredišnog host

### **Treća Grupa**

#### **43. Zadaci transportnog nivoa**

- Obezbeđuje sve potrebne funkcije za komunikaciju između aplikacija na tim hostovima.
- Na jednom hostu može biti više aplikacija koje koriste mrežu (web browser, email klijent)
- Svaka od aplikacija komunicira sa nekom drugom aplikacijom na mreži koje mogu da se nalaze na različitim hostovima.

#### **Osnovne funkcije:**

1. Segmentacija podataka koje aplikacije razmenjuju
2. Identifikacija aplikacija – portovi
3. Garancija isporuke

#### **44. Protokoli transportnog nivoa**

- Aplikacije imaju različite zahteve npr neke zahtevaju da svi segmenti budu dostavljeni na odredište da bi se procesirali podaci.
- Neke zahtevaju brzu dostavu podataka i onda trpe gubitke delova podataka – video streaming
- Neke šalju malu količinu podataka pa nema potrebe za segmentacijom npr dns
- Neke šalju malu količinu i zahtevaju brzu dostavu fps.

Zbog različitih potreba postoje i različiti protokoli na transportnom nivou

Najčešće korišćeni TCP IP protokoli:

**TCP protokol**

**UDP protokol**

#### **45. TCP protokol (uopšteno)**

Transmission Control Protokol

- Služi za prenos podataka proizvoljne dužine – **vrši segmentaciju**
- Kreira i održava **sesiju (konekciju)** između dve aplikacije čime je i omogućena garancija isporuke
- **Aplikacije se označavaju portovima** - TCP port 80 ≠ UDP port 80
- Enkapsulira se u IP paket sa oznakom protokola 6

- **Mehanizam protokola:** kreiranje konekcije, prenos podataka, zatvaranje konekcije

Opciono-----

#### ***Prenos podataka***

- Segmenti na odredište stižu proizvoljnim redosledom jer se enkapsuliraju na ip pakete
- Segmenti su obeleženi kako bi se znao redosled prilikom rekonstrukcije

- **Sequence number** – oznaka segmenta upisana je u TCP zagavlju

### **-Oznaka segmenta:**

1. Početnu vrednost za oznaku segmenata koja se dogovara kad se kreira konekcija
2. Polaznom nizu podataka bajtovi se označe **sekvencijalno**
3. Oznaka se dobije kada se **oznaka prvog bajta** u jednom segmentu **sabere sa početnom vrednosti** za oznaku **segmenata**

- U okviru jedne sesije obe strane koriste različite oznake segmenata – različite početne vrednosti koje se dogovaraju prilikom kreiranja konekcije.

- Takođe različite sesije koriste različite oznake segmenata.

- **Razlog korišćenja različitih oznaka segmenata** je da bi detektovali **duplikati** ili **segmenti iz različitih sesija**.

## **46. Portovi**

### **2. Port**

-Svaki host na mreži ima jedinstvenu IP adresu preko koje se identifikuje

-Na jednom hostu može da bude više aplikacija i svaka mora da ima jedinstvenu indentifikaciju da bi komunicirala sa drugim aplikacijama na mreži

-**Port** – broj koji se dodeljuje aplikaciji na osnovu kog se ona jedinstveno identifikuje u **okviru jednog hosta**  
Port je broj od 16bita

- Mogu se dodeljivati **statički i dinamički**.

- Klijentske aplikacije koje **iniciraju** komunikaciju **dobijaju dinamički** bilo koji slobodan port.

- Da bi ona inicirala komunikaciju **mora znati port** druge aplikacije.

- **Serverske aplikacije** koriste definisane-poznate portove koji se **dodele statički**

IANA definiše koji port koristi koja aplikacija

- **0 - 1023 - Well Known Ports** - rezervisani za **serverske aplikacije**

- **1024 - 49151 - Registered Ports**

- **49152 - 65535 - Dynamic or Private Ports**

### **Primeri:**

80 – HTTP web server

443 HTTPS server

8080 HTTP test server

21 FTP

22 SSH

25 SMTP

110 POP

- Aplikacija jedinstveno određena **IP adresom i brojem porta**

- **Socket – kombinacija IP adresa i port**

192.168.1.20:80 apk na adresi toj na portu 80

## **47. Segmentacija**

### **Segmentacija:**

- Aplikacije razmenjuju nizove podataka proizvoljne dužine
- TCP/IP mreže **su paketske mreže**- podaci se razmenjuju u paketima ograničene dužine
- **Proces segmentacije** – niz podataka koje aplikacija šalje treba da se podeli u manje delove koji mogu da se upakuju u pakete.

- Kada segmenti stignu na odredište trebaju da se rekonstruišu u originalni niz podataka i potrebno je znati redosled segmenata tako što su oni označeni brojevima i ta informacija je upisana u **zaglavlje** protokola transportnog nivoa.

**Segment** – PDU transportnog nivoa.

Sadrži:

1. Zaglavlje – kontrolni podaci relevantni za transportni nivo
2. Podaci(data, payload) – segment podataka dobijenih od aplikacije.

**MSS – Maximum Segment Size** – maksimalna veličina segmenta na transportnom nivou i **zavisi** od maksimalne veličine paketa na trećem nivou koji može da se upakuje u frejm na drugom nivou **MTU**.

MSS = MTU – veličina zaglavlja paketa

Ako je IP protokol MSS = MTU-20

## **48. Garancija isporuke**

### **Garancija isporuke**

- Pouzdanost komunikacije, garancija isporuke - zadatak transportnog nivoa
- Kreira se i održava konekcija između dve aplikacije.
- Za svaki segment se šalje potvrda da je stigao – ako nije stigla potvrda segment se šalje ponovo.

Garancija isporuke – kada se pošalje segment očekuje se potvrda da je stigao

- Koristi se **mehanizam kliznog prozora** koji podrazumeva da se definiše broj segmenata – veličina prozora koje jedan host može da pošalje pre nego što mu stigne potvrda.

Potvrda – **acknowledgement** – predstavlja segment koji u zaglavlju ima ACK flag **postavljen na 1** i u potvrdi se šalje sequence number segmenta koji se potvrđuje tj šalje se sequence number segmenta koji se očekuje i upisuje se u polje acknowledgment nuber

- Ako bi se za svaki segment slala potvrda bilo bi neefikasno

- Potvrda se šalje za poslednji segment u nizu koji je stigao i potvrda potvrđuje da su stigli i taj segment kao i svi pre njega.

-Ako je host poslao definisan broj segmenata, a u međuvremenu nije dobio potvrdu ni za jedan segment, staje sa slanjem dok ne dodje potvrda

- **Veličina prozora** se dogovara prilikom **kreiranja konekcije** i ta **vrednost može da se menja** tokom sesije
- Ako dolazi do gubitka segmenata veličina prozora se smanjuje u toku sesije da bi se smanjila potreba za ponovnim slanjem

**Kontrola toka podataka** se postiže veličinom prozora

## 49. Kreiranje i zatvaranje konekcije

- Aplikacije koje komuniciraju preko TCP protokola kreiraju i održavaju TCP sesiju
- Klijent je apk koja inicira komunikaciju a server je apk koja odgovara na zahteve drugih aplikacija

**Three way handshake** – postupak kreiranja konekcije i razmenjuju se tri TCP segmenta

Pre i u toku sesije aplikacije se nalaze u nekom od stanja:

1. Pre otvara konekcije **klijent** je u stanju **-Closed**
2. Pre otvaranja konekcije **server** je u stanju – **Listen**
3. Uspostavljanje veze: **SYN\_SENT, SYN\_RCVD**
4. Kada se uspostavi veza nalaze se u stanju **ESTABLISHED**

Three way handshake

1. **Klijent šalje** segment sa **SYN flagom** i predlogom za početnu oznaku segmenta koju će koristiti i prelazi u stanje **SYN\_SENT**

2. **Server prima** SYN segment, **šalje** segment sa **SYN i ACK flagovima** čime potvrđuje oznaku segmenta za klijenta i šalje predlog za svoju početnu vrednost za oznaku segmenta, prelazi u stanje **SYN\_RCVD**.

3. **Klijent prima** segment sa SYN i ACKflagovima i **šalje** segment sa **ACK flagom** i potvrđuje oznaku segmenta za server i prelazi u stanje **ESTABLISHED**

4. **Server prima** ACK segment i prelazi u stanje **ESTABLISHED**

**Priliko kreiranja konekcije dogovaraju se:**

1. **Početne vrednosti** oznake segmenata obe strane
2. **Veličina prozora** – obe strane šalju predlog i uzima se manja vrednost
3. **Veličina segmenta** – MSS obe strane šalju predlog uzima se manja vrednost

## **Zatvaranje konekcije**

- Konekcija se zatvara od strane **oba hosta** u sesiji

- Kada host završi sa slanjem podataka i želi da zatvori sesiju šalje segment sa flagom FIN na koji mu drugi host šalje potvrdu sa flagom ACK

- Takođe, drugi host kada završi sa slanjem šalje segment sa flag-om FIN na koji prvi šalje potvrdu sa flag-om ACK.

## 50. TCP segment

Sadrži nekoliko 32-bitnih reči

**-Prva 32.bitna reč:**

1. Source Port – port aplikacije koja šalje segment 16. bita
2. Destination port – port aplikacije kojoj se šalje segment 16-bit

**Druga 32-bitna reč**

1. Sequence number – oznaka segmenta 32 bita

**Treća 32-bitna reč**

1. Acknowledgment number - Oznaka segmenta koji se sledeći očekuje – potvrda prethodnih segmenata – 32

**Četvrta 32-bitna reč**

1. HLEN – dužina zaglavlja TCP segmenta u 32bitnim rečima – 4b
2. Reserved 4 bita
3. Flags -8 bita 8 flagova – SYN otvaranje konekcije, FIN zatvaranje , ACK potvrda segmenta
4. Window size – veličina k prozora

## 51. UDP protokol

- User Datagram Protokol jednostavan i brz
- Koristi se za prenos kratkih poruka i aplikacijama kojima je bitnija brzina prenosa podataka od garancije isporuke DNS, DHCP, SNMP
- **Enkapsulira** u IP protokol 17
- **Ne radi segmentaciju** pa je zato za kratke podatke čija je dužina manja od MSS
- Koristi portove za označavanje aplikacija – **UDP portovi**

- PDU – UDP segment

### **Delovi UDP segmenta:**

1. **Source port** – port aplikacije koja šalje segment 16 bita
2. **Destination port** – port aplikacije kojoj se šalje segment 16 bita
3. **Length** – dužina segmenta u bajtovima – 16bitta
4. **Checksum** – kontrolna suma 16 bita
5. **Podaci** – 32 bita

## 52. DNS (uopšteno)

- IP adrese teške za pamćenje i lakše se pamti ime
- Ideja je dodeliti svakoj adresi ime
- IP adresa se može promeniti u slučaju da se promeni npr internet provajder, ime ne zavisi od adrese i ne mora se menjati, **menja se samo mapiranje** imena na odgovarajuću IP adresu.
- Korisnici hosta koriste i vide samo ime, ne moraju da znaju da je došlo do promene IP adrese.
- **DNS – Domain Name System** – distribuirani sistem za opish hijerarhijski organizovanih skupova i pridruživanje podataka tim imenima.
- **Najznačajniji deo** – mapiranje imena na **IP adrese** i obrnuto.
- Bitan za funkcionisanje interneta- kao telefonski imenik za internet.
- **DNS protokol** – protokol **Aplikativnog nivoa**.
- Koristi UDP protokol na transportnom nivou i DNS server koristi UDP port 53.
- Protokolom definisana **organizacija imena**, i **način funkcionisanja servisa** i **format poruka**
- Na početku DNS **bio centralizovan sistem**
- Sva mapiranja su se nalazila u fajlu **HOSTS.TXT i fajl** se razmenjivao između korisnika
- Širenjem Interneta postalo nepraktično
- Zamenjen distribuiranim sistemom
- Sva imena se ne nalaze više u jednom fajlu, nego su **različiti DNS serveri** zaduženi za **različite skupove imena**
- HOSTS.TXT postoji i danas u operativnom sistemu

## 53. DNS imena i organizacija

Imena organizovana hijerarhijski u skupove i podskupove

### **Skup imena = domen**

- Svaki skup ima svoju oznaku a pored nje nosi i oznake svih nadskupova kojim pripada i oznake su odvojene tačkom.
- **Hijerarhija imena** je stablo gde vrh nema oznaku – **root domen**
- Ispod roota nalaze se **top level domeni** com, org, edu rs
- Ispod njega su domeni drugogo pa trećeg ... svako ime je putanja kroz stablo

## FQDN - Fully Qualified Domain Name

- Puno ime hosta uključuje i root domen koji nema oznaku [www.example.org](http://www.example.org). Obično se koriste bez root domena tj bez poslednje tačke.

- Top level domeni

Table 4. DNS - Some Top-Level Internet Domains	
Domain Name	Meaning
com	Commercial organizations
edu	Educational institutions
gov	Government institutions
int	International organizations
mil	U.S. Military
net	Major network support centers
org	Non-profit organizations
country code	ISO standard 2-letter identifier for country-specific domains

## Organizacija

- Dns je distribuirani sistem i za imena su zaduženi autorizovani DNS serveri

- Serveri organizovani hijerarhijski u odnosu na domene
- Skup imena za koje je zadužen jedan DNS server naziva se **zona DNS servera**.
- **Jedna zona obuhvata** jedan ili više domena i njihove poddomene
- DNS server može da **delegira** odgovornost za deo zone drugom DNS serveru
- **Delegirana zona** je obično **jedan od poddomena** domena servera

**RR - Resource Record** - informacija (stavka) u okviru DNS servera

Postoji više tipova RR:

1. A - mapira ime na IP adresu
2. CNAME - dodeljuje alias imenu vezanom stavkom A za IP adresu
3. NS - autorizovani server za domen
4. MX - mail server za domen

U DNS sistemu je **dostupnost podataka bitnija od ažurnosti**

- Uvek postoje **primarni i sekundarni DNS server**
- Sekundarni je kopija primarnog koja se koristi u slučaju da je primarni nedostupan
- **Izmene** se vrše na **primarnom serveru**
- Sekundarni periodično preuzima podatke od primarnog
- Klijenski hostovi imaju klijentsku stranu DNS sistema koja komunicira sa DNS serverima - **DNS resolver**
- Aplikacije koriste DNS resolver servis kada im je potrebno da saznaju IP adresu koja je vezana za neko ime
- DNS resolver šalje upite ka DNS serveru i odgovore prosleđuje aplikacijama

## 54. DNS slanje upita

- Ime se razrešava sa desna na levo i upit se šalje prvo na vrh hijerarhije DNS servera.
- Na vrhu se nalaze Root Name serveri koji su zaduženi za top level domene

**IANA** – održava root name servere

- Ima ih 13 - {a-m}.root-servers.org
- DNS resolver zna adrese Root Name servera

- Ako ime za koje se šalje upit **pripada zoni servera** on vraća direktan odgovor
- **Ako ime ne pripada zoni servera** nego je delegirano nekom drugom serveru server može da se ponaša na dva načina:

1. **Server sam prosleđuje** dalje upit drugom serveru - rekurzivan način dobijanja odgovora
2. **Server vraća informaciju kom DNS serveru** se sledećem treba obratiti, odnosno kome je delegirano ime - iterativan način dobijanja odgovora

- **Rekurzivan način je loš za servere** jer se **upit uvek šalje Root Name serverima** koji su previše opterećeni da bi rekurzivno razrešavali imena

- **Iterativan način je loš za klijenta** jer su klijenti spori i imaju lošiju internet konekciju

- **Internet provajderi** obično obezbeđuju korisnicima **lokalni DNS server** koji ima **ulogu posrednika**

- Klijentski DNS resolver šalje upit lokalnom DNS serveru koji dalje iterativno šalje upite DNS serverima

- Kada razreši ime odgovor šalje klijentu

- Na **klijentskim sistemima** se **konfiguriše adresa lokalnog DNS servera** kome se prosleđuju upiti

**Konfiguracija lokalnog DNS servera (Windows)**

1. Ručno
2. Automatski (DHCP)

- Primarni i sekundarni DNS server

**Slanje upita:**

1. Klijent (njegov resolver) šalje upit Lokalnom Name serveru
2. Lokalni Name server šalje upit root-serveru
3. Root-server šalje odgovor Lokalnom Name serveru sa informacijom ko je odgovoran za zonu na nižem nivou hijerarhije
4. Lokalni Name server šalje upit sistemu koji je definisan odgovorom root-servera
5. Dobija informaciju ko je odgovoran za zonu na nižem nivou hijerarhije
6. Lokalni Name server šalje upit sistemu koji je odgovoran za zonu kojoj pripada ime za koje se šalje upit
7. Sistem odgovara sa IP adresom kojoj je dodeljeno ime iz upita
8. Lokalni Name server odgovor prosleđuje Klijentu

- DNS serveri obično imaju cache gde privremeno čuvaju razrešena mapiranja za slučaj da ubrzo stigne isti upit

- Korisno zbog imena popularnih servisa koje koristi veći broj korisnika



## **55. Zadaci fizičkog nivoa i vrste medijuma**

- Bavi se problemima vezanim za **prenos podataka kroz medijum**.
- Standardi koji definišu **karakteristike prenosnih medijuma** – vrsta kablova koji se koriste, konektori, utičnice ... vrste signala, vrednost napona..
- Kao i standardi koji opisuju **fizičku arhitekturu mreže i način postavljanja prenosnih medijuma** u poslovne sisteme.
- Fizički nivo obuhvata i **encoding** podataka dobijenih od prenosnog nivoa u signale, kao i obrnut proces decoding na prijemu.
- **Kontroliše slanje signala kroz medijum.**

### ***Medijumi:***

- Žični – uvrnute parice, koaksijalni kabl, optičko vlakno
- Bežični – etar, atmosfera

## **56. Uvrnute parice**

- Najviše se koriste

### ***Loše karakteristike:***

1. Osetljive na elektromagnetno zračenje, podložne šumovima i slabljenju signala
2. Zbog slabljenja signala **ograničena dužina kabla**

### ***Dobre karakteristike:***

1. jeftine
2. lake za rad

- **Parice** – sastoji se od dve izolirane bakarne žice, spiralno uvrnute
- Jedna parica = jedan komunikacioni link
- **Prenosi električne signale**
- Kablovi sse sastoje od više parica, različite vrste kablova imaju različiti broj parica
- Postoje različite kategorije u odnosu na kvalitet izrade - CAT 1-7 - Danas se najčešće koriste CAT5e sa protokom do 1Gbs i CAT6 i CAT7 sa protokom do 10Gbs-
- **Koriste se** u telefonskim sistemima – linija od korisnika do centrale
- Zbog postojeće infrastrukture počele da se koriste u računarskim mrežama
- Koriste se za **kabliranje unutar LAN mreža** kao takve onda imaju **zvezda topologiju**
- U **centru zvezde** se nalazi **mrežni uređaj** koji predstavlja centralni čvor zvezde
- **Kraci zvezde** su krajnji **korisnički uređaji**

### ***Vrste kablova sa uvrnutim paricama***

#### **1. UTP - Unshielded Twisted Pair (neoklopljene parice)**

- Imaju 4 parica – 8 žica
- **Svaki par je različite boje**
  1. smeđa, plava, zelena, narandžasta
  2. u paru jedna žica obojena, druga na pruge
- Oko sve četiri parice se nalazi jedan plastični omotač
- **Osetljivi na elektromagnetno zračenje.**

## 2. STP

- pa da bi se zaštitili UTP kabl koriste se metalni omotači pa dobijamo **Shielded Twisted Pair**
  - Bolje performanse od UTP
  - Koriste se u blizini izvora **elektromagnetnog zračenja**
  - U zavisnosti gde je omotač metalni razlikujemo
- 2.1 STP – metalni omotač oko svakog para  
2.2 S/UTP metalni omotač oko sve četiri parice zajedno  
2.3 S/STP – i oko parica pojedinačno i oko svih zajedno

- Na kraju kabla se nalaze konektori
- **RJ45** – 8 pinova za 8 žica
- **RJ11** – 4 pina za 4 žice

Standardi za raspored žica

**568A** – zeleno-bela, zelena, narandžasto-bela, plava, plavobela, narandžasta, braon bela, braon

**568B** – narandžasto-bela narandžasta, zeleno bela, plava, plavobela, zelena, braonbela, braon

## 57. Koaksijalni kabl

- Bolji medijum od parice jer ima bolje karakteristike – otporan na em zračenje i manje slabljenje signala
  - Bakarni kao parica – bakarna žica u srediini, izolacija, bakarni omotač, izolacija
  - Prenos TV signala u kablovskim televizijskim mrežama
- 
- Danas kablovski operateri nude Internet kroz istu mrežu
  - Ranije se koristio za kabliranje u LAN mrežama
  - Parice jeftinije i lakše za rad pa ga potisnule
  - **Topologija magistrala sa BNC konektorima**

## 58. Optičko vlakno

- Prenosi optičke signale i koriste kao materijal plastike i stakla
  - Otporno na em zračenje, nema šuma, manje slabljenje i gubitak signala
  - Omogućava prenos na velike razdaljine i veliki propusni opseg
  - Koriste se kao backbone za LAN mreže
  - Veza u WAN mrežama
  - Imamo jezgro, omotač napravljeni od dve providne materije sa različitim indeksom prelamanja svetlosti potom imamo i zaštitini omotač
- 
- Princip rada na osnovu Snellovog zakona.
  - Indeksi prelamanja jezgra i omotača takvi da signal ostaje u jezgri, odbija se od omotača.

### **Dva tipa vlakana u odnosu na broj putanja signala kroz jezgro**

1. **Multimodno** - veći radius, više putanja
2. **Monomodno** - mali radius, jedna putanja – bolje performanse i koriste se za veće razdaljine

### **Dva izvora signala**

1. **Laser** - koristi se za monomodna vlakna jer imaju mali radijus pa im je potreban usmeren izvor signala
2. **LED diode** - koristi se za oba tipa

- Optički kabl je napravljen od više optičkih vlakana spojenih u jedan snop

- Sve se završava konektorom, nema utičnica
- Kablovi se spajaju adapterima za dva ženska kraja
- Postoji više vrsta konektora

#### **Način spajanja**

- Konektor fabrički spojen sa parčetom vlakna - **pig tail**
- Spaja se vlakno na vlakno - **splicing**
- Uređaj - Splicer

### **59. Bežični medijum**

- Etar – za slanje signala se koriste radio i mikrotalasne frekvencije
- **Osetljiv** na em zračenje
- Prenosu podataka mogu da smetaju bežični telefoni, mikrotalasne pećnice, fluorescentno svetlo i drugi izvori elektromagnetnog zračenja
- **Nije fizički ograničen** kao žični medijumi tako da svako može da ima pristup
- Veliki problem sigurnost podataka
- Dobar za amfiteatre, holove,...
- Nije dobar za poslovne sisteme

### **60. Strukturirano kabliranje i podsistemi**

- Način kabliranja koji podržava komunikacione sisteme
- Kabliranje se radi planski po standardima
- Standardima opisano kako postaviti kablovsku infrastrukturu u poslovni sistem tako da ona zadovoljava sve zahteve komunikacije.

#### **Cilj**

1. Fleksibilnost prilikom priključena krajnjih korisničkih uređaja
2. Prenos različitih tipova podataka (govor, podaci)
3. Garantovane karakteristike u propusnom opsegu

#### **Standardi definišu:**

1. Podsisteme kablovskog sistema
2. Topologije i razdaljine u sistemu
3. Načine povezivanja medijuma
4. Načine testiranja
5. Obeležavanje opreme
6. Sigurnosne mere (uzemljenje i protivpožarna zaštita)

Kablovski sistem treba da traje minimum 10 godina

Strukturirano kabliranje podrazumeva kabliranje kampusa

- **Kampus** - nekoliko objekata na nekom prostoru
- Jedan objekat može da se posmatra kao kampus - Spens, Filozofski fakultet
- **Preporučena topologija - zvezda** sa više hijerarhijskih nivoa

#### ***Podsistemi kablovskog sistema***

Kampus kabliranje

1. Ulazak u objekte 1
2. Prostorije za opremu 2
3. Vertikalno kabliranje 3
4. Telekomunikacioni ormari 4
5. Horizontalno kabliranje 5
6. Radni prostori 6

- **Kampus kabliranje** - povezivanje objekata u okviru kampusa (od čvorišta kampusa do čvorišta objekta)
- **Vertikalno kabliranje** - povezivanje spratova unutar objekta (od čvorišta objekta do čvorišta sprata)
- **Horizontalno kabliranje** - povezivanje radnih prostora (od čvorišta sprata od priključne kutije)
- Zvezda sa tri hijerarhijska nivoa
- **Čvorište** - **centralni čvor zvezde**

#### *Ulazak u objekte*

- Mesto na kome se **povezuje spoljašnje kabliranje sa unutrašnjim**
- Napolju kablovi u zemlji, unutra **kablovi u zidu, na zidu, na podu....**
- Različiti uslovi, mogu da se koriste se različiti kablovi
- **Media Converter** - uređaj za spajanje dve različite vrste kablova
- Standardi definišu kako se ulazi u objekat

### **61. Prostorije za opremu i telekomunikacioni ormari**

- U njima se nalaze **telekomunikacioni ormari** i ostala **telekomunikaciona oprema**
- Standardi definišu veličinu prostora, temperaturu, vlažnost vazduha, uzemljenje..
- **Veličina** se određuje u odnosu na **broj krajnjih korisničkih uređaja** ili u odnosu na površinu radnih oblasti
- 100 m2 radnih oblasti - 0.75 m2 prostorije za opremu

#### *Telekomunikacioni ormari*

- Nalaze se u prostorijama za opremu
- U njih se smešta aktivna i pasivna telekomunikaciona oprema i vrši se sva prespajanja
- Mogu biti zatvoreni sa sve četiri strane, da imaju samo tri strane ili samo šine
- Razmak između instalacionih perforiranih šina je 19 inča tako da se uređaji prave da budu širine 19 inča
- Visina se izražava u jedinicama **Rack unit – 1U =1.75 inča**

#### **Patch panel** - panel sa gusto napakovanim utičnicama

- Instalira se u telekomunikacioni ormar pa je širine 19"
- Sa zadnje strane kablovi, sa prednje utičnice
- Može da bude 12-portni, 24-portni, 48-portni,...
- Svi kablovi koji dolaze do ormara završavaju se sa zadnje strane patch panela
- **Svakoj utičnici u radnim prostorima** odgovara **jedna utičnica na patch panelu**
- Patch kablom se spaja utičnica na patch panelu sa portom odgovarajućeg mrežnog uređaja

### **62. Radni prostori**

- U radnim prostorima se nalaze krajnji korisnički uređaji - Računar, telefon, nadzorna kamera...
- Kancelarija, učionica, šalter sala...
- U radnim prostorima se od **mrežne opreme nalaze priključne kutije i korisnički kablovi**
- **Kabliranje** obuhvata **deo od priključne kutije do krajnjeg korisničkog uređaja**.
- Bitna je fizička lokacija radnog mesta da bi se odredila lokacija priključne kutije
- Po standardu kabl **dužine do 3 metra**
- Koriste se **UTP kablovi**
- Najveći broj **kvarova** na mreži uzrokovan je **kidanjem kablova** u radnim prostorima
- **Priključna kutija** treba da bude što bliže **korisničkom uređaju**

- **Radni prostori** su bitni za **određivanje dimenzije mreže**
- **Dimenzija mreže** = broj radnih mesta \* broj priključaka po radnom mestu
- Radno mesto se optimalno oprema sa 3 priključka, a minimalno sa 2 (računar, telefon, buduće upotrebe)
- **Broj radnih mesta se može odrediti na 3 načina:**
  1. Prebrojavanjem radnih mesta (ako poslovni sistem već postoji)
  2. Arhitektonski projekat (ako je arhitekta projektovao lokaciju radnih mesta)
  3. Izračunavanjem
- Najbolje koristiti **sve tri metode i uzeti najveću vrednost** (da ne bi došlo do potrebe za proširenjem mreže)

#### **Izračunavanje broja radnih mesta u prostoriji**

1. 10 - 12 m<sup>2</sup> prostora jedno radno mesto
  2. 5 - 6 m<sup>2</sup> prostora za svako naredno
- Namena prostora takođe određuje broj radnih mesta
  - U amfiteatre i holove nema smisla stavljati priključne kutije po zidu
  - **Direktorova kancelarija - jedno radno mesto**

### **63. Horizontalno kabliranje**

Kabliranje sprata zgrade

- Obuhvata **deo od priključnih kutija** u radnim prostorima **do telekomunikacionog ormara** u čvorištu sprata
- Spajaju se priključne kutije u radnim prostorima sa portovima na patch panelu čvorišta sprata
- **Topologija zvezda** - čvorište je centralni čvor zvezde
- 90% kablova od celog kablovskog sistema

#### **Koriste se UTP kablovi**

- Zbog karakteristika kabla **dužina kabla** ograničena na **100 metara**
  1. 90m od kutije do patch panela
  2. 7m u ormaru za patch kablove
  3. 3m za korisničke kablove

#### **Kablovi se postavljaju**

1. Na zid - kroz kanalnice
  2. U zid - kroz bužir creva
  3. Kroz spuštene plafon ili dupli pod
- Ne treba da idu paralelno sa kablovima za struju
  - Kreće se od tlocrta sprata
  - Izračuna se dimenzija mreže i odredi položaj priključnih kutija
  - Odredi se broj čvorišta i lokacije čvorišta na spratu
  - Razdaljina između čvorišta i priključne kutije ne sme biti veća od 90m
  - Ako ima većih razdaljina pravi se više čvorišta
  - Definišu se trase kablova od priključnih kutija do čvorišta

### **64. Vertikalno i kampus kabliranje**

- Kabliranje između spratova - između telekomunikacionih ormara na različitim spratovima
- Spajaju se **protovi na patch panelu čvorišta sprata** sa portovima na **patch panelu čvorišta objekta**
- **Topologija zvezda** - čvorište objekta centralni čvor zvezde

#### **Koriste se:**

1. Optički kablovi (preporučeno) - multimodna vlakna
2. UTP - za deonice kraće od 100m i manji propusni opseg

## Kablovi se postavljaju kao i kod horizontalnog kabliranja

1. Na zid - kroz kanalnice
2. U zid - kroz bužir creva
3. Kroz spuštene plafon ili dupli pod

Ne treba da idu paralelno sa kablovima za struju

## Kampus kabliranje

- Kabliranje između objekata u kampusu
- Spajaju se portovi na **patch panelu čvorišta kampusa** sa portovima **na patch panelu čvorišta objekta**
- **Topologija zvezda - čvorište kampusa** centralni čvor zvezde
- Veliki saobraćaj, velike razdaljine
- Koriste se **optički kablovi**
- Kablovi se provlače kroz vazduh ili kroz zemlju
- Nikad na zemlju!
  
- Vazdušno se koristi se samo tamo gde ne može podzemno ili ako već postoji infrastruktura za vazdušno
- Kabel izložen kiši, vetru, pticama...
- Podzemno je preporučeno standardom
- Kablovi idu kroz kablovsku kanalizaciju

## 65. Kodiranje

- Prevođenje podataka u signale i obrnuto
- **Obuhvata dva procesa:**
  1. Encoding - prevođenje niza bitova u predefinisani kod
  2. Signaling - promena fizičke veličine u vremenu
- Signal - promena fizičke veličine u vremenu

## Signaling

- **Signaling tehnika** definiše kako se bitovi predstavljaju signalima
- Postoje različite tehnike
- **Bit time** - trajanje jednog signala koji predstavlja jedan bit, koliko vremenski jedan signal koristi medijum
- Prijemna strana mora znati gde je početak i gde je kraj jednog signala

## Kako obezbediti sinhronizaciju

1. Pre slanja konkretnih signala poslati niz signala za sinhronizaciju (npr. niz 01010101)
2. Ugraditi takt u samu signaling tehniku

## Primeri nekih jednostavnih signaling tehnika(danas se u praksi koriste složenije)

### 1. NRZ - Nonreturn to zero

- Dva različita napona za 0 i 1
- Napon konstantan u intervalu signala
- **Problem sinhronizacije** u slučaju dugačkog niza **0 ili 1**

### 2. NRZI - Nonreturn to zero inverted

- 1 - kodira se promenom naponskog nivoa
- 0 - nema promene

**Problem sinhronizacije** u slučaju dugačkog niza **0**

### 3. Manchester

- 0 - promena sa višeg nivoa na niži
- 1 - promena sa nižeg nivoa na viši
- Promena na sredini intervala signala
- **Uključen i takt**
- Rešen problem sinhronizacije ali su signali veće frekvencije što zahteva veći propusni opseg

### **Encoding**

- **NRZ** - problem sinhronizacije za dugačak niz 0 ili 1
- **Manchester** - potrebna **2x veća frekvencija**
- Kako napraviti niz bitova tako da nema dugačak podniz 0 ili 1 (da bi mogao da se koristi NRZ)
- Encoding - prevođenje niza bitova u predefinisani kod
- Kodovi - grupe bitova koji ne sadrže sve 0 ili sve 1, prepoznatljivi na obe strane komunikacije
- Signali se **posmatraju u grupama** i traži se kom kodu odgovaraju, bolja detekcija grešaka
- **Rešen problem sinhronizacije**

### **4B/5B**

- 4 bita podataka se koduju 5-bitnim kodom
- 5-bitni kod se prenosi preko medijuma
- Kodovi takvi da ne sadrže sve 0 ili sve 1
- Prenosi se veća količina podataka ali je rešen problem sinhronizacije i lakša je detekcija grešaka
- 4B/5B je jednostavna tehnika, danas se koriste mnogo kompleksnije (8B/10B, 64B/66B...)