

## SWITCH

Predstavlja mrežni uređaj koji radi na podatkovnom sloju te omogućava povezivanje i komunikaciju različitih uređaja. On koristi MAC adrese da bi poslao pakete podataka na odgovarajući port. Switch upravlja protokom podataka u mreži tako što emituje primljene mrežne pakete samo onim uređajima kojima su paketi namjenjeni. Svaki uređaj koji je konektovan na port može vršiti transfer podataka na bilo koji drugi u bilo koje vrijeme bez ometanja ostalih prenosa.

Glavne funkcije switch-a su:

1. Preusmjeravanje paketa (switching):
  - Switch prima podatke u obliku paketa od jednog uređaja u mreži i preusmjerava ih ka odgovarajućem uređaju u istoj mreži koristeći MAC adresu odredišta.
2. Rad sa MAC adresama:
  - Switch koristi MAC adresu svakog uređaja da bi odredio gdje da pošalje podatke. On održava MAC tabelu (sadrži MAC adresu računara, interface switcha koji vodi do računara i vrijeme kada je stavka za računar upisana u tabelu) koja mapira MAC adrese na fizičke portove na switchu.
3. Unicast, Multicast i Broadcast:
  - Unicast: Ako switch pronađe odgovarajući uređaj sa ciljnom MAC adresom, on šalje podatke samo tom uređaju.
  - Multicast: Ako se podaci šalju više uređajima, switch, može prepoznati i usmjeriti ih ka više portova.
  - Broadcast: Ako ne može da pronađe destinaciju u svojoj tabeli, switch šalje podatke svim uređajima u mreži.
4. Segregacija mreže i smanjenje kolizija:
  - Switch dijeli mrežu na više podatkovnih domena, čime smanjuje kolizije jer omogućava komunikaciju između uređaja na različitim portovima bez uticaja na druge uređaje.

Princip rada:

- Prvi korak – Skladištenje MAC adresa:
  - Kada uređaj (npr. računar) pošalje paket podataka switch-u, switch analizira MAC adresu odredišta iz okvira. Ako ne zna MAC adresu, switch je postavi u svoju tabelu i šalje paket svim uređajima.
- Drugi korak – Preusmjeravanje paketa:
  - Ako switch već ima upisanu MAC adresu u svojoj tabeli, on zna na koji port treba da pošalje paket i direktno ga prosljeđuje tom uređaju.

- Treći korak – Ažuriranje tabele:
  - Switch redovno ažurira svoju tabelu sa MAC adresama kako bi bio siguran da podaci uvijek odlaze na pravi port

Razlika switch-a i hub-a:

Hub je osnovni uređaj koji šalje sve podatke svim uređajima u mreži, što može uzrokovati kolizije i smanjenje performansi. Switch šalje podatke samo na određite na osnovu MAC adresa.

## VRSTE SWITCH-A

Mrežni switch-evi se koriste za povezivanje različitih uređaja u mreži, kao što su računari, serveri, štampači i drugi uređaji. Postoji nekoliko vrsta mrežnih switcheva, u zavisnosti od njihovih karakteristika i namjene. Glavne vrste su:

### 1. Unmanaged Switch (neupravljivi switch):

- Plug-and-play
- Nemaju mogućnost konfiguracije
- Manji broj portova za povezivanje
- Niska cijena

### 2. Managed Switch (upravljivi switch):

- Mogu se konfigurirati pomoću CLI (Command Line Interface) ili web interface
- Većinom nisu plug-and-play, zahtjevaju inicijalnu konfiguraciju
- Veći broj portova u odnosu na neupravljive switcheve
- Jako skupi

### 3. Smart Switch (pametni switch):

- Dozvoljavaju određen nivo konfiguracije
- Srednji broj portova
- Plug-and-play
- Cijenovno su pristupačniji od potpuno upravljivih switcheva

### 4. Modular Switch (modularni switch):

- Omogućavaju dodavanje modula za proširenje prema potrebama korisnika čime se omogućava fleksibilnost u slučaju promjene i proširenja mreže.
- Moduli za proširenje su specifični i ovise od svrhe korištenja (za firewall, bežično povezivanje, analizu mreže). Također mogu omogućavati dodatni interface (mrežni portovi npr.), napajanje ili ventilatore za hlađenje.
- Modularni switchevi su dosta skuplji zbog mogućnosti proširenja.

Četiri svojstva switcha na koje treba obratiti pažnju su:

1. Brzina switcha – switchevi su dostupni sa različitim brzinama (Mbps). Npr. 100 Mbps – Fast Ethernet, 1000 Mbps – Gigabit Ethernet, 10000 Mbps – Ten Gigabit.
2. Broj portova – može varirati od switcha do switcha ovisno od potreba korisnika. Variraju od 5, 8, 10, 16, 24, 48.
3. Power over Ethernet – PoE switchevi omogućavaju napajanje uređaja kao npr. IP telefon, nadzorna kamera ili wireless access point-a (ubiquiti) pomoću kabela koji se koristi za prenos podataka. Ovi uređaji su skuplji nego standardni switchevi.

## TELNET

Telnet je komunikacijski protokol, koji uspostavlja dvosmjerni 8-bitni komunikacijski kanal između dva računara. Osnovna uloga da omogući rad korisnika na udaljenim računarima. U svakodnevnoj upotrebi pojam telnet se povezuje sa istoimenim programom koji koristi Telnet protokol. Razvijen je u ranim 1970. i predstavlja jedan od najstarijih protkola aplikacijskog sloja.

Ovaj servis je izgrađen na klijent-server arhitekturi što znači da zahtjeva od korisnika posjedovanje klijentske aplikacije i da na računaru na koji korisnik želi da se poveže bude instalirana serverska komponenta servisa. Ovo podrazumijeva otvorene portove za povezivanje i aplikaciju spremnu za komunikaciju tim portovima.

Nakon uspostavljanja inicijalne veze Telnet protokola ovaj servis poprima karakteristike centralizirane arhitekture. To znači da svaka operacija od strane klijenta (npr. pritisak tastera na tastaturi) se istovremeno prosljeđuje serveru. Na taj način korisnik može obavljati operacije na udaljenom računaru na isti način kao da sjedi direktno ispred računara i koristi lokalnu tastaturu i monitor.

Glavni razlog zašto se danas Telnet rijetko koristi za udaljeni pristup računarima je sigurnost. Telnet protokol sve akcije korisnika uključujući i slanje korisničkog imena i lozinke i rezultate instrukcija šalje u izvornom obliku što ga čini nesigurnim za korištenje na mrežama čije je kanale moguće prislušivati. Dodatni razlog pada popularnosti ovog servisa je pojava grafičkog korisničkog interfejsa (GUI – Graphical User Interface) za koji ovaj protokol nije dizajniran.

Bez obzira na sve rjeđu upotrebu Telnet servisa za rad na udaljenim računarima većina modernih operativnih sistema danas se isporučuje sa uključenom klijentskom komponentom nekog od novijih protokola iste namjene.

Podrazumijevani port Telnet servisa je 23 a transportni protokol TCP.

Za nasljednike Telnet protokola mogu se smatrati SSH (engl. Secure Shell, obezbijuje sigurnost putem šifriranja podataka) na i Remote Desktop (omogućava grafički korisnički interfejs) na MS Windows platformi.

Telnet za povezivanje podrazumijeva sljedeće komande:

```
telnet 192.168.1.100 (port, standardni ako ne napišemo je 23), npr. 192.168.1.100 80
```

```
login: your_username (nakon naredbe za povezivanje, server pita za prijavu)
```

```
Password: your_password
```

## SSH

SSH (Secure Shell ili Secure Socket Shell) je mrežni protokol koji daje korisnicima siguran način pristupa računaru putem mreže. Kao što se upotreba pojma Telnet često odnosi na program koji implementira isti protokol, tako se i SSH odnosi na skup uslužnih programa koji implemeniraju SSH protokol. Prva verzija ovog protokola nastala je 1995. godine, a u istoj su pronađeni sigurnosni nedostaci pa je 2006. godine izbačena druga verzija koja se i danas koristi.

Secure Shell pruža jaku autentifikaciju šifrom i javnim ključem, kao i komunikaciju sa šifriranim podacima između dva računala koja su povezana putem otvorene mreže, kao što je internet.

SSH koristi klijent-server model, povezujući klijentsku SSH aplikaciju na čijem kraju se prikazuje sesija sa serverom na čijem kraju je pokrenuta sesija. SSH implementacije uključuju podršku za aplikacijske protokole koji se koriste za emulaciju terminala ili prijenos datoteka.

Programi koji implementiraju SSH dizajnirani su da zamijene nesigurne programe kao što su Telnet, remote login (rlogin) i remote shell (rsh). SSH omogućava iste funkcije kao i navedeni programi, koje uključuju prijavu i pokretanje terminal sesije na udaljenom računaru, također omogućava mijenjanje programa za prenos podataka kao što je FTP. SSH radi na TCP transportnom protokolu i tipično na portu 22.

Primjer komande povezivanja na server je sljedeći:

```
ssh UserName@SSHserver.primjer.com
```

SSH dolazi uz svaki Unix, Linux i Mac server. Koristi se za udaljeni pristup resursima, udaljeno slanje naredbi na server, ažuriranje servera, upravljanje server hardware-om i upravljanje router-ima.

## VLAN

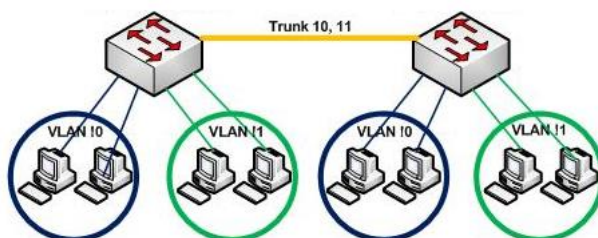
Virtualna lokalna mreža (engl. Virtual Local Area Network -VLAN) je način logičke segmentacije mreže koja se može dinamički mijenjati i nije ovisna o fizičkoj topologiji mreže. Ova vrsta mreže predstavlja skupinu računara koji mogu biti u jednoj ili više odvojenih mreža, a te mreže su konfigurirane na način da je računarima omogućena međusobna komunikacija kao da se nalaze na istoj fizičkoj mreži.

Kada se ne koriste VLAN-ovi i svi uređaji su spojeni na jedan switch, može doći do narušavanja performansi mreže za velik broj korisnika, a ukoliko su korisnici na fizički udaljenim lokacijama, nije ih moguće spojiti na istu LAN mrežu. VLAN rješava ovaj problem odvajanjem grupa korisnika na njihove virtualne mreže a ujedno omogućava pristup korisnika udaljene mreže nekoj virtualnoj mreži. Izolacija korisnika od ostatka mreže također poboljšava sigurnost mreže. Administracija mreže je također olakšana korištenjem VLAN-a.

Povezivanje računara obavlja se konfiguracijom switch-a. Kod statičkog VLAN-a potrebno je konfigurirati svaki port na switchu, odnosno odrediti kojem VLAN-u pripada.

Postoje dva tipa konfiguracije porta kod VLAN mreža a to su:

**Trunk veza** – označena veza kojom se spajaju switch-evi međusobno ili switch i router. Kroz trunk veze se propušta promet na način da se tačno zna koji promet je namijenjen kojem VLAN-u. Ovime npr. računari spojeni na VLAN 10 prvog switcha i računari spojeni na VLAN 10 drugog switcha mogu komunicirati međusobno kao da su u lokalnoj mreži. Na trunk vezi potrebno je naglasiti koji VLAN-ovi se propuštaju.



**Slika 1.** Trunk veza između dva switch-a

**Access veza** – neoznačena veza na kojoj promet ulazi ili izlazi bez oznake VLAN-a. To su portovi switch-a na koje se povezuju računari ili drugi uređaji. Ako se promet sa određenog access priključka šalje kroz trunk vezu tom prometu se dodaje oznaka definiranog VLAN-a.

Portovi switch-a koji se nalaze u različitim VLAN-ovima ne mogu komunicirati direktno, već im je za to potreban uređaj koji radi na mrežnom sloju (router). U zaglavlje mrežnog paketa kod trunk veze potrebno je naglasiti kojem VLAN-u pripada taj paket.

## Vrste VLAN-a

### Statički VLAN

Statički VLAN je onaj u kojem se VLAN dodjela ručno konfigurira na svakom portu switcha. To znači da je svaki port dodijeljen određenom VLAN-u, a uređaji povezani na te portove automatski postaju članovi tog VLAN-a. Članstvo u VLAN-u ostaje fiksno, osim ako mrežni administrator ručno ne promijeni konfiguraciju porta. Iako su statički VLAN-ovi relativno jednostavni za konfiguraciju i sigurni, mogu postati nezgodni u većim mrežama jer svaki put kada se uređaj premjesti na drugi port ili VLAN, switch mora biti ponovno konfiguriran. Statički VLAN-ovi su najbolji za manje ili stabilnije mreže u kojima se uređaji ne premještaju često ili ne mijenjaju lokacije.

### Dinamički VLAN

S druge strane, dinamički VLAN omogućuje automatsku dodjelu VLAN-a na temelju specifičnih kriterija, poput MAC adrese uređaja. Uređaji se automatski stavljaju u odgovarajući VLAN bez potrebe za ručnom intervencijom. Ovaj pristup posebno je koristan u velikim ili dinamičnim okruženjima gdje korisnici ili uređaji često ulaze, izlaze ili se premještaju u mreži. Iako dinamički VLAN-ovi nude veću fleksibilnost i skalabilnost, zahtijevaju dodatnu infrastrukturu i mogu biti manje sigurni ako se ne upravlja pravilno.

## ZADACI ZA KONFIGURACIJU SWITCHA

1. Podesiti hostname switcha na “etsbisw”.

```
enable  
config terminal  
hostname etsbisw  
exit  
exit
```

2. Podesiti šifru za pristup switchu na “sifra123”.

```
enable  
config terminal  
password sifra123
```

```
exit
```

```
exit
```

**3.** Podesiti hostname switcha na “etsbiswitch” i šifru za pristup na “abcdefgh”.

```
enable
```

```
config terminal
```

```
hostname etsbiswitch
```

```
password abcdefgh
```

```
exit
```

```
exit
```

**4.** Na upravljivom switchu prikazati tabelu svih VLAN mreža a zatim uključiti mrežu VLAN 10.

```
enable
```

```
config terminal
```

```
show vlan
```

```
vlan 10
```

```
exit
```

```
exit
```

**5.** Na upravljivom switchu uključiti mrežu VLAN 5 i dodati joj port fastEthernet5/1, koji će služiti za povezivanje korisničkih uređaja na switch (access mode).

```
enable
```

```
config terminal
```

```
vlan 5
```

```
interface fastEthernet5/1
```

```
switchport mode access
```

```
switchport access vlan 5
```

```
exit
```

```
exit
```

```
exit
```

**6.** Na upravljivom switchu uključiti mrežu VLAN 4 i dodati joj port fastEthernet0/1, koji će služiti za povezivanje korisničkih uređaja na switch. Zatim prikazati tabelu svih VLAN mreža.

```
enable
config terminal
vlan 4
interface fastEthernet0/1
switchport mode access
switchport access vlan 4
exit
exit
show vlan
exit
```

**7.** Na upravljivom switchu uključiti mrežu VLAN 6 i dodati joj portove fastEthernet0/1 i fastEthernet1/1 koji će služiti za povezivanje korisničkih uređaja na switch.

```
enable
config terminal
vlan 6
interface fastEthernet0/1
switchport mode acces
switchport access vlan 6
exit
interface fastEthernet1/1
switchport mode acces
switchport access vlan 6
exit
exit
exit
```

**8.** Na upravljivom switchu uključiti mreže VLAN 7 i VLAN 8, zatim na obje mreže dodati po jedan proizvoljno odabran port.

```
enable
config terminal
vlan 7
```

```
interface fastEthernet0/1
switchport mode access
switchport access vlan 7
exit

vlan 8

interface fastEthernet1/1
switchport mode access
switchport access vlan 8
exit

exit

exit
```