

Računalne mreže - Virtualna lokalna mreža (VLAN)

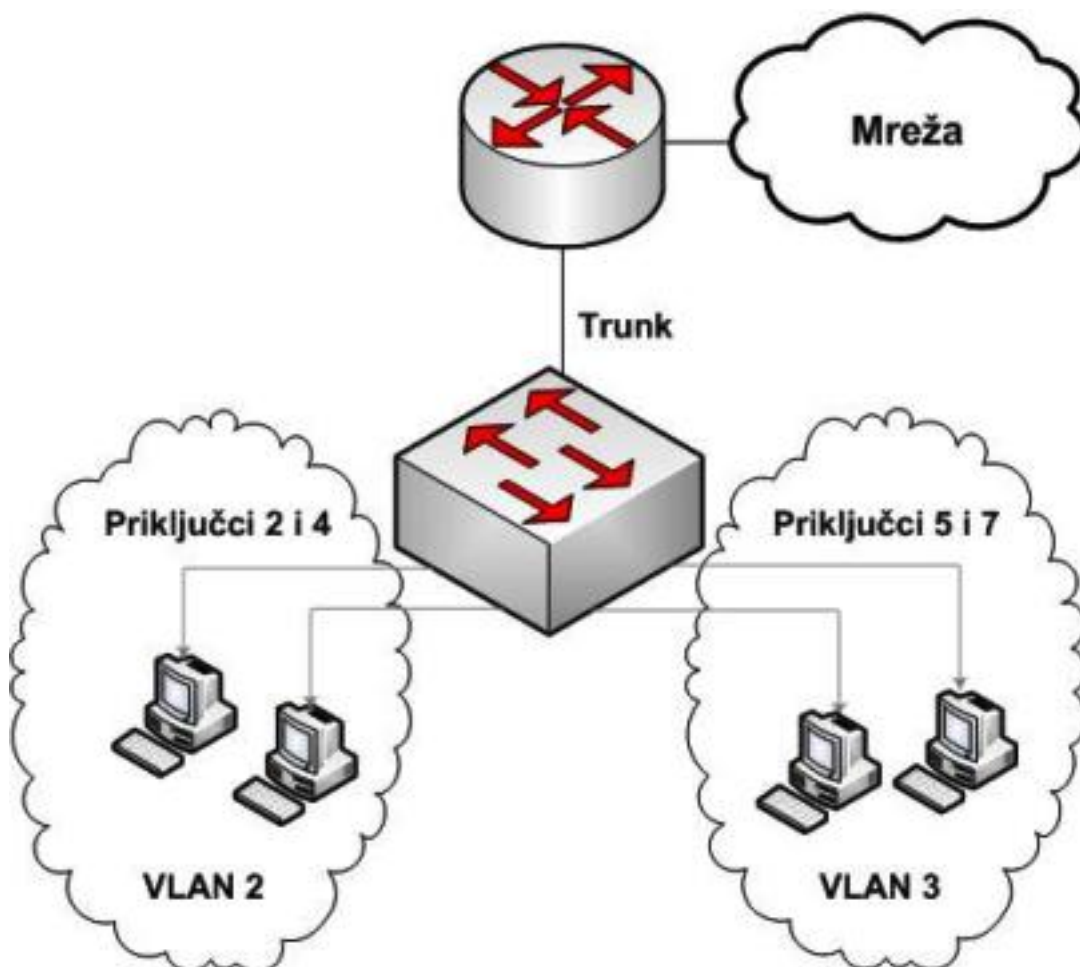
Virtualna lokalna mreža (engl. Virtual Local Area Network - VLAN) je način logičke segmentacije mreže koja se može dinamički mijenjati i nije ovisna o fizičkoj topologiji mreže. Tehnologija virtualnih lokalnih mreža je definirana standardom IEEE 802.1Q (poznat i kao dot1q).

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

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

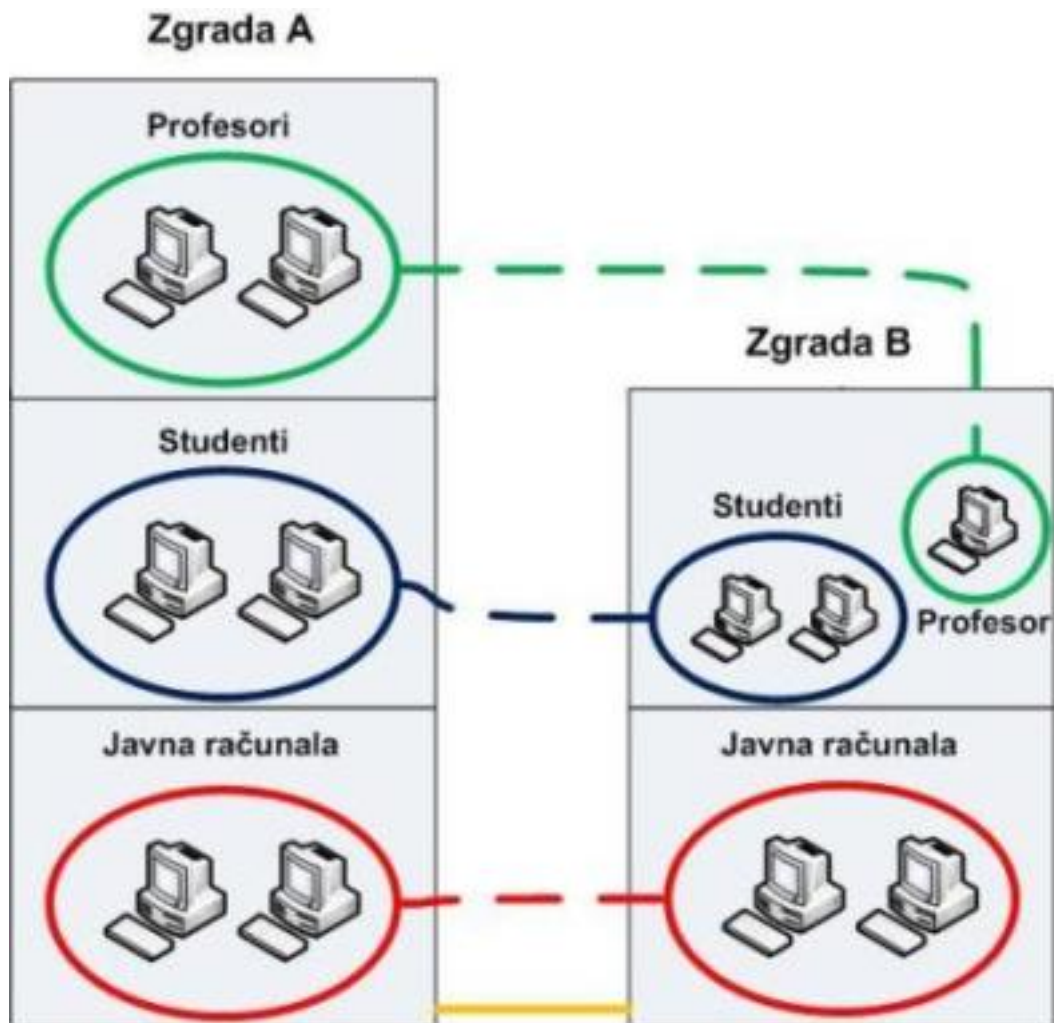
Zbog svega navedenog, poželjno je razdvojiti određenu vrstu korisnika i izolirati ju od ostalih, a za to se u današnjim računalnim mrežama koristi tehnologija virtualnih lokalnih mreža.

Koncept VLAN-ova prikazan je na slici:



Dobar primjer koji pokazuje opravdanost korištenja VLAN-ova je organizacija mreže fakulteta

(prikazana na slici dolje). Profesori iz zgrada A i B su stavljeni u isti VLAN i tako odvojeni od studentskih i javnih računala. Dakle, iako su javna, studentska i računala profesora spojena na isti prospojnik, njihov promet je odvojen i praktički je nemoguće nekome iz jednog VLAN-a vidjeti promet drugog VLAN-a (osim preko nekog uređaja mrežne razine što je objašnjeno kasnije u članku).

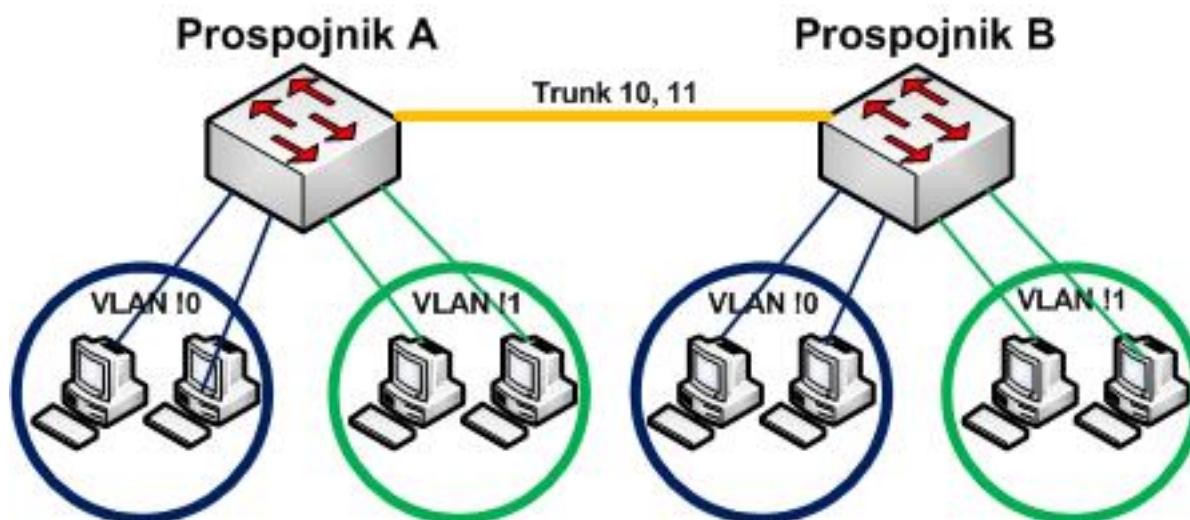


Povezivanje računala obavlja se konfiguracijom prospojnika. Priključci (engl. port) na prospojniku se u odgovarajući VLAN smještaju statički. Administrator mreže mora za svaki priključak odrediti pripadnost određenom VLAN-u.

Postoje dva tipa veza (priključaka):

- trunk veza
- access veza

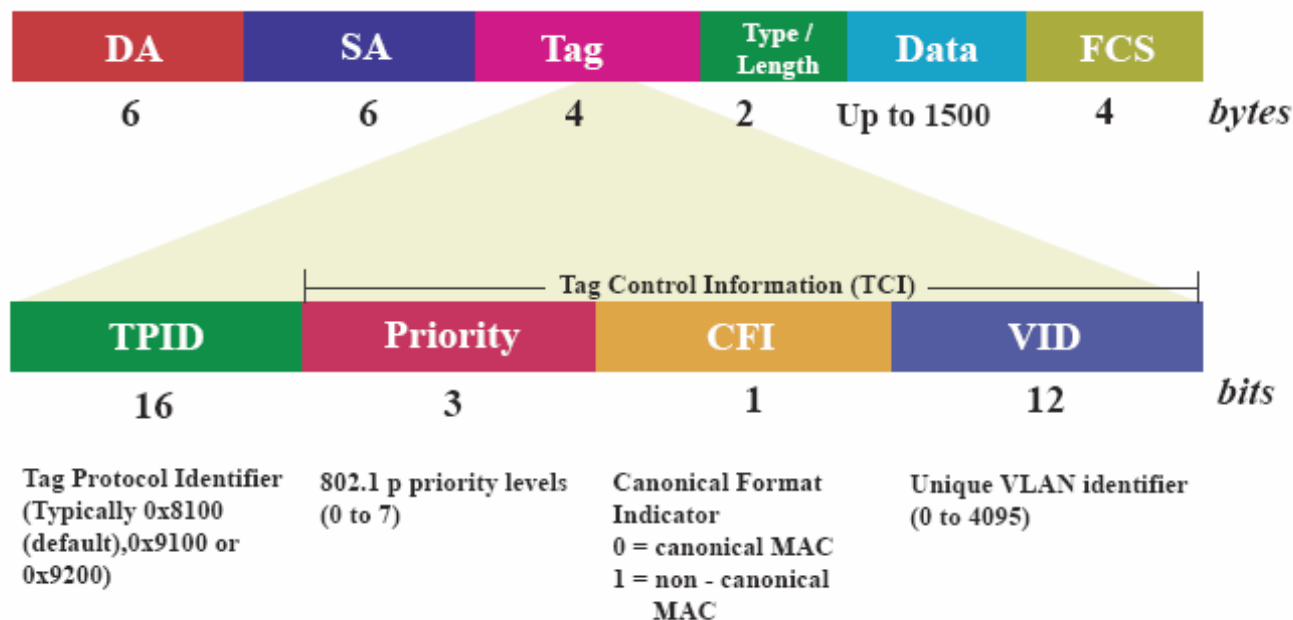
Trunk veza (engl. trunk link) je označena (engl. tagged) veza kojom se spajaju prospojnici međusobno ili prospojnik i usmjernik (engl. router). Kroz trunk veze se propušta promet na način da se točno zna koji promet je namijenjen kojem VLAN-u. Ovime npr. računala spojena na VLAN 10 prospojnika A i računala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



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

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

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



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

Postoje dvije vrste implementacije prospajanja na L3 razini:

- sklopovska

- programska

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

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

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

Konfiguracija VLAN-ova na Cisco prospoju

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

```
SW#vlan database
SW(vlan)#vlan 2
SW(vlan)#vlan 3
```

Priključci prospoju dodaju se u željeni VLAN ovim nizom naredbi:

```
SW#configure terminal
SW(config)#interface fa0/2
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 2
SW(config-if)#interface fa0/4
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 2
SW(config-if)#interface fa0/5
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 3
SW(config-if)#interface fa0/7
SW(config-if)#switchport mode access
SW(config-if)#switchport access vlan 3
```

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

Trunk priključak konfigurira se sljedećim nizom naredbi:

```
SW#configure terminal
SW(config)#interface Gi0/1
SW(config-if)#switchport mode trunk
```

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

- [Logirajte](#) [1] se za dodavanje komentara

sri, 2009-11-25 09:24 - Eldis Mujarić **Kategorije:** [Mreža](#) [2]

Vote: 2

Vaša ocjena: Nema Average: 2 (1 vote)

Source URL: <https://sysportal.carnet.hr/node/671>

Links

[1] <https://sysportal.carnet.hr/sysportallogin>

[2] <https://sysportal.carnet.hr/taxonomy/term/29>