

Lab 2: Osnovna konfiguracija VLAN mreža

Teorijska osnova vježbe

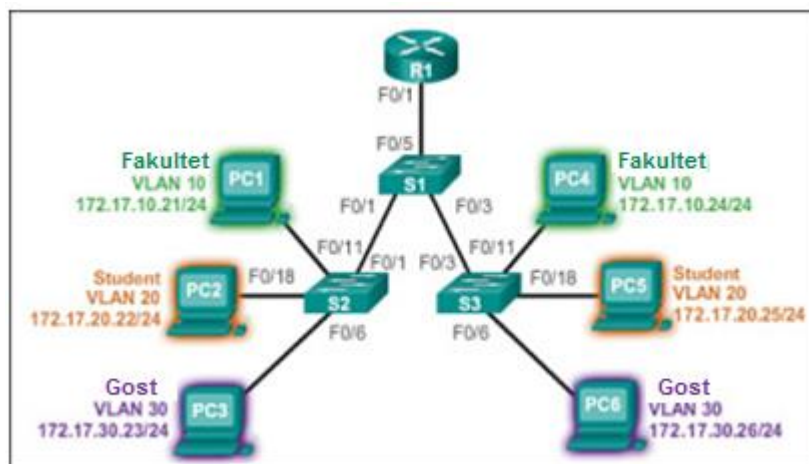
VLAN je skraćenica od engleskog termina “*Virtual Local Area Network*”, koji označava grupu računara koja se ponaša kao da su svi povezani na isti prenosni medijum, iako se fizički nalaze u različitim djelovima LAN mreže.

Dodavanje novih računara u mrežu, kao i uvođenje u rad klijent-server i multimedijalnih aplikacija povećava opterećenje mreže, što može dovesti i do ozbiljnih zastoja u radu. Suština rada *Ethernet*-a je u detekciji i izbjegavanju kolizija paketa, pri čemu sa povećanjem inteziteta mrežnog saobraćaja istovremeno raste i broj kolizija a opada efikasnost mreže. Strategija borbe sa ovim problemom je u smanjenju broja kolizija, ali i u eliminisanju dodatnog mrežnog saobraćaja, koji mahom čine tzv. *broadcast* i *multicast* paketi (*broadcast* paketi su adresirani na sve računare u jednom *Ethernet* segmentu, dok se *multicast* paketi šalju grupi računara). VLAN-ovi smanjuju broj kolizija i nivo *broadcast* i *multicast* saobraćaja virtuelnom podjelom mreže na manje djelove.

Prednosti VLAN mreža

Primarne prenosti korišćenja VLAN-a su:

- **Sigurnost:** Grupe koje imaju osjetljive podatke su izolovane od ostatka mreže, čime se smanjuje mogućnost pristupa povjerljivim informacijama. Na Slici 1. je ilustrovan primjer gdje su računari akademskog osoblja univerzitetske mreže pridruženi VLAN-u 10 i potpuno odvojeni i zaštićeni od saobraćaja koji generišu studenati i gosti fakulteta u VLAN-ovima 20 i 30.



Slika 1. Prikaz mreže podijeljene u VLAN-ove

- **Smanjenje troškova:** Smanjenje troškova je rezultat smanjene potrebe za skupim nadogradnjama mreže usled efikasnijeg korišćenja postojećih kapaciteta.
- **Bolje performanse:** Definisane većeg broja *broadcast* domena smanjuje broj kolizija u mreži i samim tim povećava njenu efikasnost. Podjela mreže u VLAN-ove smanjuje broj uređaja koji pripadju istom *broadcast* domenu. Tako na primjer u mreži sa Slike 1 postoji šest računara, ali su oni grupisani u tri *broadcast* domena: Fakultet, Student i Gost.
- **Povećanje efikasnosti IT osoblja:** VLAN olakšava upravljanje mrežom zato što korisnici sa istim zahtjevima prema mreži dijele iste resurse. To olakšava IT osoblju da identifikuje funkciju VLAN-a na osnovu odgovarajućeg imena. VLAN-ovi sa Slike 1 su zbog lakše identifikacije imenovani kao Fakultet (*VLAN 10*), Student (*VLAN 20*) i Gost (*VLAN 30*).
- **Jednostavnije upravljanje projektima i aplikacijama:** VLAN-ovi vrše agregaciju korisnika i mrežnih uređaja u cilju zadovoljavanja poslovnih i geografskih zahtjeva.

Tipovi VLAN-ova

Različiti tipovi VLAN-ova koji se koriste u modernim mrežama. Neki tipovi su definisani saobraćajnim klasama, dok su drugi definisani na osnovu specifičnih funkcija koje obavljaju.

Data VLAN

Ovaj tip VLAN-a je konfigurisan da prenosi saobraćaj generisan od strane korisnika. VLAN koji nosi govor ili kontrolni (*management*) saobraćaj ne može biti tipa *data*. Praksa je da se prenos govornog i kontrolnog saobraćaja vrši izolovano od saobraćaja podataka.

Default VLAN

Svi portovi *switch*-a postaju dio *default* VLAN-a nakon inicijalne konfiguracije. Portovi koji pripadaju ovom tipu VLAN-a su u istom *broadcast* domenu. Ovo dozvoljava bilo kojem uređaju konektovanom na nekom portu *switch*-a da komunicira sa ostalim uređajima na drugim portovima. *Default* VLAN za *Cisco switch*-eve je VLAN 1 i nije ga moguće izbrisati.

Native VLAN

Native VLAN je dodijeljen 802.1Q *trunk* portovima. *Trunk* port je krajnja tačka linka između *switch*-eva koji podržavaju prenos saobraćaja većeg broja VLAN-ova. 802.1Q *trunk* port prihvata saobraćaj koji dolazi iz različitih VLAN-ova (tagovani saobraćaj) kao i onaj koji nije generisan u okviru VLAN mreže (netagovani saobraćaj). Tagovani saobraćaj se klasifikuje po tagu (oznaci) od 4 bajta umetnutom u osnovno zaglavlje *Ethernet* frejma. Tag specificira VLAN kojem frejm pripada. Netagovani saobraćaj se smješta u *native* VLAN, koji je po *default*-u VLAN 1. *Native* VLAN je definisan od strane *IEEE* 802.1Q standarda i mora biti isti na oba kraja *trunk* linka.

Management VLAN

Management VLAN je bilo koji VLAN konfigurisan u svrhu mogućnosti upravljanja *switch*-em. VLAN 1 je *management VLAN* po *defaultu*. Prilikom kreiranja *management VLAN*-a na *switch*-u, virtuelnim interfejsima (SVI - Switch Virtual Interface) koji pripadaju tom VLAN-u se dodjeljuju IP adresa i *subnet* maska.

5.4 Tipovi linkova u konfiguraciji VLAN-a

Trunk je tačka-tačka link između dva mrežna uređaja na kojima je konfigurisano više od jednog VLAN-a. Preko *trunk*-a se prenosi cjelokupni VLAN saobraćaj. *Cisco* podržava IEEE 802.1Q za upravljanje *trunk*-ovima na *Fast Ethernet*, *Gigabit Ethernet* i *10-Gigabit Ethernet* interfejsima.

VLAN *trunk*-ovi značajno povećavaju efikasnost VLAN mreža. Oni omogućavaju da uređaji koji su u istom VLAN-u, a povezani na različitim *switch*-evima, mogu da međusobno komuniciraju bez intervencije rutera.

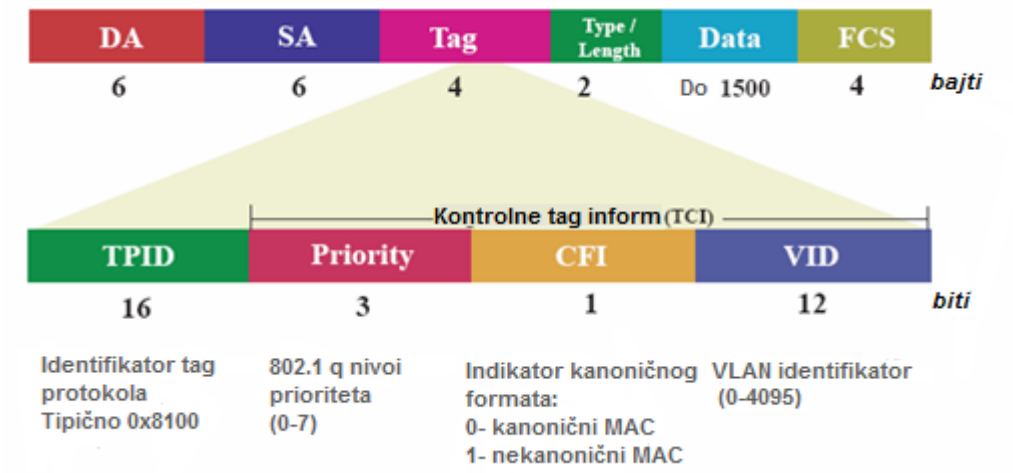
VLAN *trunk*-ovi ne pripadaju posebnom VLAN-u; to je kanal između *switch*-eva i rutera koji se koristi od strane više VLAN-ova. *Trunk* takođe može biti korišćen za komunikaciju između mrežnog uređaja i servera ili nekog drugog uređaja koji je opremljen sa odgovarajućom 802.1Q mrežnom karticom (NIC). Po *default-u* kod *Cisco Catalyst switch*-a su svi VLAN-ovi podržani na *trunk* portu.

Pristupni link (eng. *access link*) prihvata i prosleđuje neoznačene frejmove, tj. frejmove bez oznake VLAN-a. To su linkovi preko kojih se na *switch* povezuju računari ili drugi krajnji uređaji. Ako se frejm sa određenog pristupnog porta šalje na *trunk* link, dodaje mu se oznaka (eng. *tag*) odgovarajućeg VLAN-a. Sa druge strane, frejm koji dođe sa *trunk* linka predaje *access* portu odgovarajućeg VLAN-a netagovan.

Portovi koji se nalaze u različitim VLAN-ovima ne mogu međusobno komunicirati, već im je za to potreban uređaj koji radi na mrežnom (L3) nivou.

Za identifikovanje pripadnosti određenog paketa nekom VLAN-u koristi se 802.1Q zaglavlje koje sadrži informaciju o identifikatoru VLAN-a. Svi podaci koji se prenose *trunk* linkom imaju 802.1Q zaglavlje. Na osnovu 802.1Q zaglavlja podaci se kasnije prosleđuju odgovarajućem VLAN-u.

Format 802.1Q zaglavlja prikazan je na Slici 2.



Slika 2. Format 802.1Q zaglavlja

Praktični dio vježbe

Dijagram topologije:

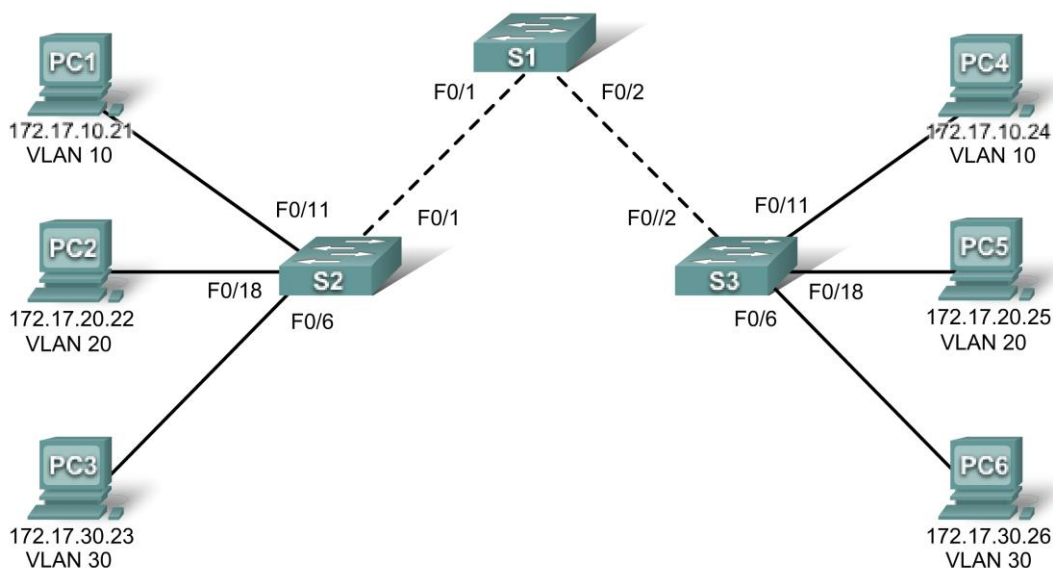


Tabela adresiranja:

Uređaj (Hostname)	Interfejs	IP adresa	Subnet maska	Default Gateway
S1	VLAN 99	172.17.99.11	255.255.255.0	N/A
S2	VLAN 99	172.17.99.12	255.255.255.0	N/A
S3	VLAN 99	172.17.99.13	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	172.17.30.23	255.255.255.0	172.17.30.1
PC4	NIC	172.17.10.24	255.255.255.0	172.17.10.1
PC5	NIC	172.17.20.25	255.255.255.0	172.17.20.1
PC6	NIC	172.17.30.26	255.255.255.0	172.17.30.1

Inicijalna konfiguracija portova (switch 2 i 3)

Portovi	VLAN	Mreža
Fa0/1 – 0/5	802.1q Trunks (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Guest (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Staff	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Students	172.17.20.0 /24

Ciljevi vježbe

- Osnovna konfiguracija *switch*-a
- Kreiranje VLAN-ova
- Dodjeljivanje portova VLAN-ovima
- Dodavanje i mijenjanje konfiguracije portova
- Provjera VLAN konfiguracije
- Omogućavanje *trunking* moda na *inter-switch* konekcijama
- Provjera *trunk* konfiguracije
- Čuvanje VLAN konfiguracije

Zadatak 1: Priprema mreže

Korak 1: Povezati mrežu u skladu sa dijagramom topologije.

Napomena: Poželjno je koristiti 2960 *switch*-eve. Ukoliko koristite 2900 ili 2950 *switch*-eve, rezultati komandi mogu biti drugačiji. Takođe, određene komande mogu biti nedostupne.

Korak 2: Izbrisati postojeće konfiguracije *switch*-eva i inicijalizovati sve portove u *shutdown* stanje.

Ući u globalni konfiguracioni mod iz privilegovanog EXEC moda. Deaktivirati sve portove na *switch*-evima. Dobra praksa je da svi nepovezani portovi budu deaktivirani.

```
Switch#erase startup-config
Switch#configure terminal
Switch(config)#interface range fa0/1-24
Switch(config-if-range)#shutdown
Switch(config-if-range)#interface range gi0/1-2
Switch(config-if-range)#shutdown
```

Zadatak 2: Osnovna konfiguracija *switch*-eva

Korak 1: Konfigurisati *switch*-eve u skladu sa sledećim upustvom:

- Dodijeliti hostname svakom *switch*-u.
- Isključiti DNS lookup.
- Konfigurisati *password etf* za EXEC mod.
- Konfigurisati *password cisco* za konekcije putem konzole.
- Konfigurisati *password cisco* za vty konekcije.

Korak 2: Aktivirati korisničke portove na S2 i S3.

```
S2(config)#interface range fa0/6, fa0/11, fa0/18
S2(config-if-range)#switchport mode access
S2(config-if-range)#no shutdown
```

```
S3(config)#interface range fa0/6, fa0/11, fa0/18
S3(config-if-range)#switchport mode access
S3(config-if-range)#no shutdown
```

Zadatak 3: Konfigurirati i aktivirati Ethernet interfejs

Korak 1: Konfigurirati IP adrese računara u mreži.

Zadatak 4: Konfigurirati VLAN-ove na *switch*-evima.

Korak 1: Kreirati VLAN-ove na *switch*-u S1.

```
S1(config)#vlan 10
S1(config-vlan)#name staff
S1(config-vlan)#vlan 20
S1(config-vlan)#name students
S1(config-vlan)#vlan 30
S1(config-vlan)#name guest
S1(config-vlan)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#end
S1#
```

Korak 2: Provjeriti da li su VLAN-ovi kreirani na *switch*-u S1.

Koristiti **show vlan brief** komandu za provjeru VLAN konfiguracije.

```
S1#show vlan brief
```

VLAN	Name	Status	Ports
1	default	active	Fa0/1, Fa0/2, Fa0/4, Fa0/5 Fa0/6, Fa0/7, Fa0/8, Fa0/9 Fa0/10, Fa0/11, Fa0/12, Fa0/13 Fa0/14, Fa0/15, Fa0/16, Fa0/17 Fa0/18, Fa0/19, Fa0/20, Fa0/21 Fa0/22, Fa0/23, Fa0/24, Gi0/1 Gi0/2
10	staff	active	
20	students	active	
30	guest	active	
99	management	active	

Korak 3: Konfigurirati VLAN-ove na *switch*-evima S2 i S3.

Kreirati i imenovati VLAN-ove 10, 20, 30 i 99 na S2 i S3 koristeći komande iz Koraka 1. Provjeriti ispravnost konfiguracije sa **show vlan brief** komandom.

Koji portovi su trenutno dodijeljeni VLAN-ovima koje ste kreirali?

Korak 4: Dodijeliti portove VLAN-ima na S2 i S3.

Portovi se dodijeljuju u interfejs konfiguracionom modu **switchport access vlan *vlan-id*** komandom. Portovi se mogu dodijeljivati pojedinačno ili grupno preko **interface range** komande. U nastavku su date komande za S3, ali potrebno je konfigurirati na sličan način i S2. Sačuvajte konfiguraciju kada završite.

```
S3(config)#interface range fa0/6-10
S3(config-if-range)#switchport access vlan 30
S3(config-if-range)#interface range fa0/11-17
S3(config-if-range)#switchport access vlan 10
S3(config-if-range)#interface range fa0/18-24
S3(config-if-range)#switchport access vlan 20
```

```
S3(config-if-range)#end
S3#copy running-config startup-config
Destination filename [startup-config]? [enter]
Building configuration...
[OK]
```

Korak 5: Provjeriti koji portovi su dodati kojim VLAN-ovima.

Koristiti **show vlan id** *vlan-id* komandu na S2 za provjeru portova dodijeljenih VLAN-u 10.

Koji portovi si dodijeljeni VLAN-u 10?

Napomena: Komanda **show vlan name** *ime-vlana* daje isti rezultat.

Informacije o VLAN-ovima koji su konfigurisani na portovima mogu se takođe dobiti preko **show interfaces** *interfejs switchport* komande.

Korak 6: Konfigurisati menadžment VLAN.

Menadžment VLAN je bilo koji VLAN koji se konfigurise da može da pristupa upravljačkim mogućnostima *switch*-a. VLAN 1 služi kao menadžment VLAN po *default*-u ukoliko se ne specificira drugi VLAN. **Menadžment VLAN-u je potrebno dodijeliti IP adresu i subnet masku.**

Inicijalna konfiguracija Cisco *switch*-eva definiše VLAN 1 kao *default* VLAN. Stoga VLAN 1 nije dobar izbor za menadžment VLAN. Ne želimo da svaki korisnik koji se na *switch* povezuje *default* VLAN-om ima pristup upravljačkim funkcijama. U prethodnom dijelu vježbe VLAN 99 je konfigurisan kao menadžment VLAN.

U interfejs konfiguracionom modu koristite komandu **ip address** za dodjelu menadžment adrese *switch*-evima.

```
S1(config)#interface vlan 99
S1(config-if)#ip address 172.17.99.11 255.255.255.0
S1(config-if)#no shutdown
S2(config)#interface vlan 99
S2(config-if)#ip address 172.17.99.12 255.255.255.0
S2(config-if)#no shutdown
S3(config)#interface vlan 99
S3(config-if)#ip address 172.17.99.13 255.255.255.0
S3(config-if)#no shutdown
```

Dodjela menadžment adresa omogućava IP komunikaciju između *switch*-eva i dozvoljava bilo kojem hostu koju je povezan na port dodijeljen VLAN-u 99 da se poveže na *switch*. S obzirom da je VLAN 99 definisan kao menadžment VLAN, bilo koji port koji se dodijeli ovom VLAN-u se smatra menadžment portom. Stoga, treba voditi računa o kontroli pristupa VLAN-u 99.

Korak 7: Konfigurisati *trunking* i *native* VLAN na svim *switch*-evima.

Trunk-ovi su konekcije između *switch*-eva koje dozvoljavaju *switch*-evima da prosleđuju saobraćaj iz svih VLAN-ova. Po *default*-u **trunk** port pripada svim VLAN-ovima, za razliku od pristupnog (**access**) porta, koji može da pripada samo jednom VLAN-u.

Native VLAN se dodjeljuje 802.1Q **trunk** portu. Na topologiji sa slike, **native** VLAN je VLAN 99. **Trunk** port 802.1Q podržava saobraćaj iz više VLAN-ova (tagovani saobraćaj) kao i saobraćaj koji ne dolazi iz VLAN-a (netagovani saobraćaj). Netagovani saobraćaj se smješta u **native** VLAN. Na konkretnoj topologiji, netagovani saobraćaj se generiše od strane računara koji su povezani na **native** VLAN. Jedna od prednosti korišćenja **native** VLAN-a je kompatibilnost za tradicionalnim LAN mrežama u kojima se generiše netagovani saobraćaj. Dobra praksa je ne koristiti VLAN 1 kao **native** VLAN.

Koristiti **interface range** komandu u globalnom konfiguracionom modu za pojednostavljeno konfigurisanje trunk portova:


```

S1(config)#interface range fa0/1-5
S1(config-if-range)#switchport mode trunk
S1(config-if-range)#switchport trunk native vlan 99
S1(config-if-range)#no shutdown
S1(config-if-range)#end

S2(config)# interface range fa0/1-5
S2(config-if-range)#switchport mode trunk
S2(config-if-range)#switchport trunk native vlan 99
S2(config-if-range)#no shutdown
S2(config-if-range)#end

S3(config)# interface range fa0/1-5
S3(config-if-range)#switchport mode trunk
S3(config-if-range)#switchport trunk native vlan 99
S3(config-if-range)#no shutdown
S3(config-if-range)#end

```

Provjeriti da li su **trunk**-ovi ispravno konfigurirani sa **show interface trunk** komandom.

```
S1#show interface trunk
```

```

Port          Mode          Encapsulation  Status        Native vlan
Fa0/1         on            802.1q         trunking      99
Fa0/2         on            802.1q         trunking      99

Port          Vlans allowed on trunk
Fa0/1         1-4094
Fa0/2         1-4094

Port          Vlans allowed and active in management domain
Fa0/1         1,10,20,30,99
Fa0/2         1,10,20,30,99

Port          Vlans in spanning tree forwarding state and not pruned
Fa0/1         1,10,20,30,99
Fa0/2         1,10,20,30,99

```

Korak 8: Provjeriti da li *switch*-evi mogu da komuniciraju.

Sa S1 pingujte menadžment adresu *switch*-eva S2 i S3.

```
S1#ping 172.17.99.12
```

```
S1#ping 172.17.99.13
```

Korak 9: Pingujte različite hostove sa PC2.

Pingujte sa hosta PC2 host PC1 (172.17.10.21). Da li je ping bio uspješan?

Pingujte sa hosta PC2 IP adresu 172.17.99.12 VLAN-a 99. Da li je ping bio uspješan?

Hostovi u različitim pod mrežama i u različitim VLAN-ovima ne mogu da komuniciraju bez L3 uređaja koji će da rutira između pod mreža.

Pingujte sa hosta PC2 host PC5. Da li je ping bio uspješan?

S obzirom da je PC2 u istom VLAN-u i u istoj pod mreži kao PC5, ping je uspješan.

Korak 10: Premjestiti PC1 u isti VLAN kao PC2.

Port na koji je povezan PC2 (S2 Fa0/18) je dodijeljen VLAN-u 20, a port na koji je povezan PC1 (S2 Fa0/11) je dodijeljen VLAN-u 10. Dodijelite S2 Fa0/11 port VLAN-u 20. Nema potrebe za uklanjanjem porta iz konfiguracije jednog VLAN-a da bi se on premjestio u drugi VLAN. Čim se port dodijeli novom VLAN-u, briše se iz konfiguracije prethodnog VLAN-a.

```
S2#configure terminal
```

```
Enter configuration commands, one per line. End with CNTL/Z.
```

```
S2(config)#interface fastethernet 0/11
```

```
S2(config-if)#switchport access vlan 20
```

```
S2(config-if)#end
```

Pingujte sa hosta PC2 host PC1. Da li je ping bio uspješan?

Iako su portovi na koje su povezani PC1 i PC2 u istom VLAN-u, ping nije uspješan jer su PC1 i PC2 i dalje u različitim podmrežama pa ne mogu direktno da komuniciraju.

Korak 11: Promijeniti IP adresu i mrežu PC1.

Podesiti IP adresu PC1 na 172.17.20.22. Maska podmreže i *gateway* mogu ostati nepromijenjeni. Još jednom pingujte sa PC2 računar PC1.

Da li je ping bio uspješan? Zašto?