

Lab 3: Osnovna VTP konfiguracija

TEORIJSKA OSNOVA VJEŽBE

VTP protokol koristi se za konfigurisanje VLAN-ova na nivou mreže. Osnovna karakteristika i najznačajnija prednost ovog protokola je ta što drastično smanjuje administrativno održavanje virtuelnih mreža. Naime, kada se definiše novi VLAN na VTP serveru, informacije o tom VLAN-u se distribuira do svih *switch*-eva koji pripadaju istom VTP domenu, čime se isključuje potreba za pojedinačnim konfigurisanjem VLAN-ae na svakom *switch*-u.

VTP domen, koji se najčešće naziva VLAN menadžment domen, sastoji se od *switch*-eva koji su pod istim administrativnim okriljem i dijele isti naziv VTP domena. *Switch* može biti dio samo jednog VTP domena, a VLAN baze (dio flash memorije koji sadrži spisak svih VLAN-ova) učesnika domena su međusobno sinhronizovane.

Switch-evi unutar VTP domena mogu da rade u jednom od četiri radna moda:

- **VTP server:** Može da kreira, briše, mijenja VLAN-ove i specificira odgovarajuće parametre kao što su VTP verzija, VTP *pruning* i ime VTP domena. VTP server dijeli svoju VLAN bazu ostalim uređajima unutar VTP domena.
- **VTP klijent:** Prenosi VTP ažuriranja preko svojih *trunk*-ova, ali ne može kreirati, brisati i mijenjati VLAN-ove.
- **VTP transparent:** Uređaji koji rade u ovom modu ne dijele svoju VLAN bazu niti je kreiraju na osnovu poruka koje prime od serverskih uređaja na svojim *trunk* portovima. Oni samo prosleđuju VTP ažuriranja koje prime od drugih.
- **VTP off:** Mod koji je sličan VTP *transparent* modu, ali ne podržava prosleđivanje VTP ažuriranja.

PRAKTIČNI DIO VJEŽBE

Dijagram topologije

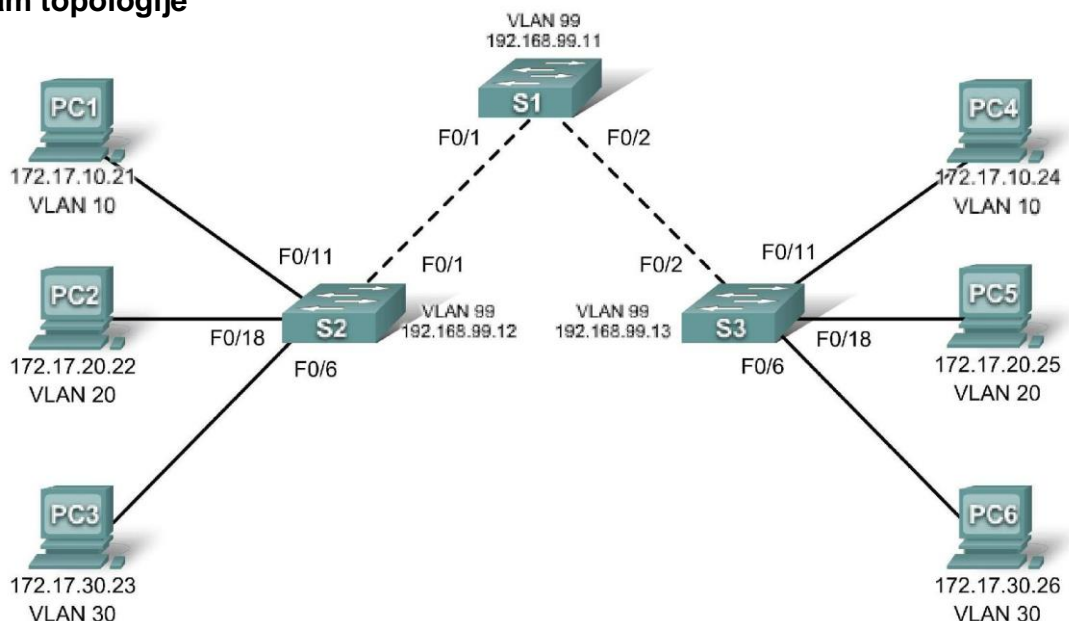


Tabela adresiranja

Uređaj (Hostname)	Interfejs	IP Adresa	Maska podmreže	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

Dodjela portova (Switch 2 i 3)

Ports	Assignment	Network
Fa0/1 – 0/5	802.1q Trunk (Native VLAN 99)	172.17.99.0 /24
Fa0/6 – 0/10	VLAN 30 – Gost (Default)	172.17.30.0 /24
Fa0/11 – 0/17	VLAN 10 – Fakultet/Osoblje	172.17.10.0 /24
Fa0/18 – 0/24	VLAN 20 – Studenti	172.17.20.0 /24

Ciljevi vježbe:

Tokom vježbe savladate:

- Kreiranje mrežne topologije u Packet Tracer-u.
- Brisanje startup konfiguracije i učitavanje default stanja
- Konfigurisanje VLAN Trunking Protokola (VTP) na *switch*-evima
- Aktiviranje trunking moda na inter-switch konekcijama
- Provjeravanje trunk konfiguracije
- Modifikovanje VTP moda
- Kreiranje VLAN-ova na VTP serveru.
- Razlike u radu VTP transparentnog, server i klijent moda.
- Dodjeljivanje portova VLAN-ovima.
- Čuvanje VLAN konfiguracije.
- Aktiviranje VTP pruning opcije.

Zadatak 1: Priprema mreže

Korak 1: Povezati mrežu u skladu sa dijagramom topologije.

Poželjno je koristiti 2960 switch-eve. Sa drugim modelima switch-eva rezultati mogu biti drugačiji. Na starijim verzijama switch-eva neke od komandi nisu dostupne.

Primijetićete da je u Tabeli adresiranja specificiran gateway za PC uređaje. To se odnosi na IP adresu lokalnog rutera koji nije razmatran u ovoj laboratorijskoj vježbi. Ruter je neophodan da bi uređaji iz različitih VLAN-ova mogli da komuniciraju.

Korak 2: Izbrisati postojeće konfiguracije na switch-evima.

Koristite **show vlan** komandu da bi potvrdili da postoji samo *default* VLAN i da su svi portovi dodijeljeni VLAN-u 1.

```
S1#show vlan
```

VLAN Name	Status	Ports
1 default	active	Fa0/1, Fa0/2, Fa0/3, 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 Gig1/1, Gig1/2
1002 fddi-default	active	
1003 token-ring-default	active	
1004 fddinet-default	active	
1005 trnet-default	active	

Korak 3: Deaktivirajte sve portove shutdown komandom.

```
S1(config)#interface range fa0/1-24  
S1(config-if-range)#shutdown  
S1(config-if-range)#interface range gi0/1-2  
S1(config-if-range)#shutdown
```

```
S2(config)#interface range fa0/1-24  
S2(config-if-range)#shutdown  
S2(config-if-range)#interface range gi0/1-2  
S2(config-if-range)#shutdown
```

```
S3(config)#interface range fa0/1-24  
S3(config-if-range)#shutdown  
S3(config-if-range)#interface range gi0/1-2  
S3(config-if-range)#shutdown
```

Korak 4: Aktivirajte korisničke portove na S2 i S3.

Konfigurirajte *access* mod na korisničkim portovima. Na osnovu dijagrama topologije utvrdite koji su portovi povezani na korisničke uređaje.

```
S2(config)#interface fa0/6  
S2(config-if)#switchport mode access  
S2(config-if)#no shutdown  
S2(config-if)#interface fa0/11  
S2(config-if)#switchport mode access  
S2(config-if)#no shutdown  
S2(config-if)#interface fa0/18  
S2(config-if)#switchport mode access  
S2(config-if)#no shutdown  
S3(config)#interface fa0/6  
S3(config-if)#switchport mode access  
S3(config-if)#no shutdown  
S3(config-if)#interface fa0/11  
S3(config-if)#switchport mode access  
S3(config-if)#no shutdown  
S3(config-if)#interface fa0/18  
S3(config-if)#switchport mode access  
S3(config-if)#no shutdown
```

Zadatak 2: Osnovna konfiguracija *switch*-eva.

Konfigurirajte S1, S2, i S3 *switch*-eve u skladu sa sledećim upustvom i sačuvajte konfiguraciju:

- Dodijelite *hostname* u skladu sa dijagramom topologije
- Deaktivirajte *DNS lookup*
- Konfigurirajte *EXEC mod password: class*
- Konfigurirajte *password* za konzolne konekcije: **cisco**
- Konfigurirajte *password* za vty konekcije: **cisco**

(Procedura za S1 je prikazana ispod)

```
Switch>enable
Switch#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#hostname S1
S1(config)#enable secret class
S1(config)#no ip domain-lookup
S1(config)#line console 0
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#line vty 0 15
S1(config-line)#password cisco
S1(config-line)#login
S1(config-line)#end
%SYS-5-CONFIG_I: Configured from console by console
S1#copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
```

Zadatak 3: Konfigurirajte Ethernet interfejsa na PC uređajima

Konfigurirajte IP adrese i *default gateway* za PC1, PC2, PC3, PC4, PC5, i PC6 u skladu sa tabelom koja je data na početku vježbe.

Provjeriti da li radi ping između PC1 i PC4, PC2 i PC5, i PC3 i PC6.

Zadatak 4: Konfigurirati VTP na *switch*-evima

VTP dozvoljava mrežnom administratoru da kontroliše instance VLAN-ova u mreži kreiranjem tzv. VTP domena. U svakom domenu jedan ili više *switch*-eva su konfigurirani kao VTP serveri. VLAN-ovi se zatim kreiraju na VTP serveru, a server distribuira informacije o VLAN-ovima ostalim *switch*-evima unutar domena. Uobičajena VTP konfiguracija podrazumijeva podešavanje radnog moda, domena i *password*-a. U ovoj laboratorijskoj vježbi koristimo S1 kao VTP server a S2 i S3 konfigurisaćemo da rade u VTP klijent modu ili VTP transparentnom modu.

Korak 1: Provjeriti trenutna VTP podešavanja na sva tri *switch*-a.

```
S1#show vtp status
```

```
VTP Version : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode : Server

VTP Domain Name :
VTP Pruning Mode : Disabled
VTP V2 Mode : Disabled
VTP Traps Generation : Disabled
MD5 digest : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)
```

S2#**show vtp status**

```
VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name      :
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
```

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
Local updater ID is 0.0.0.0 (no valid interface found)

S3#**show vtp status**

```
VTP Version           : 2
Configuration Revision : 0
Maximum VLANs supported locally : 255
Number of existing VLANs : 5
VTP Operating Mode    : Server
VTP Domain Name      :
VTP Pruning Mode     : Disabled
VTP V2 Mode          : Disabled
VTP Traps Generation : Disabled
MD5 digest           : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
```

Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00

Primjetimo da svi *switch*-evi rade u server modu. Serverski mod je default VTP mod za većinu Cisco Catalyst *switch*-eva.

Korak 2: Konfigurirati radni mod, ime domena i VTP *password* na *switch*-evima.

Podesiti ime VTP domena na **Lab3** i VTP *password* na **cisco** na sva tri *switch*-a. Konfigurirajte S1 da radi VTP server modu, S2 u klijent modu, a S3 u transparentnom modu.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#vtp domain Lab3
Changing VTP domain name from NULL to Lab3
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#end
```

```
S2(config)#vtp mode client
Setting device to VTP CLIENT mode
S2(config)#vtp domain Lab3
Changing VTP domain name from NULL to Lab3
S2(config)#vtp password cisco
Setting device VLAN database password to cisco
S2(config)#end
```

```
S3(config)#vtp mode transparent
Setting device to VTP TRANSPARENT mode.
S3(config)#vtp domain Lab3
Changing VTP domain name from NULL to Lab3
S3(config)#vtp password cisco
Setting device VLAN database password to cisco
S3(config)#end
```

Napomena: *Switch* koji radi u klijentskom modu može da nauči ime VTP domena od serverskog *switch*-a, ali samo ako je domen klijentskog *switch*-a **null** (prazno) stanje. Klijentski *switch* neće naučiti ime domena ukoliko je neko drugo ime prethodno konfigurirano. Iz tog razloga, dobra praksa je da se ime VTP domena manuelno konfigurira na svim *switch*-evima. *Switch*-evi u različitim VTP domenima ne razmjenjuju VLAN informacije.

Korak 3: Konfigurirajte *trunking* i *native VLAN* za *trunking* portove *switch*-eva.

Koristite **interface range** komandu u globalnom konfiguracionom modu da bi pojednostavili postupak konfiguracije.

```
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
```

Korak 4: Konfigurirajte *security* (politiku zaštite) na S2 i S3 *switch*-evima.

Konfigurirajte portove fa0/6, fa0/11, i fa0/18 tako da dozvoljavaju pristup sam jednom hostu i da uče MAC adresu hosta dinamički.

```
S2(config)#interface fa0/6
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/11
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#interface fa0/18
S2(config-if)#switchport port-security
S2(config-if)#switchport port-security maximum 1
S2(config-if)#switchport port-security mac-address sticky
S2(config-if)#end
```

```
S3(config)#interface fa0/6
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/11
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#interface fa0/18
S3(config-if)#switchport port-security
S3(config-if)#switchport port-security maximum 1
S3(config-if)#switchport port-security mac-address sticky
S3(config-if)#end
```

Korak 5: Konfigurirajte VLAN-ove na VTP serveru.

Potrebno je konfigurirati četiri VLAN-a:

- VLAN 99 (management)
- VLAN 10 (fakultet/osoblje)
- VLAN 20 (studenti)
- VLAN 30 (gosti)

Konfigurisanje ovih VLAN-ova na VTP serveru.

```
S1(config)#vlan 99
S1(config-vlan)#name management
S1(config-vlan)#exit
S1(config)#vlan 10
S1(config-vlan)#name fakultet/osoblje
S1(config-vlan)#exit
S1(config)#vlan 20
S1(config-vlan)#name studenti
S1(config-vlan)#exit
S1(config)#vlan 30
S1(config-vlan)#name gosti
S1(config-vlan)#exit
```

Provjeriti da li su VLAN-ovi kreirani **show vlan brief** komandom na S1.

Korak 6: Provjeriti da li su informacije o VLAN-ovima kreiranim na S1 distribuirane do S2 i S3.

Koristite **show vlan brief** komandu na S2 i S3 za provjeru VLAN konfiguracije.

S2#**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/
10	fakultet/osoblje	active	
20	studenti	active	
30	gosti	active	
99	management	active	

S3#**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
1002	fddi-default	act/unsup	
1003	token-ring-default	act/unsup	
1004	fddinet-default	act/unsup	
1005	trnet-default	act/unsup	

Zašto S2 i S3 imaju različite VLAN konfiguracije?

Korak 7: Kreirajte novi VLAN na *switch*-evima S2 i S3.

```
S2(config)#vlan 88
%VTP VLAN configuration not allowed when device is in CLIENT mode.

S3(config)#vlan 88
S3(config-vlan)#name test
S3(config-vlan)#
```

Zašto je moguće kreirati novi VLAN na S2 ali ne i na S3?

Izbrisati VLAN 88 sa *switch*-a S3.

```
S3(config)#no vlan 88
```

Korak 8: Manuelno konfigurišite VLAN-ove na *switch*-u S3.

```
S3(config)#vlan 99
S3(config-vlan)#name management
S3(config-vlan)#exit
S3(config)#vlan 10
S3(config-vlan)#name fakultet/osoblje
S3(config-vlan)#exit
S3(config)#vlan 20
S3(config-vlan)#name studenti
S3(config-vlan)#exit
S3(config)#vlan 30
S3(config-vlan)#name gosti
S3(config-vlan)#exit
```

Korak 9: Konfigurišite management interfejsne na svakom *switch*-u.

```
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
```

Provjerite da li su *switch*-evi ispravno konfigurirani korišćenjem ping komade. Sa S1 pingujte *management* interfejsne S2 i S3. Sa S2 pingujte *management* interfejs *switch*-a S3.

Da li je ping bio uspješan? Ukoliko nije, napravili ste neku grešku u konfiguraciji.

Korak 10: Dodijeliti portove VLAN-ovima.

Portove dodijeliti u skladu sa tabelom datoj na početku vježbe. Dodjela portova se ne konfiguriše preko VTP-a. Stoga, mora se izvršiti manuelno na svakom *switch*-u ili dinamički uz pomoć VMPS severa. U nastavku su date komande samo za S3, ali potrebno je konfigurirati i *switch*-eve S2 i S1 na sličan način. 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]
S3#
```


Zadatak 5: Konfigurirati VTP Pruning na *switch*-evima.

VTP pruning omogućava VTP serveru da suzbije *broadcast* saobraćaj iz određenog VLAN-a prema *switch*-evima koji nemaju ni jedan port u tom VLAN-u. Po *default*-u, sav *broadcast* saobraćaj i nepoznati *unicast* saobraćaj se šalje preko čitavog VLAN-a. Svi *switch*-evi u mreži primaju sve *broadcast* pakete. Ovo se može spriječiti konfiguriranjem VTP *pruning* opcije. Na ovaj način se kapacitet mreže efikasnije koristi jer se *broadcast* paketi ne šalju *switch*-evima kojima ti paketi nisu potrebni. Na VTP serveru *pruning* se konfigurira **vtp pruning** komandom u globalnom konfiguracionom modu. Ova konfiguracija se zatim distribuira VTP klijentima. Kako S3 radi u VTP transparentnom modu, *pruning* opcija se mora manuelno konfigurirati na tom *switch*-u.

Provjeriti VTP *pruning* konfiguraciju na svakom *switch*-u **show vtp status** komandom. VTP *pruning* mod treba biti aktivan na svakom *switch*-u.

```
S1#show vtp status
VTP Version                : 2
Configuration Revision     : 17
Maximum VLANs supported locally : 255
Number of existing VLANs   : 9
VTP Operating Mode         : Server
VTP Domain Name            : Lab3
VTP Pruning Mode           : Enabled
<output omitted>
```