

VTP protokol

Sadržaj

- * Motivi za uvođenje VTP protokola i koncept sinhronizacije domena
 - * Princip rada VTP-a
 - * Konfiguracija VTP protokola
 - * Konfiguracija L3 sviča
-
- Literatura: *CCNA Exploration LAN Switching and Wireless*, kompletno poglavlje 4
 - Dokumentacija za L3 3560

Motivi za uvođenje VTP protokola i koncept sinhronizacije domena

Potreba za centralizovanim upravljanjem virtualnim mrežama

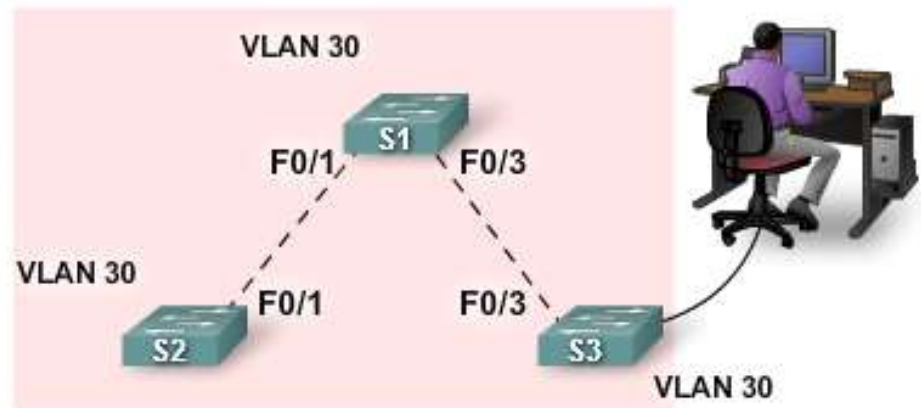
- * Da bi se dodao novi VLAN na grupi od nekoliko svičeva potrebno je kreirati VLAN na svakom sviču

Existing VLANs:

- VLAN 10 - faculty/staff
- VLAN 20 - students
- VLAN 99 - management VLAN

VLAN Management Task:

- Add VLAN 30 - guest



Potreba za centralizovanim upravljanjem virtualnim mrežama

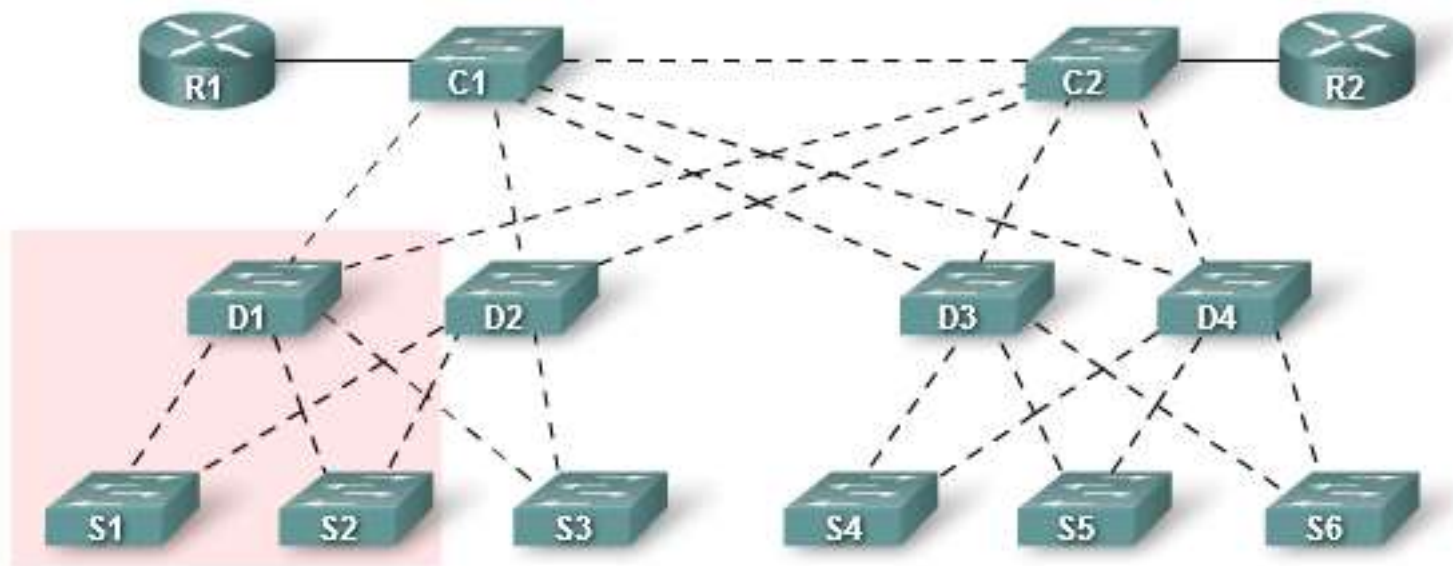
* Ukoliko je broj svičeva na mreži veliki, javlja se nekoliko problema:

- Vremenski je zahtevan prelazak sa sviča na svič radi dodavanja virtualne mreže
- Mogućnost greške
- Vremenski zahtevne izmene

Potreba za centralizovanim upravljanjem virtualnim mrežama

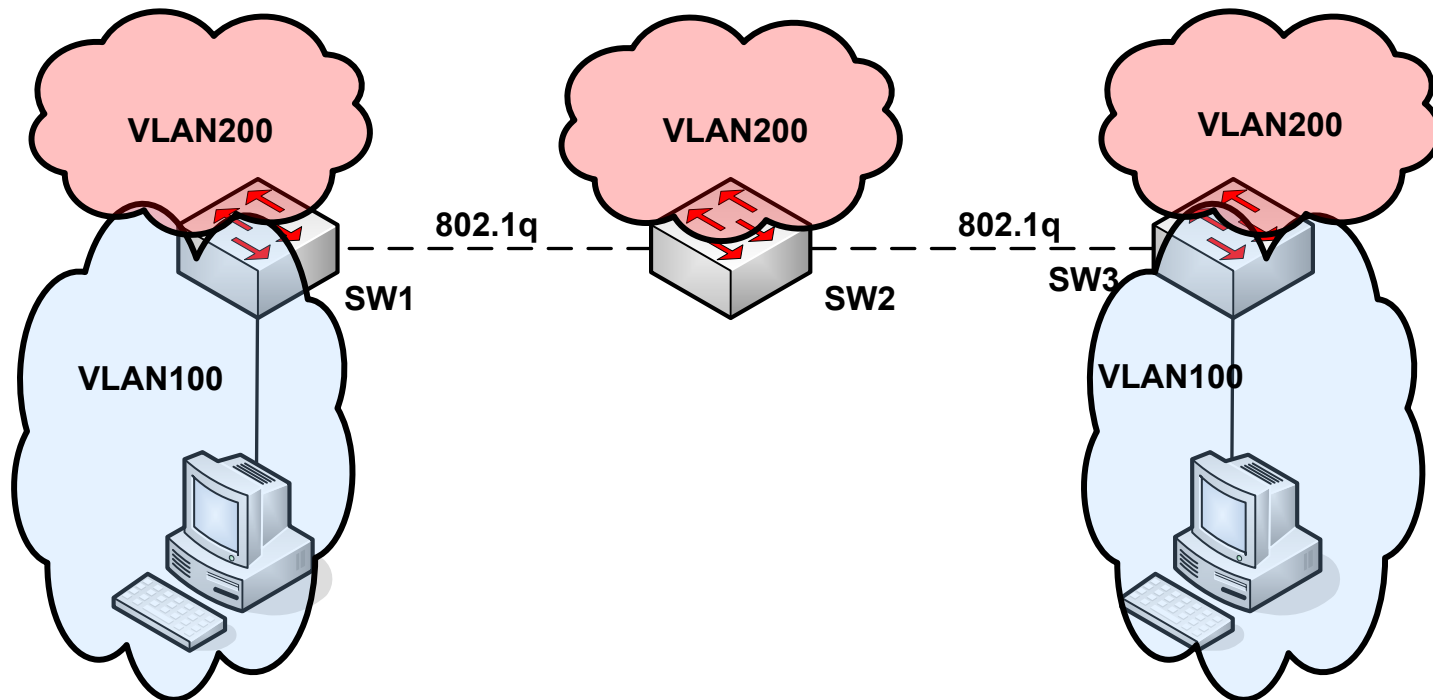
Existing VLANs: 10 ,20 99

VLAN Management Task: Add VLAN 30



Potreba za centralizovanim upravljanjem virtualnim mrežama

- * Ukoliko mreža ima 3 kaskadno vezana sviča kao na slici, i na primer je na svičevima 1 i 3 kreiran VLAN 100:
 - ukoliko svič 2 nema kreiran VLAN 100, propagacija ovog VLAN-a će biti zabranjena preko njegovih trankova, t.j. preciznije, neće biti uključen ovaj VLAN u trank.



Sinhronizacija baza sa VLAN-ovima

* Informacije o VLAN-ovima na Cisco svičevima

- nalaze se u fajlu vlan.dat i ne može se manipulirati njima direktno, već preko naredbi za rad sa vlanovima IOS-a

* Automatska sinhronizacija baza sa VLAN-ovima

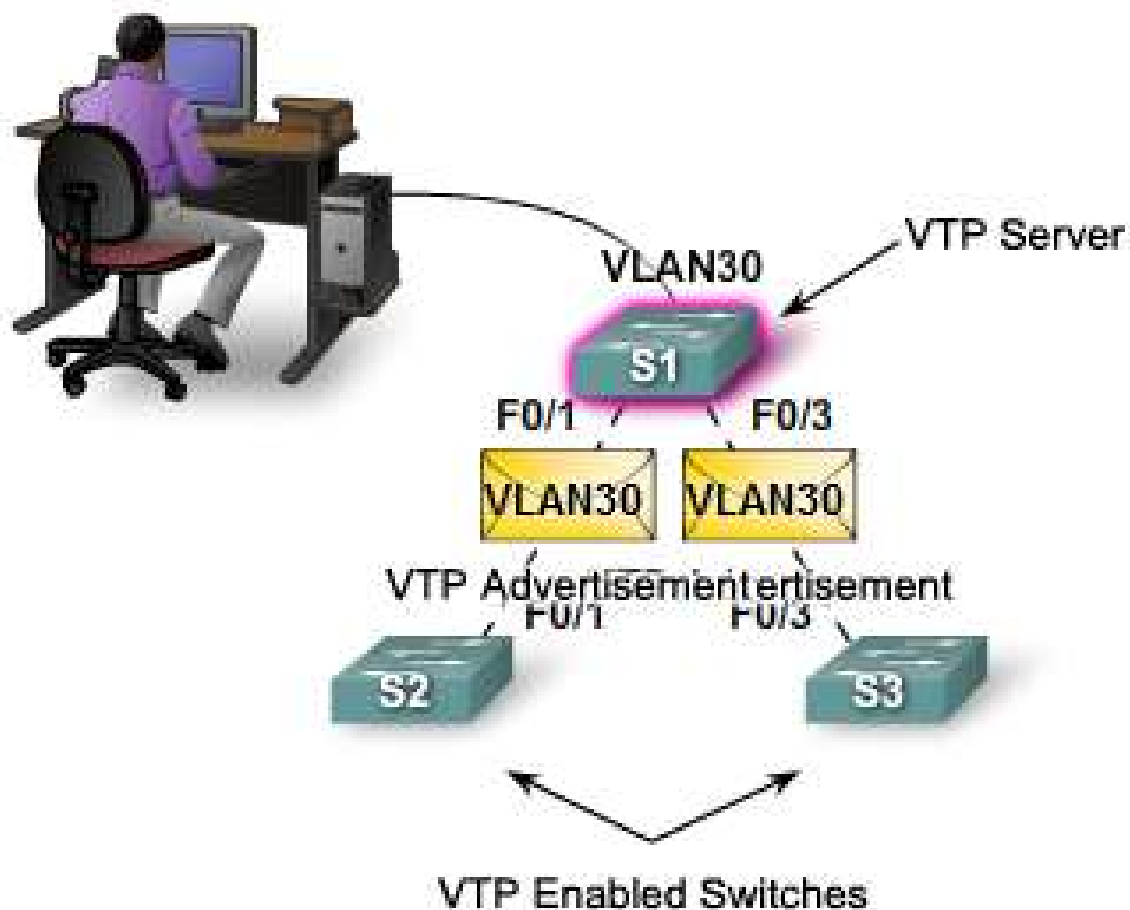
- ubrzava postupak manipulacije sa VLAN-ovima
- garantuje da svi svičevi u administrativnom domenu imaju iste VLAN-ove

* Protokol za automatsku sinhronizaciju:

- VTP - **V**LAN **T**runking **P**rotocol (Cisco, vlasnički protokol)
- GVRP - **G**eneric **V**LAN **R**egistration **P**rotocol ekvivalent na Juniper svičevima

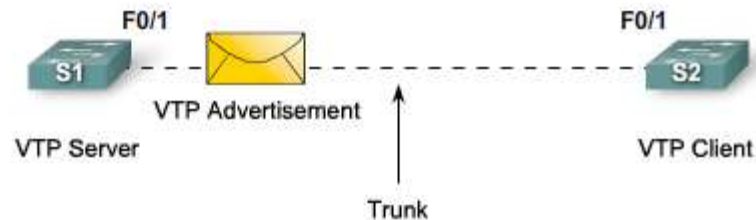
VTP

- * Na mreži sa svičevima sa VTP protokolom dovoljno je manipulaciju vršiti na jednom sviču

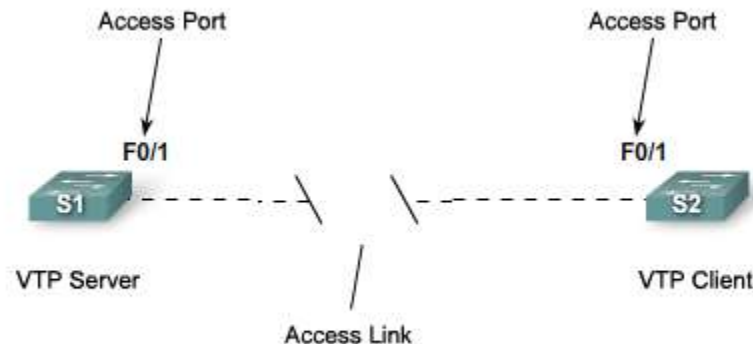


VTP

- * Svičevi razmenjuju VTP poruke isključivo preko trunk linkova
- * VTP menadžer (IOS servis) na sviču dozvoljava VTP svičevima razmenu informacija o VLAN-ovima



VTP advertisements are exchanged between the switches.



Port F0/1 on switch S1 and port F0/1 on switch S2 revert to access switch ports.

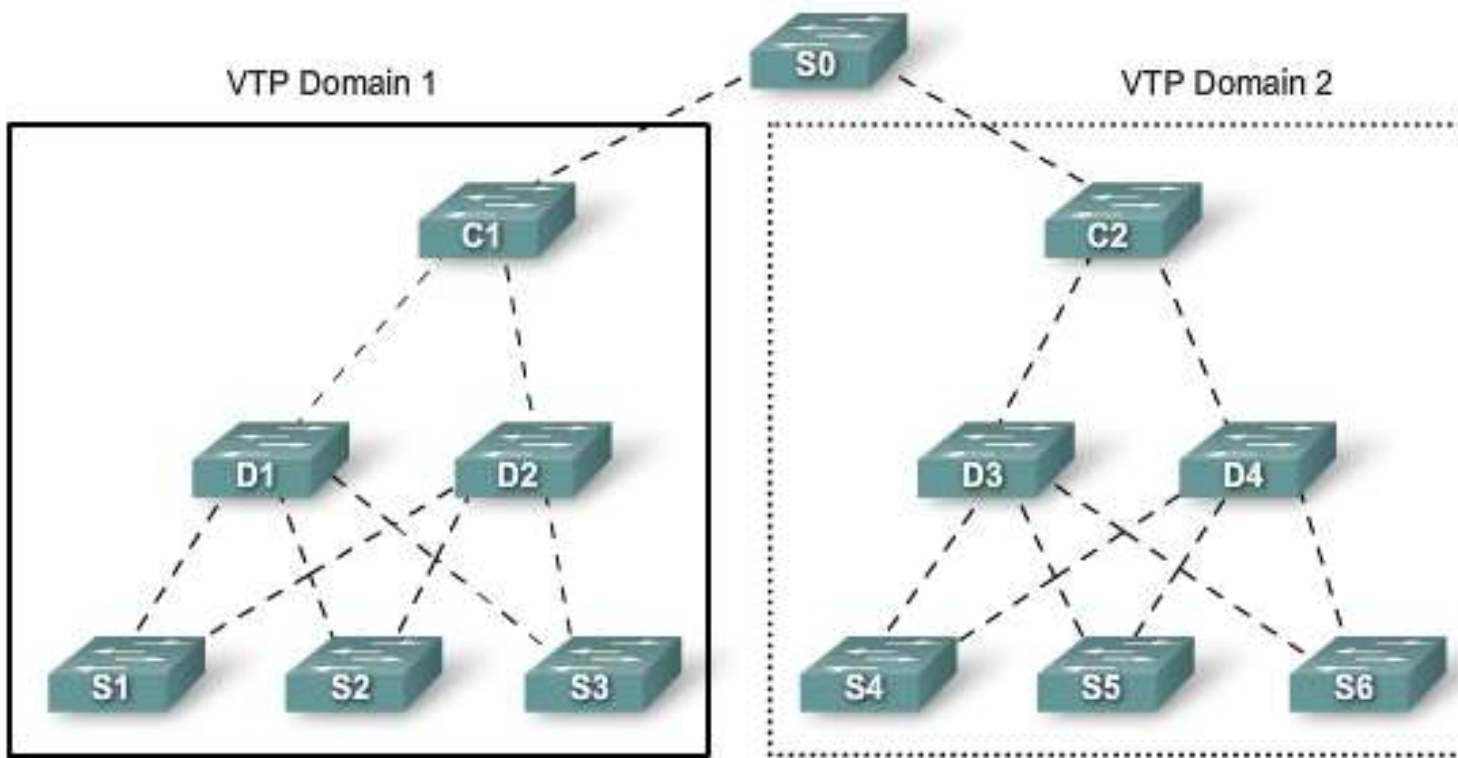
Prednosti korišćenja protokola za sinronizaciju

- * Konzistencija VLAN-ova na celoj mreži
- * Jednostavno praćenje i manipulacija
- * Automatsko podešavanje trunca prilikom dodavanja novog VLAN-a za prenos frejmova sa tog vlana na celoj mreži

VTP terminologija i komponente

* VTP domen

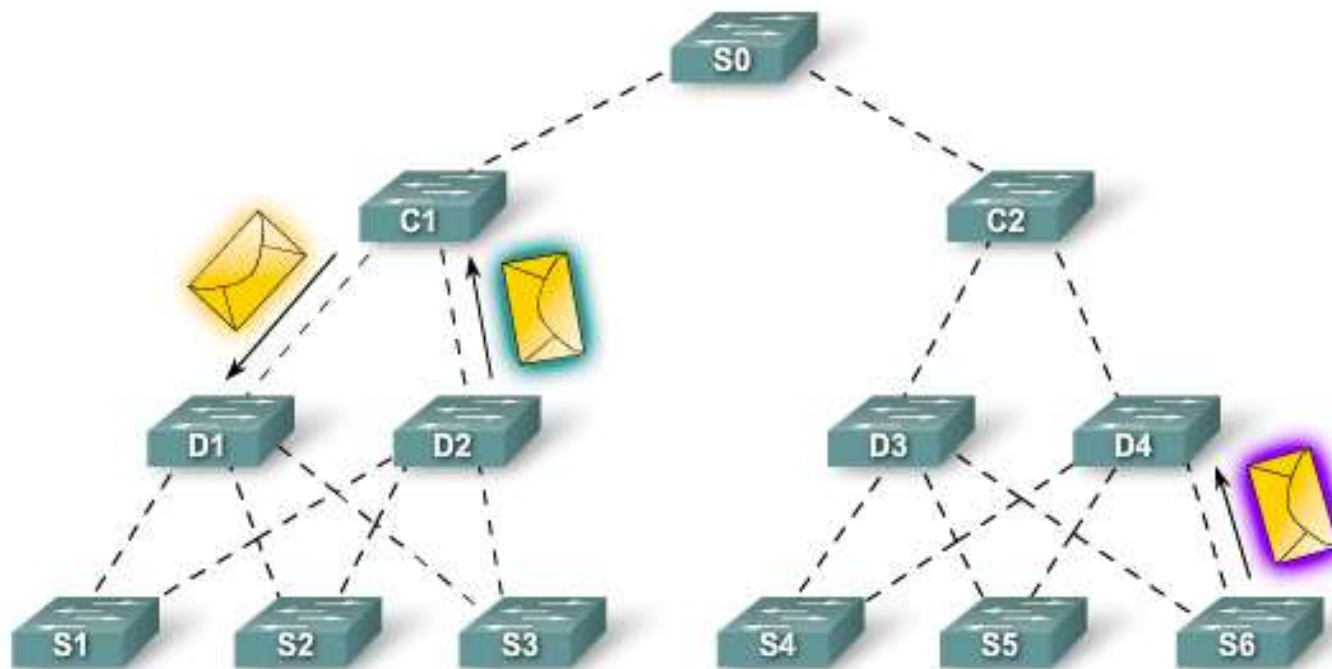
- Skup svičeva koji razmenjuju informacije i čije se VLAN baze sinhronizuju



VTP terminologija i komponente

* VTP paketi (advertisements)

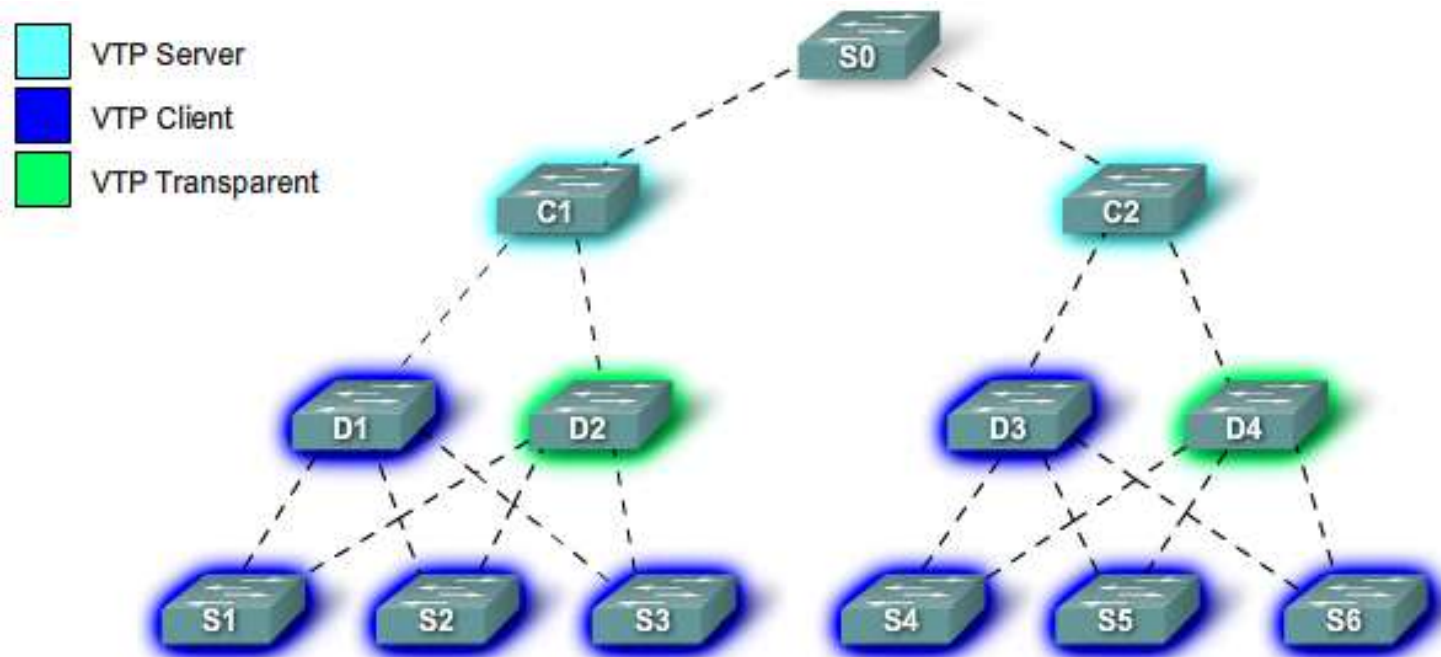
- Paketi koje razmenjuju svičevi u VTP domenu



VTP terminologija i komponente

* VTP modovi

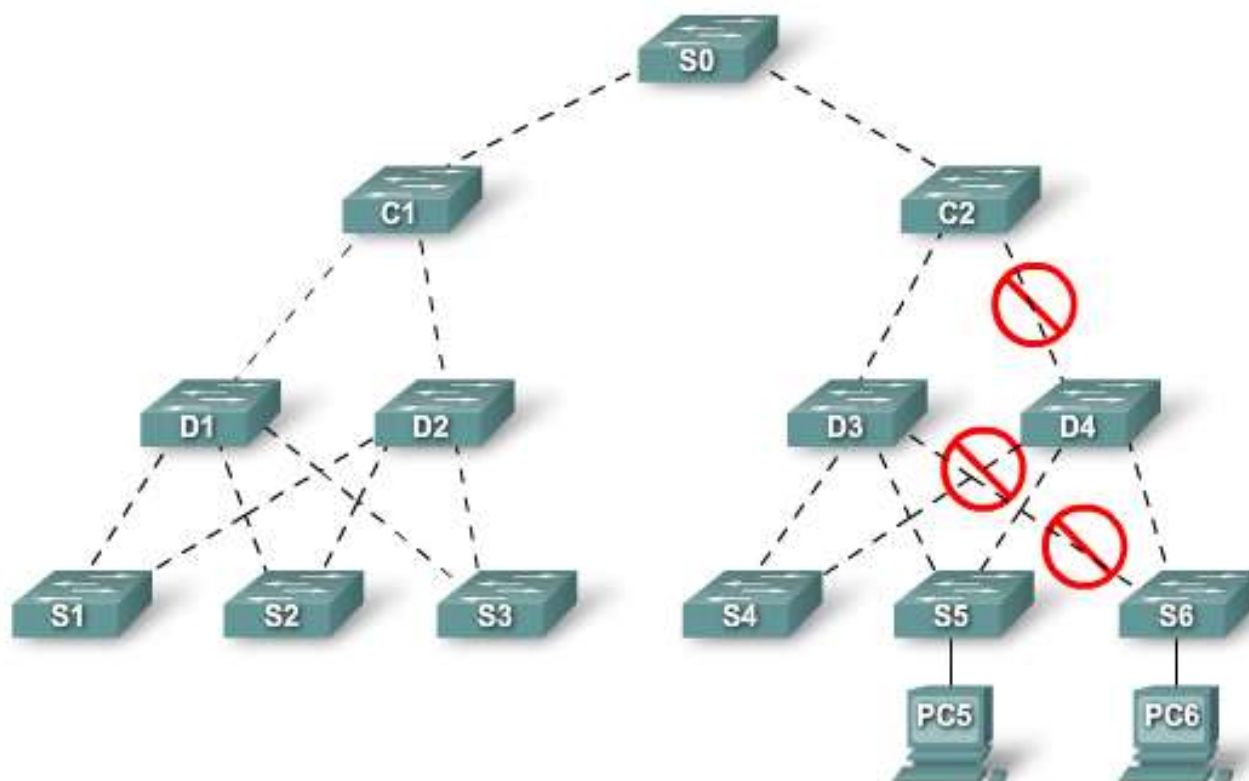
- Svičevi u VTP domenu mogu biti u jednom od sledeća 3 moda
 - Server
 - Client
 - Transparent



VTP terminologija i komponente

* VTP pruning (odsecanje)

- VTP automatski može da zabrani VLAN na tranku ako detektuje da nema potrebe slati brotkast "na tu stranu mreže" jer tamo nema računara (uređaja) koji pripadaju tom VLAN-u

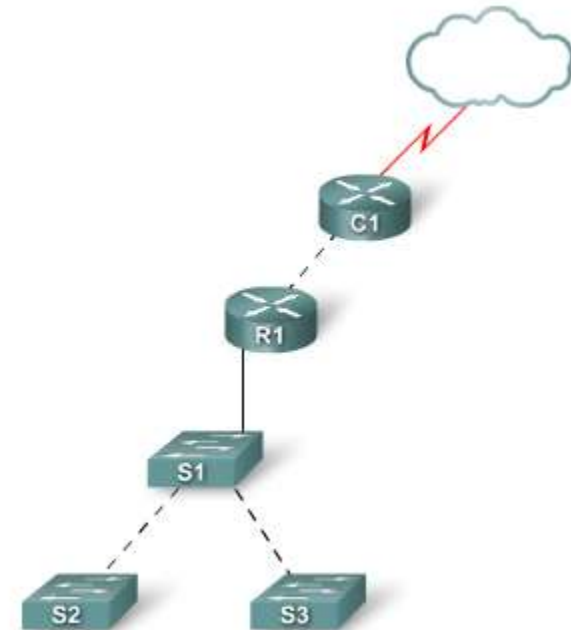


Princip rada VTP-a

Default konfiguracija na Cisco 2960

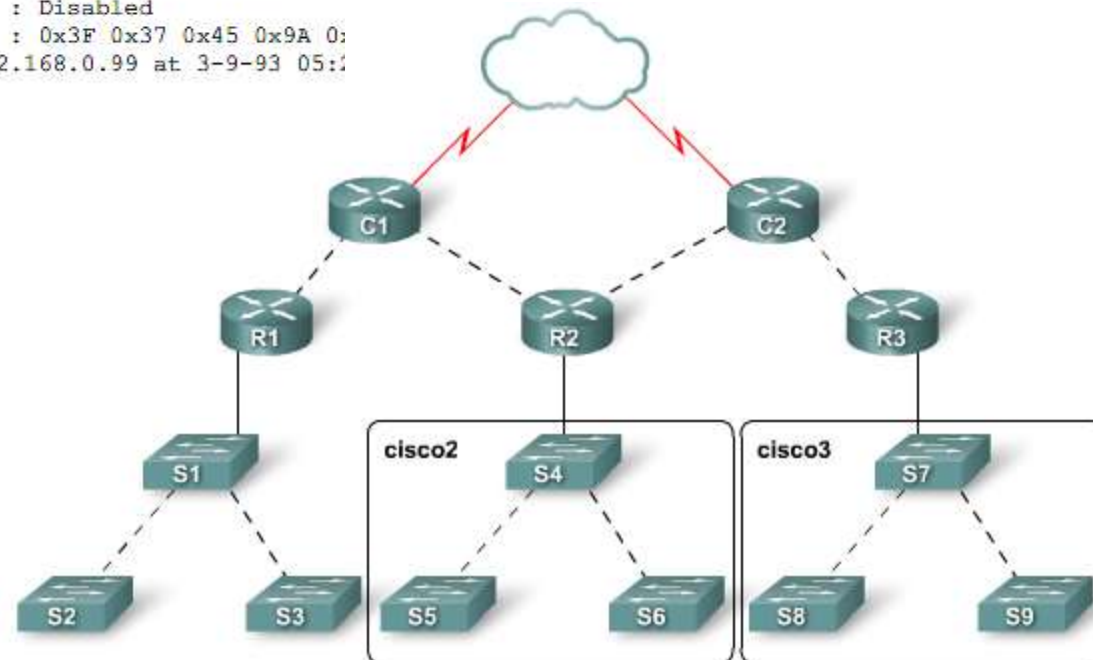
VTP Version = 1
VTP Domain Name = null
VTP Mode = Server
Config Revision = 0
VLANs = 1

```
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                 : 0x3F 0x37 0x45 0x9A 0x37 0x53 0xA6 0xDE
Configuration last modified by 0.0.0.0 at 3-1-93 00:14:07
S1#
```



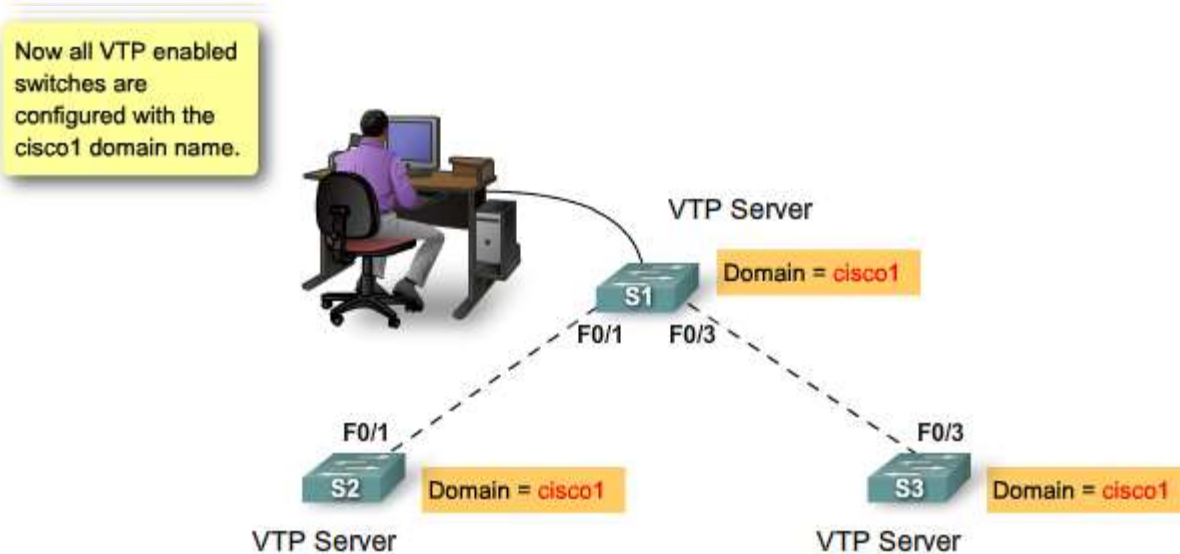
VTP domen

```
S4#show vtp status
VTP Version                : 1
Configuration Revision      : 3
Maximum VLANs supported locally : 255
Number of existing VLANs    : 8
VTP Operating Mode         : Server
VTP Domain Name            : cisco2
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MDS digest                 : 0x3F 0x37 0x45 0x9A 0:
Configuration last modified by 192.168.0.99 at 3-9-93 05:1
S4#
```



Propagacija imena domena

- * Ukoliko do sviča koji nema podešen VTP domen (domain=null) dođe VTP advert, svič će prihvatiti ime domena iz adverta



Struktura VTP frejma

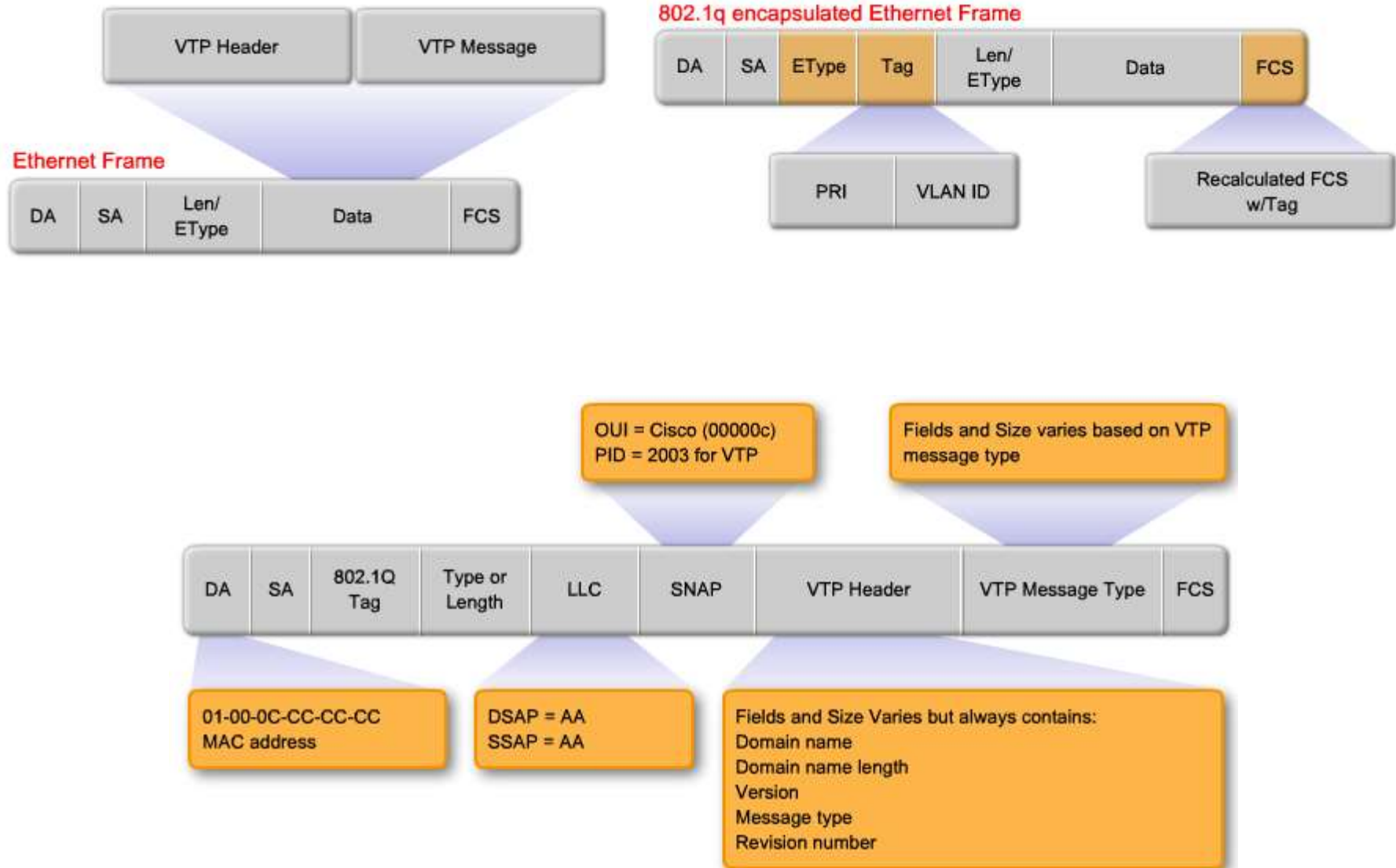
* VTP sadrži sledeće globalne informacije:

- Ime VTP domena
- Identifikator sviča koji vrši *update* i vreme (timestamp)
- MD5 potpis za zaštitu integriteta poruke (opciono)
- Oznaaku tipa frejma

* Informacije o VLAN-u sadržane u VTP paketu

- VLAN ID
- Ime
- Tip
- Status
- Dodatne specifične informacije o VLAN-u

Struktura VTP frejma



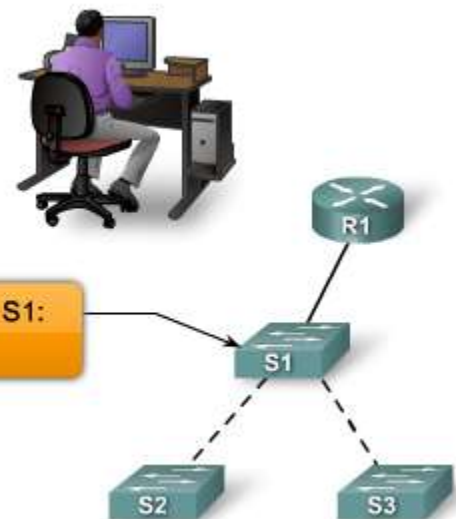
Broj revizije

* Broj revizije baze se koristi za sinhronizaciju baza VLAN-ova na svim svičevima

- Ukoliko primalac VTP poruke utvrdi da ima bazu sa nižim brojem revizije, od pošiljaoca zahteva "dopunu" informacija
- Default vrednost na nekonfigurisanom sviču je 0
- Svaka manipulacija sa VLAN-ovima (dodavanje, brisanje, promena imena) inkrementira broj revizije

```
S1#show vtp status
VTP Version                : 2
Configuration Revision      : 3
Maximum VLANs supported locally : 255
Number of existing VLANs    : 8
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                 : 0x3F 0x37 0x45 0x9A 0x37 0x5
Configuration last modified by 192.168.0.99 at 3-9-93 05:20:38
S1#
```

VLANs added on S1:
10, 20, 30



Tipovi VTP paketa

* Postoje 3 tipa VTP paketa

• Summary

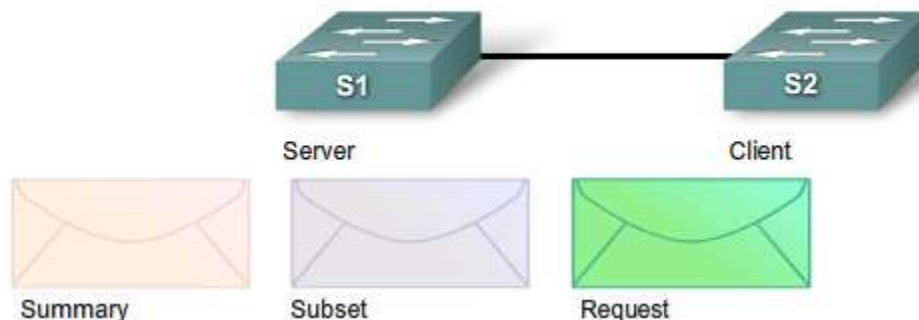
- Paket koji sadrži generalne informacije o VLAN bazi, kao što je broj revizije
- Šalje se
 - Na svakih 5 minuta
 - Prilikom izmene podataka o VLAN-ovima

• Request

- Ukoliko primalac ustanovi da ima "nižu reviziju" baze, šalje paket ovog tipa i traži "update" od svog broja revizije do trenutne revizije

• Subset

- "Update" sa svim izmenama koje su se desile između dve revizije: revizije koju ima primalac i revizije koju ima server



Summary VTP packet

Summary Advertisement			
Version	Code	Followers	MgmtID Len
Management Domain Name (Zero-Padded to 32 Bytes)			
Configuration Revision Number			
Updater Identity			
Update Timestamp (12 Bytes)			
MD5 Digest (16 Bytes)			

Request VTP packet

Advertisement Request			
Version	Code	Rsvd	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Start Value			

Subset VTP packet

Subset Advertisements			
Version	Code	Seq-Number	MgmtD Len
Management Domain Name (zero-padded to 32 bytes)			
Configuration Revision Number			
VLAN-info Field 1			
:			
VLAN-info Field N			

The VLAN-info field contains information for each VLAN and is formatted as follows:

VLAN-Info			
Info Length	Status	VLAN-Type	VLAN-name Len
ISL VLAN-id		MTU Size	
802.10 Index			
VLAN-name (Padded with 0s to Multiples of 4 bytes)			

VTP modovi

VTP Modes

	VTP Server	VTP Client	VTP Transparent
Description	Manage Domain and VLAN configurations.	Updates VTP configurations VTP client switches cannot change VLAN configurations.	Able to manage local VLAN configurations. Local VLAN configurations not shared with VTP network.
Respond to VTP advertisements?	Participates fully.	Participates fully.	Only Forwards VTP advertisements.
Global VLAN configuration preserved on restart?	Yes, global configurations stored in NVRAM.	No, global configurations stored in RAM, not in NVRAM.	No, local VLAN configuration only is stored in NVRAM.
Update other VTP enabled switches?	Yes	Yes	No

VTP modovi

* S obzirom na karakteristike modova, sledeće kombinacije su moguće:

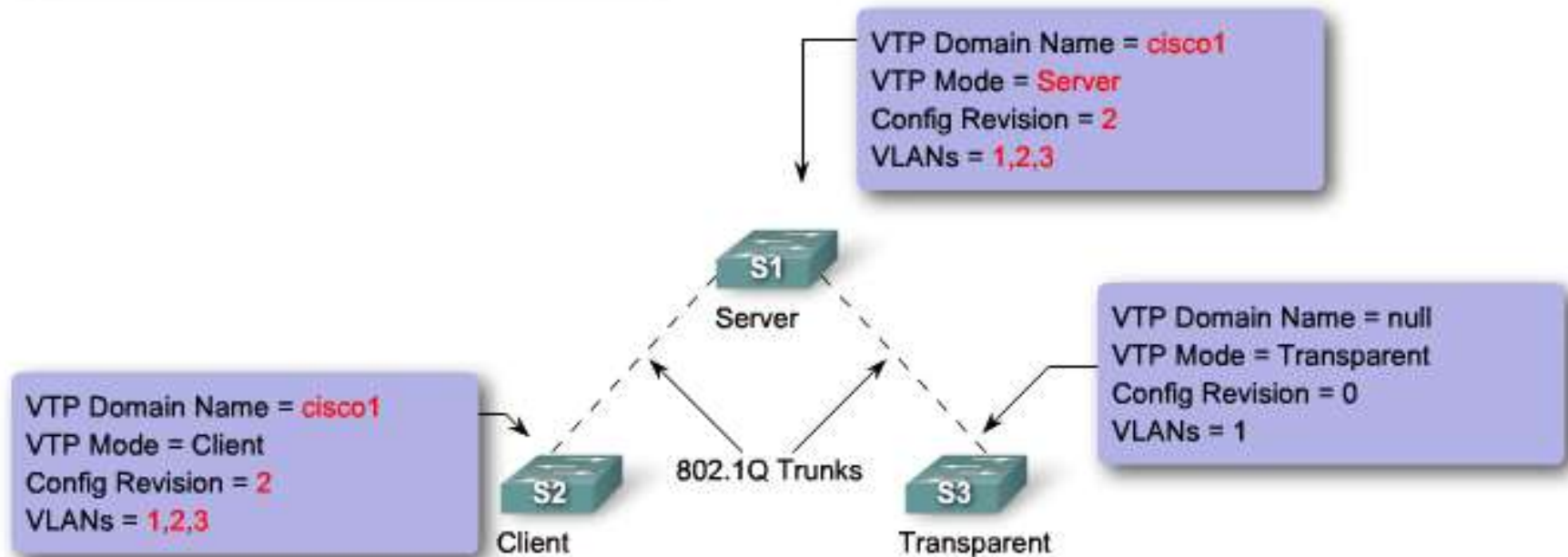
- 1 server na mreži i proizvoljan broj klijenata i transparentnih svičeva
- 2 severa na mreži i proizvoljan broj klijenata i transparentnih svičeva
- proizvoljan broj servera na mreži, i proizvoljan broj klijenata i transparentnih svičeva
- svi svičevi su serveri

* Najčešće korišćena i preporučena je varijanta sa 2 servera.

* Razlog...

Primer rada VTP-a

Switch S2 updates its VLAN configuration.



Primer rada VTP-a sa transparentnim svičem

Throughout this sequence switch S3 only forwards VTP advertisements
Revision number and VLAN configurations are unchanged

VTP Domain Name =
cisco1
VTP Mode = Server
Config Revision = 2
VLANs = 1,2,3



VTP Domain Name =
cisco1
VTP Mode = Transparent
Config Revision = 0
VLANs = 1,2,3,4,5,6

VTP Domain Name =
cisco1
VTP Mode = Client
Config Revision = 2
VLANs = 1,2,3



VTP Domain Name =
cisco1
VTP Mode = Client
Config Revision = 2
VLANs = 1,2,3

VTP pruning

```
S1#show interfaces trunk
Port  Mode  Encapsulation  Status  Native vlan
Fa0/1  on    802.1q         trunking  1
Fa0/3  on    802.1q         trunking  1

Port  Vlans allowed on trunk
Fa0/1 1-1005
Fa0/3 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005

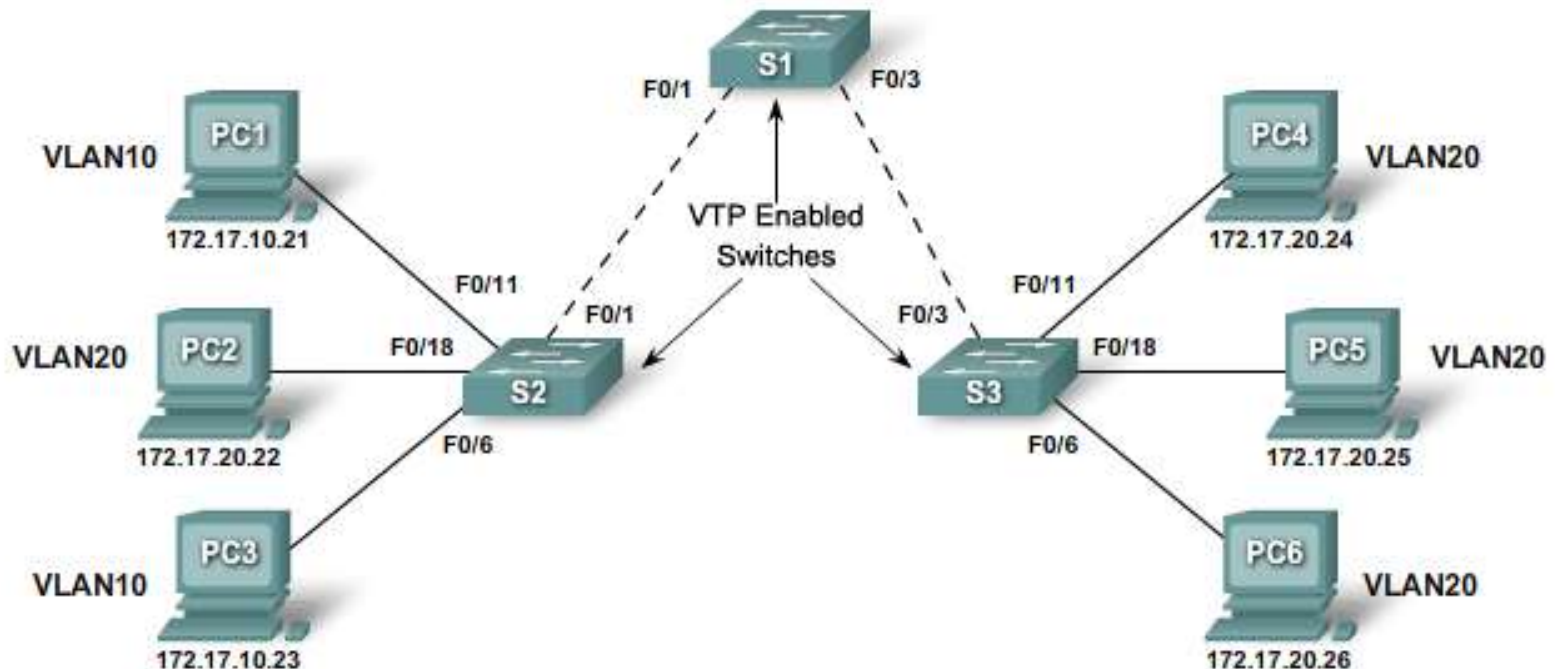
Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,10,20,1002,1003,1004,1005
Fa0/3 1,10,20,1002,1003,1004,1005
S1#
```

```
S2#show interfaces trunk
Port  Mode  Encapsulation  Status  Native vlan
Fa0/1  on    802.1q         trunking  1

Port  Vlans allowed on trunk
Fa0/1 1-1005

Port  Vlans allowed and active in management domain
Fa0/1 1,10,20,1002,1003,1004,1005

Port  Vlans in spanning tree forwarding state and not pruned
Fa0/1 1,20,1002,1003,1004,1005
S2#
```



VTP pruning

- * VTP pruning je po default-u isključen
- * Naredba za uključivanje je
 - vtp pruning
- * Naredbu je potrebno izdati samo na serveru, u globalnom konfiguracionom modu

Konfiguracija VTP protokola

Naredbe za podešavanje VTP-a

* Podešavanje domena

- SW(config)#vtp domain <ime>

* Podešavanje šifre za eventualni kriptografski potpis VTP paketa

- SW(config)#vtp password <ime>

* Podešavanje moda

- SW(config)#vtp mode {server | client | transparent}

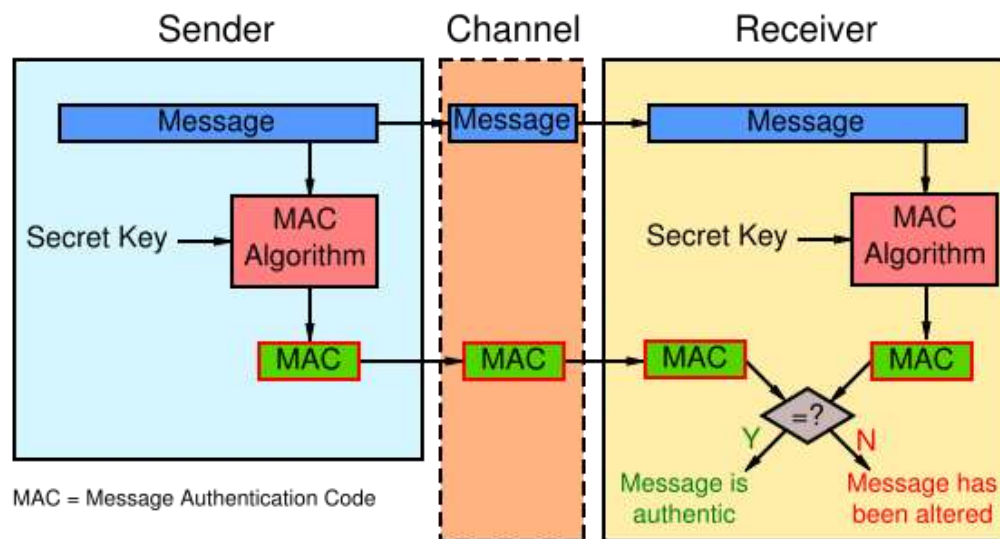
* Omogućavanje pruning opcije

- SW(config)#vtp pruning

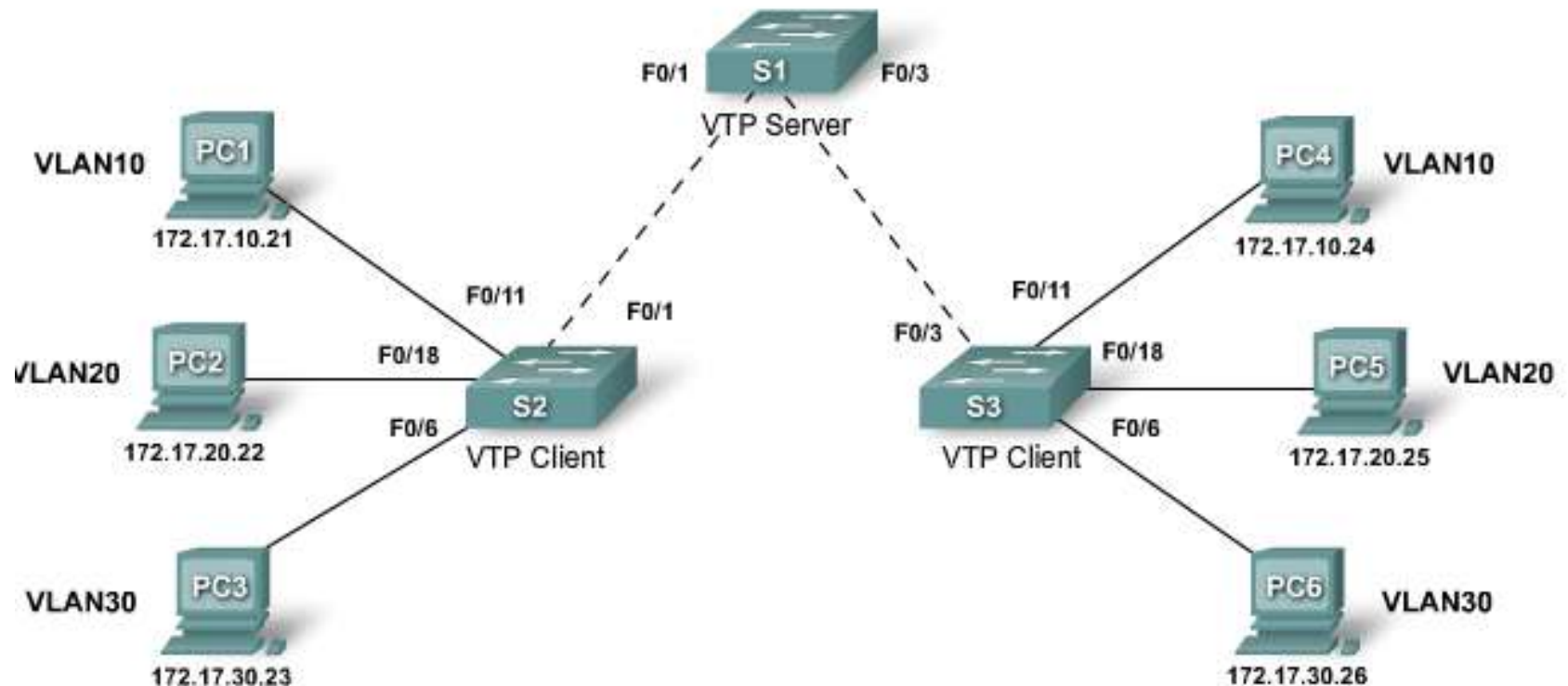
* Boj revizije se može resetovati promenom imena domena

MD5 kriptografski potpis

- * VTP paketi se šalju u plain-text modu, pa je jednostavno prisliškivanjem saznati ime domena.
- * Ukoliko napadač zna ime domena, može zlonamerno na mrežu dodati novi svič, podesiti mu domen i obrisati sve vlanove na mreži.
- * U tom slučaju, svičevi reaguju kao kod brisanja VLAN-a – gase sve portove koji su dodeljeni obrisanom VLAN-u
- * Da se ova situacija ne bi desila, VTP svičevima se može zadati šifra za razmenu paketa.
- * Šifra koju zadaje administrator se koristi za formiranje kriptografskog potpisa paketa. Inače, poruke se idalje prenose u plain-text formatu.



Topologija koja će biti korišćena u primeru



Redosled aktivnosti prilikom konfiguracije

VTP Configuration Guidelines

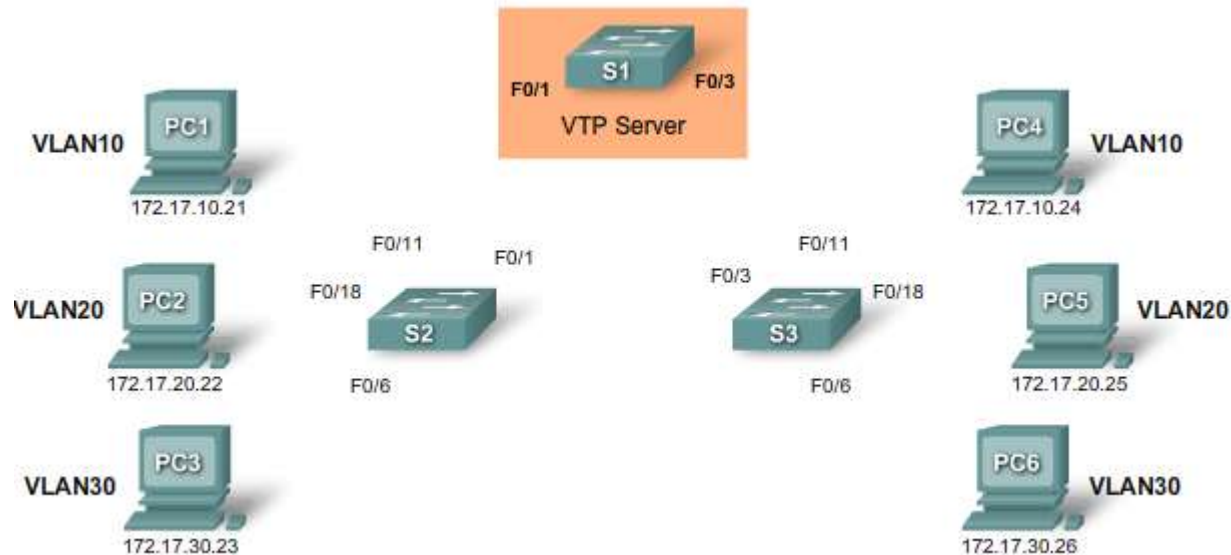
On the VTP Server:

- Confirm default settings
- Configure 2 switches as VTP servers
- Configure the VTP domain on the first switch in the network
- Ensure all switches are in the same VTP protocol version mode
- Configure VLANs and trunk ports

On the VTP Client:

- Confirm default settings
- Configure VTP client mode
- Configure trunks
- Connect to VTP server
- Verify VTP status
- Configure access ports

Konfiguracija VTP servera



```
S1#show vtp status
VTP Version                : 1
Configuration Revision     : 0
Maximum VLANs supported locally : 64
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                 : 0x7D 0x5A 0xA6 0x0E 0x9A 0
Configuration last modified by 0.0.0.0 at 0-0-00 0
S1#
```

```
S1(config)#vtp version 1
VTP mode already in V1.
S1(config)#exit
S1#
```

```
S1#configure terminal
S1(config)#vtp domain cisco1
Changing VTP domain name from NULL to cisco1
S1(config)#exit
S1#show vtp status
VTP Version                : 1
Configuration Revision     : 0
Maximum VLANs supported locally : 64
Number of existing VLANs   : 5
VTP Operating Mode         : Server
VTP Domain Name            : cisco1
<output omitted>
S1#
```

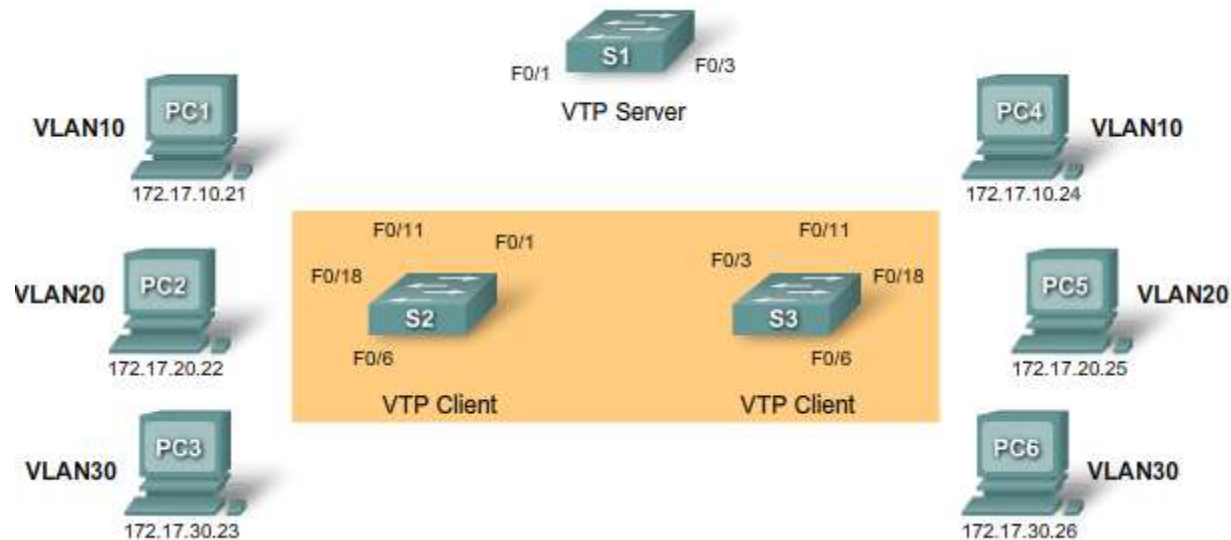
Kreiranje VLAN-ova

- * VLAN-ovi se mogu kreirati pre ili posle postavljanja trankova. Ukoliko se kreiraju posle, propagiraće se prvim sledećim *summary* advertom.
- * Svaka promena inicira inkrement revizije.

```
S1#show vlan brief
VLAN  Name                Status    Ports
-----
<output omitted>
10    faculty             active
20    student              active
30    guest                active
<output omitted>
S1#show interfaces 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
<output omitted>
S1#show vtp status
VTP Version                : 1
Configuration Revision      : 6
Maximum VLANs supported locally : 64
Number of existing VLANs    : 8
VTP Operating Mode          : Server
VTP Domain Name             : cisco1
```

Adding a name to a VLAN is
considered a revision;
3 VLANs + 3 Names = 6

Podešavanje klijenata

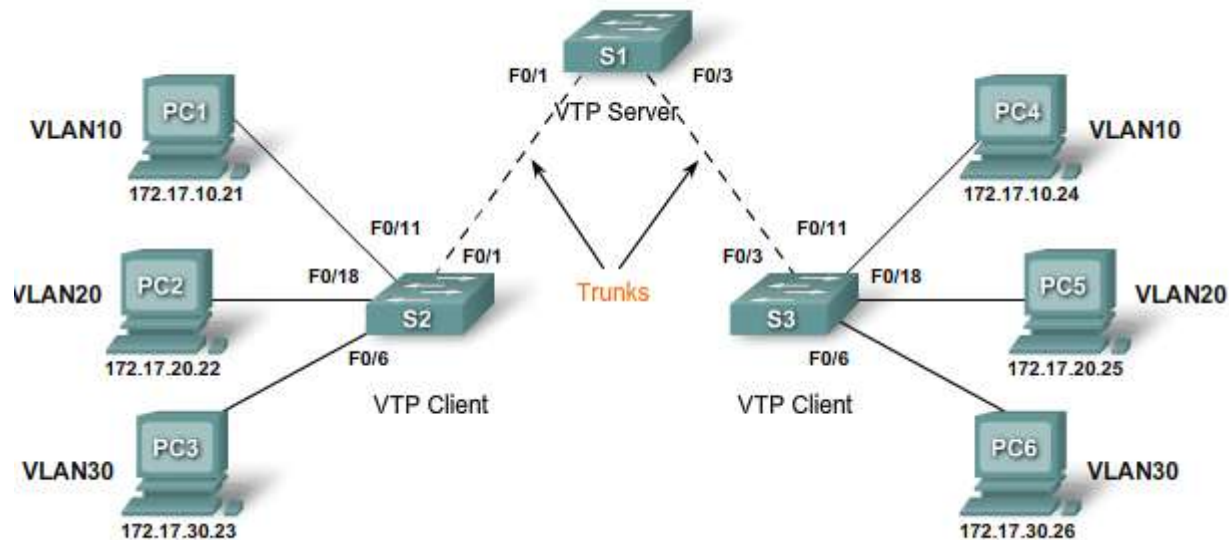


```
S2#show vtp status
VTP Version: 1
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode         : Server
VTP Domain Name            : 
VTP Pruning Mode           : Disabled
VTP V2 Mode                : Disabled
VTP Traps Generation       : Disabled
MD5 digest                  : 0x7D 0x5A 0xA6 0x0E 0
Configuration last modified by 0.0.0.0 at 0-0-00 00:
S2#
```

```
S2#configure terminal
S2(config)#vtp mode client
Setting device to VTP CLIENT mode.
S2(config)#exit
S2#show vtp status
VTP Version                  : 1
Configuration Revision       : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Client
...
S2#
```


Podešavanje trankova

- * Nakon podešavanja trankova, VLAN-ovi se propagiraju sa prvim VTP summary advert-om.



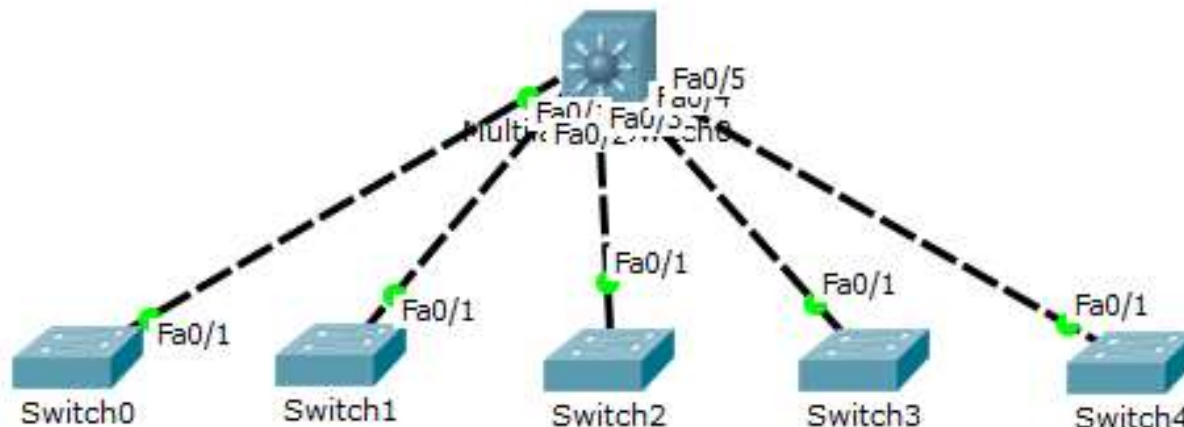
Konfiguracija L3 sviča

L3 svičevi

- * L3 svičevi, pored opcije rutiranja paketa i rada na 3. nivou OSI modela, (obično) imaju i podršku za
 - VTP
 - DTP
 - 802.1q
- * Ovo umnogome može skratiti vreme potrebno za konfiguraciju mreže.

L3 svičevi

- * S obzirom da su L3 svičevi na mreži obično svičevi sa najboljim performansama, uglavnom su kandidati za VTP servere.
- * Tipična mreža koja uključuje access i distribution nivo prikazana je na slici.
- * Ovu mrežu je kompletno moguće podesiti samo sa L3 sviča korišćenjem VTP i DTP protokola (ne računajući pripadnost pojedinih portova na svičevima access nivoa VLAN-ovima, ovo se radi direktno na sviču)



Konfiguracija

- L3(config)#ip routing
- L3(config)#int range fa0/1-5
- L3(config-if-range)#switchport mode trunk
- L3(config-if-range)#exit
- L3(config)#vtp domain projektovanje
- L3(config)#vlan 10
- L3(config-vlan)#name deset
- L3(config-vlan)#exit
- L3(config)#vlan 20
- L3(config-vlan)#name dvadeset
- L3(config-vlan)#exit
- L3(config)#interface vlan 10
- L3(config-if)#ip address 192.168.10.1 255.255.255.0
- L3(config-if)#exit
- ...