1.1 – SRWE – Training - PacketKnows – Configure VLANs, VTP, and DTP Answers

Device	Interface	IPv4 Address	Subnet Mask
PC1	E0	192.168.10.1	255.255.255.0
PC2	E0	192.168.20.1	255.255.255.0
PC3	E0	192.168.30.1	255.255.255.0
PC4	E0	192.168.30.2	255.255.255.0
PC5	E0	192.168.20.2	255.255.255.0
PC6	E0	192.168.10.2	255.255.255.0
S1	VLAN99	192.168.99.1	255.255.255.0
S2	VLAN99	192.168.99.2	255.255.255.0
S3	VLAN99	192.168.99.3	255.255.255.0

NOTE

- **Power all the devices first by clicking the triangle button on the upper navbar.**
- **Right click the device then click the web console first to configure on the device**
- **Always type “save” when configuring IP addresses of PC’s**

Objectives

Part 1: Configure and Verify DTP
Part 2: Configure and Verify VTP

Background / Scenario

As the number of switches in a network increases, the administration necessary to manage the VLANs and trunks can be challenging. To ease some of the VLAN and trunking configurations, VLAN trunking protocol (VTP) allows a network administration to automate the management of VLANs. Trunk negotiation between network devices is managed by the Dynamic Trunking Protocol (DTP).

In this activity, you will configure trunk links between the switches. You will configure a VTP server and VTP clients in the same VTP domain. You will also observe the VTP behavior when a switch is in VTP transparent mode. You will assign ports to VLANs and verify end-to-end connectivity with the same VLAN.

Part 1: Configure and Verify DTP

In Part 1, you will configure trunk links among the switches, and you will configure VLAN 999 as the native VLAN.

Step 1: Verify VLAN configuration.

Verify the configured VLANs on the switches.

a. On S1, click the **CLI** tab. At the prompt, enter **enable** and enter the **show vlan brief** command to verify the configured VLANs on S1.

```
VLAN Name Status Ports

---- -------------------------------- --------- -----------
-------------------

1 default active Et0/0, Et0/1, Et0/2, Et0/3, Et1/2, Et1/3,
Et2/0, Et2/1, Et2/2, Et2/3, Et3/0, Et3/1, Et3/2, Et3/3,
Et4/0, Et4/1, Et4/2, Et4/3, Et5/0, Et5/1, Et5/2, Et5/3,
Et6/0, Et6/1, Et6/2, Et6/3, Et7/0, Et7/1, Et7/2, Et7/3

99 Management active

999 VLAN0999 active

1002 fddi-default act/unsup

1003 token-ring-default act/unsup

1004 fddinet-default act/unsup

1005 trnet-default act/unsup
```

b. Repeat step a. on S2 and S3. What VLANs are configured on the switches?

VLANs 99 and 999 are configured on all the switches.

Step 2: Configure Trunks on S1, S2, and S3.

Dynamic trunking protocol (DTP) manages the trunk links between Cisco switches. Currently all the switchports are in the default trunking mode, which is dynamic auto. In this step, you will change the trunking mode to dynamic desirable for the link between switches S1 and S2. For the link between switches S1 and S3, the link will be set as a static trunk. Use VLAN 999 as the native VLAN in this topology.

a. On S1, configure the trunk link to static trunk link on the Ethernet 1/0 interface.

```
S1(config)# interface e1/0

S1(config-if)# switchport trunk encapsulation dot1q

S1(config-if)# switchport mode trunk
```

b. For the trunk link between S1 and S3, configure a static trunk link on the GigabitEthernet 0/2 interface.

```
S1(config)# interface e1/0

S1(config-if)# switchport trunk encapsulation dot1q

S1(config-if)# switchport mode trunk



S3(config)# interface e1/1

S3(config-if)# switchport trunk encapsulation dot1q

S3(config-if)# switchport mode trunk
```

c. Configure VLAN 999 as the native VLAN for the trunk links on S1.

```
S1(config)# interface range e1/0-

S1(config-if-range)# switchport trunk native vlan 999
```

What messages did you receive on S1? How would you correct it?

%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/2 (999), with S3 GigabitEthernet0/2 (1).
%CDP-4-NATIVE_VLAN_MISMATCH: Native VLAN mismatch discovered on GigabitEthernet0/1 (999), with S2 GigabitEthernet0/1 (1).
To correct native VLAN mismatch, configure VLAN 999 as the native VLAN on S2 and S3.

e. On S2 and S3, configure VLAN 999 as the native VLAN.

f. Verify trunking is successfully configured on all the switches. You should be able ping one switch from another switch in the topology using the IP addresses configured on the SVI.

Part 2: Configure and Verify VTP

S1 will be configured as the VTP server and S2 will be configured as VTP clients. All the switches will be configured to be in the VTP domain **CCNA** and use the VTP password **cisco**.
VLANs can be created on the VTP server and distributed to other switches in the VTP domain. In this part, you will create 3 new VLANs on the VTP server, S1. These VLANs will be distributed to S2 using VTP. Observe how the transparent VTP mode behaves.

Step 1: Configure S1 as VTP server.

Configure S1 as the VTP server in the **CCNA** domain with the password **cisco**.

a. Configure S1 as a VTP server.

```
S1(config)# vtp mode server

Setting device to VTP SERVER mode.
```

b. Configure **CCNA** as the VTP domain name.

```
S1(config)# vtp domain CCNA

Changing VTP domain name from NULL to CCNA
```

c. Configure **cisco** as the VTP password.

```
S1(config)# vtp password cisco

Setting device VLAN database password to cisco
```

Step 2: Verify VTP on S1.

a. Use the show vtp status command on the switches to confirm that the VTP mode and domain are configured correctly.

```
S1# show vtp status

VTP Version : 2

Configuration Revision : 0

Maximum VLANs supported locally : 255

Number of existing VLANs : 7

VTP Operating Mode : Server

VTP Domain Name : CCNA

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0x8C 0x29 0x40 0xDD 0x7F 0x7A 0x63 0x17

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

Local updater ID is 192.168.99.1 on interface Vl99 (lowest
numbered VLAN interface found)
```

b. To verify the VTP password, use the **show vtp password** command.

```
S1# show vtp password

VTP Password: cisco
```

Step 3: Add S2 and S3 to the VTP domain.

Before S2 and S3 will accept VTP advertisements from S1, they must belong to the same VTP domain. Configure S2 and S3 as VTP clients with CCNA as the VTP domain name and cisco as the VTP password. Remember that VTP domain names are case sensitive.

a. Configure S2 as a VTP client in the **CCNA** VTP domain with the VTP password **cisco**.

```
S2(config)# vtp mode client
```

```
Setting device to VTP CLIENT mode.

S2(config)# vtp domain CCNA

Changing VTP domain name from NULL to CCNA

S2(config)# vtp password cisco

Setting device VLAN database password to cisco
```

b. To verify the VTP password, use the **show vtp password** command.

```
S2# show vtp password

VTP Password: cisco
```

c. Configure S3 to be in the **CCNA** VTP domain with the VTP password **cisco**. Switch S3 will stay in VTP transparent mode.

```
S3(config)# vtp domain CCNA

Changing VTP domain name from NULL to CCNA

S3(config)# vtp password cisco

Setting device VLAN database password to cisco
```

d. Enter **show vtp status** command on all the switches to answer the following question.

Notice that the configuration revision number is 0 on all three switches. Explain.

The configuration revision number increments by one every time a VLAN is added, deleted, or modified. No additional configurations have been made to VLANs on any of the switches.

Step 4: Create more VLANs on S1.

a. On S1, create VLAN 10 and name it Red.

```
S1(config)# vlan 10

S1(config-vlan)# name Red
```

b. Create VLANs 20 and 30 according to the table below.

VLAN Number	VLAN Name
10	Red
20	Blue
30	Yellow

c. Verify the addition of the new VLANs. Enter **show vlan brief** at the privileged EXEC mode.
Which VLANs are configured on S1?

VLANs 1, 10, 20, 30, 99, and 999.

d. Confirm configuration changes using the **show vtp status** command on S1 and S2 to confirm that the VTP mode and domain are configured correctly. Output for S2 is shown here:

```
S2# show vtp status

VTP Version : 2

Configuration Revision : 6

Maximum VLANs supported locally : 255

Number of existing VLANs : 10

VTP Operating Mode : Client

VTP Domain Name : CCNA

VTP Pruning Mode : Disabled

VTP V2 Mode : Disabled

VTP Traps Generation : Disabled

MD5 digest : 0xE6 0x56 0x05 0xE0 0x7A 0x63 0xFB 0x33

Configuration last modified by 192.168.99.1 at 3-1-93
00:21:07
```

How many VLANs are configured on S2? Does S2 have the same VLANs as S1? Explain.

S2 has 10 VLANs, the same number as S1. Because S1 is the VTP server and S2 is a VTP client in the CCNA domain, S2 has received the VLAN information from S1.

Step 5: Observe VTP transparent mode.

S3 is currently configured as VTP transparent mode.

a. Use **show vtp status** command to answer the following question.
How many VLANs are configured on S3 currently? What is the configuration revision number? Explain your answer.

Currently there are 7 VLANs on S3. The configuration revision number is 0 because S3 is in transparent mode and VLAN configurations have not been changed since switch startup.
How would you change the number of VLANs on S3?

While S3 is in transparent mode, it will not implement the VLAN information from the VTP server, so all of the VLANs changes either need to be configured manually, or S3 can be changed to a VTP client to implement the VLAN information from VTP server.
b. Change VTP mode to client on S3.

Use show commands to verify the changes on VTP mode. How many VLANs exists on S3 now? 10
Note: VTP advertisements are flooded throughout the management domain every five minutes, or whenever a change occurs in VLAN configurations. To accelerate this process, you can switch between Realtime mode and Simulation mode until the next round of updates. However, you may have to do this multiple times because this will only forward Packet Tracer's clock by 10 seconds each time. Alternatively, you can change one of the client switches to transparent mode and then back to client mode.

Step 6: Assign VLANs to Ports

Use the **switchport mode access** command to set access mode for the access links. Use the **switchport access vlan** *vlan-id* command to assign a VLAN to an access port.

a. Assign VLANs to ports on S2 using assignments from the table above.

```
S2(config-if)# interface range e2/0-3
S2(config-if-range)# switchport mode access

S2(config-if-range)# switchport access vlan 10

S2(config-if-range)# interface range e3/0-3

S2(config-if-range)# switchport mode access
```

```
S2(config-if-range)# switchport access vlan 20
S2(config-if-range)# interface range e4/0-3
S2(config-if-range)# switchport mode access
S2(config-if-range)# switchport access vlan 30
```

b. Assign VLANs to ports on S3 using assignment from the table above.

Step 7: Verify end to end connectivity.

a. From PC0 ping PC5.

b. From PC1 ping PC4.

c. From PC2 ping PC3.

Script
Switch S1

```
config t
vtp mode server
vtp domain CCNA
vtp password cisco
vlan 10
 name Red
vlan 20
 name Blue
vlan 30
 name Yellow
interface e1/0
switchport trunk encapsulation dot1q
switchport mode trunk
 switchport trunk native vlan 999
```

```
interface e1/1
switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
end
```

Switches S2 and S3

```
enable
config t
vtp mode client
vtp domain CCNA
vtp password cisco
interface e1/0
switchport trunk encapsulation dot1q
 switchport mode trunk
 switchport trunk native vlan 999
interface e1/1
switchport trunk encapsulation dot1q
switchport mode trunk
 switchport trunk native vlan 999
interface range e2/0-3
 switchport mode access
 switchport access vlan 10
interface range e3/0-3
 switchport mode access
```

```
 switchport access vlan 20
interface range e4/0-3
 switchport mode access
 switchport access vlan 30
end
```