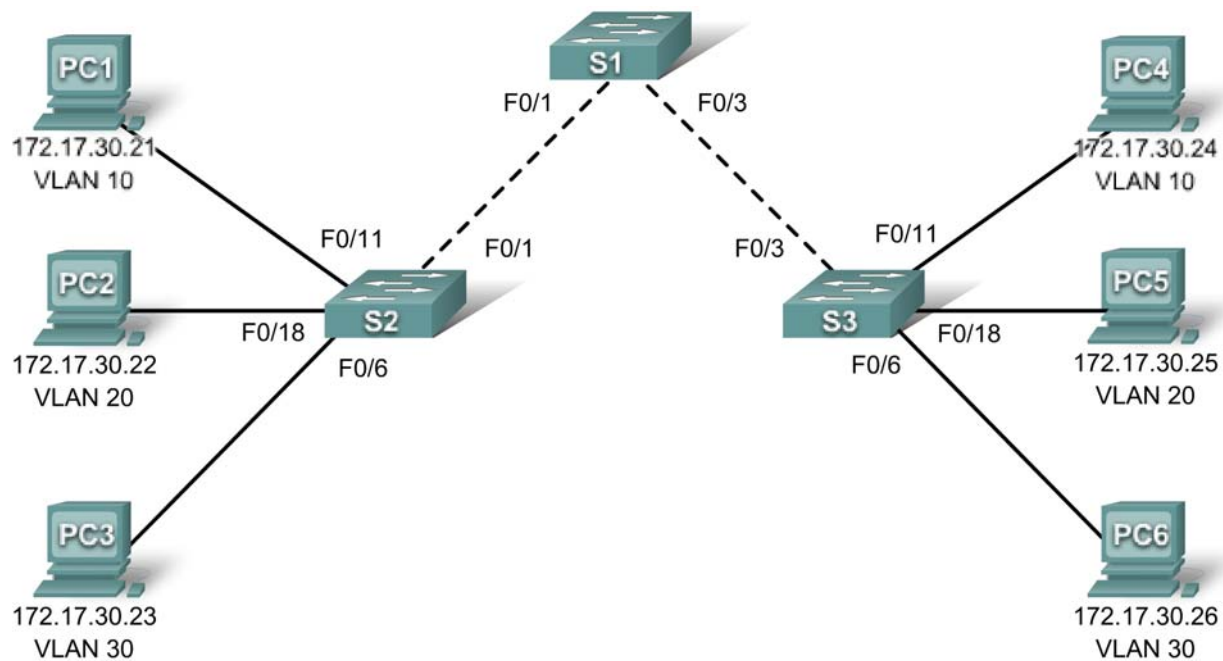


PT Activity 4.3.3: Configure VTP

Topology Diagram



Learning Objectives

- Investigate the current configuration.
- Configure S1 as VTP server.
- Configure S2 and S3 as VTP clients.
- Configure VLANs on S1.
- Configure trunks on S1, S2, and S3.
- Verify VTP status on S1, S2, and S3.
- Assign VLANs to ports on S2 and S3.
- Verify VLAN implementation and test connectivity

Introduction

In this activity, you will practice configuring VTP. When Packet Tracer first opens, the switches already contain a partial configuration. The user EXEC password is **cisco** and the privileged EXEC password is **class**.

Task 1: Investigate the Current Configuration

Step 1. Verify the current running configuration on the switches.

What configurations are already present on the switches?

Step 2. Display the current VLANs on each switch.

Are there any VLANs present? Are the VLANs user created VLANs or default VLANs?

```
S1#show vlan brief
```

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	

Completion should be at 0% at the end of this Task.

Task 2: Configure S1 as VTP Server**Step 1. Configure the VTP mode command.**

S1 will be the server for VTP. Set S1 to server mode.

```
S1(config)#vtp mode server
Device mode already VTP SERVER.
S1(config)#
```

Notice that the switch is already set to server mode by default. However, it is important that you explicitly configure this command to insure the switch is in server mode.

Step 2. Configure the VTP domain name.

Configure S1 with **CCNA** as the VTP domain name. Remember that VTP domain names are case sensitive.

```
S1(config)#vtp domain CCNA
Changing VTP domain name from NULL to CCNA
S1(config)#
```

Step 3. Configure the VTP domain password.

Configure S1 with **cisco** as the VTP domain password. Remember that VTP domain passwords are case sensitive.

```
S1(config)#vtp password cisco
Setting device VLAN database password to cisco
S1(config)#
```

Step 4. Confirm configuration changes.

Use the **show vtp status** command on S1 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 : 64
Number of existing VLANs    : 5
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
Configuration last modified by 0.0.0.0 at 0-0-00 00:00:00
```

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

```
S1#show vtp password
VTP Password: cisco
S1#
```

Step 5. Check results.

Your completion percentage should be 8%. If not, click **Check Results** to see which required components are not yet completed.

Task 3: Configure S2 and S3 as VTP Clients**Step 1. Configure the VTP mode command.**

S2 and S3 will be VTP clients. Set these two switches to client mode.

Step 2. Configure the VTP domain name.

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

Step 3. Configure the VTP domain password.

S2 and S3 must also use the same password before they can accept VTP advertisements from the VTP server. Configure S2 and S3 with **cisco** as the VTP domain password. Remember that VTP domain passwords are case sensitive.

Step 4. Confirm configuration changes.

Use the **show vtp status** command on each switch to confirm that the VTP mode and domain are configured correctly. Output for S3 is shown here.

```
S3#show vtp status
VTP Version                : 2
Configuration Revision      : 0
Maximum VLANs supported locally : 64
Number of existing VLANs    : 5
VTP Operating Mode          : Client
```

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

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

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

```
S3#show vtp password
VTP Password: cisco
S3#
```

Step 5. Check results.

Your completion percentage should be 31%. If not, click **Check Results** to see which required components are not yet completed.

Task 4: Configure VLANs on S1

VLANs can be created on the VTP server and distributed to other switches in the VTP domain. In this task you will create 4 new VLANs on the VTP server, S1. These VLANs will be distributed to S2 and S3 via VTP.

Step 1. Create the VLANs.

For grading purposes in Packet Tracer, the VLAN names are case-sensitive.

- VLAN 10 named **Faculty/Staff**
- VLAN 20 named **Students**
- VLAN 30 named **Guest(Default)**
- VLAN 99 named **Management&Native**

Step 2. Verify VLANs.

Use the **show vlan brief** command to verify the VLANs and their names.

```
S1#show vlan brief
```

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
10	Faculty/Staff	active	
20	Students	active	
30	Guest(Default)	active	

```
99    Management&Native      active
1002  fddi-default            active
1003  token-ring-default      active
1004  fddinet-default         active
1005  trnet-default           active
```

If you enter the same command on S2 and S3, you will notice that the VLANs are not in their VLAN database? Why not?

Step 4. Check results.

Your completion percentage should be 46%. If not, click **Check Results** to see which required components are not yet completed.

Task 5: Configure Trunks on S1, S2, and S3

Use the **switchport mode trunk** command to set trunk mode for each of the trunk links. Use the **switchport trunk native vlan 99** command to set VLAN 99 as the native VLAN.

Step 1. Configure FastEthernet 0/1 and FastEthernet 0/3 on S1 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Once configured, Dynamic Trunking Protocol (DTP) will bring up the trunk links. You can verify S2 and S3 are now trunking by entering the **show interface fa0/1 switchport** command on S2 and the **show interface fa0/3 switchport** command on S3.

If you wait a few minutes for Packet Tracer to simulate all the processes, S1 will advertise the VLAN configuration to S2 and S3. This can be verified on S2 or S3 with both the **show vlan brief** command and the **show vtp status** command.

However, it is a best practice to configure both sides of the trunk links to the **on** mode.

Step 2. Configure Fast Ethernet 0/1 on S2 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Step 3. Configure Fast Ethernet 0/3 on S3 for trunking.

Enter the appropriate commands to configure trunking and set VLAN 99 as the native VLAN.

Step 5. Check results.

Your completion percentage should be 77%. If not, click **Check Results** to see which required components are not yet completed.

Task 6: Verify VTP Status

Using the **show vtp status** and **show vlan brief** commands, verify the following.

- S1 should show server status.
- S2 and S3 should show client status.
- S2 and S3 should have VLANs from S1.

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 since 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. (The configuration revision numbering may differ on actual routers versus routers in Packet Tracer. This activity is not grading the configuration revision numbers.)

What is the configuration revision number? _____

Is the configuration revision number higher than the number of VLANs you created?

What is the current number of existing VLANs? _____

Why are there more existing VLANs than the four you created?

Completion should still be at 77% at the end of this Task.

Task 7: 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.

Step 1. Assign VLANs to ports on S2.

- Fa0/11 on VLAN 10
- Fa0/18 on VLAN 20
- Fa0/6 on VLAN 30

Step 2. Assign VLANs to ports on S3.

- Fa0/11 on VLAN 10
- Fa0/18 on VLAN 20
- Fa0/6 on VLAN 30

Step 4. Check results.

Your completion percentage should be 100%. If not, click **Check Results** to see which required components are not yet completed.

Task 8: Verify VLAN Implementation and Test Connectivity

Step 1. Verify VLAN configuration and port assignments.

Use the **show vlan brief** command to verify VLAN configuration and port assignments on each switch. Compare your output to the topology.

Step 2. Test connectivity between PCs.

Pings between PCs on the same VLAN should succeed, while pings between PCs on different VLANs should fail.

From PC1 ping PC4.

From PC2 ping PC5.

From PC3 ping PC6.