CCNA 3 v6.0 Study Material – Chapter 2: Scaling VLANs

September 5, 2017

Chapter 2 – Sections & Objectives

2.1 VTP, Extended VLANs, and DTP

Configure enhanced inter-switch connectivity technologies.

2.2 Troubleshoot Multi-VLAN Issues

Troubleshoot issues in an inter-VLAN routing environment.

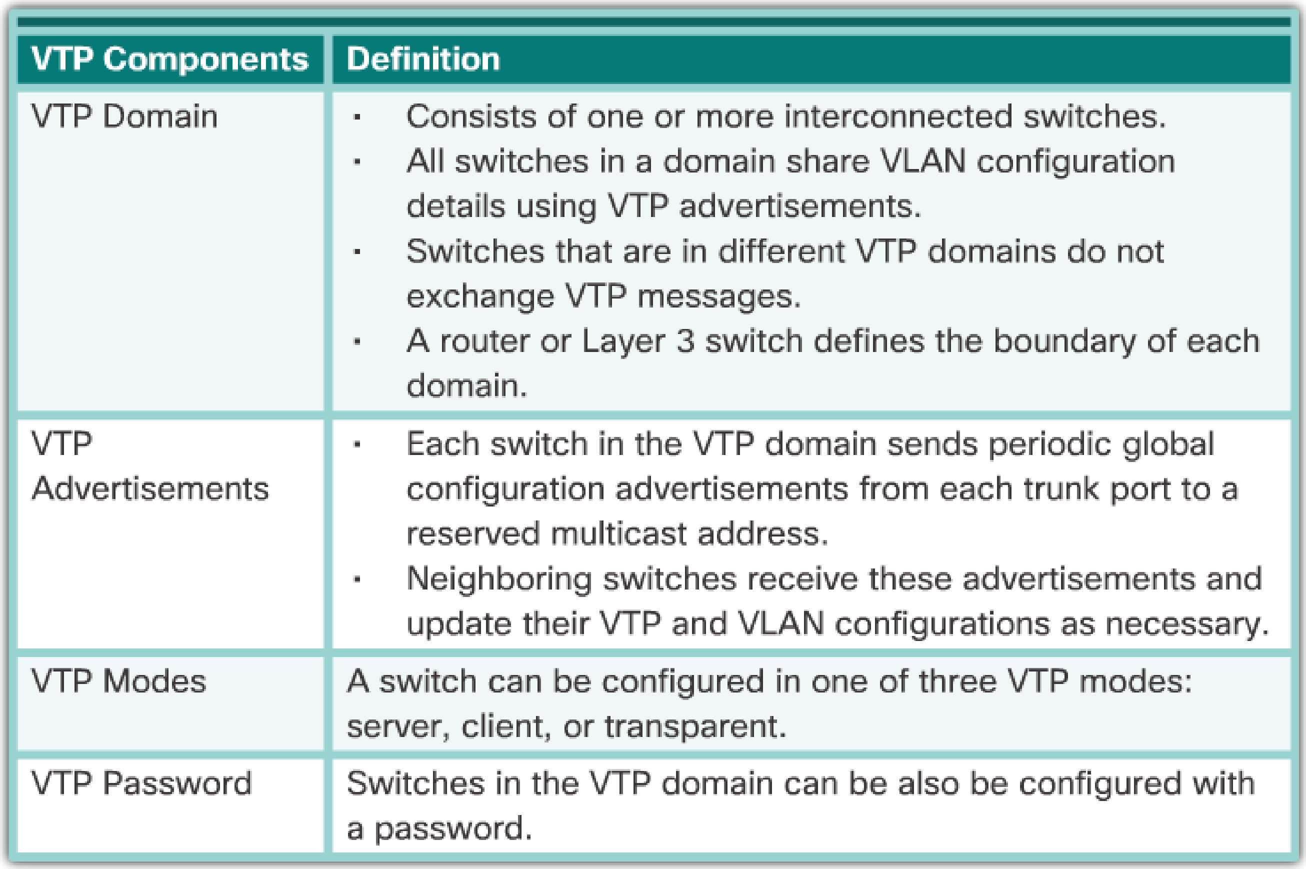
2.3 Layer 3 Switching

Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.

2.1 VTP, Extended VLANs, and DTP

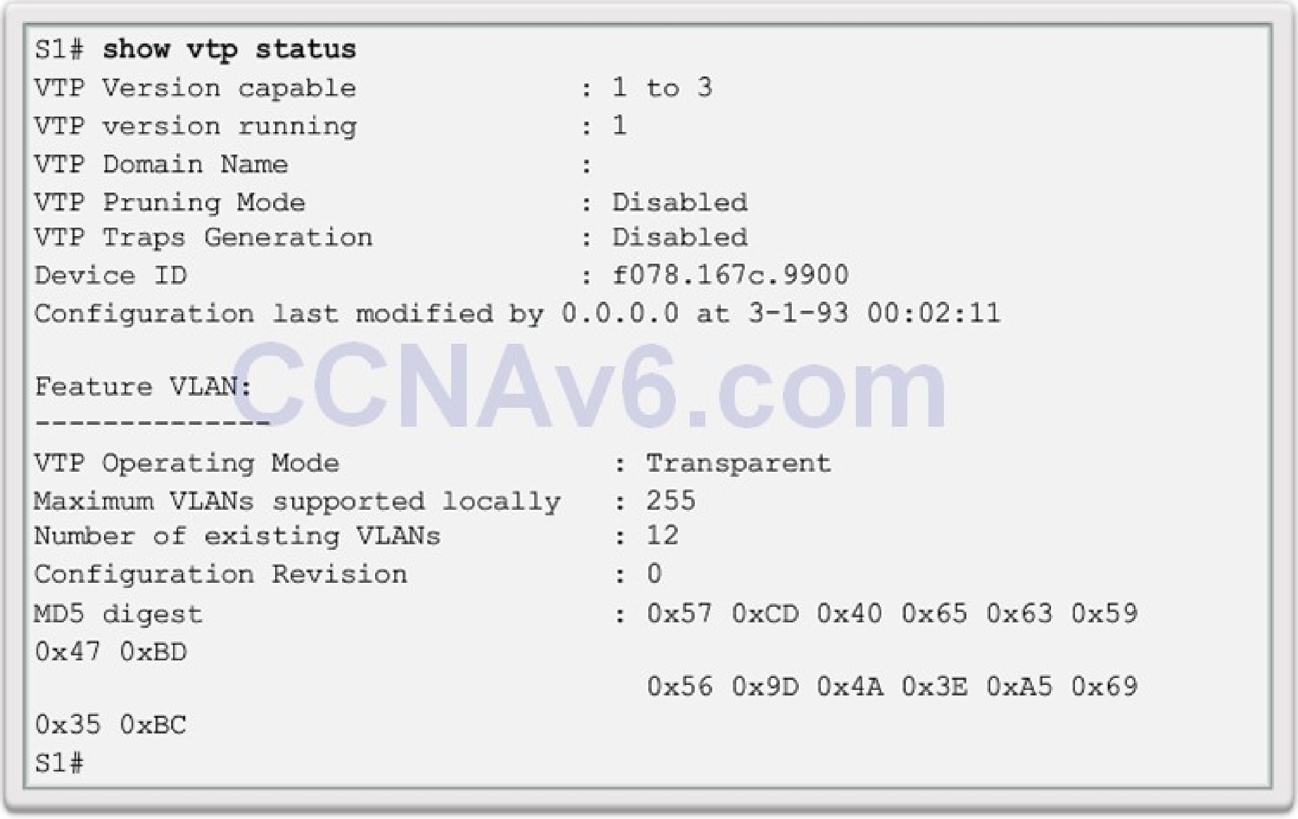
VTP Concepts and Operation

- VLAN trunking protocol (VTP) allows a network administrator to manage VLANs on a switch configured as a VTP server.
- VTP stores VLAN configurations in a database called vlan.dat.
- A switch can be configured in one of three VTP modes:
- Server
- Client
- Transparent
- VTP includes three types of
- advertisements:
- Summary
- Advertisement request
- Subset advertisements



VTP Components	Definition
VTP Domain	▪ Consists of one or more interconnected switches. ▪ All switches in a domain share VLAN configuration details using VTP advertisements. ▪ Switches that are in different VTP domains do not exchange VTP messages. ▪ A router or Layer 3 switch defines the boundary of each domain.
VTP Advertisements	▪ Each switch in the VTP domain sends periodic global configuration advertisements from each trunk port to a reserved multicast address. ▪ Neighboring switches receive these advertisements and update their VTP and VLAN configurations as necessary.
VTP Modes	A switch can be configured in one of three VTP modes: server, client, or transparent.
VTP Password	Switches in the VTP domain can be also be configured with a password.

- VTP has 3 versions
- The show vtp status privileged EXEC command displays the VTP status.



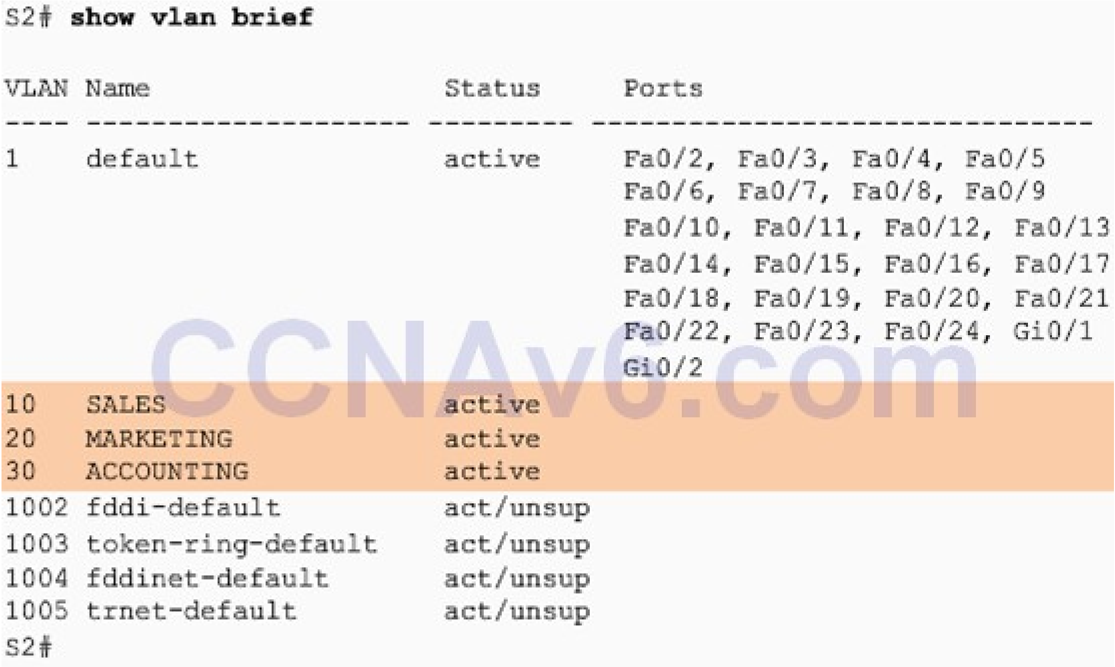
```
S1# show vtp status
VTP Version capable                : 1 to 3
VTP version running                : 1
VTP Domain Name                    :
VTP Pruning Mode                   : Disabled
VTP Traps Generation               : Disabled
Device ID                          : f078.167c.9900
Configuration last modified by 0.0.0.0 at 3-1-93 00:02:11

Feature VLAN:
--------------
VTP Operating Mode                   : Transparent
Maximum VLANs supported locally      : 255
Number of existing VLANs             : 12
Configuration Revision               : 0
MD5 digest                           : 0x57 0xCD 0x40 0x65 0x63 0x59
0x47 0xBD
                                       0x56 0x9D 0x4A 0x3E 0xA5 0x69
0x35 0xBC
S1#
```

- The configuration revision number is used when determining whether a switch should keep its existing VLAN database, or overwrite it with the VTP update sent by another switch.
- When a switch is added to a network, ensure that it has a default VTP configuration.

VTP Configuration

- There are 5 steps to VTP configuration:
- Configure the VTP Server.
- Configure the VTP Domain Name and Password.
- Configure the VTP Clients.
- Configure VLANs on the VTP Server.
- Verify the VTP Clients have received the new VLAN information.

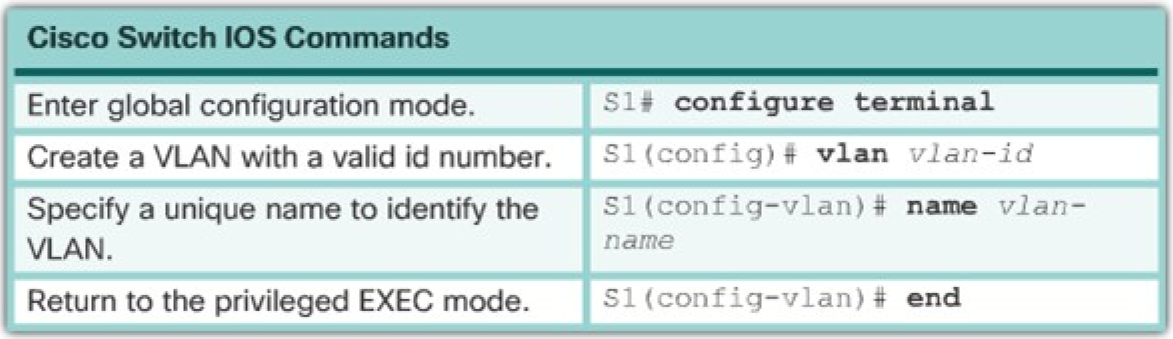


```
S2# show vlan brief

VLAN Name                             Status    Ports
---- -------------------------------- --------- -------------------------------
1    default                          active    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, Gi0/1
                                                Gi0/2
10   SALES                            active
20   MARKETING                        active
30   ACCOUNTING                       active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup
S2#
```

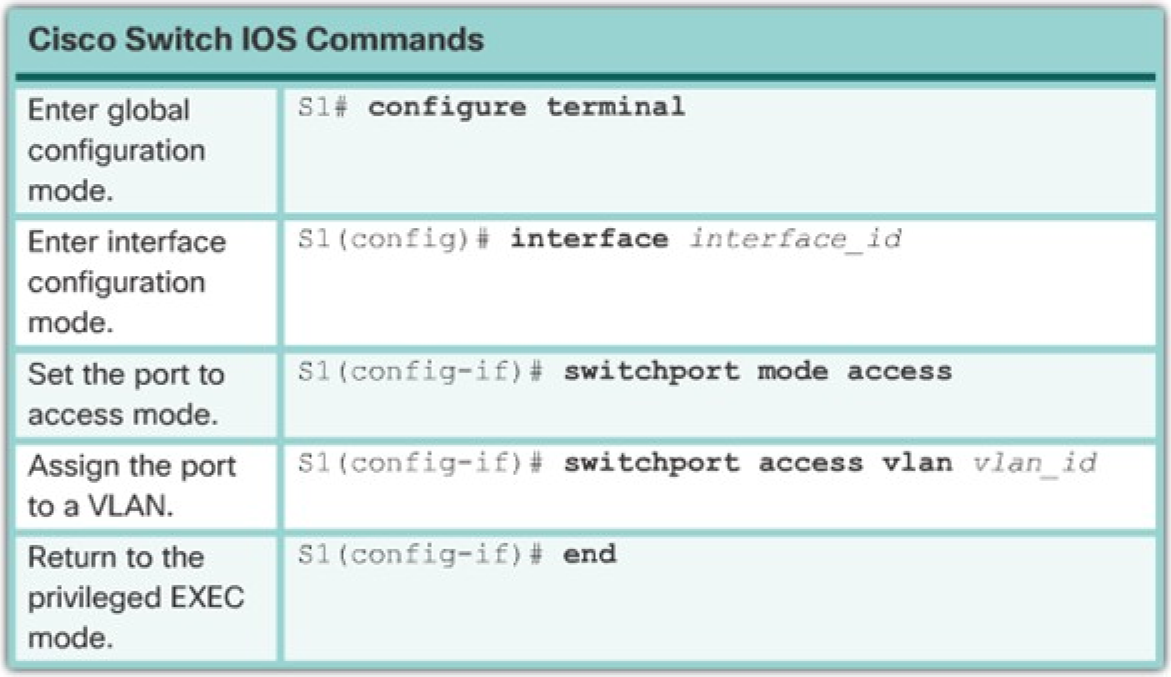
Extended VLANs

- Normal range VLANs are identified by a VLAN ID between 1 and 1005.
- Extended range VLANs are identified by a VLAN ID between 1006 and 4094.
- VTP does not learn extended range VLANs.
- Creating a VLAN
- In addition to entering a single VLAN ID, a series of VLAN IDs can be entered that are separated by commas, or as range of VLAN IDs separated by hyphens.



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`S1(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`S1(config-vlan)# end`

- Assigning Ports to VLANs
- After creating a VLAN, the next step is to assign ports to the VLAN.



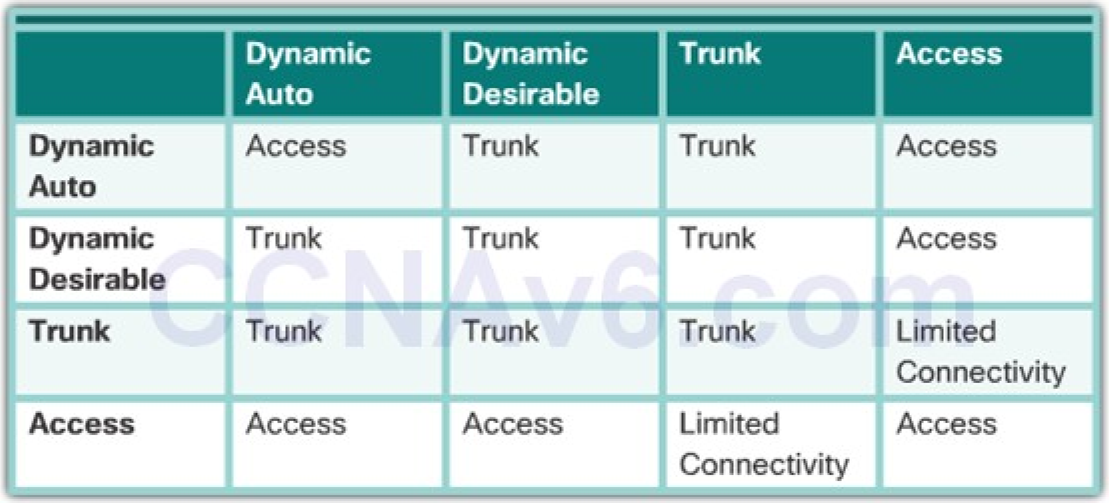
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Return to the privileged EXEC mode.	`S1(config-if)# end`

- Verifying VLAN Information
- VLAN configurations can be validated using Cisco IOS show commands.
- Configuring Extended VLANs
- To configure an extended VLAN on a 2960 switch it must be set to VTP transparent mode.

Dynamic Trunking Protocol

- DTP
- DTP manages trunk negotiation only if the port on the neighbor switch is configured in a trunk mode that supports DTP.
- Turn off DTP on interfaces on a Cisco switch that is connected to devices that do not support DTP.

- To enable trunking from a Cisco switch to a device that does not support DTP, use the switchport mode trunk and switchport nonegotiate interface configuration mode commands.
- There are 5 commands to support different trunking modes:
- switchport mode access
- switchport mode dynamic auto
- switchport mode dynamic desirable
- switchport mode trunk
- switchport nonegotiate

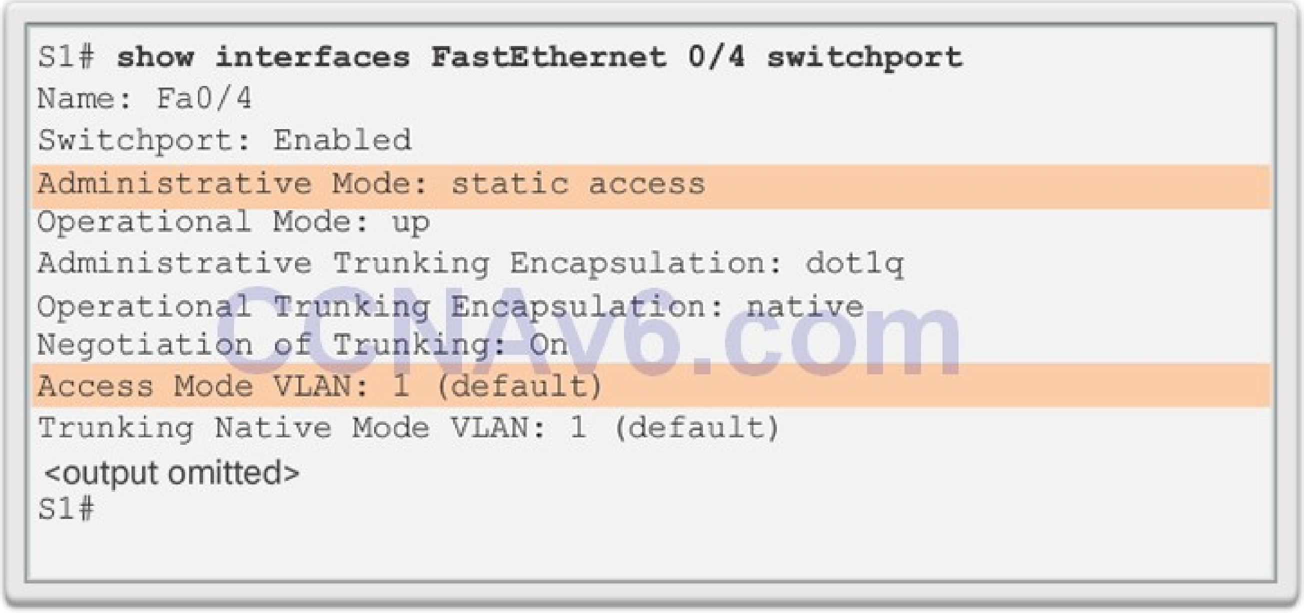


	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Limited Connectivity
Access	Access	Access	Limited Connectivity	Access

2.2 Troubleshoot Multi-VLAN Issues

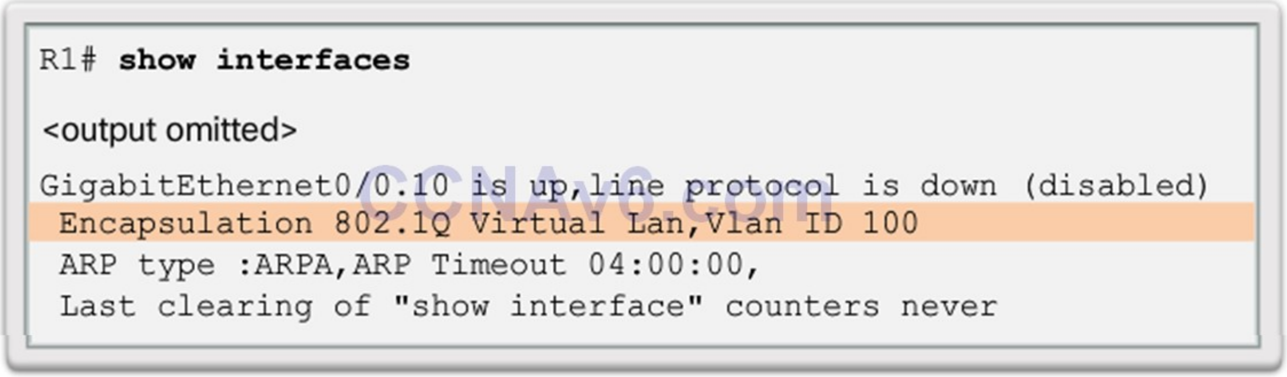
Inter-VLAN Configuration Issues

- To delete a VLAN, use the no vlan vlan-id global configuration mode command.
- If a switch port is not configured for the correct VLAN, devices configured on that VLAN cannot connect to the router interface.
- When a problem is suspected with a switch configuration, use the various verification commands to examine the configuration and identify the problem.



```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
<output omitted>
S1#
```

- Interface Issues
- When enabling inter-VLAN routing on a router, one of the most common configuration errors is to connect the physical router interface to the wrong switch port.
- Verify Routing Configuration
- With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface.
- Using the show interfaces and the show running-config commands can be useful in troubleshooting this type of issue.



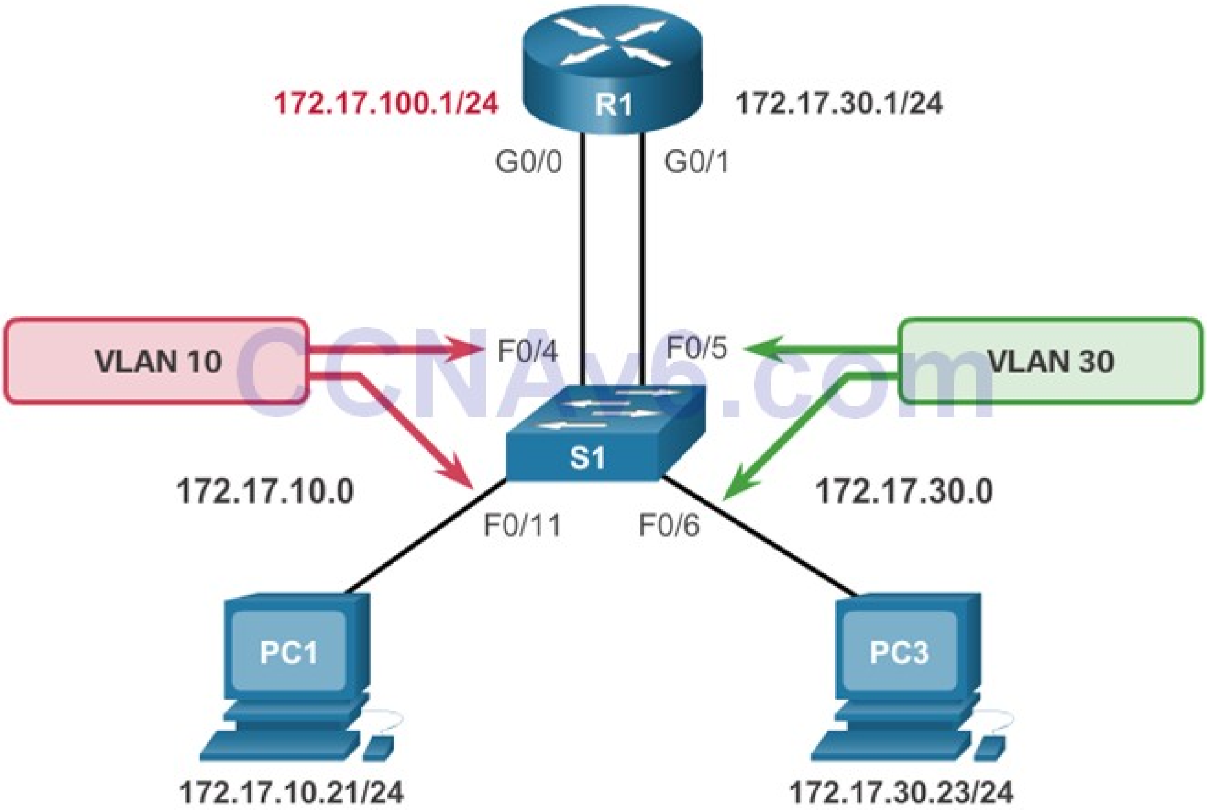
```
R1# show interfaces

<output omitted>

GigabitEthernet0/0.10 is up,line protocol is down (disabled)
 Encapsulation 802.1Q Virtual Lan,Vlan ID 100
 ARP type :ARPA,ARP Timeout 04:00:00,
 Last clearing of "show interface" counters never
```

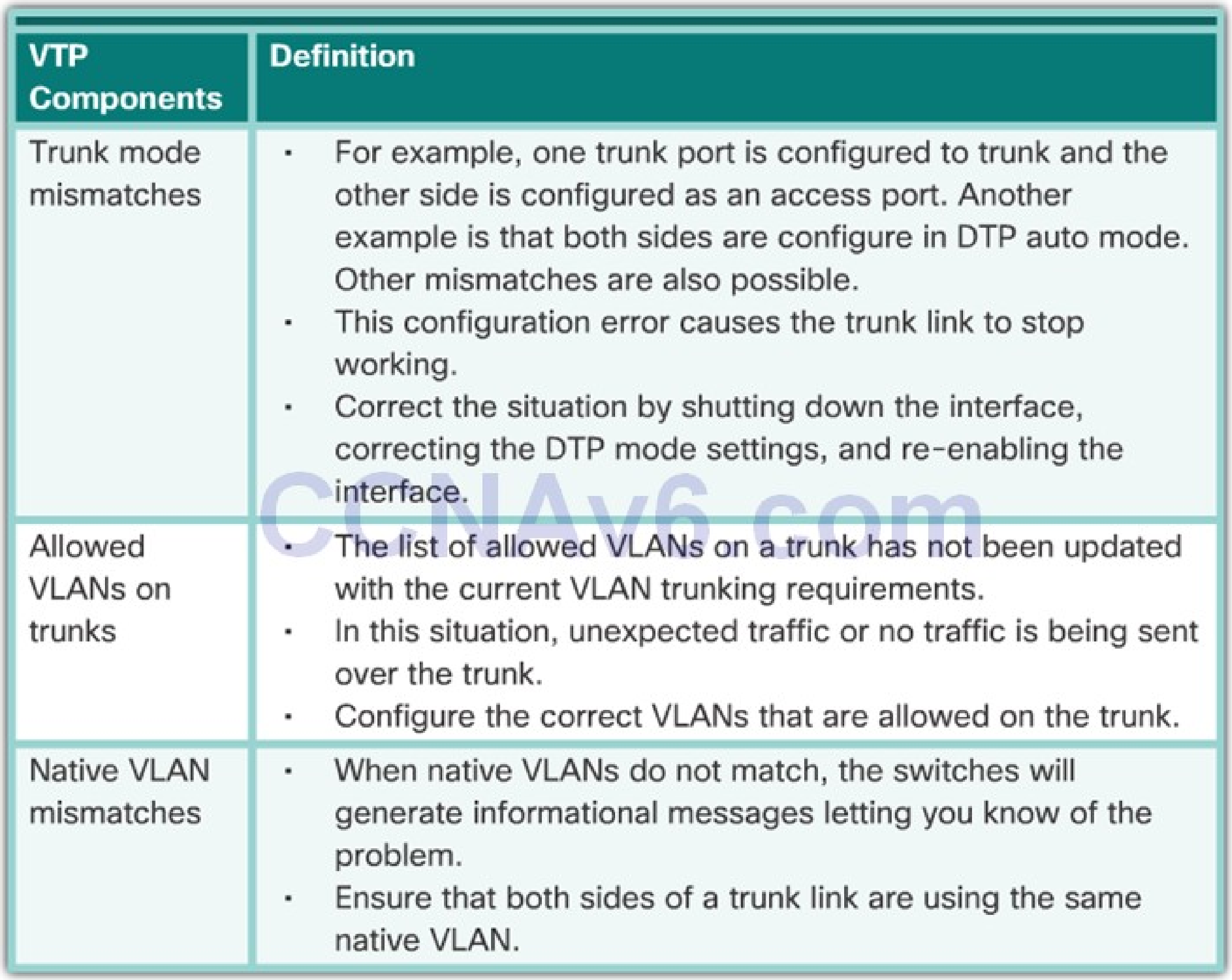
IP Addressing Issues

- IP Addresses and Subnet Masks
- For inter-VLAN routing to operate, a router must be connected to all VLANs, either by separate physical interfaces or by subinterfaces.
- Each interface, or subinterface, must be assigned an IP address that corresponds to the subnet to which it is connected.
- Use the show running-config and show ip interface commands to verify IP address and subnet masks.



VTP and DTP Issues

- Troubleshoot VTP Issues
- There are 5 common problems with VTP:
- Incompatible VTP Versions
- VTP Password Issues
- Incorrect VTP Domain Name
- All Switches Set to Client Mode
- Incorrect Configuration Revision
- Number
- Troubleshoot DTP Issues
- there are three common problems
- associated with trunks.
- Trunk mode mismatches
- Allowed VLANs on trunks
- Native VLAN mismatches

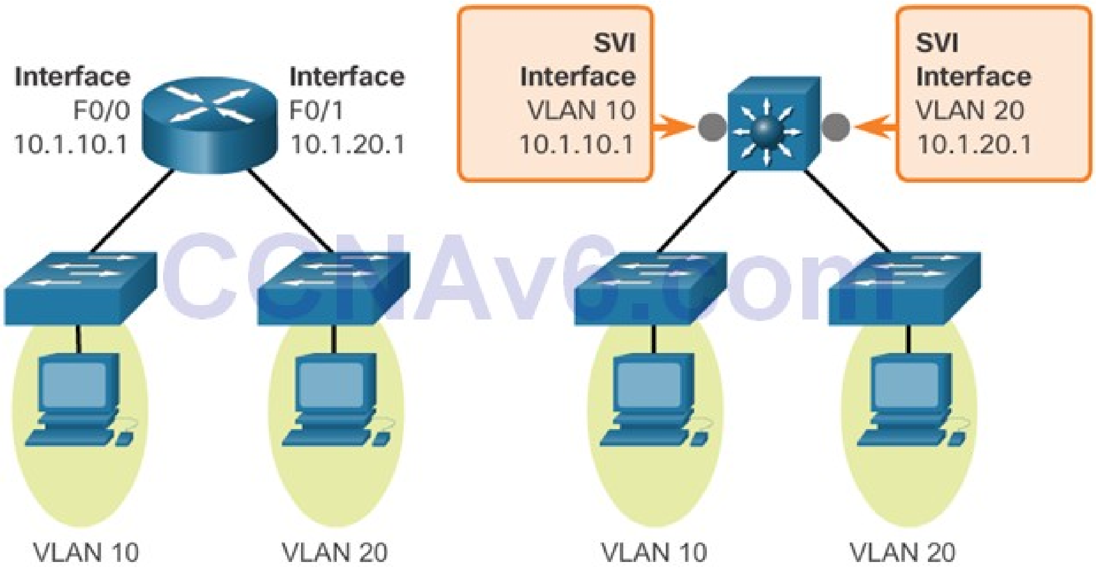


VTP Components	Definition
Trunk mode mismatches	• For example, one trunk port is configured to trunk and the other side is configured as an access port. Another example is that both sides are configure in DTP auto mode. Other mismatches are also possible. • This configuration error causes the trunk link to stop working. • Correct the situation by shutting down the interface, correcting the DTP mode settings, and re-enabling the interface.
Allowed VLANs on trunks	• The list of allowed VLANs on a trunk has not been updated with the current VLAN trunking requirements. • In this situation, unexpected traffic or no traffic is being sent over the trunk. • Configure the correct VLANs that are allowed on the trunk.
Native VLAN mismatches	• When native VLANs do not match, the switches will generate informational messages letting you know of the problem. • Ensure that both sides of a trunk link are using the same native VLAN.

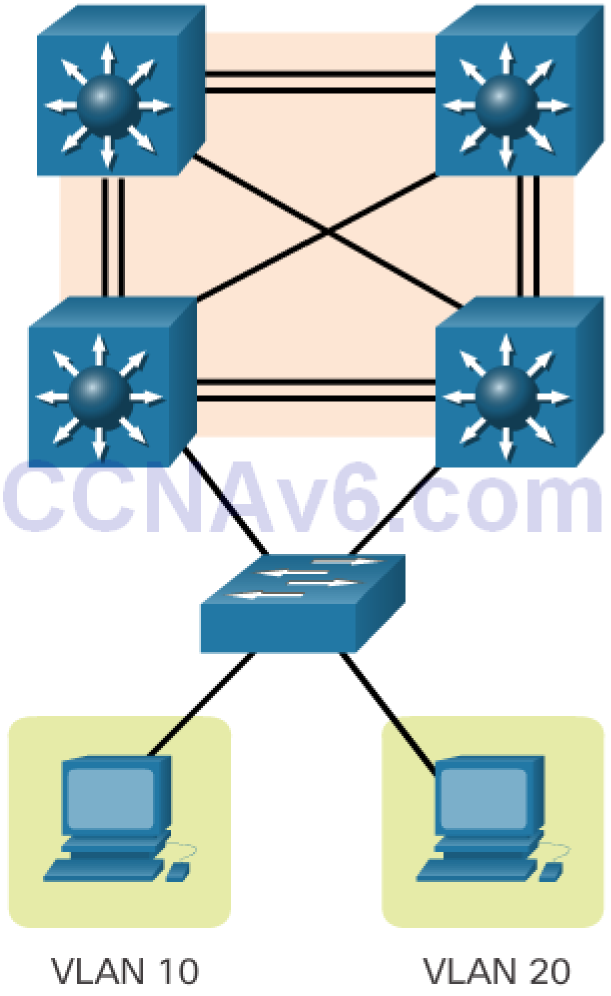
2.3 Layer 3 Switching

Layer 3 Switching Operation and Configuration

- Layer 3 Switching
- Modern enterprise networks use multilayer switches to achieve high-packet processing rates using hardware-based switching.
- Catalyst multilayer switches support the following types of Layer 3 interfaces:
- Routed port
- Switch virtual interface (SVI)
- Inter-VLAN Routing and SVIs
- Routing can be transferred to the core and the distribution layers (and sometimes even the access layer) without impacting network performance.
- An SVI can be created for any VLAN that exists on the switch.
- SVIs are created the first time the VLAN interface configuration mode is entered for a particular VLAN SVI.



- Inter-VLAN Routing with Routed Ports
- A routed port is a physical port that
- acts similarly to an interface on a router.
- A routed port is not associated with
- a particular VLAN.
- Routed ports on a Cisco IOS switch do
- not support subinterfaces.
- Routed ports are used for point-to-point
- links.
- To configure routed ports, use the
- no switchport interface configuration mode
- command on the appropriate ports.



Troubleshoot Layer 3 Switching

- Layer 3 Switch Configuration Issues
- Check the following configurations for accuracy:
- VLANs – VLANs must be defined across all the switches. VLANs must be enabled on the trunk ports. Ports must be in the right VLANs.
- SVIs – SVIs must have the correct IP address or subnet mask. SVIs must be up. Each SVI must match with the VLAN number.
- Routing – Routing must be enabled. Each interface or network should be added to the routing protocol, or static routes entered, where appropriate.
- Hosts – Hosts must have the correct IP address or subnet mask. Hosts must have a default gateway associated with an SVI or routed port.

2.4 Chapter Summary

Summary

- VLAN Trunking Protocol (VTP) reduces administration of VLANs in a switched network. A switch configured as the VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout the domain.
- The three VTP modes are Server, Client and Transparent.
- The configuration revision number is used when determining whether a VTP switch should keep or update its existing VLAN database. A switch will overwrite its existing VLAN database if it receives a VTP update from another switch in the same domain with a higher configuration revision number. Therefore, when a switch is being added to a VTP domain it must have the default VTP configuration or a lower configuration revision number than the VTP server.
- Troubleshooting VTP can also involve dealing with errors caused by incompatible VTP versions and incorrectly configured domain names or passwords.
- Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP), which operates on a point-to-point basis between network devices. DTP is a Cisco proprietary protocol that is automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches. A general best practice when a trunk link is required is to set the interface to trunk and nonegotiate. On links where trunking is not intended, DTP should be turned off.
- When troubleshooting DTP, problems can be related to trunk mode mismatches, allowed VLANS on a trunk, and native VLAN mismatches.
- Layer 3 switching using Switch Virtual Interfaces (SVIs) is a method of inter-VLAN routing that can be configured on Catalyst 2960 switches. An SVI with appropriate IP addressing is configured for each VLAN and provides Layer 3 processing for packets to or from all switch ports associated with those VLANs.
- Another method of Layer 3 inter-VLAN routing is using routed ports. A routed port is a physical port that acts similarly to an interface on a router. Routed ports are mostly configured between switches in the core and distribution layer.
- Troubleshooting inter-VLAN routing with a router or a Layer 3 switch are similar. Common errors involve VLAN, trunk, Layer 3 interface, and IP address configurations.