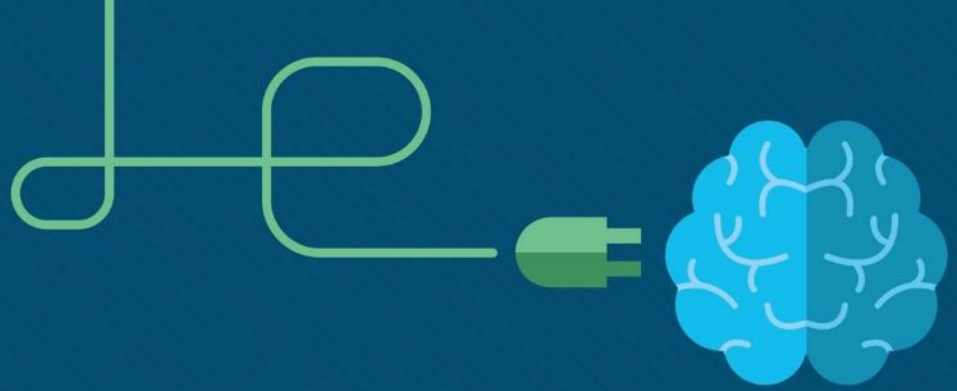


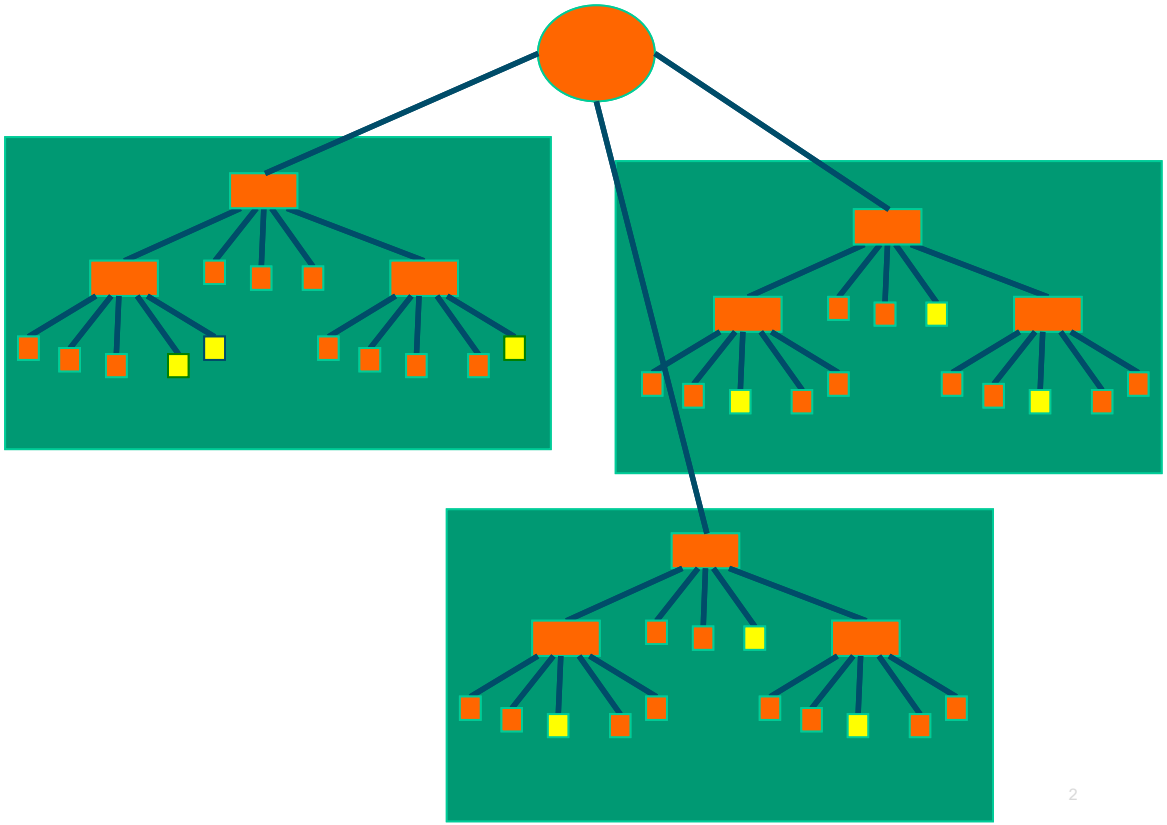
Chapter 2: Scaling VLANs

CCNA Routing and Switching

Scaling Networks v6.0

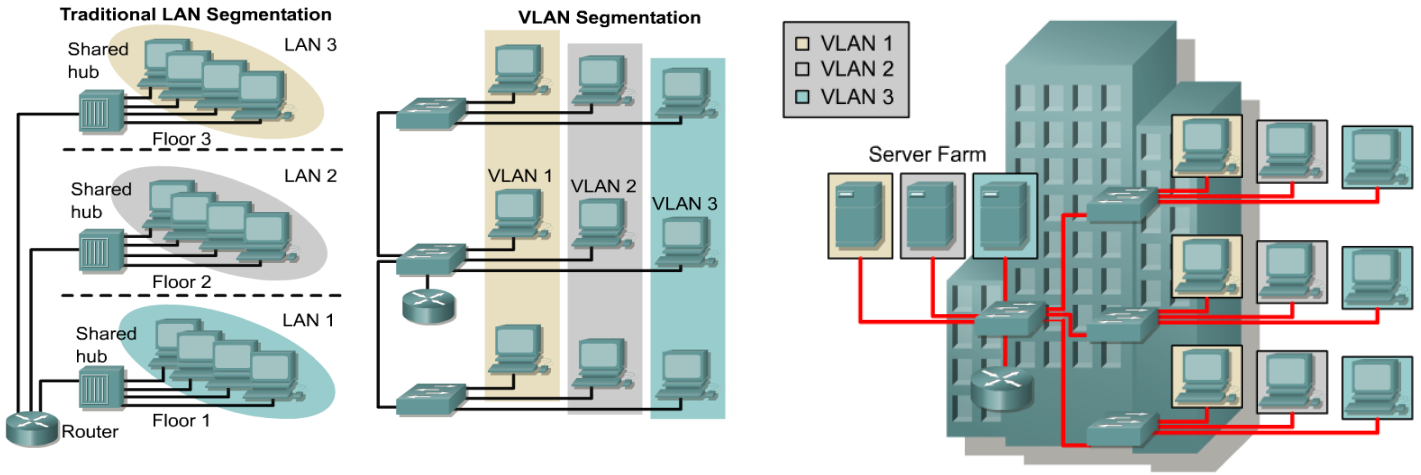
Virtual LANs (VLANs)

- Allows us to split switches into separate (virtual) switches
- Only members of a VLAN can see that VLAN's traffic
- Inter-VLAN traffic must be routed (i.e. go through a router) because they are separate subnets



VLAN introduction

- **VLANs provide segmentation based on broadcast domains.**
- VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.
- All workstations and servers used by a particular workgroup share the same VLAN, regardless of the physical connection or location.

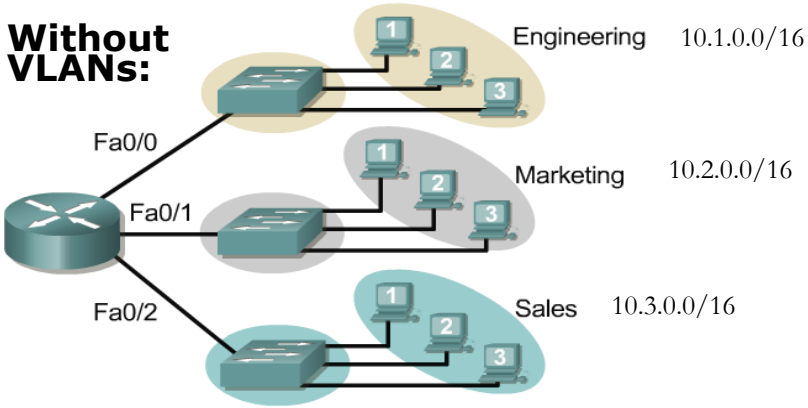


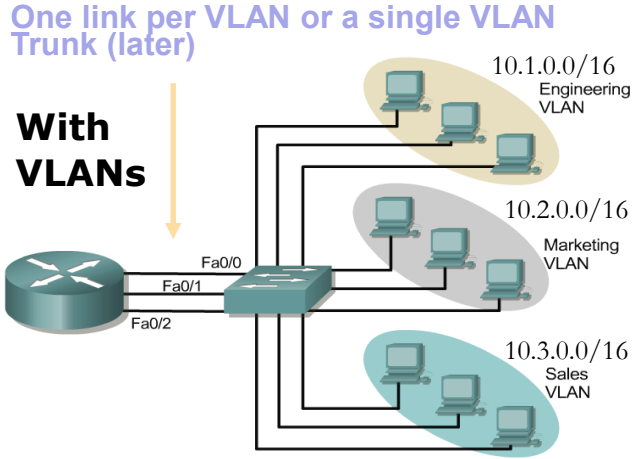
Local VLANs

- 2 VLANs or more within a single switch
- VLANs address scalability, security, and network management. Routers in VLAN topologies provide broadcast filtering, security, and traffic flow management.
- ***Edge ports***, where end nodes are connected, are configured as members of a VLAN
- The switch behaves as several virtual switches, sending traffic only within VLAN members.
- Switches may not bridge any traffic between VLANs, as this would violate the integrity of the VLAN domain.
- Traffic should only be routed between VLANs.

Broadcast domains with VLANs and routers

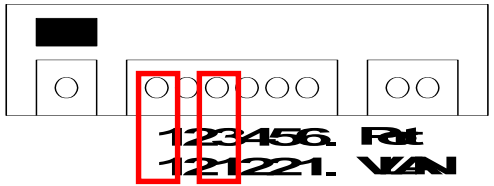
- Without VLANs, each group is on a different IP network and on a different switch.
- Using VLANs. Switch is configured with the ports on the appropriate VLAN. Still, each group on a different IP network; however, they are all on the same switch.
- What are the broadcast domains in each?

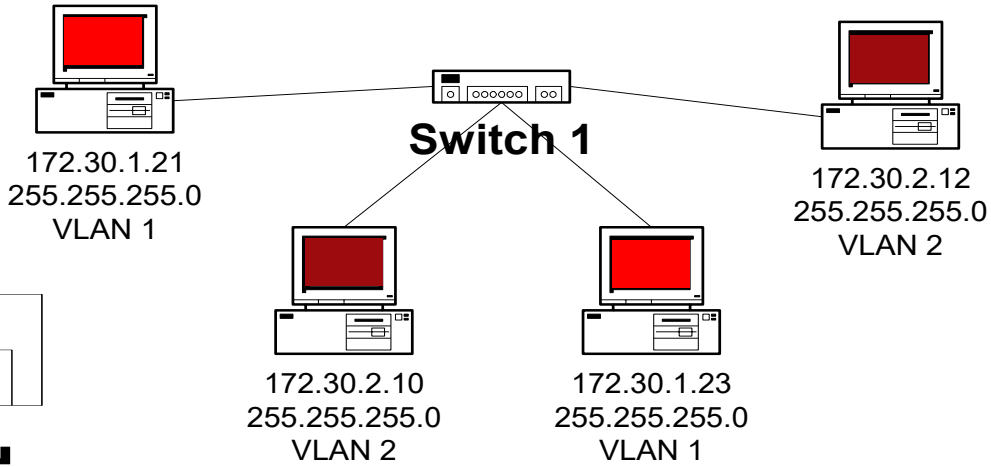




VLANs

- VLANs are assigned to switch ports.
- There is no “VLAN” assignment done on the host.
- In order for a host to be a part of that VLAN, it must be assigned an IP address that belongs to the proper subnet.
- *Remember:* ***VLAN = Subnet***



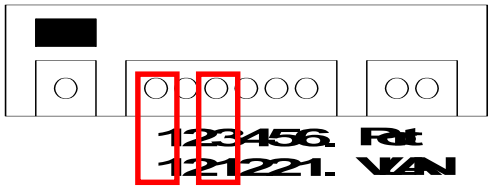


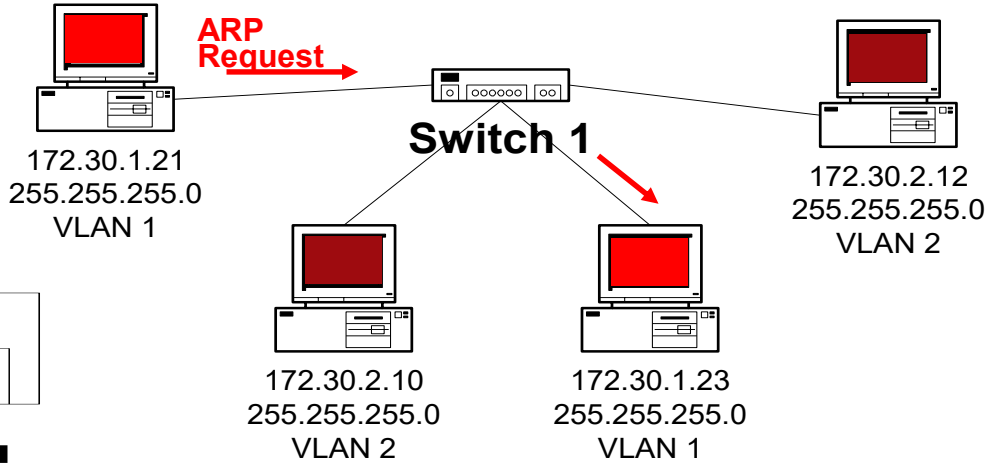
Two **VLANs** = Two **subnets**

- Two Subnets

VLANs

- VLANs separate broadcast domains == subnets.
  - e.g. without VLAN the ARP would be seen on all subnets.
- Assigning a host to the correct VLAN is a 2-step process:
  - Connect the host to the correct port on the switch.
  - Assign to the host the correct IP address depending on the VLAN membership





Two **VLANs** = Two **subnets**

- Two Subnets

Good reasons to use VLANs

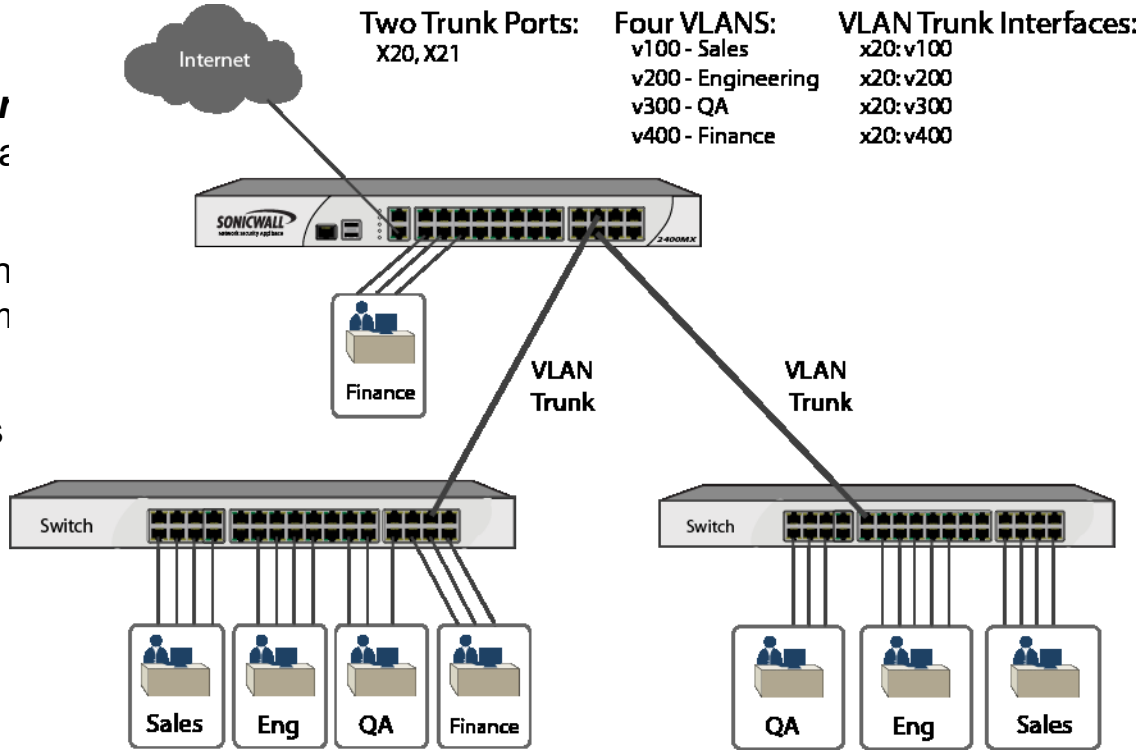
- You want to segment your network into multiple subnets, but can't buy enough switches
  - Hide sensitive infrastructure like IP phones, building controls, etc.
- Separate control traffic from user traffic
  - Restrict who can access your switch management address

Bad reasons to use VLANs

- Because you can, and you feel cool ☺
- Because they will completely secure your hosts (or so you think)
- Because they allow you to extend the same IP network over multiple separate buildings

VLANs across switches

- Two switches can exchange traffic from one or more VLANs
- Inter-switch links are configured as ***trun*** carrying frames from all or a subset of a VLANs
  - Trunking is the point to point connection more than one Ethernet switch and som network devices like switch or a router.
- Each frame carries a ***tag*** that identifies VLAN it belongs to



VLANS increase complexity

- You can no longer “just replace” a switch
  - Now you have VLAN configuration to maintain
  - Field technicians need more skills
- You have to make sure that all the switch-to-switch trunks are carrying all the necessary VLANs
  - Need to keep in mind when adding/removing VLANs
- Do not build “VLAN spaghetti”
  - Extending a VLAN to multiple buildings across trunk ports
  - Bad idea because:
    - Broadcast traffic is carried across all trunks from one end of the network to another
    - Broadcast storm can spread across the extent of the VLAN
    - Maintenance and troubleshooting nightmare

2.1 VTP, Extended VLANs, and DTP

VTP Overview

- As the number of switches increases on a small or medium-sized business network, the overall administration required to manage virtual local area networks (VLANs) and trunks in the network becomes challenging.
- VLAN Trunking Protocol (VTP) reduces administration in a switched network.
- A switch in VTP server mode can manage additions, deletions, and renaming of VLANs across the domain.
- For example, when a new VLAN is added on the VTP server, the VLAN information is distributed to all switches in the domain.
- This eliminates the need to configure the new VLAN on every switch.
- VTP is a Cisco proprietary protocol that is available on most of the Cisco Catalyst Series products.

VTP Overview

- VLAN trunking protocol (VTP) allows a network administrator to manage VLANs on a switch configured as a VTP server.
- The VTP server distributes and synchronizes VLAN information over trunk links to VTP-enabled switches throughout the switched network.

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.

Note: VTP advertisements will not be exchanged if the trunk between the switches is inactive or if the trunk is misconfigured.

VTP Modes

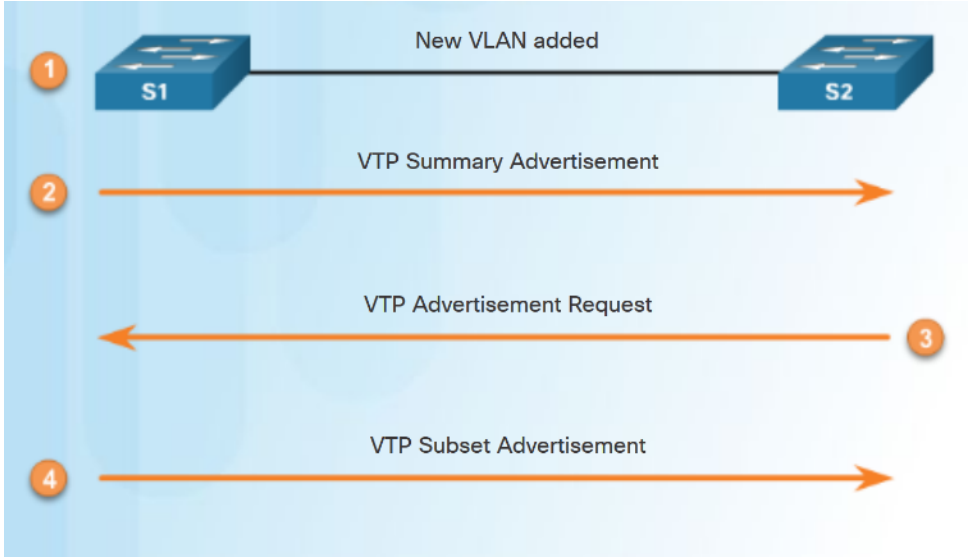
VTP Mode	Definition
VTP Server	• VTP servers advertise the VTP domain VLAN information to other VTP-enabled switches in the same VTP domain. • VTP servers store the VLAN information for the entire domain in NVRAM. • Switches configured in VTP server mode are allowed to create, delete, or rename VLANs for the domain.
VTP Client	• VTP clients function the same way as VTP servers, but you cannot create, change, or delete VLANs on a VTP client. • A VTP client only stores the VLAN information for the entire domain while the switch is on. • A switch reset deletes the VLAN information. • You must configure VTP client mode on a switch.
VTP Transparent	• Transparent switches do not participate in VTP except to forward VTP advertisements to VTP clients and VTP servers. • VLANs that are created, renamed, or deleted on transparent switches are local to that switch only. • To create an extended VLAN, a switch must be configured as a VTP transparent switch when using VTP versions 1 or 2.

VTP Modes (Cont.)

VTP Question	VTP Server	VTP Client	VTP Transparent
What are the differences?	• Manages domain and VLAN configuration. • Multiple VTP servers can be configured.	• Updates local VTP configurations. • VTP client switches cannot change VLAN configurations.	• Manages local VLAN configurations. • VLAN configurations are not shared with VTP network.
Does it respond to VTP advertisements?	Participates fully	Participates fully	Only forwards VTP advertisements
Is the global VLAN configuration preserved on restart?	Yes, global configurations are stored in NVRAM	No, global configurations are stored in RAM only	No, local VLAN configuration is only stored in NVRAM
Does it update other VTP-enabled switches?	Yes	Yes	No

VTP Advertisements

- Three types of VTP Advertisements:
  - **Summary advertisements** – contain VTP domain name and configuration revision number.
  - **Advertisement request -** response to a summary advertisement message when the summary advertisement contains a higher configuration revision number than the current value.
  - **Subset advertisements -** contain VLAN information including any changes.



Default VTP configuration

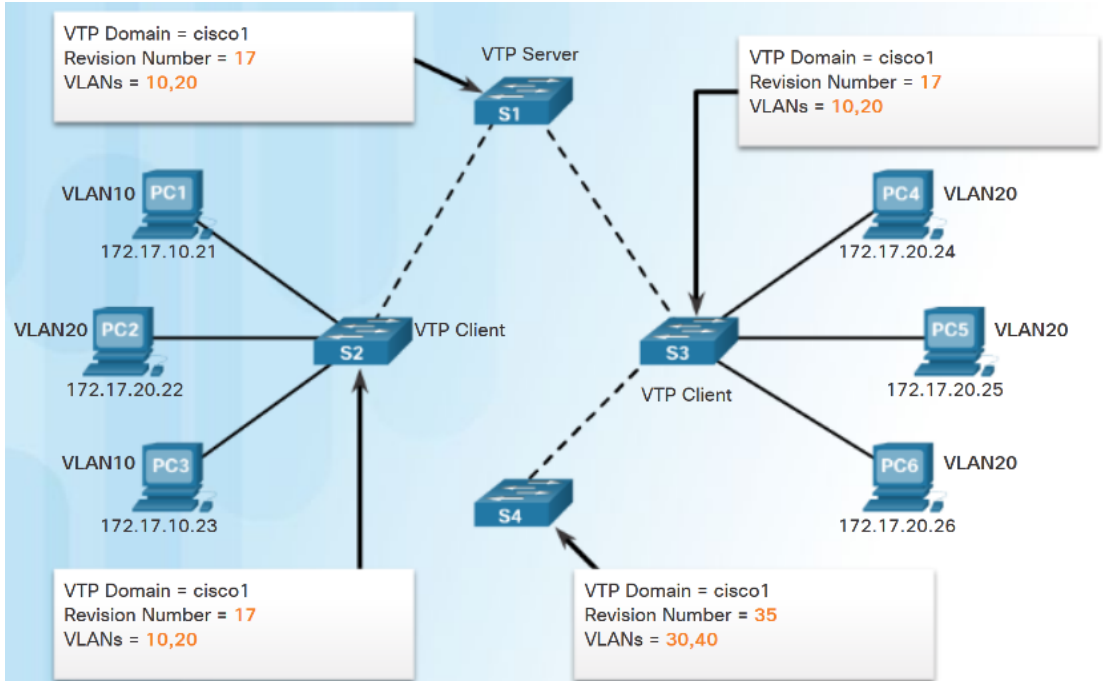
Verify Default VTP Status

```
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 **show vtp status** command displays the VTP status which includes the following:
  - VTP Version capable and running
  - VTP Domain Name
  - VTP Pruning Mode
  - VTP Traps Generation
  - Device ID
  - Configuration Last Modified
  - VTP Operating Mode
  - Maximum VLANs Supported Locally
  - Number of Existing VLANs
  - Configuration Revision
  - MD5 Digest

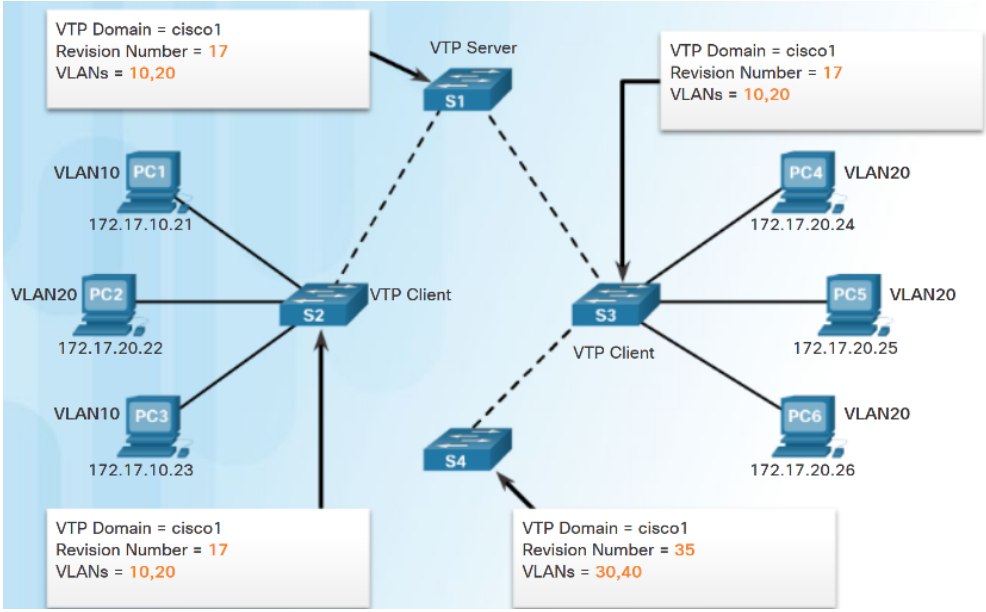
VTP Caveats

- VTP configuration revision number is stored in NVRAM.
- To reset VTP configuration revision number to zero:
  - Change the switch's VTP domain to a nonexistent VTP domain and then change the domain back to the original name.
  - Change the switch's VTP mode to transparent and then back to previous VTP mode.

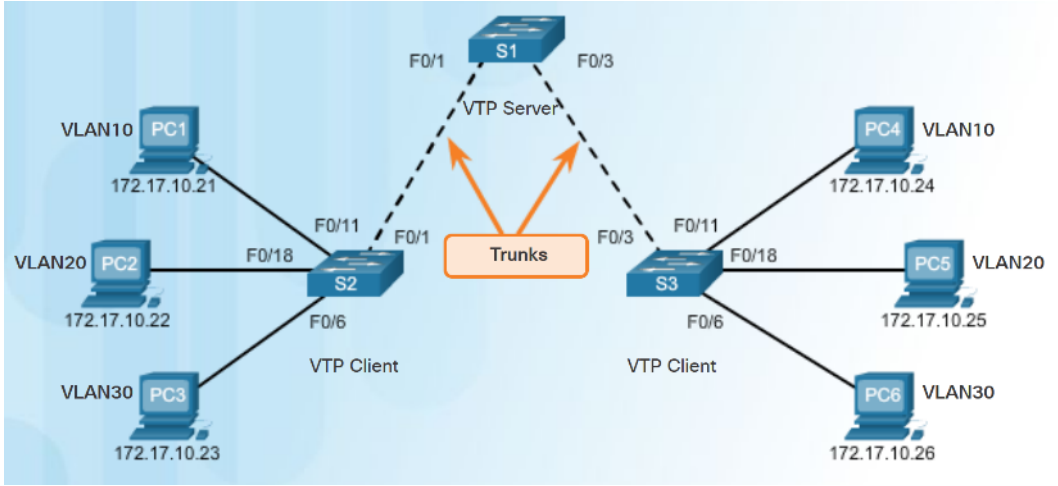


VTP Caveats (Cont.)

- See graphic:
  - S4 is added. The startup config has not been erased and VLAN.DAT file on S4 has not been deleted. S4 has the same VTP domain name configured as other two switches but its revision number is 35, which is higher than the revision number on the other two switches.
  - S4 has VLAN 1 and is configured with VLAN 30 and 40. S4 does not have VLANs 10 and 20 in its database. Because S4 has a higher revision number, the rest of the switches in the domain will sync to S4's revision.
  - Consequence is VLANs 10 and 20 will no longer exist on the switches, leaving clients that are connected to ports belonging to those non-existing VLANs without connectivity.



VTP Configuration Overview



- Steps to Configure VTP:
  - **Step 1** - Configure the VTP Server
  - **Step 2** - Configure the VTP Domain Name and Password
  - **Step 3** - Configure the VTP Clients
  - **Step 4** - Configure VLANs on the VTP Server.
  - **Step 5** - Verify the VTP clients have received the new VLAN information.

Step 1 – Configure the VTP Server

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# vtp mode ?
  client           Set the device to client mode.
  off              Set the device to off mode.
  server           Set the device to server mode.
  transparent      Set the device to transparent mode.

S1(config)# vtp mode server
Setting device to VTP Server mode for VLANS.
S1(config)# end
S1#
```

```
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
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode                  : Server
Maximum VLANs supported locally     : 255
Number of existing VLANs            : 5
Configuration Revision              : 0
MD5 digest                          : 0x57 0xCD 0x40 0x65 0x63 0x59 0x47 0xBD
                                      0x56 0x9D 0x4A 0x3E 0xA5 0x69 0x35 0xBC

S1#
```

- Use the **vtp mode server** command to configure a switch as a VTP server.
  - Confirm all switches are configured with default configuration before issuing this command to avoid problems with configuration revision numbers.
- Use the **show vtp status** to verify.
  - Notice configuration revision number is still set to 0 and number of existing VLANS is 5.
  - The 5 VLANs are the default VLAN 1 and VLANs 1002-1005.

Step 2 – Configure the VTP Domain Name and Password

- Use the **vtp domain** *domain-name* command to configure the domain name.
  - VTP client must have same domain name as the VTP server before it will accept VTP advertisements.
- Configure a password using the **vtp password** *password* command.
  - Use the **show vtp password** command to verify.

```
S1(config)# vtp domain ?
  WORD The ascii name for the VTP administrative domain.

S1(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 02:55:42.768: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG:
VTP domain name changed to CCNA.
S1(config)#
```

```
S1(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S1(config)# end
S1# show vtp password
VTP Password: cisco12345
S1#
```

Step 3 – Configure the VTP Clients

```
S2(config)# vtp mode client
Setting device to VTP Client mode for VLANS.
S2(config)# vtp domain CCNA
Changing VTP domain name from NULL to CCNA
*Mar 1 00:12:22.484: %SW_VLAN-6-VTP_DOMAIN_NAME_CHG: VTP domain name changed to CCNA.
S2(config)# vtp password cisco12345
Setting device VTP password to cisco12345
S2(config)#
```

- Use the **vtp mode client** command to configure the VTP clients.
- Use same domain name and password as VTP server.

Step 4 – Configure VLANs on the VTP Server

- Use the **vlan** *vlan-number* command to create VLANs.
- Use **show vlan brief** to verify the VLANs.
- Use **show vtp status** to verify server status.
  - Every time a VLAN is added the configuration register is incremented

```
S1(config)# vlan 10
S1(config-vlan)# name SALES
S1(config-vlan)# vlan 20
S1(config-vlan)# name MARKETING
S1(config-vlan)# vlan 30
S1(config-vlan)# name ACCOUNTING
S1(config-vlan)# end
S1#
```

```
S1# show vlan brief

VLAN Name                Status    Ports
---- ------------------- --------- -------------------------
1    default             active    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
S1#
```

```
S1# show vtp status
VTP Version capable             : 1 to 3
VTP version running             : 1
VTP Domain Name                 : CCNA
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 02:02:45
Local updater ID is 0.0.0.0 (no valid interface found)

Feature VLAN:
--------------
VTP Operating Mode              : Server
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
Configuration Revision          : 6
MD5 digest                      : 0xFE 0x8D 0x2D 0x21 0x3A 0x30 0x99 0xC8
                                  0xDB 0x29 0xBD 0xE9 0x48 0x70 0xD6 0xB6

S1#
```

VTP Configuration

Step 5 – Verify that the VTP Clients Have Received the New VLAN Information

- Use the **show vlan brief** command to verify that the client received the new VLAN information.
- Verify client status using the **show vtp status** command.

```
S2# show vtp status
VTP Version capable             : 1 to 3
VTP Version running             : 1
VTP Domain Name                 : CCNA
VTP Pruning Mode                : Disabled
VTP Traps Generation            : Disabled
Device ID                       : b07d.4729.2400
Configuration last modified by 0.0.0.0 at 3-1-93 02:02:45

Feature VLAN:
--------------
VTP Operating Mode              : Client
Maximum VLANs supported locally : 255
Number of existing VLANs        : 8
Configuration Revision          : 6
MD5 digest                      : 0xFE 0x8D 0x2D 0x21 0x3A 0x30 0x99 0xC8
                                  0xDB 0x29 0xBD 0xE9 0x48 0x70 0xD6 0xB6

S2#
```

```
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#
```

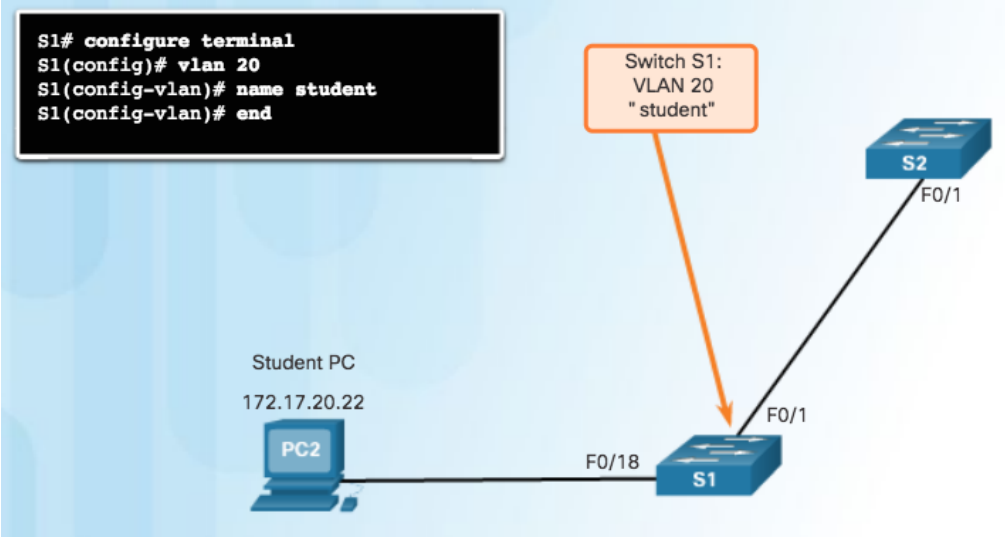
VLAN Ranges on Catalyst Switches

- Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.
- Normal range VLANs are numbered 1 to 1,005.
  - Stored in vlan.dat file
- Extended range VLANs are numbered 1,006 to 4,094.
  - Not stored in vlan.dat file
  - VTP does not learn

```
Switch# 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
                                   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
```

Type	Definition
Normal range VLANs	• Used in small- and medium-sized business and enterprise networks. • Identified by VLAN IDs between 1 and 1005. • IDs 1 and 1002 to 1005 are automatically created and cannot be removed. (IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface [FDDI] VLANs.) • Configurations are stored within a VLAN database file called **vlan.dat**, which is stored in flash memory.
Extended range VLANs	• Used by service providers and large organizations to extend their infrastructure to a greater number of customers. • Identified by a VLAN ID between 1006 and 4094. • Support fewer VLAN features than normal range VLANs. • Configurations are saved in the running configuration file.

Creating a VLAN



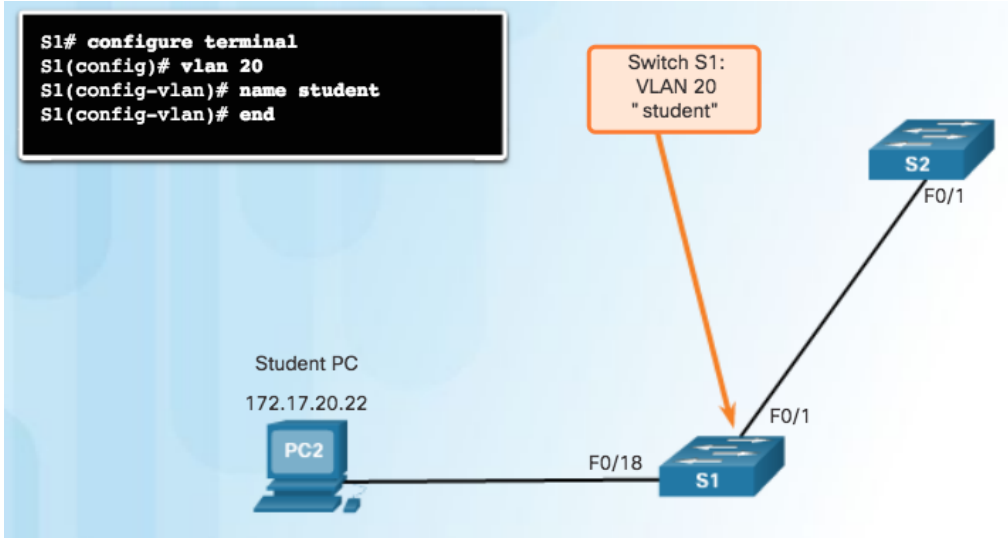
- Normal range VLANs are stored in flash in vlan.dat
- Use **vlan** *vlan-id* to create a VLAN
  - Use **name** *vlan-name to name the VLAN*
  - Naming each VLAN is considered a best practice in switch configuration.
- To configure multiple VLANs, a series of VLAN IDs can be entered separated by commas, or a range of VLAN IDs separated by hyphens.
  - **vlan 100,102,105-107**

Assigning Ports to VLANs

- Access port can belong to only one VLAN at a time.
  - Only exception is when an IP phone is connected to the port. Then there are two VLANs associated with the port: one for voice and one for data.

Note: Use the **interface range** command to simultaneously configure multiple interfaces.

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

```
S1# show vlan name student

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------
20   student                           active    Fa0/11, Fa0/18

VLAN Type  SAID       MTU   Parent RingNo BridgeNo Stp  BrdgMode Trans1 Trans2
---- ----- ---------- ----- ------ ------ -------- ---- -------- ------ ------
20   enet  100020     1500  -      -      -        -    -        0      0

Remote SPAN VLAN
----------------
Disabled

Primary Secondary Type              Ports
------- --------- ----------------- ------------------------

S1# show vlan summary
Number of existing VLANs              : 7
Number of existing VTP VLANs          : 7
Number of existing extended VLANS     : 0

S1#
```

- Commands to verify VLANs:
  - **show vlan**
  - **show interfaces**
  - **show vlan name** *vlan-name*
  - **show vlan brief**
  - **show vlan summary**
  - **show interfaces vlan** *vlan-id*

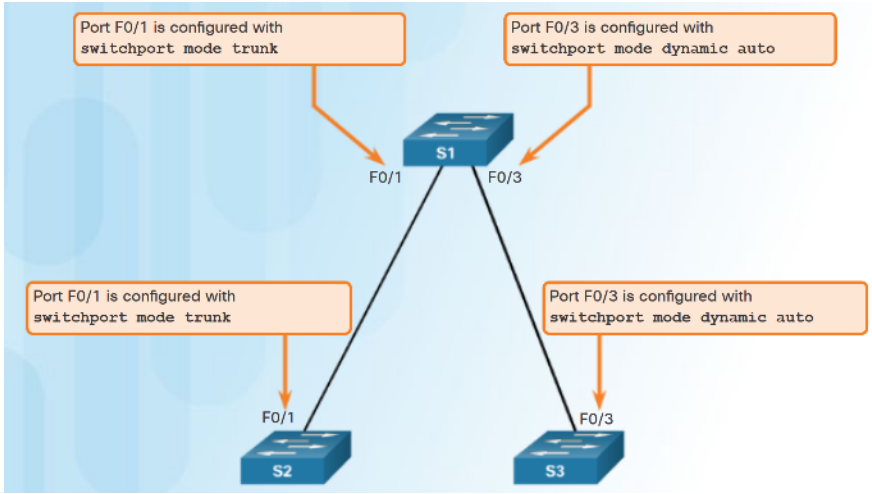
Configuring Extended VLANs

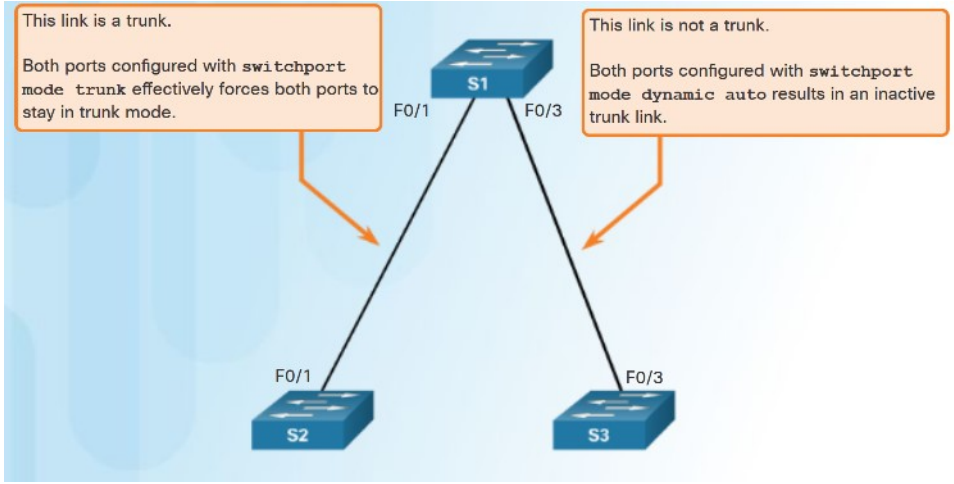
```
S1(config)# vtp mode transparent
Setting device to VTP Transparent mode for VLANS.
S1(config)# vlan 2000
S1(config-vlan)# end
S1#
```

```
S1# show vlan brief

VLAN  Name                      Status    Ports
----  ------------------------- --------- -------------------------------
1     default                   active    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
1002 fddi-default              act/unsup
1003 token-ring-default        act/unsup
1004 fddinet-default           act/unsup
1005 trnet-default             act/unsup
2000 VLAN2000                  active
S1#
```

- Extended range VLANs are identified by a VLAN ID between 1006 and 4094.
- To configure an extended VLAN on a 2960 switch it must be set to VTP transparent mode. (By default 2960 switches do not support Extended range VLANs.)

Introduction to DTP





- Trunk negotiation is managed by the Dynamic Trunking Protocol (DTP)
  - DTP is a Cisco proprietary protocol
  - automatically enabled on Catalyst 2960 and Catalyst 3560 Series switches.
- To enable trunking from a Cisco switch to a device that does not support DTP, use the **switchport mode trunk** and **switchport nonegotiate**

Negotiated Interface Modes

- Different trunking modes:
  - **Switchport mode access** - interface becomes a nontrunk interface.
  - **Switchport mode dynamic auto** - interface becomes a trunk if the neighboring interface is set to trunk or desirable mode.
  - **Switchport mode dynamic desirable** - interface becomes a trunk if the neighboring interface is set to trunk, desirable, or dynamic auto mode.
  - **Switchport mode trunk** - interface becomes a trunk even if the neighboring interface is not a trunk interface.
  - **Switchport nonegotiate** - prevents the interface from generating DTP frames.

	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

```
S1# show dtp interface f0/1
DTP information for FastEthernet0/1:
  TOS/TAS/TNS:                              TRUNK/ON/TRUNK
  TOT/TAT/TNT:                              802.1Q/802.1Q/802.1Q
  Neighbor address 1:                       0CD996D23F81
  Neighbor address 2:                       000000000000
  Hello timer expiration (sec/state):       12/RUNNING
  Access timer expiration (sec/state):      never/STOPPED
  Negotiation timer expiration (sec/state): never/STOPPED
  Multidrop timer expiration (sec/state):   never/STOPPED
  FSM state:                                S6:TRUNK
  # times multi & trunk                     0
  Enabled:                                  sim
  In STP:                                   no

<output omitted>
```

- Configure trunk links statically whenever possible.
- Use **show dtp interface** to verify DTP.

2.2 Troubleshoot Multi-VLAN Issues

Deleting VLANs

Assume S1 has VLANs 10, 20, and 99 configured, VLAN 99 is assigned to ports Fa0/18 through Fa0/24.

```
S1# conf t
Enter configuration commands, one per line. End with CNTL/Z.
S1(config)# no vlan 99
S1(config)# exit
S1# show vlan id 99
VLAN id 99 not found in current VLAN database
S1#
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, Gig0/1, Gig0/2
10   VLAN0010            active
20   VLAN0020            active
1002 fddi-default        active
1003 token-ring-default  active
1004 fddinet-default     active
1005 trnet-default       active
S1#
```

- Deleting a VLAN from a switch that is in VTP server mode removes the VLAN from all switches in the VTP domain.

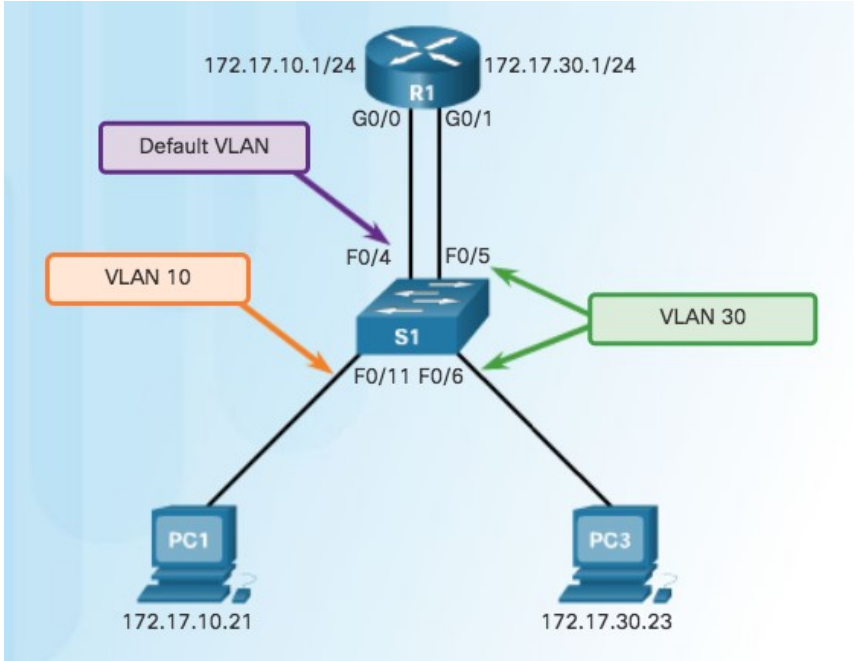
Note: You cannot delete the default VLANs (i.e., VLAN 1, 1002 - 1005).

- Use the **no vlan** *vlan-id* global configuration mode command to delete a VLAN.
- Any ports assigned to that VLAN become inactive. They remain inactive until assigned to a new VLAN.

Switch Port Issues

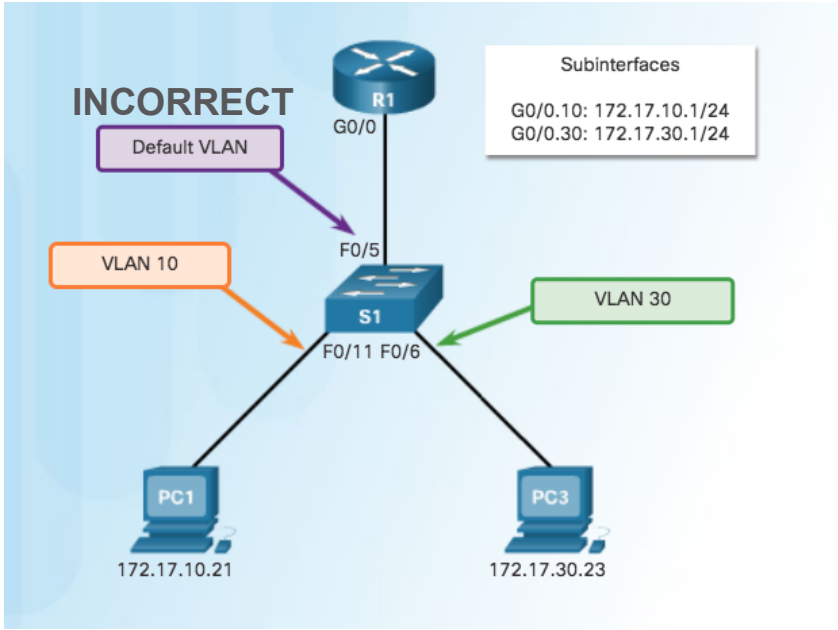
- When using the legacy routing model for inter-VLAN routing, the switch ports connected to the router interfaces must be configured with the correct VLANs.

- S1 F0/4 is in the default VLAN
- Must be in access mode, VLAN 10



Switch Port Issues (Cont.)

- When using the router-on-a-stick routing model the interface on the switch connected to the router must be configured as a trunk port.



- Interface F0/5 on switch S1 is not configured as a trunk and is left in the default VLAN for the port

Verify Switch Configuration

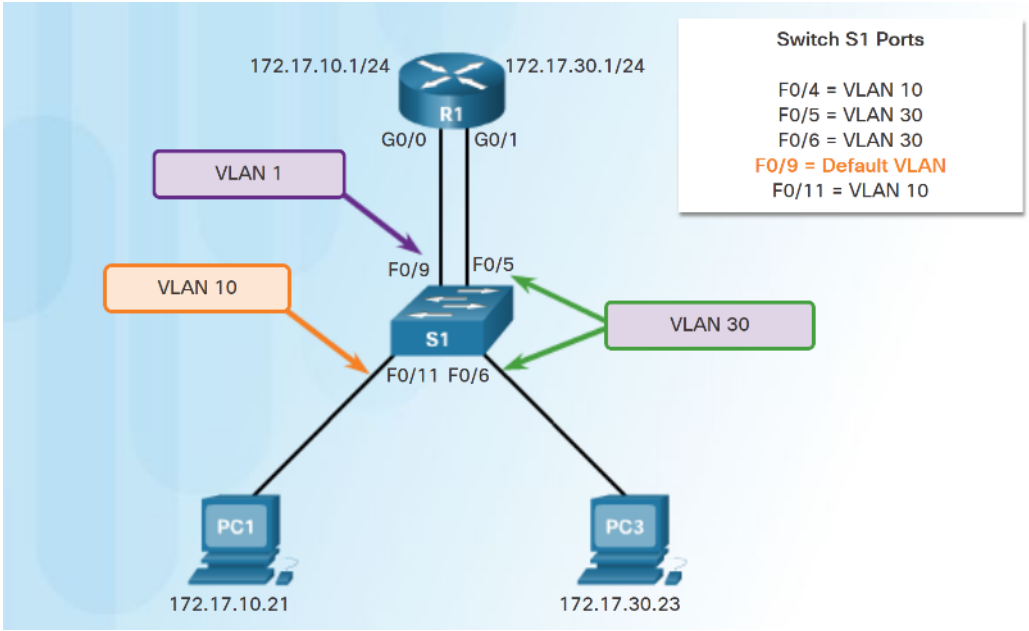
```
S1# show interfaces FastEthernet 0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: up
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native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

S1#
```

- Commands to verify switch configuration:
  - **show interfaces** *interface-id* **switchport**
  - **show running-config**

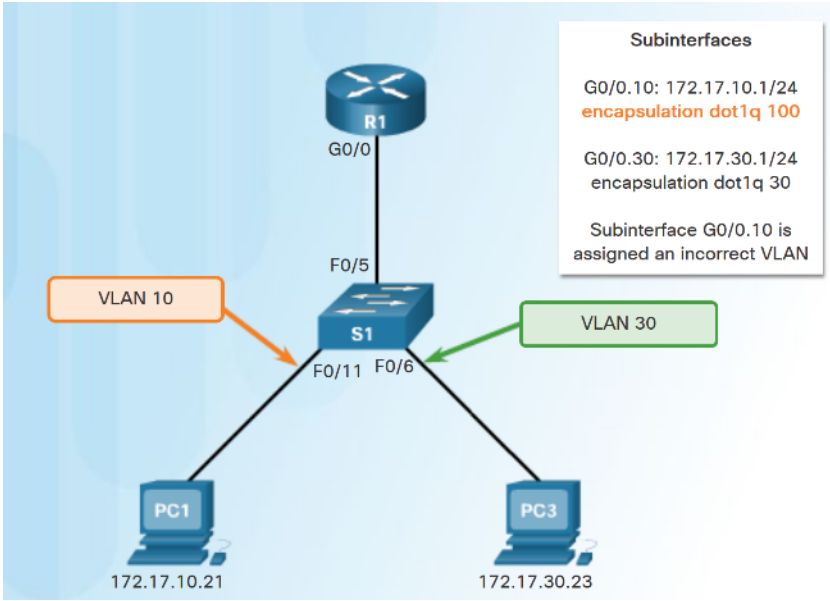
```
S1# show interfaces f0/4 switchport
Name: Fa0/4
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native

<output omitted>
S1#
S1# show run
Building configuration...

<output omitted>
!
interface FastEthernet0/4
switchport mode access
!

<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.



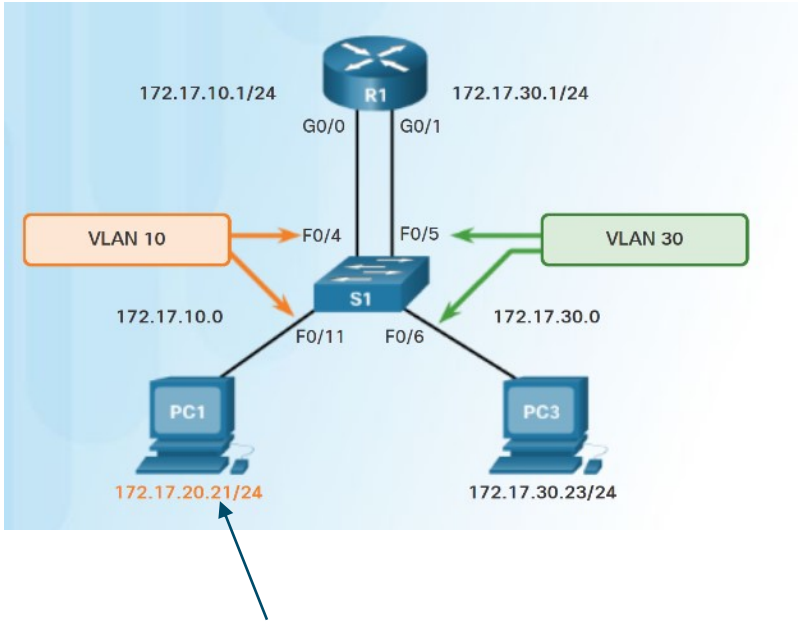
Verify Routing Configuration



- With router-on-a-stick configurations, a common problem is assigning the wrong VLAN ID to the subinterface.
- Use **show interfaces** and the **show running-config** commands to verify the routing configurations.

```
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

<output omitted>
R1# show run
Building configuration...
Current configuration : 505 bytes

!
<output omitted>
interface GigabitEthernet0/0.10
  encapsulation dot1Q 100
  ip address 172.17.10.1 255.255.255.0
!
interface GigabitEthernet0/0.30
```

Errors with IP Addresses and Subnet Masks



Incorrect IP address

- 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.
- Each PC must be configured with an IP address within the VLAN it is assigned to.

Verifying IP Address and Subnet Mask Configuration Issues

- A common error is to incorrectly configure an IP address for a subinterface.
  - Use **show run** and s**how ip interface** to verify IP addressing.
- Another error is incorrectly addressing the end device.
  - Use **ipconfig** to verify the address on a Windows PC

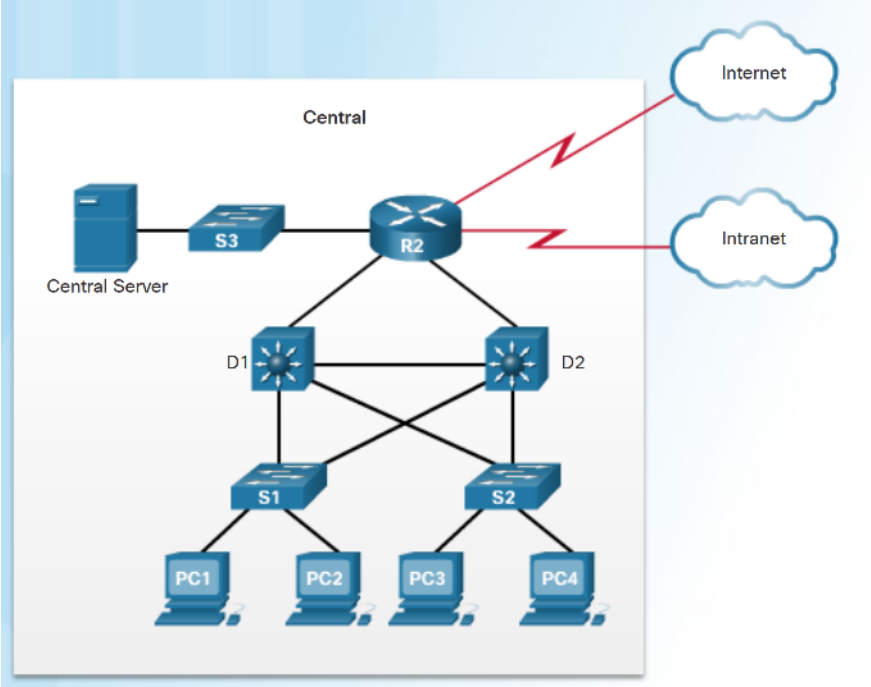
```
R1# show run
Building configuration...
<output omitted>
!
interface GigabitEthernet0/0
 no ip address
 duplex auto
 speed auto
!
interface GigabitEthernet0/0.10
 encapsulation dot1Q 10
 ip address 172.17.20.1 255.255.255.0
!
interface GigabitEthernet0/0.30

<output omitted>
R1#
R1# show ip interface

<output omitted>
GigabitEthernet0/0.10 is up, line protocol is up
  Internet address is 172.17.20.1/24
  Broadcast address is 255.255.255.255
```

```
Packet Tracer PC Command Line 1.0
PC1> ip config
Invalid Command.

PC1> ipconfig

IP Address.....................: 172.17.20.21
Subnet Mask....................: 255.255.255.0
Default Gateway................: 172.17.10.1

PC1>
```

This PC1 should be in the VLAN 10 subnet
So this should be: 172.17.10.21 with a subnet mask of 255.255.255.0

2.3 Layer 3 Switching

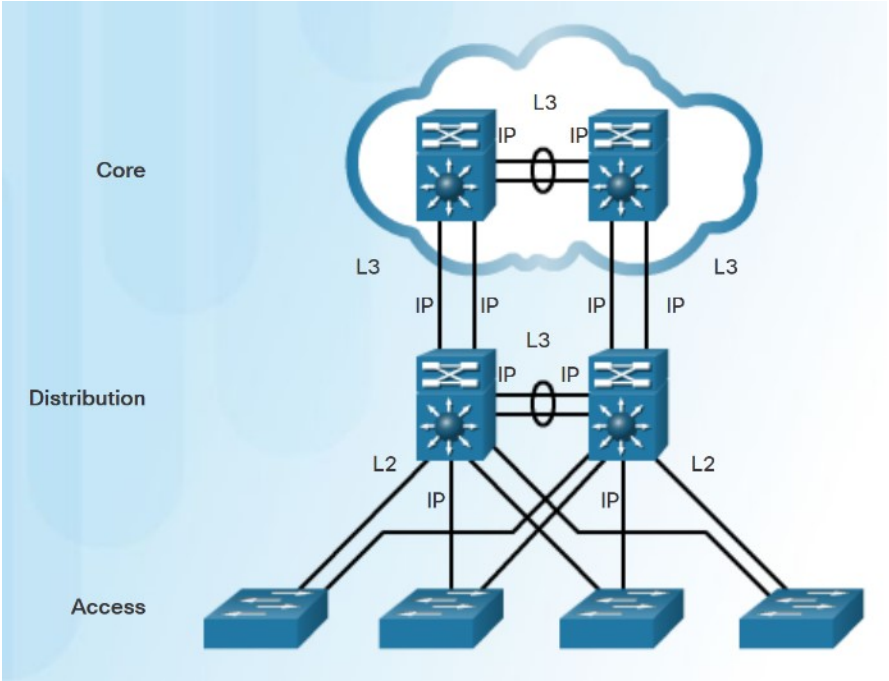
Introduction to Layer 3 Switching



- Multilayer switches provide high-packet processing rates using hardware-based switching.
- Catalyst multilayer switches support the following types of Layer 3 interfaces:
  - **Routed port** - A layer 3 interface
  - **Switch virtual interface (SVI)** - Virtual Interface for inter- VLAN routing
- All Layer 3 Cisco Catalyst switches support routing protocols, but several models require enhanced software for specific routing protocol features.
- Catalyst 2960 Series switches running IOS 12.2(55) or later, support static routing.

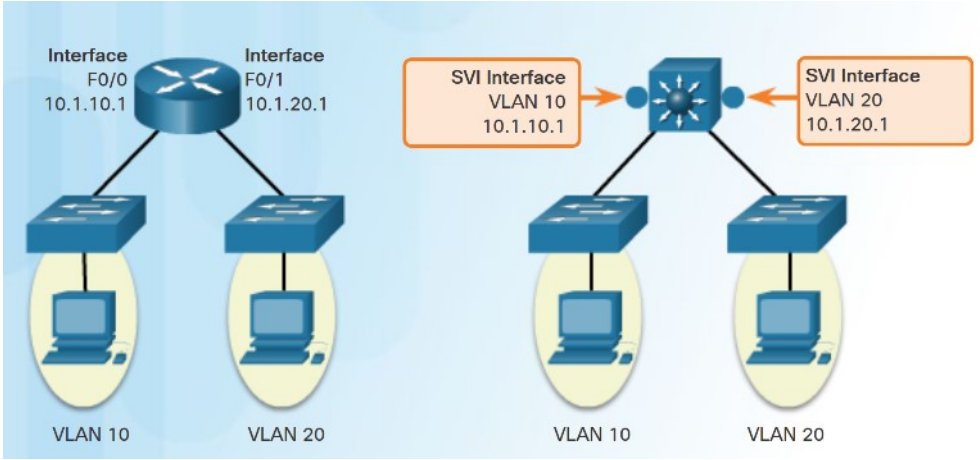
Inter-VLAN Routing with Switch Virtual Interfaces

- In the early days of switched networks, switching was fast and routing was slow. Therefore the layer 2 switching portion was extended as much as possible into the network.
- Now routing can be performed at wire speed, and is performed at both the distribution and core layers.
- Distribution switches are configured as Layer 3 gateways using Switch Virtual Interfaces (SVIs) or routed ports.
- Routed ports are usually implemented between the distribution and core layers.

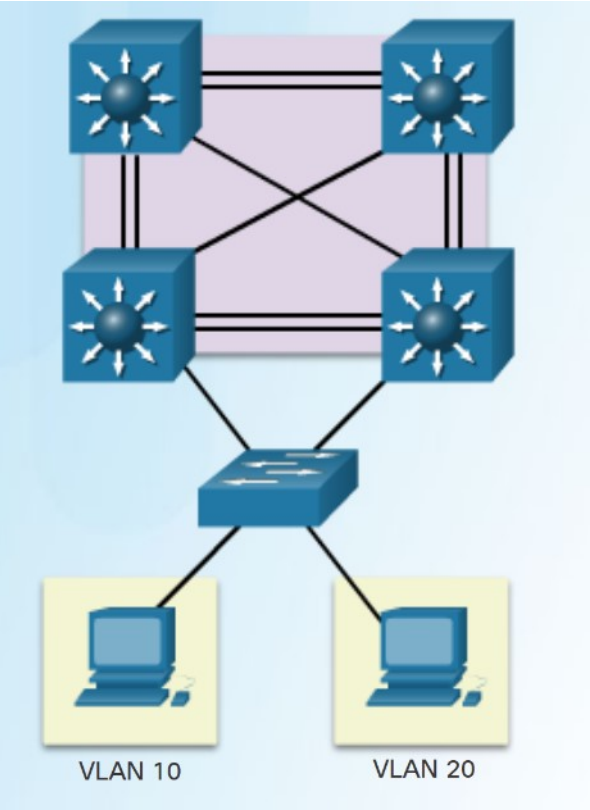


Inter-VLAN Routing with Switch Virtual Interfaces (Cont.)

- An SVI is a virtual interface that is configured within a multilayer switch:
  - To provide a gateway for a VLAN so that traffic can be routed into or out of that VLAN.
  - To provide Layer 3 IP connectivity to the switch.
  - To support routing protocol and bridging configurations.
- Advantages of SVIs:
  - Faster than router-on-a-stick.
  - No need for external links from the switch to the router for routing.
  - Not limited to one link. Layer 2 EtherChannels can be used to get more bandwidth.



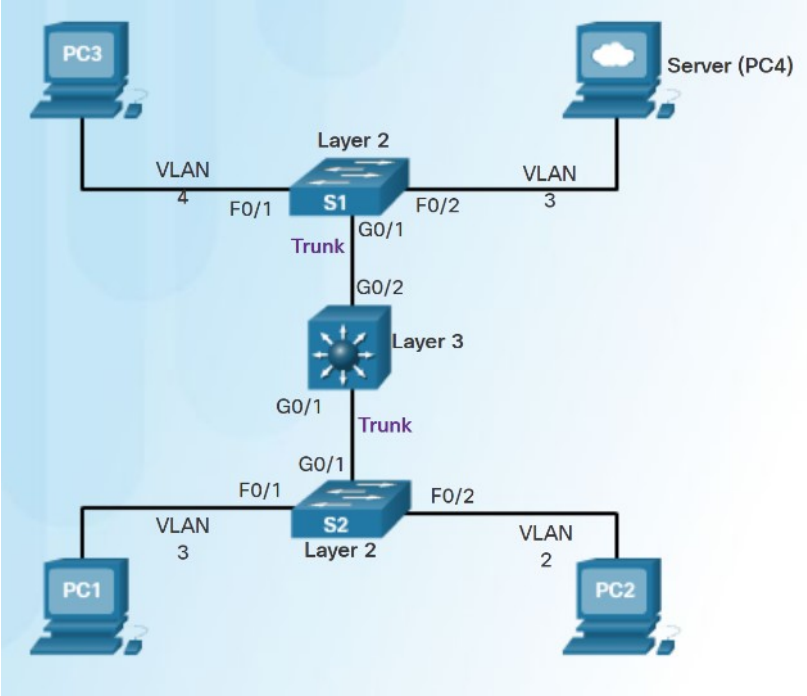
Inter-VLAN Routing with Routed Ports



- A routed port is a physical port that acts similarly to an interface on a router:
  - It is not associated with a particular VLAN.
  - It does not support subinterfaces.
- Routed ports are primarily configured between switches in the core and distribution layer.
- Use the **no switchport interface** command on the appropriate port to configure a routed port.

Note: Routed ports are not supported on Catalyst 2960 Series switches.

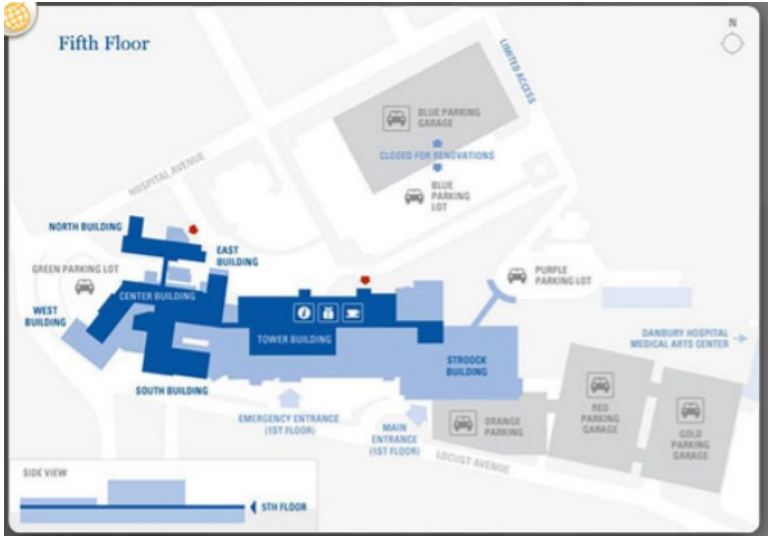
Layer 3 Switch Configuration Issues



- To troubleshoot Layer 3 switching issues check the following:
  - **VLANs** – verify correct configuration.
  - **SVIs** - verify correct IP, subnet mask and VLAN number.
  - **Routing** - verify that either static or dynamic routing is correctly configured and enabled.
  - **Hosts** – verify correct IP, subnet mask, and default gateway.

Example: Troubleshooting Layer 3 Switching

- There are four steps to implementing a new VLAN:
  - **Step 1.** Create and name a new VLAN 500 on the fifth floor switch and on the distribution switches.
  - **Step 2.** Add ports to VLAN 500 and ensure that the trunk is set up between distribution switches.
  - **Step 3.** Create an SVI interface on the distribution switches and ensure that IP addresses are assigned.
  - **Step 4.** Verify connectivity.
- The troubleshooting plan checks for the following:
  - **Step 1.** Verify that all VLANs have been created.
  - **Step 2.** Ensure that ports are in the right VLAN and trunking is working as expected.
  - **Step 3.** Verify SVI configurations.



Chapter 2: Scaling VLANs

- 2.1 VTP, Extended VLANs, and DTP
  - Configure enhanced inter-switch connectivity technologies.
    - Compare VTP versions 1 and 2.
    - Configure VTP versions 1 and 2.
    - Configure extended VLANs.
    - Configure Dynamic Trunking Protocol (DTP).
- 2.2 Troubleshoot Multi-VLAN Issues
  - Troubleshoot issues in an inter-VLAN routing environment.
    - Troubleshoot common inter-VLAN configuration issues.
    - Troubleshoot common IP addressing issues in an inter-VLAN routed environment.
    - Troubleshoot common VTP and DTP issues in an inter-VLAN routed environment.

Chapter 2: Scaling VLANs

- 2.3 Layer 3 Switching
  - Implement inter-VLAN routing using Layer 3 switching to forward data in a small to medium-sized business LAN.
    - Configure inter-VLAN routing using Layer 3 switching.
    - Troubleshoot inter-VLAN routing in a Layer 3 switched environment.