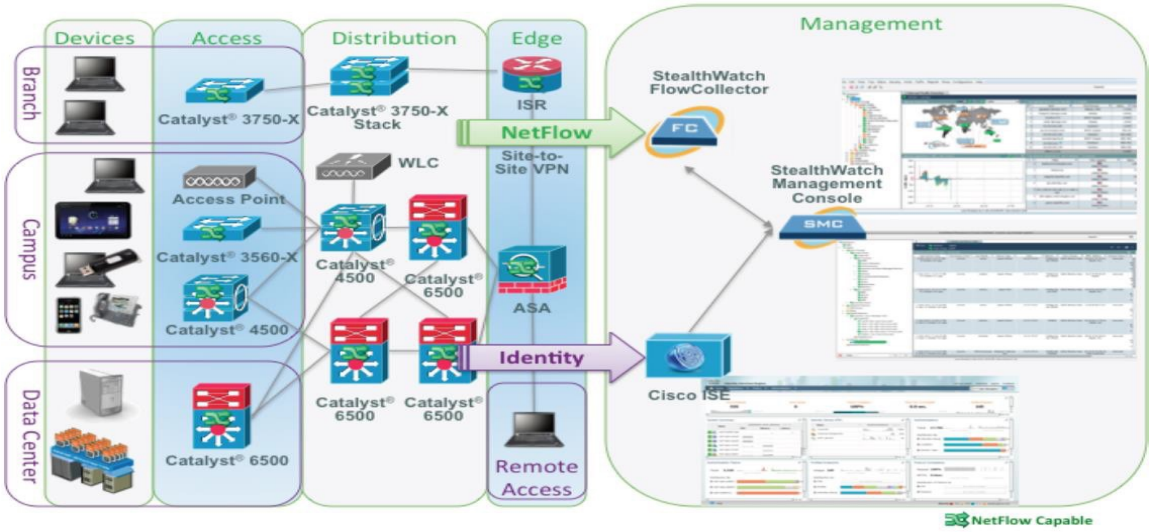
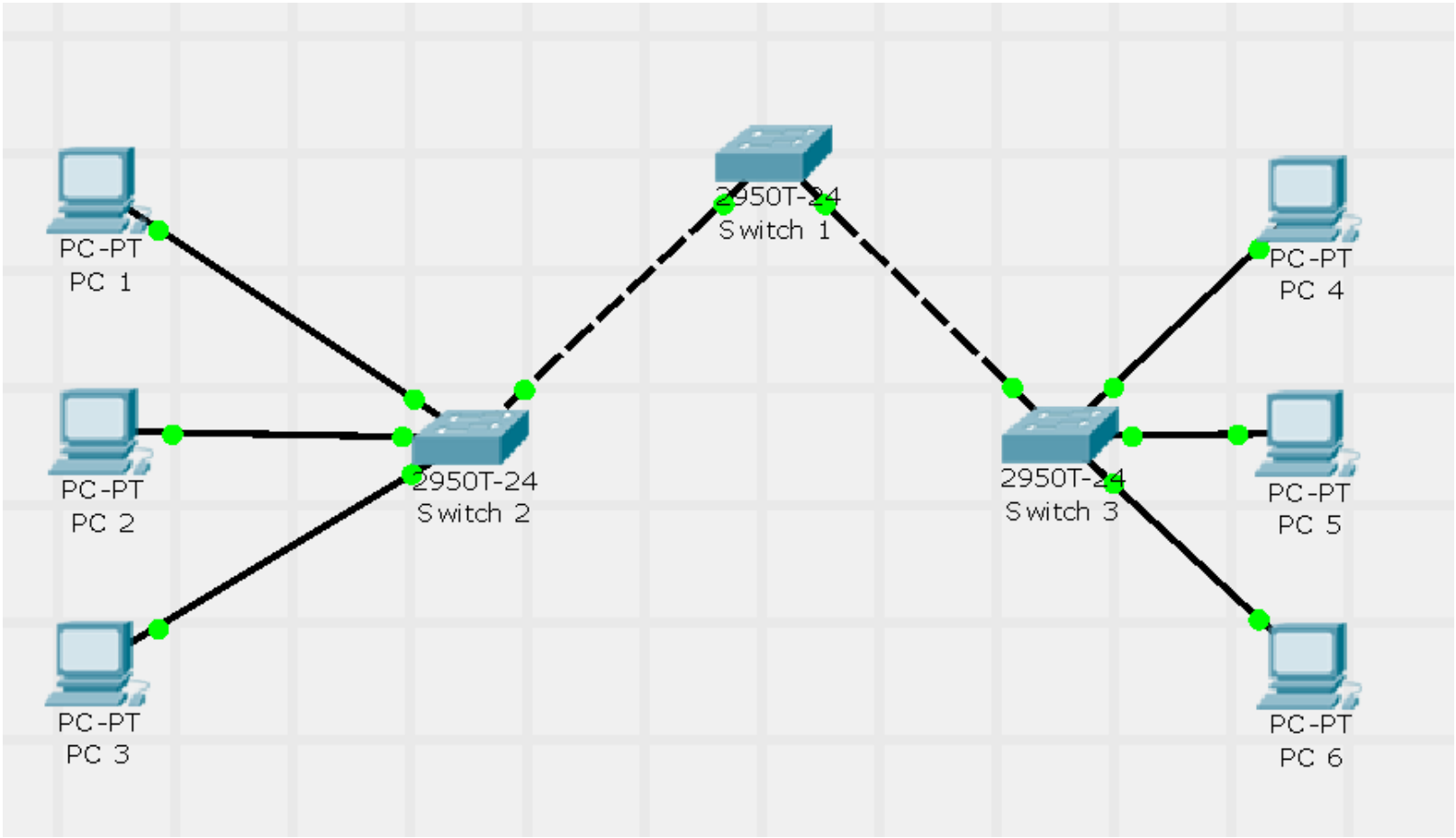
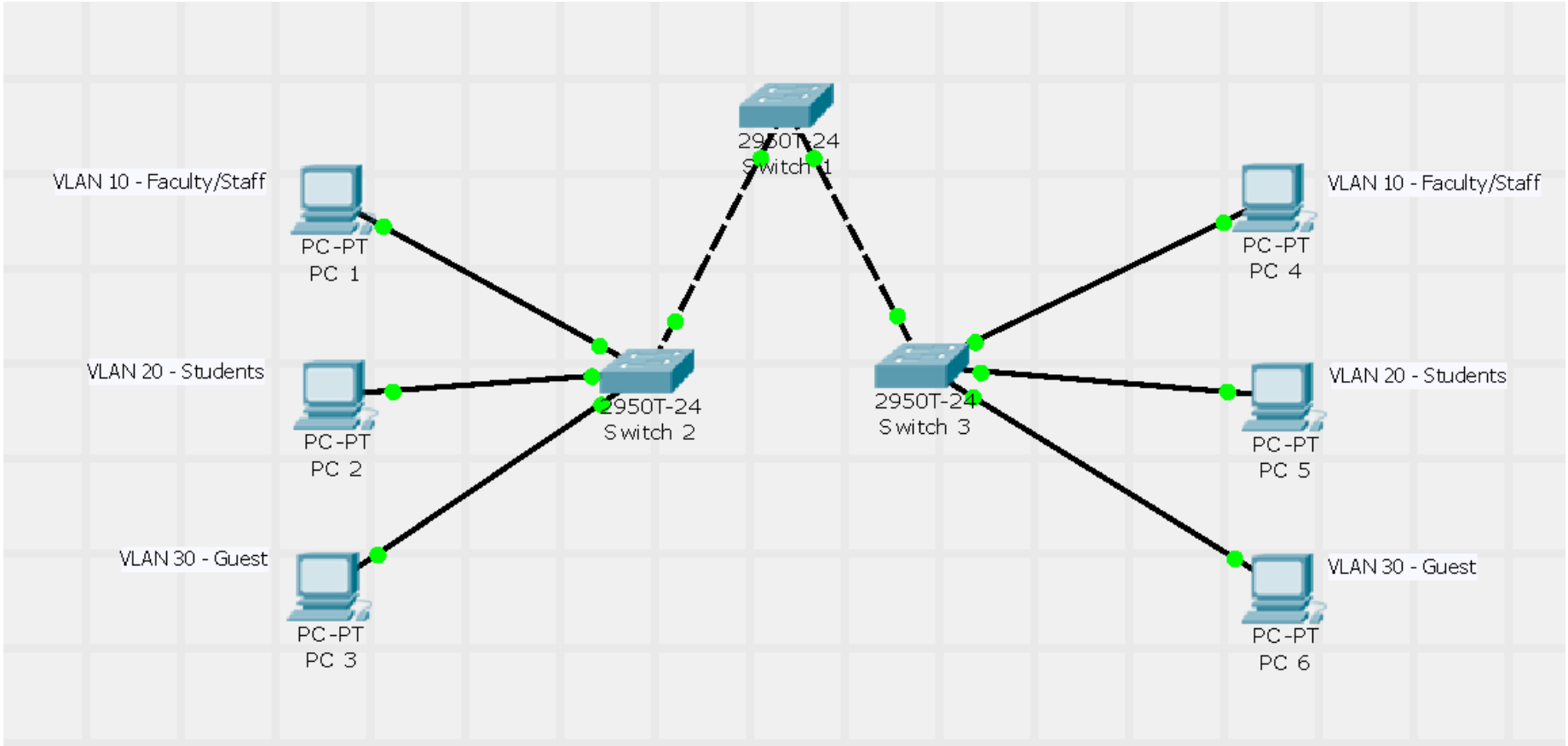
CIS 3250
VLANs



How Many Broadcast Domains?

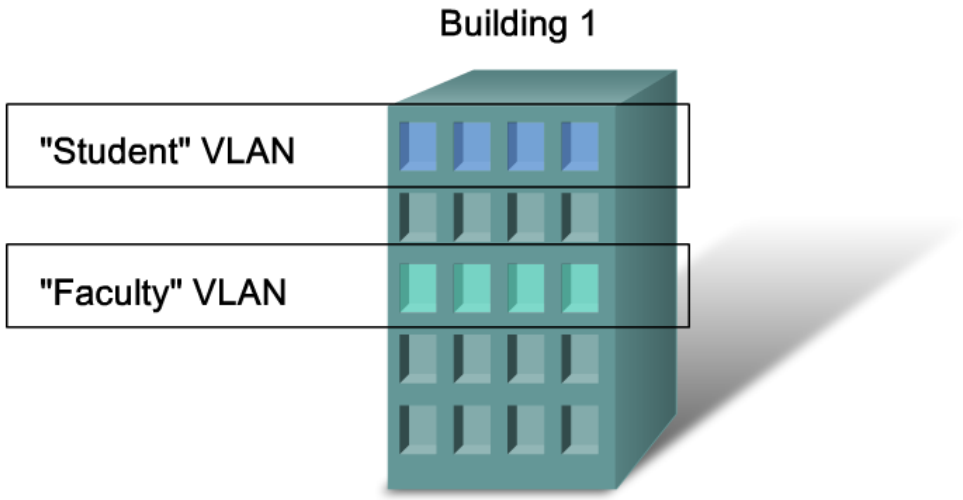


How to Create Broadcast Domains?



The Role of VLANs in a Converged Network

What is a VLAN?

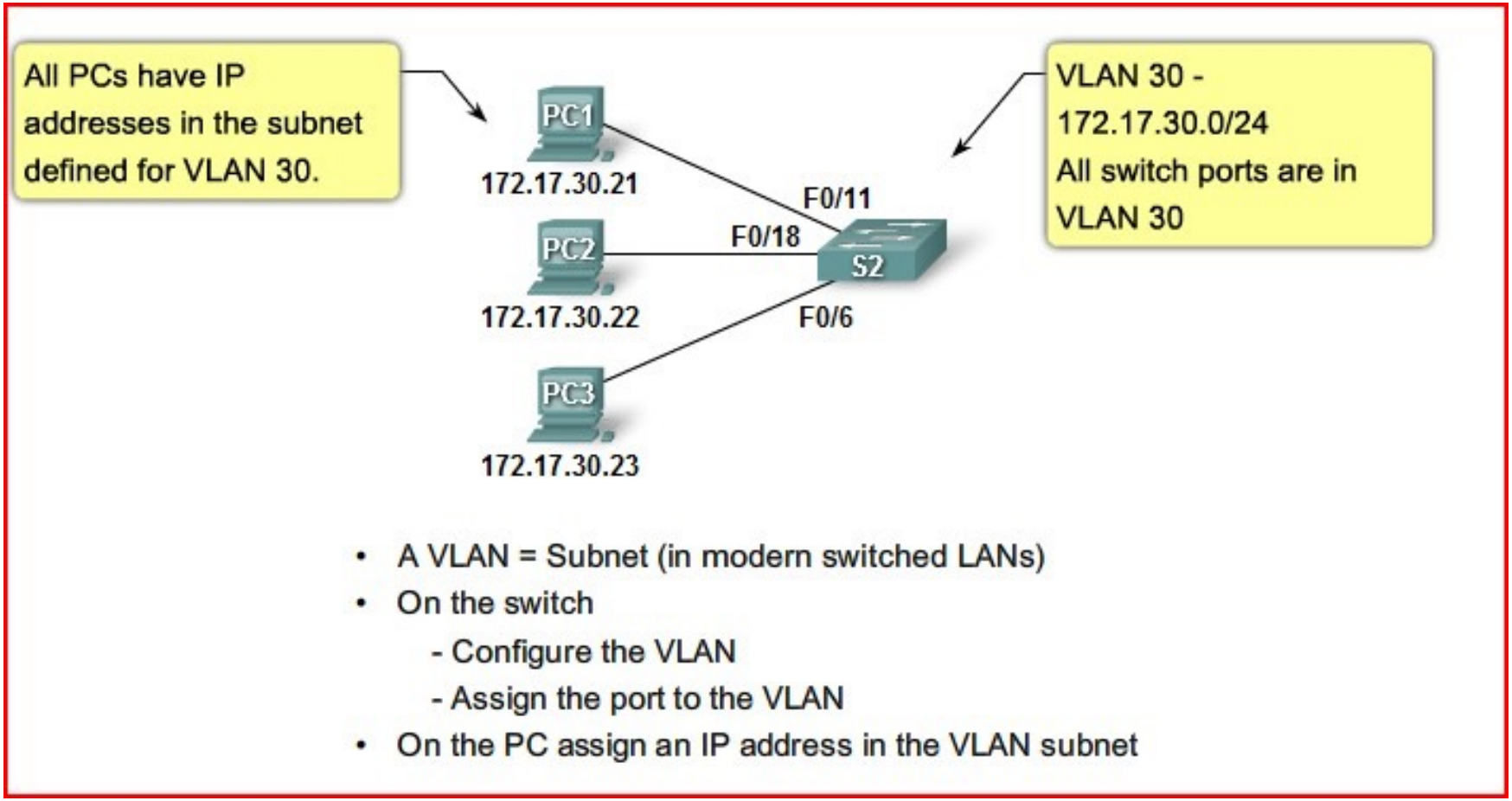


- A VLAN is an independent LAN network.
- A VLAN allows student and faculty PCs to be separated although they share the same infrastructure.
- A VLAN can be named for easier identification

What is a VLAN?

- A VLAN is a logically separate IP subnetwork.
- VLANs allow multiple IP subnetworks to exist on the same switched network.
- For computers to communicate on the same VLAN, each must have an IP address and a subnet mask consistent with that VLAN.
- The switch must be configured with the VLAN, and each relevant port in the switch must be assigned to the VLAN.
- A switch port with a singular VLAN configured is called an access port.
- Remember: just because two computers are physically connected to the same switch does NOT mean they can communicate.
- Devices on two separate networks and subnets must communicate via a router (Layer 3), whether or not VLANs are used.

What is a VLAN?



VLAN Benefits

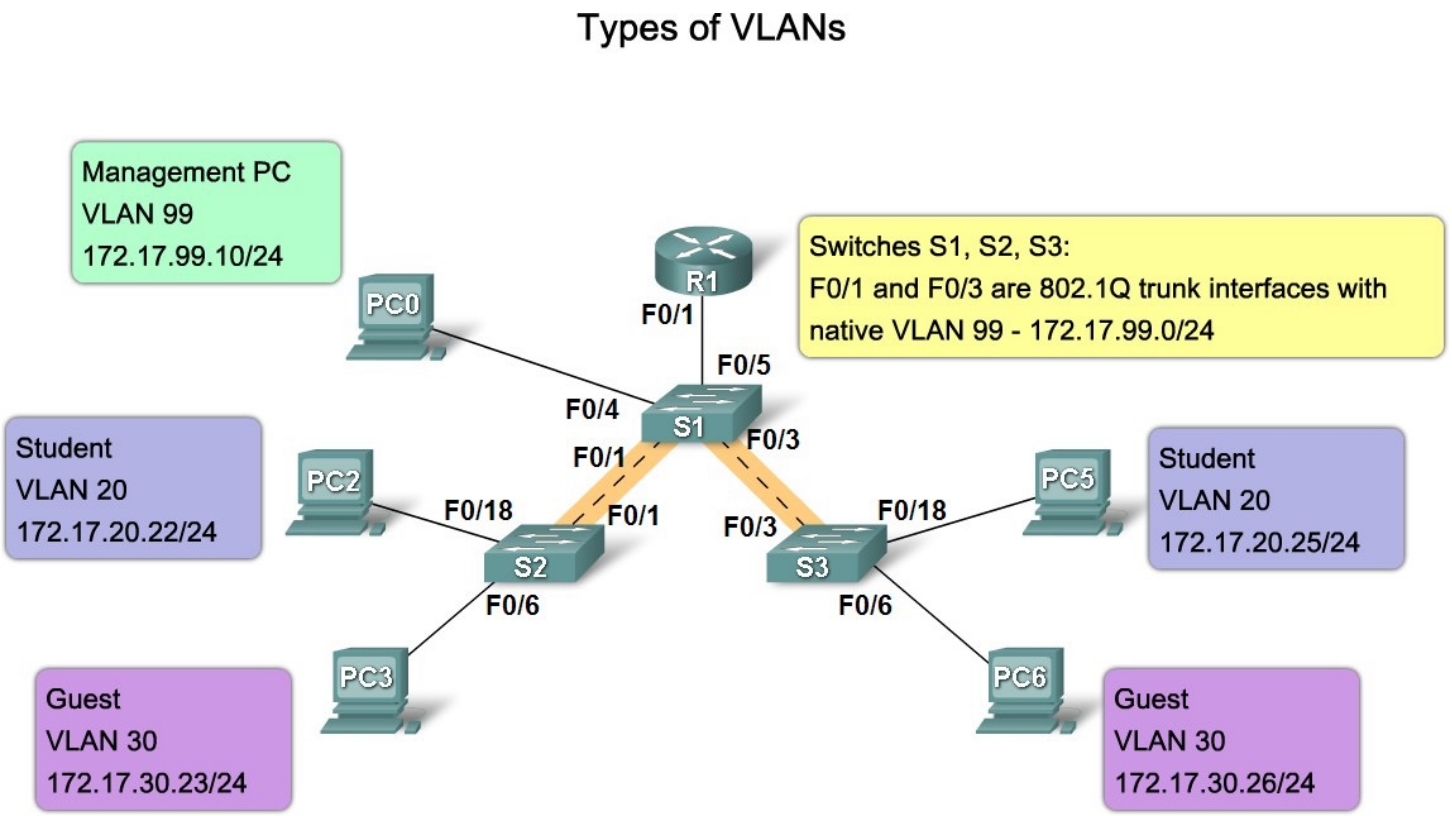
- **Security** - Groups that have sensitive data are separated from the rest. Access Control Lists (ACL) can be used at Layer 3.
- **Cost reduction** - Cost savings result from less need for expensive network upgrades and more efficient use of existing infrastructure.
- **Higher performance** - Dividing flat Layer 2 networks into multiple logical workgroups (broadcast domains) reduces traffic.
- **Broadcast storm mitigation** - Dividing a network into VLANs reduces the number of devices that may participate in a broadcast storm.
- **Improved IT staff efficiency** - VLANs make it easier to manage the network because VLANs can be configured without buying new hardware.
- More straightforward **project or application management** - VLANs aggregate users and network devices to support business or geographic requirements.

VLAN Characteristics

- VLAN ID
  - Normal-range IDs
    - 1 – 1005
    - 1002 -1005 reserved for Token Ring and FDDI VLANs
    - 1 and 1002 to 1005 are automatically created and cannot be removed
    - Stored in the vlan.dat file in flash memory
  - Extended-range IDs
    - 1006 – 4094
    - Designed for service providers
    - Have fewer options than normal range VLANs
    - Stored in the running configuration file
- A Cisco Catalyst 2960 switch supports 255 normal and extended range VLANs

The Role of VLANs in a Converged Network

- Describe the different types VLANs



Data VLAN (or “User” VLAN)

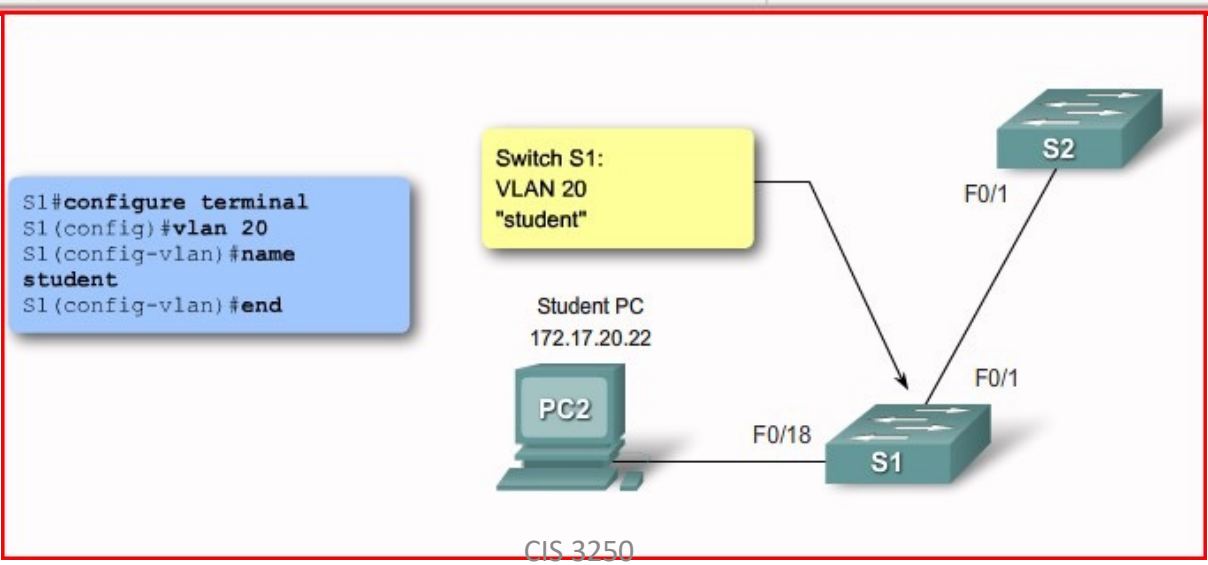
- A data VLAN is a VLAN that is configured to carry only user-generated traffic.
- A VLAN could carry voice-based traffic or traffic used to manage the switch, but this traffic would not be part of a data VLAN.
- It is common practice to separate voice and management traffic from user data traffic.
- The importance of separating user data from switch management control data and voice traffic is highlighted using a special term used to identify VLANs that only carry user data - a "data VLAN." A data VLAN is sometimes referred to as a user VLAN.

Default VLAN

- All switch ports become a member of the default VLAN after the initial boot-up of the switch.
- Having all the switch ports participate in the default VLAN makes them all part of the same broadcast domain. This allows any device connected to any switch port to communicate with other devices on other switch ports.
- The default (Ethernet) VLAN for Cisco switches is VLAN 1.
- VLAN 1 has all the features of any VLAN, except that you cannot rename or delete it.
- Layer 2 control traffic, such as CDP and spanning tree protocol traffic, will always be associated with VLAN 1 - this cannot be changed.
- It is a security best practice to change the default VLAN to a VLAN other than VLAN 1; this entails configuring all the ports on the switch to be associated with a default VLAN other than VLAN 1

Adding a VLAN

Cisco IOS CLI Command Syntax	
Switch from privileged EXEC mode to global configuration mode.	`S1#configure terminal`
Create a VLAN. Vlan id is the VLAN number that is to be created. Switches to VLAN configuration mode for VLAN vlan id.	`S1(config)#vlan vlan id`
(Optional) Specify a unique VLAN name to identify the VLAN. If no name is entered the VLAN number, padded zeros, is appended the word 'VLAN', for example, VLAN0020.	`S1(config-vlan)#name vlan name`
Return to privileged EXEC mode. You must end your configuration session for the configuration to be saved in the vlan.dat file and for configuration to take effect.	`S1(config-vlan)#end`



Verify VLAN Creation

```
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
                                                Gi0/1, Gi0/2
20   student                          active
1002 fddi-default                     act/unsup
1003 token-ring-default               act/unsup
1004 fddinet-default                  act/unsup
1005 trnet-default                    act/unsup


S1#conf t
```

Assigning a Port to a VLAN

Cisco IOS CLI Command Syntax	
Enter global configuration mode.	`S1#configure terminal`
Enter the interface to assign the VLAN.	`S1(config)#interface` *interface id*
Define the VLAN membership mode for the port.	`S1(config-if)#switchport mode access`
Assign the port to a VLAN.	`S1(config-if)#switchport access vlan` *vlan id*
Return to privileged EXEC mode.	`S1(config-if)#end`

Remember the `show vlan` output?
To which VLAN do all ports belong by default?

Show VLAN Command

```
S1#show vlan name student

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

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

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

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

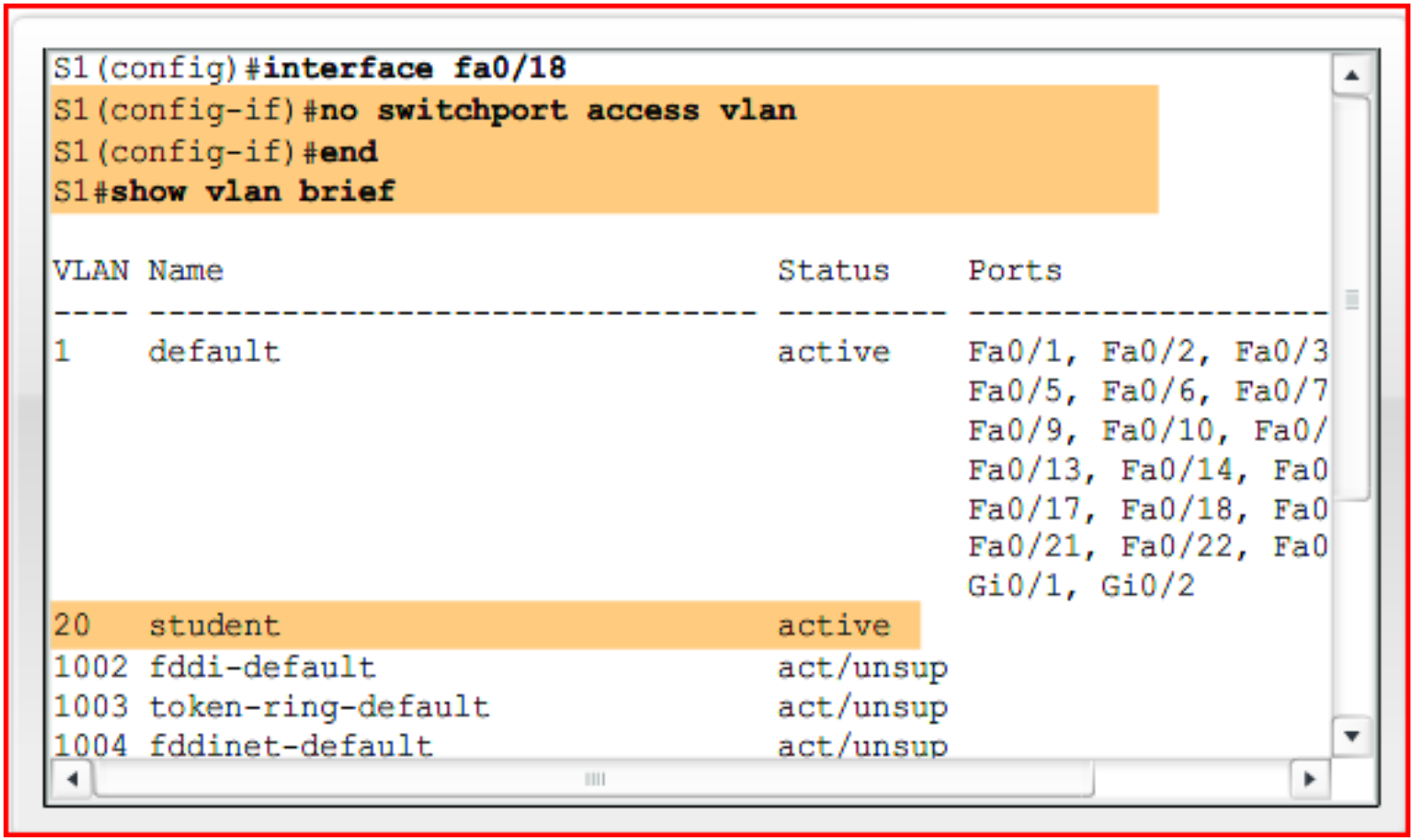
Show Interfaces

```
S1#show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia 001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input never, output never, output hang never
  Last clearing of "show interface" counters never
  Input queue: 0/75/0/0 (size/max/drops/flushes); Total output drops: 0
  Queueing strategy: fifo
  Output queue: 0/40 (size/max)
  5 minute input rate 0 bits/sec, 0 packets/sec
  5 minute output rate 0 bits/sec, 0 packets/sec
     0 packets input, 0 bytes, 0 no buffer
     Received 0 broadcasts (0 IP multicast)
     0 runts, 0 giants, 0 throttles
     0 input errors, 0 CRC, 0 frame, 0 overrun, 0 ignored
     0 packets output, 0 bytes, 0 underruns
```

Show Interfaces

```
S1#show interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
```

Manage Port Membership

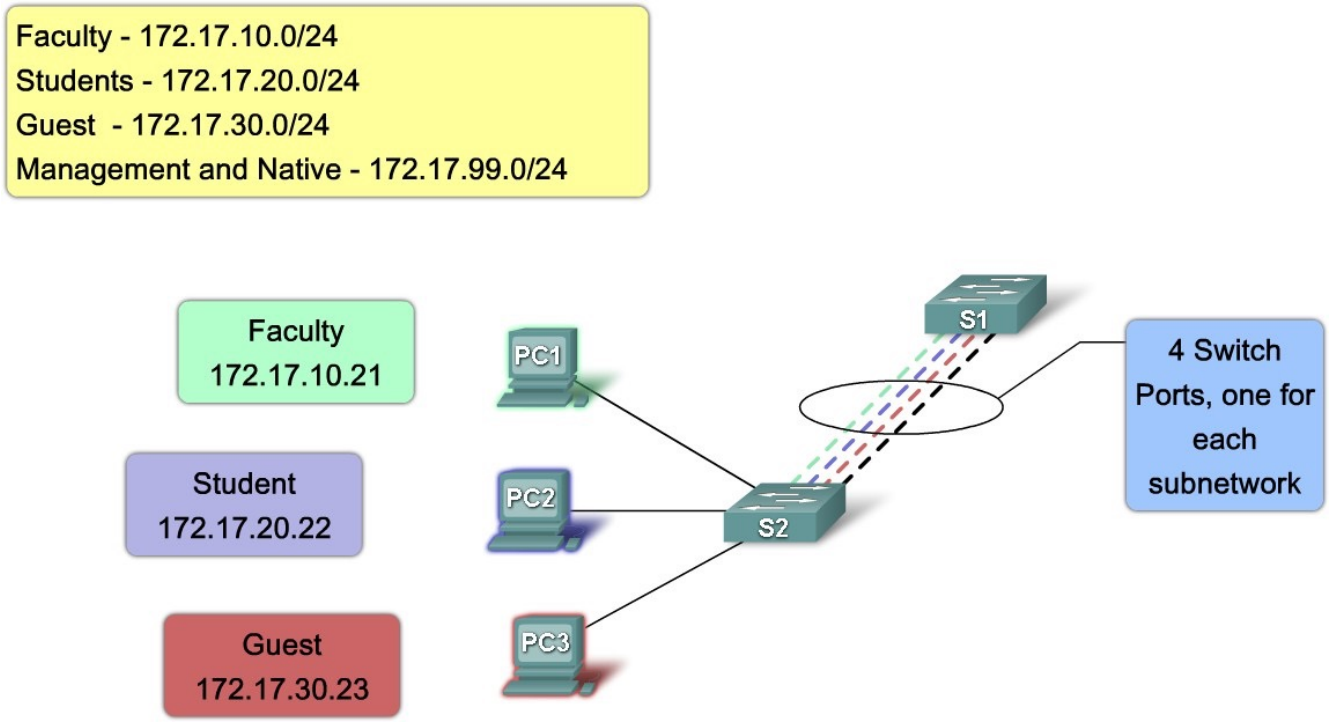


```
S1(config)#interface fa0/18
S1(config-if)#no switchport access vlan
S1(config-if)#end
S1#show vlan brief

VLAN Name                              Status    Ports
---- --------------------------------- --------- -------------------
1    default                           active    Fa0/1, Fa0/2, Fa0/3
                                                 Fa0/5, Fa0/6, Fa0/7
                                                 Fa0/9, Fa0/10, Fa0/
                                                 Fa0/13, Fa0/14, Fa0
                                                 Fa0/17, Fa0/18, Fa0
                                                 Fa0/21, Fa0/22, Fa0
                                                 Gi0/1, Gi0/2
20   student                           active
1002 fddi-default                      act/unsup
1003 token-ring-default                act/unsup
1004 fddinet-default                   act/unsup
```

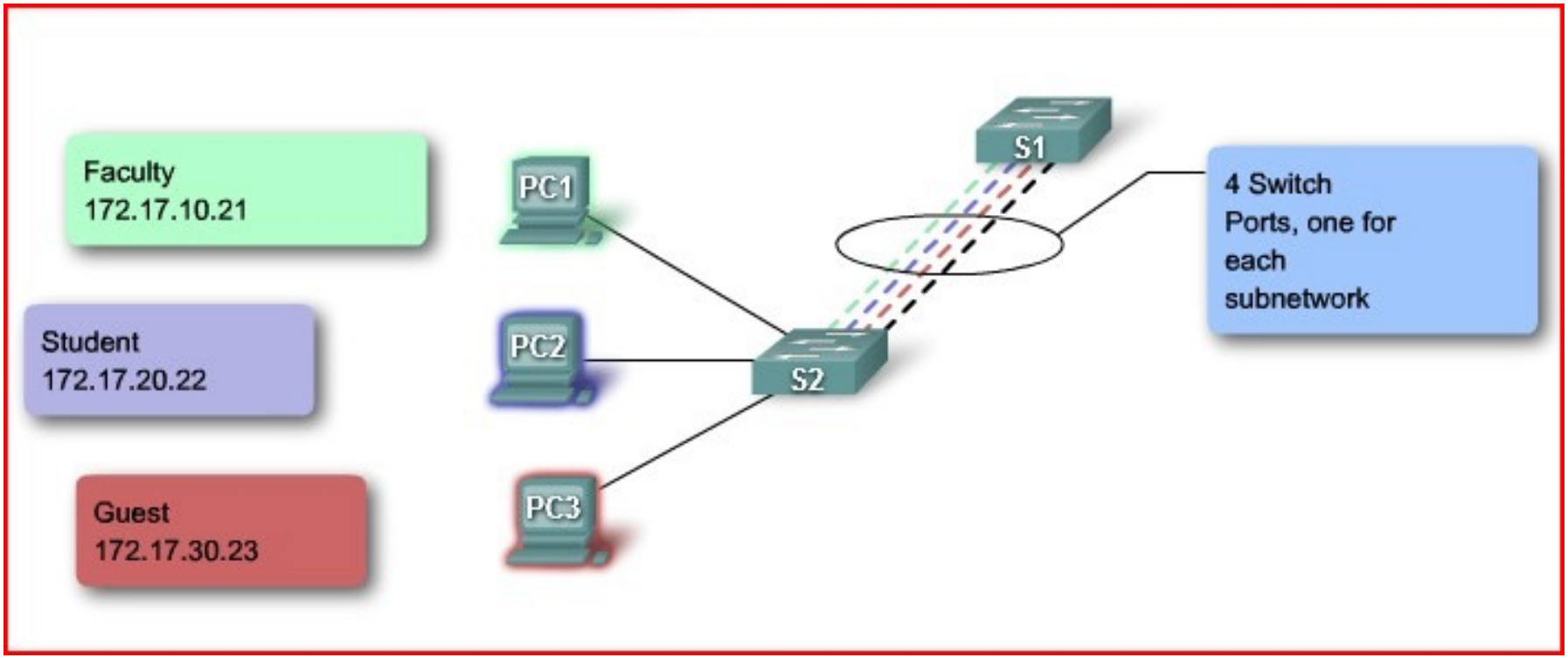
Default VLAN 2

- Some administrators use the term "default VLAN" to mean a VLAN other than VLAN 1 defined by the administrator as the VLAN that all ports are assigned to when they are not in use.
- In this case, the only role that VLAN 1 plays is handling Layer 2 control traffic for the network.

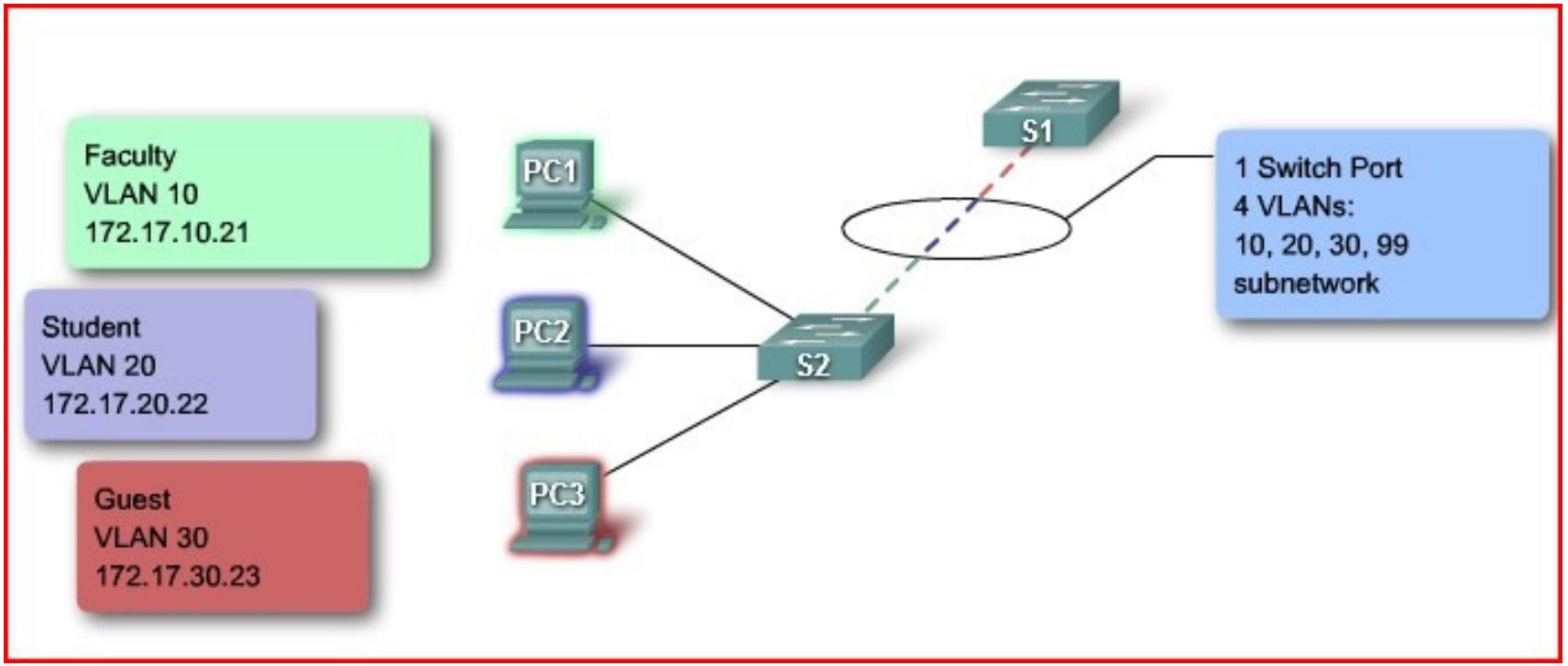
The Role of Trunking VLANs in a Converged Network



VLANs Without Trunks



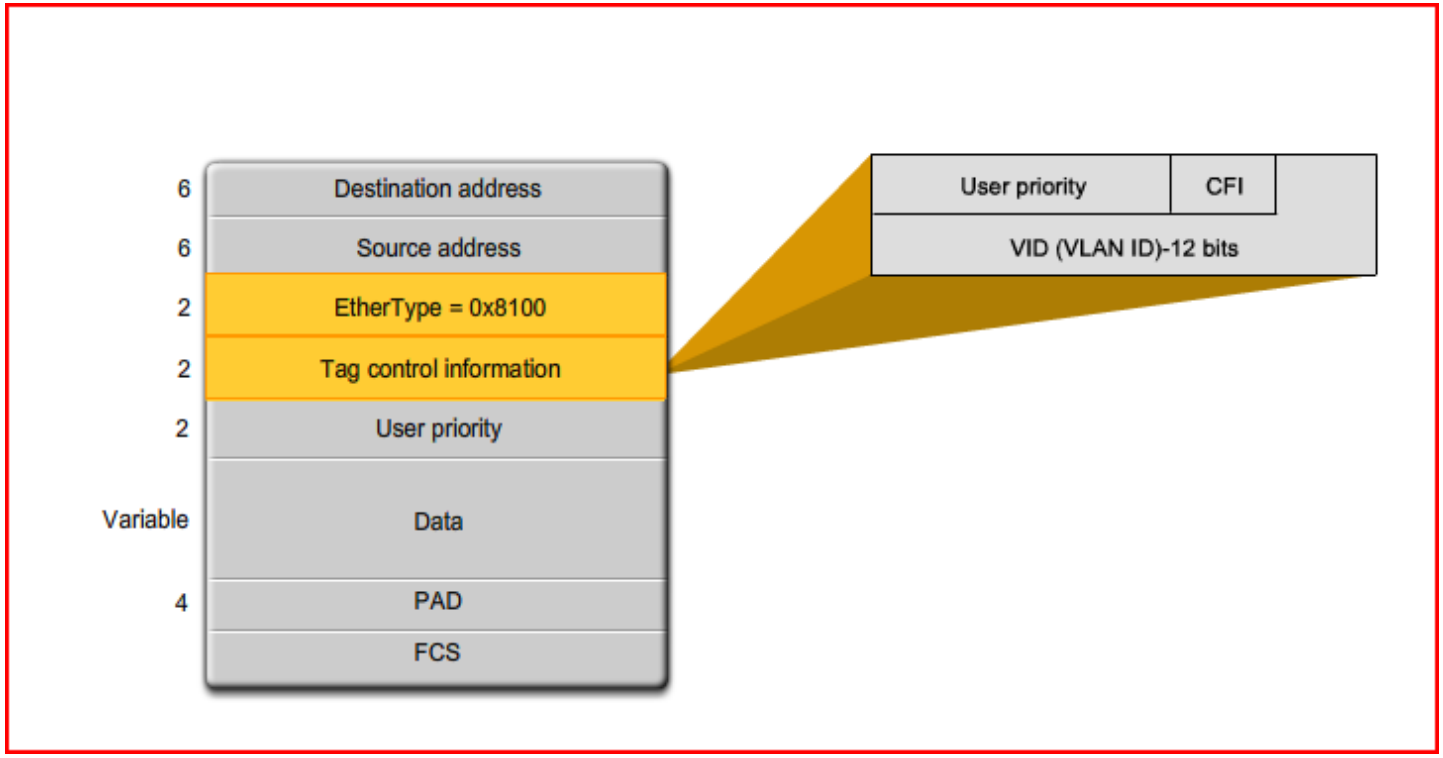
VLANs With Trunks



VLAN Frame Tagging

- Switches are Layer 2 devices. They only use the Ethernet frame header information to forward packets.
- The frame header does not contain information about which VLAN the frame belongs.
- When Ethernet frames are placed on a trunk, they need additional information about the VLANs they belong to. This is accomplished by using the 802.1Q encapsulation header. This header adds a tag to the original Ethernet frame specifying the VLAN to which the frame belongs.
- VLAN IDs can be in a normal range, 1-1005, and an extended range, 1006-4094. How do VLAN IDs get inserted into a frame?

VLAN Frame Tagging



When the switch receives a frame on a port configured in access mode with a static VLAN, the switch takes apart the frame and inserts a VLAN tag, recalculates the FCS and sends the tagged frame out a trunk port.

Management VLAN

- A management VLAN is any VLAN you configure to access the management capabilities of a switch.
- VLAN 1 would serve as the management VLAN if you did not proactively define a unique VLAN to serve as the management VLAN.
- You assign the management VLAN an IP address and subnet mask.
- A switch can be managed via HTTP, Telnet, SSH, or SNMP. The out-of-the-box configuration of a Cisco switch has VLAN 1 as the default VLAN.
- VLAN 1 would be a wrong choice as the management VLAN; you wouldn't want an arbitrary user connecting to a switch to default to the management VLAN.

Native VLAN

- To distinguish between tagged and untagged frames, Cisco uses the concept of trunk ports and the native VLAN for trunk ports.
- The IEEE decided that, for backward compatibility, it was desirable to support a VLAN that is not associated explicitly with any tag on an 802.1Q link. This VLAN is implicitly used for all the untagged traffic received on an 802.1Q capable port.
- A native VLAN is assigned to an 802.1Q trunk port.
- An 802.1Q trunk port supports both tagged traffic and untagged traffic—the 802.1Q trunk port associates untagged traffic to the native VLAN.
- Native VLANs are set out in the IEEE 802.1Q specification to maintain backward compatibility with untagged traffic common to legacy LAN scenarios. For our purposes, a native VLAN serves as a common identifier on opposing ends of a trunk link. It is a best practice to use a VLAN other than VLAN 1 as the native VLAN.

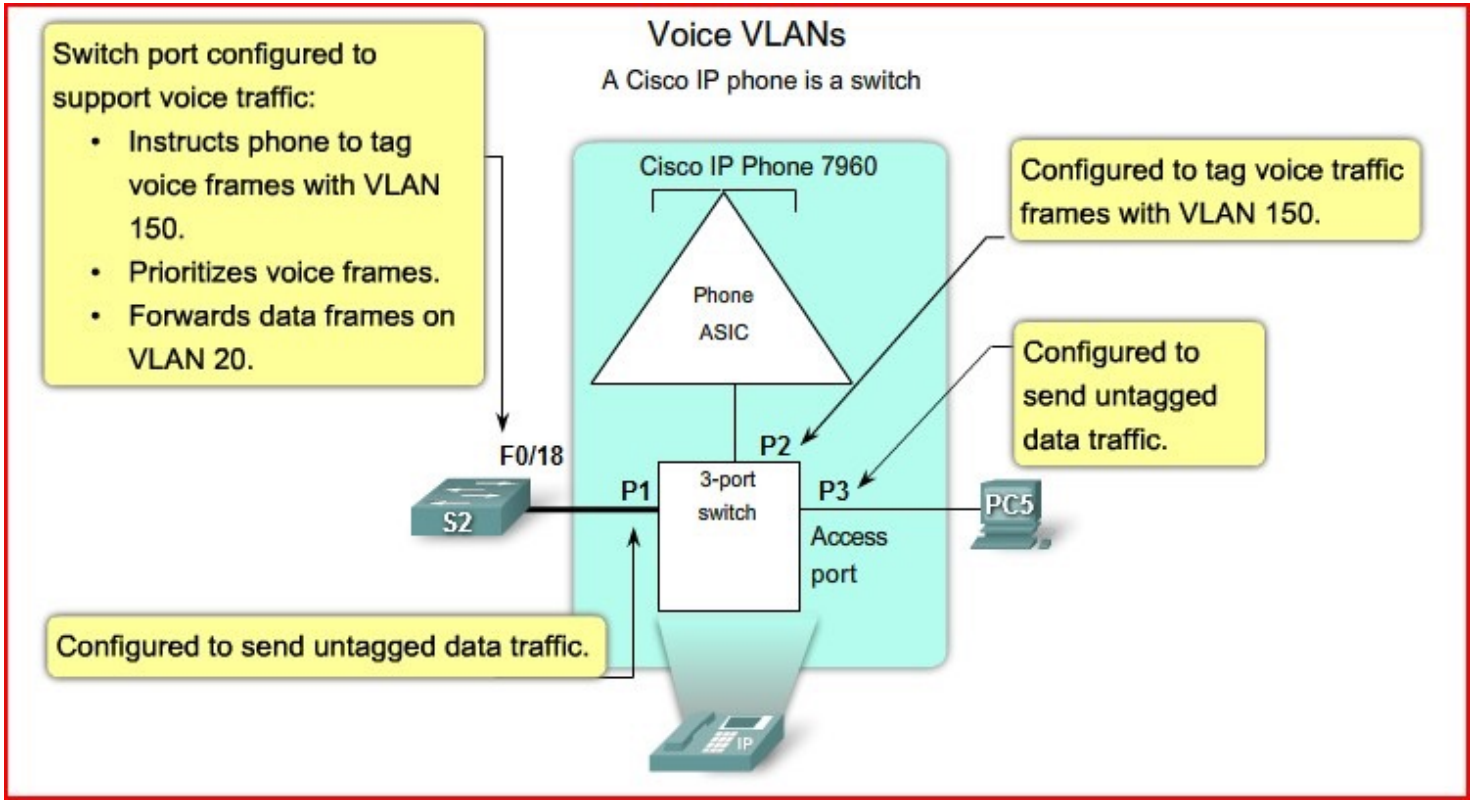
VLAN Types – Confused?

- Default VLAN
- Data (or User) VLAN
- Native VLAN
- Management VLAN

Voice VLAN

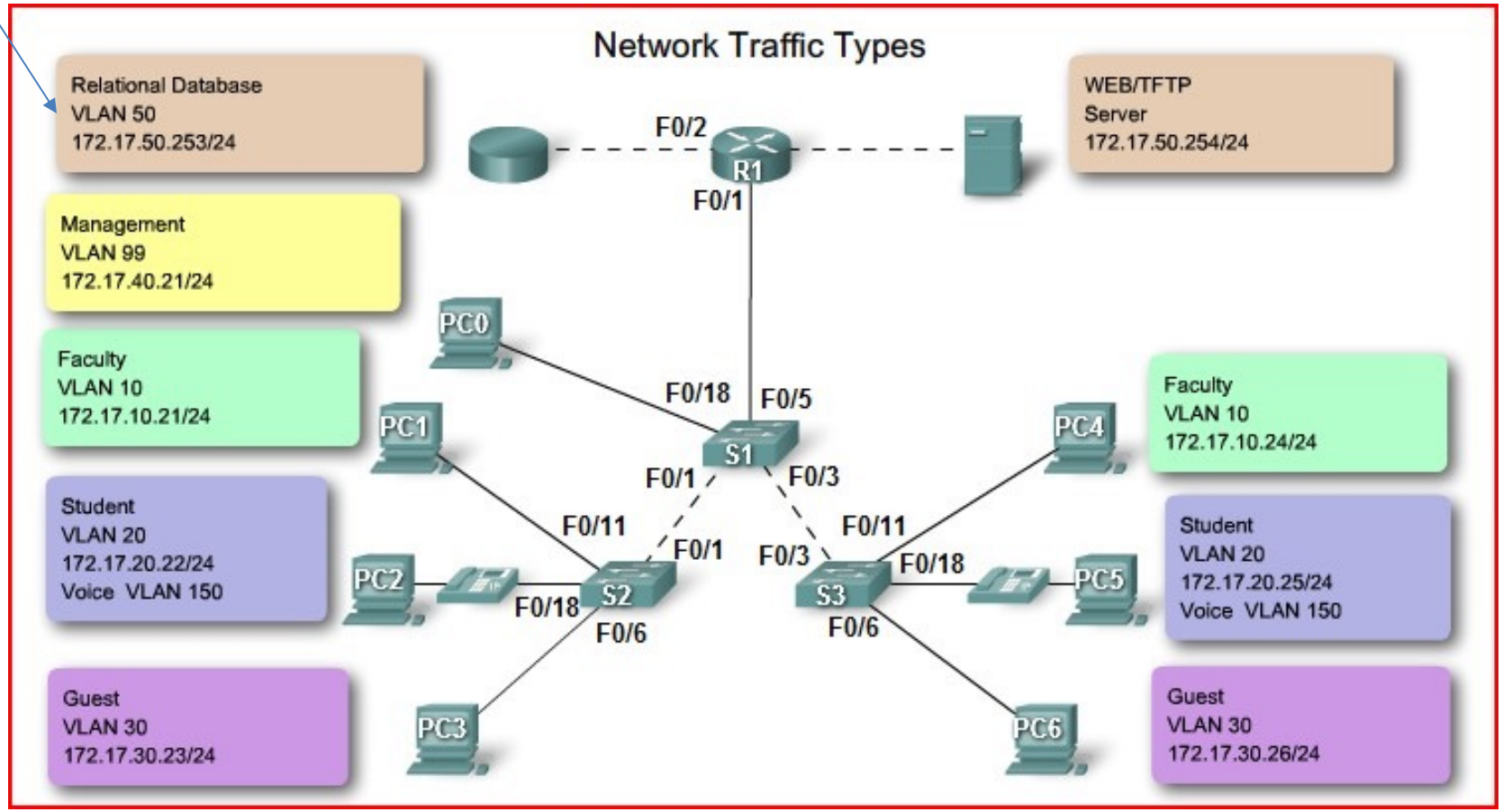
- Requirements:
  - –Assured bandwidth to ensure voice quality
  - –Transmission priority over other types of network traffic
  - –Ability to be routed around congested areas on the network
  - –Delay of less than 150 milliseconds (ms) across the network
- To meet these requirements, the entire network must be designed to support VoIP.
- The details of how to configure a network to support VoIP are beyond the scope of the course, but it is helpful to summarize how a voice VLAN works between a switch, a Cisco IP phone, and a computer.

Voice VLANs

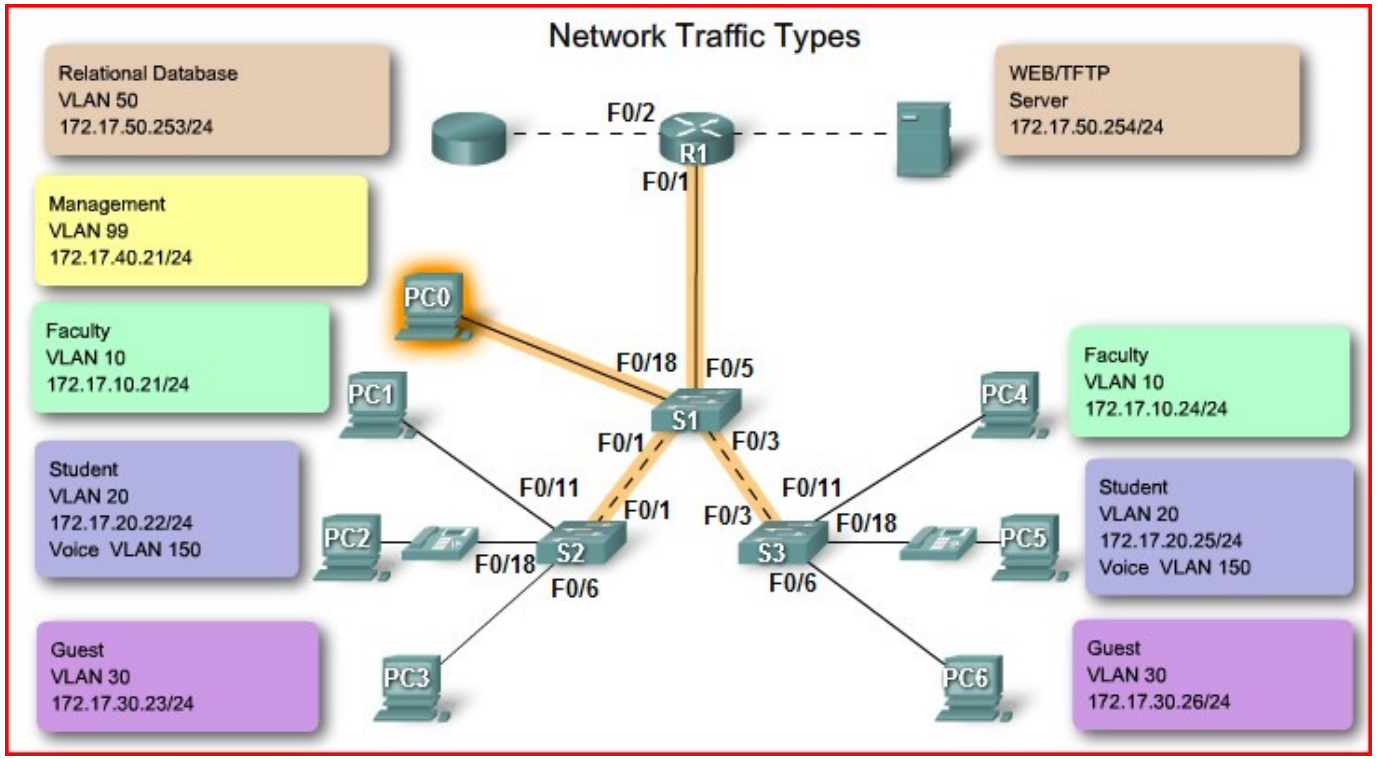

Voice VLANs
A Cisco IP phone is a switch
Switch port configured to support voice traffic:
• Instructs phone to tag voice frames with VLAN 150.
• Prioritizes voice frames.
• Forwards data frames on VLAN 20.
Cisco IP Phone 7960
Phone ASIC
Configured to tag voice traffic frames with VLAN 150.
Configured to send untagged data traffic.
F0/18
P2
P1
3-port switch
P3
S2
PC5
Access port
Configured to send untagged data traffic.
IP

Network Traffic Types

Does this make sense?



Network Management and Control Traffic

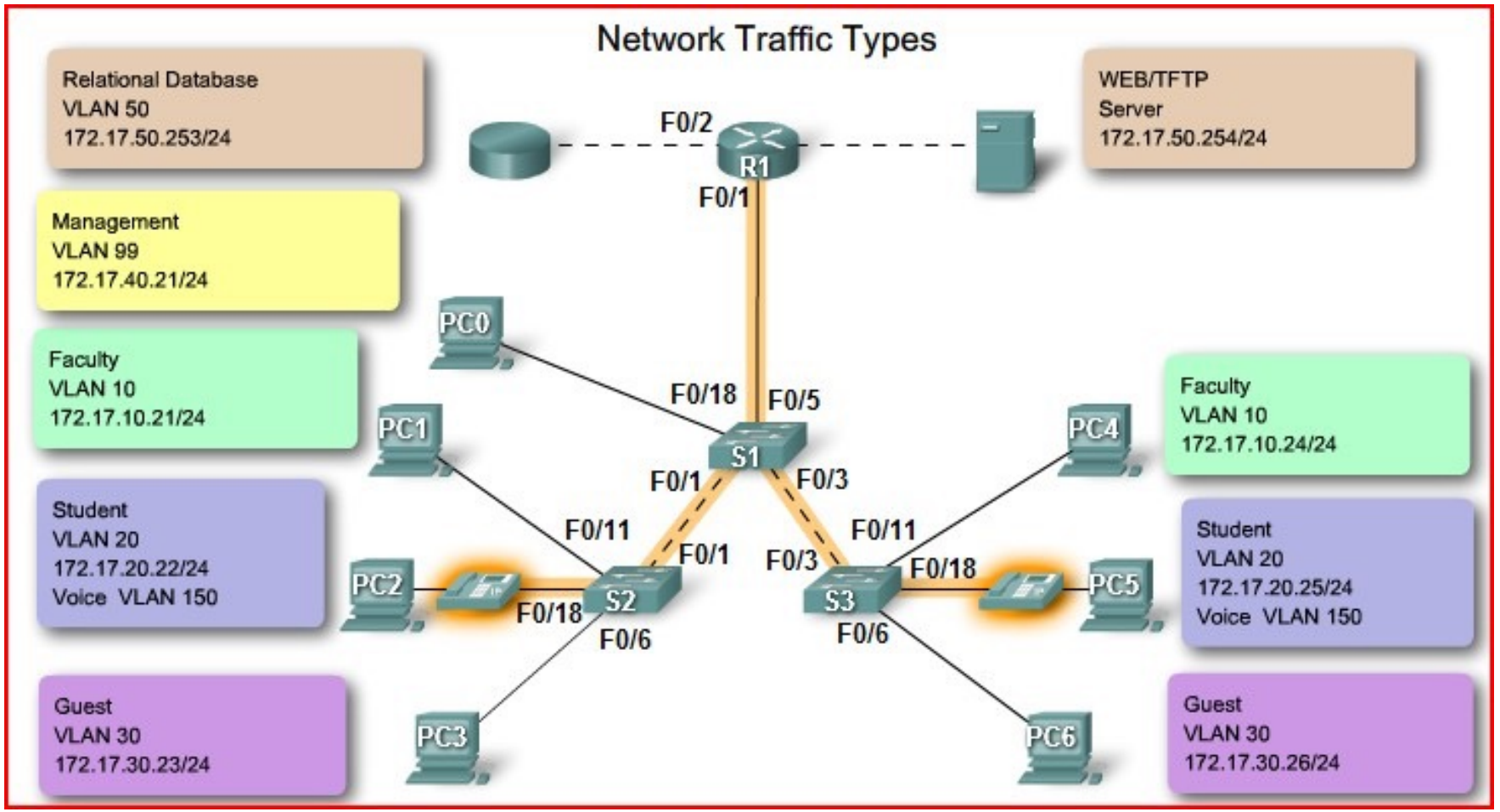


This slide confuses network management traffic (always on VLAN 1) with the management VLAN (used to manage the switches remotely).

Different types of network management and control traffic:

- Cisco Discovery Protocol (CDP)
- Simple Network Management Protocol (SNMP)
- Remote Monitoring (RMON)

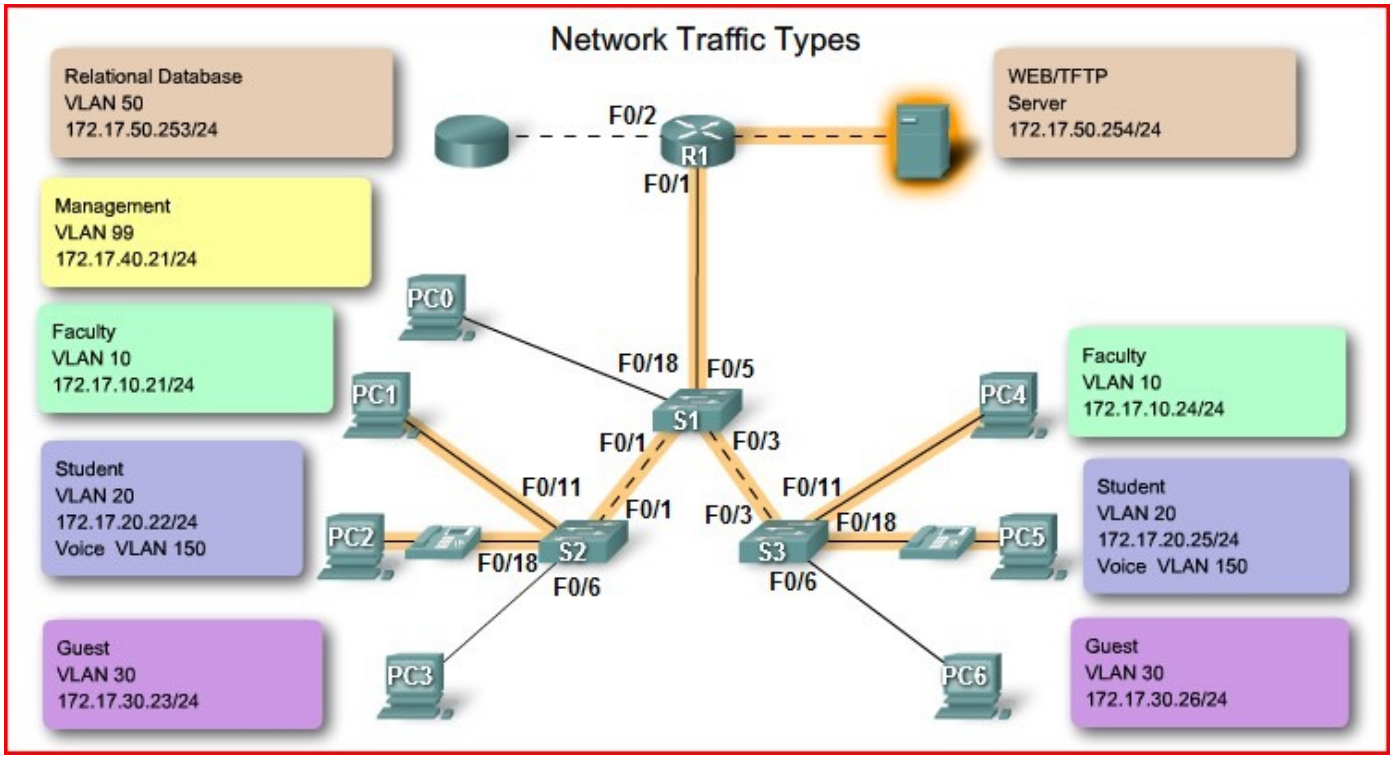
IP Telephony



IP Telephony

- The types of IP telephony traffic are signaling traffic and voice traffic.
- Signaling traffic is responsible for call setup, progress, and teardown, traversing the network end to end.
- The other type of telephony traffic consists of the actual voice conversation data packets.
- In a network configured with VLANs, assigning a VLAN other than VLAN 1 as the management VLAN is strongly recommended.
- Data traffic should be associated with a data VLAN (other than VLAN 1), and voice traffic should be associated with a voice VLAN.

Multicast Traffic



IP Multicast

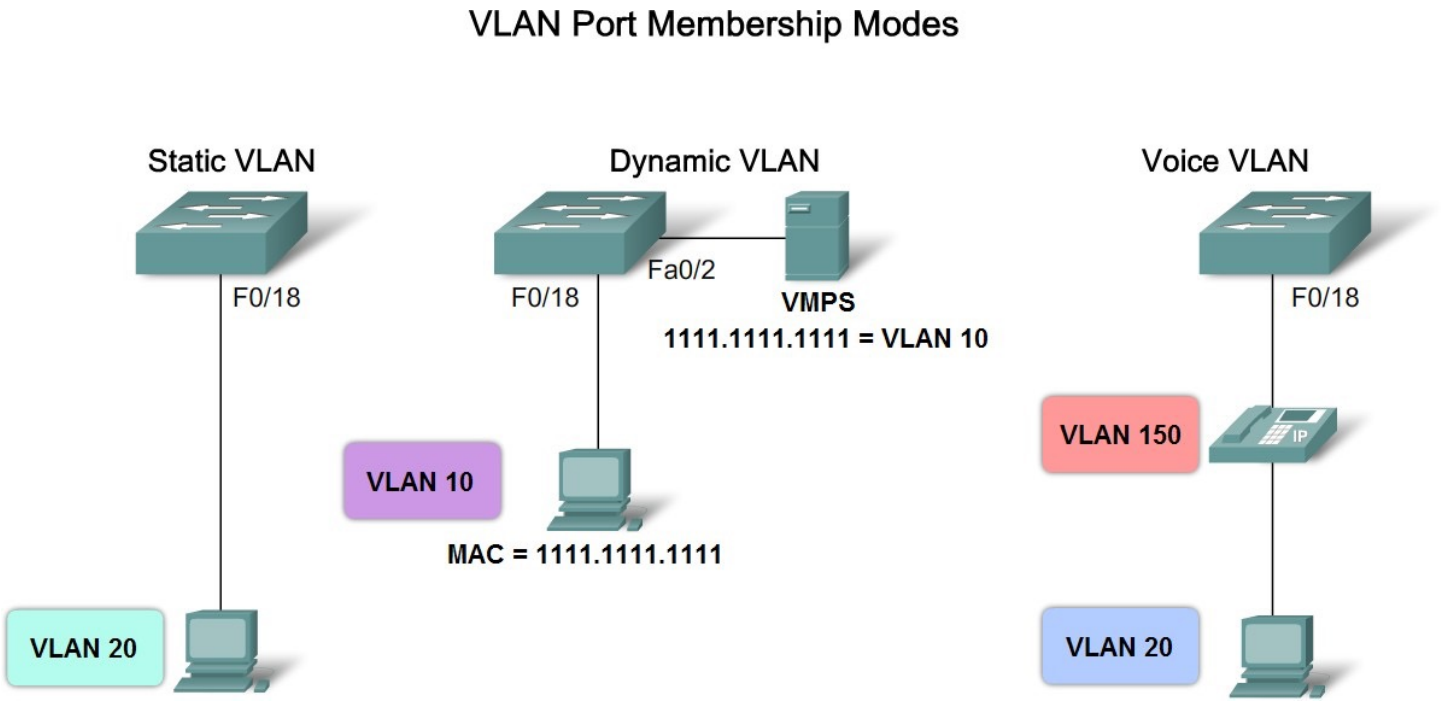
- IP multicast traffic is sent from a particular source address to a multicast group identified by a single IP and MAC destination-group address pair.
- Applications that generate this type of traffic are Cisco IP/TV broadcasts, routing protocols, and video streaming applications.
- Multicast traffic can produce a large amount of data streaming across the network.
- When the network supports multicast traffic, VLANs should be configured to ensure multicast traffic only goes to those user devices that use the service provided, such as remote video or audio applications. Routers must be configured to ensure that multicast traffic is forwarded to the network areas where it is requested.

Normal Data

- Normal data traffic is related to file I/O, print services, e-mail database access, and other shared network applications typical of business uses.
- VLANs are a natural solution for this type of traffic because you can easily segment users by their functions or geographic area to manage their specific needs.

The Role of VLANs in a Converged Network

- Describe the VLAN port membership modes



Static VLAN

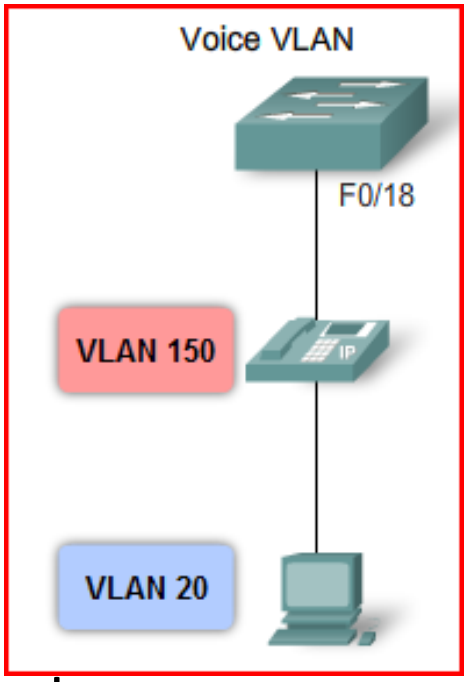
- Static VLAN - Ports on a switch are manually assigned to a VLAN.

```
S3#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
S3(config)#interface fastEthernet0/18
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```

Dynamic VLAN

- This mode is not widely used in production networks nor explored in this course.
- Dynamic VLAN membership is configured using a special VLAN Membership Policy Server (VMPS). The server uses VLAN-to-MAC address mappings.
- With the VMPS, you assign switch ports to VLANs dynamically based on the source MAC address of the device connected to the port.
- The benefit comes when you move a host from a port on one switch in the network to a port on another switch in the network. The switch dynamically assigns the new port to the proper VLAN for that host.
- High administrative overhead.

Voice VLAN



- In the figure, VLAN 150 is the voice VLAN, and VLAN 20 is the data VLAN.
- It is assumed that the network has been configured to ensure that voice traffic can be transmitted with a priority status over the network.
- When a phone is first plugged into a switch port that is in voice mode, the switch port sends messages to the phone providing the phone with the appropriate voice VLAN ID and configuration.
- The IP phone tags the voice frames with the voice VLAN ID and forwards all voice traffic through that VLAN.

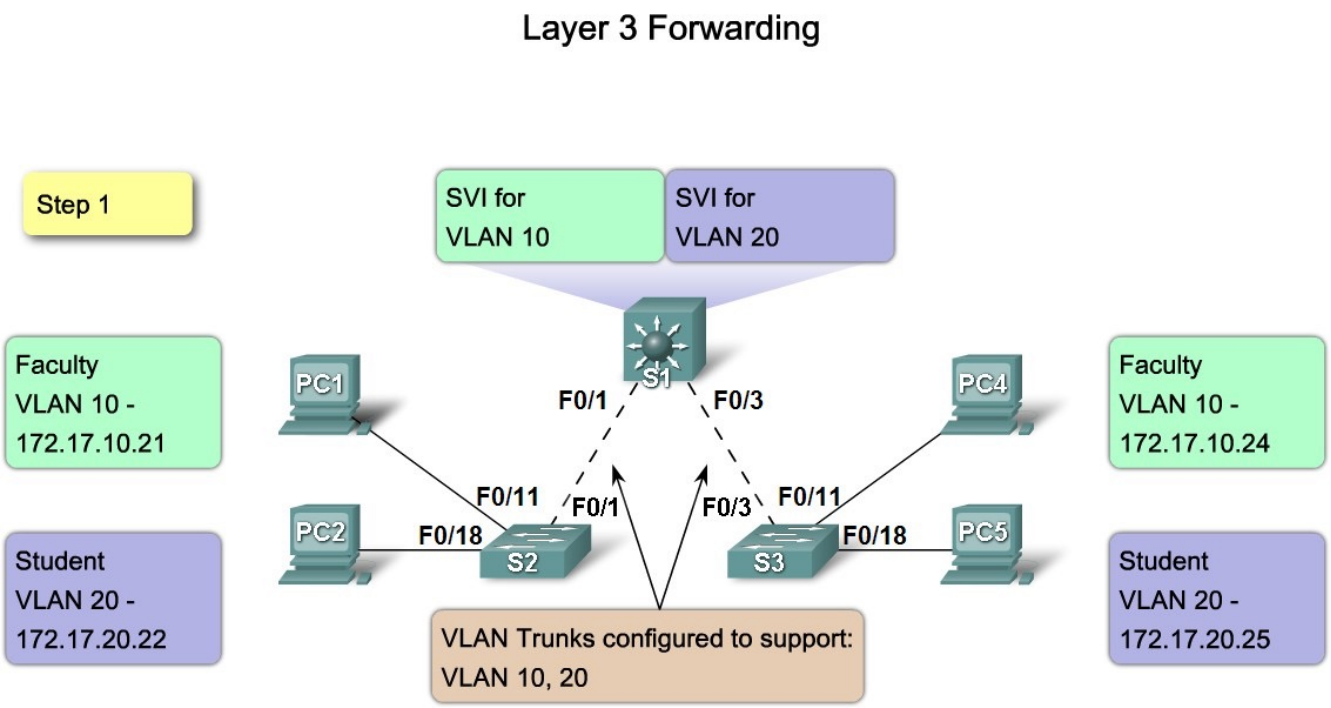
Configuring a Voice VLAN

```
S3#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S3(config)#interface fastEthernet 0/18
S3(config-if)#mls qos trust cos
S3(config-if)#switchport voice VLAN 150
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
```

```
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (VLAN0020)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (VLAN0150)
```

The Role of VLANs in a Converged Network

- Describe how to manage broadcast domains with VLANs



VLAN Tag – EtherType Field

- Set to the hexadecimal value of 0x8100.
- This value is called the tag protocol ID (TPID) value. With the EtherType field set to the TPID value, the switch receiving the frame knows to look for information in the tag control information field.
- The tag control information field contains the following:
  - Three bits of user priority - Used by the 802.1p standard (beyond the scope of this course), which specifies how to provide expedited transmission of Layer 2 frames.
  - 1 bit of Canonical Format Identifier (CFI) - Enables Token Ring frames to be carried across Ethernet links easily.
  - Twelve bits of VLAN ID (VID) - VLAN identification numbers; supports up to 4096 VLAN IDs.

Tagged Frames on the Native VLAN

- Some devices that support trunking, tag native VLAN traffic as a default behavior.
- Control traffic sent on the native VLAN should be untagged.
- If an 802.1Q trunk port receives a tagged frame on the native VLAN, it drops the frame.
- When configuring a switch port on a Cisco switch, you need to identify these devices and configure them so that they do not send tagged frames on the native VLAN.
- Devices from other vendors that support tagged frames on the native VLAN include IP phones, servers, routers, and non-Cisco switches.

Untagged Frames on the Native VLAN

- When a Cisco switch trunk port receives untagged frames it forwards those frames to the native VLAN.
- The default native VLAN is VLAN 1. When you configure an 802.1Q trunk port, a default Port VLAN ID (PVID) is assigned the value of the native VLAN ID.
- All untagged traffic coming in or out of the 802.1Q port is forwarded based on the PVID value.
- For example, if VLAN 99 is configured as the native VLAN, the PVID is 99 and all untagged traffic is forward to VLAN 99. If the native VLAN has not been reconfigured, the PVID value is set to VLAN 1.

Native VLAN Configuration

Cisco IOS CLI Command Syntax	
Enter global configuration mode on switch S1.	`S1#configure terminal`
Enter interface configuration mode.	`S1(config)#interface F0/1`
Define the F0/1 interface as an IEEE 802.1Q trunk.	`S1(config-if)#switchport mode trunk`
Configure the VLAN 99 to be the native VLAN.	`S1(config-if)#switchport trunk native vlan 99`
Return to privileged EXEC mode.	`S1(config-if)#end`

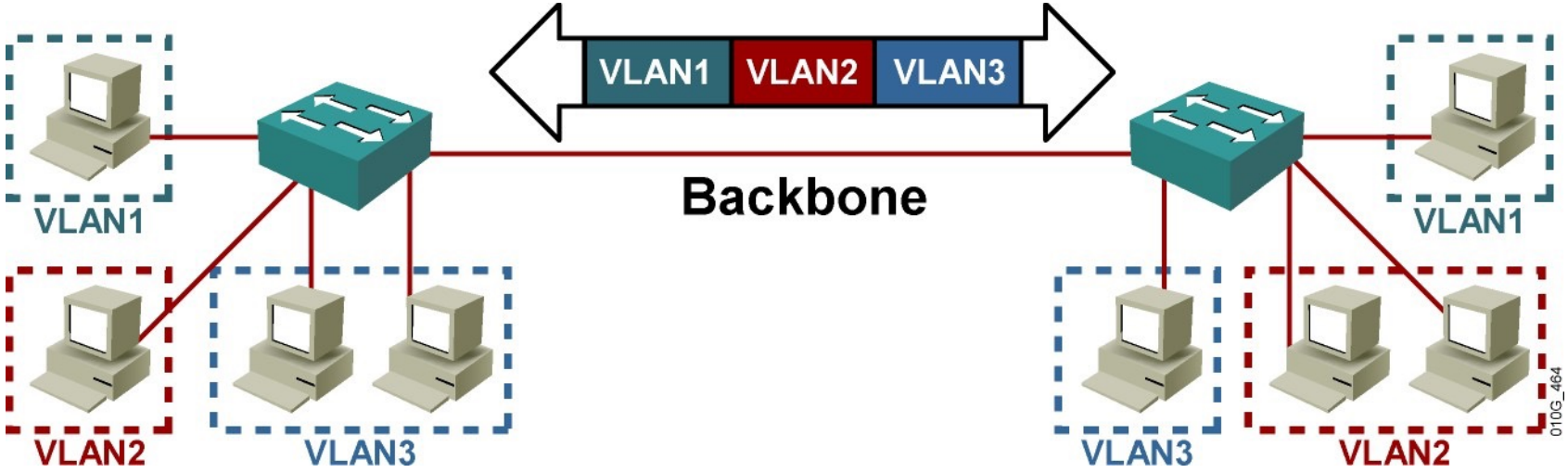
Trunking Modes

- A Cisco switch can be configured to support two types of trunk ports, IEEE 802.1Q and ISL.
- Today, only 802.1Q is used. However, legacy networks may still use ISL.
- An IEEE 802.1Q trunk port supports simultaneous tagged and untagged traffic.
- An 802.1Q trunk port is assigned a default PVID, and all untagged traffic travels on the port default PVID.
- All untagged traffic and tagged traffic with a null VLAN ID are assumed to belong to the port default PVID.
- A packet with a VLAN ID equal to the outgoing port default PVID is sent untagged. All other traffic is sent with a VLAN tag.

Dynamic Trunking Protocol (DTP)

- DTP is a Cisco proprietary protocol. DTP is automatically enabled on a switch port when certain trunking modes are configured on the switch port.
- DTP manages trunk negotiation only if the port on the other switch is configured in a trunk mode that supports DTP. DTP supports both ISL and 802.1Q trunks. This course focuses on the 802.1Q implementation of DTP.
- A detailed discussion on DTP is beyond the scope of this course; however, you will enable it in the labs and activities associated with the chapter. Switches do not need DTP to do trunking, and some Cisco switches and routers do not support DTP. To learn about DTP support on Cisco switches, visit:
  http://www.cisco.com/en/US/tech/tk389/tk689/technologies_tech_note09186a008017f86a.shtml

Trunking



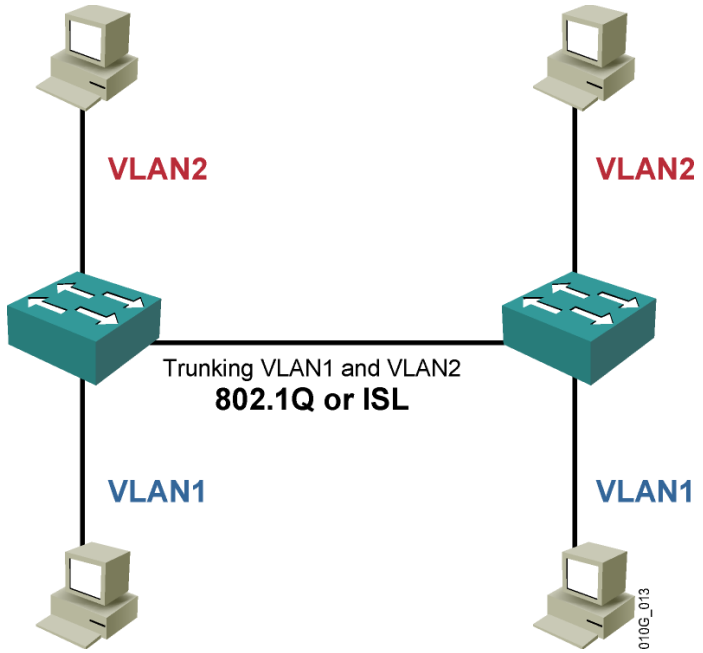
- What is a VLAN trunk?
  - Trunks carry traffic for multiple VLANs across the same physical link.
- What are the two trunking protocols used by Cisco switches?

Comparing ISL and 802.1Q

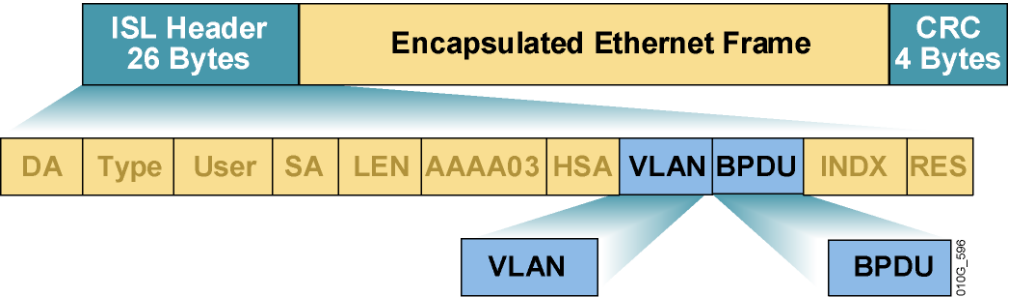
ISL	802.1Q
Proprietary	Nonproprietary
Encapsulated	Tagged
Protocol independent	Protocol dependent
Encapsulates the old frame in a new frame	Adds a field to the frame header

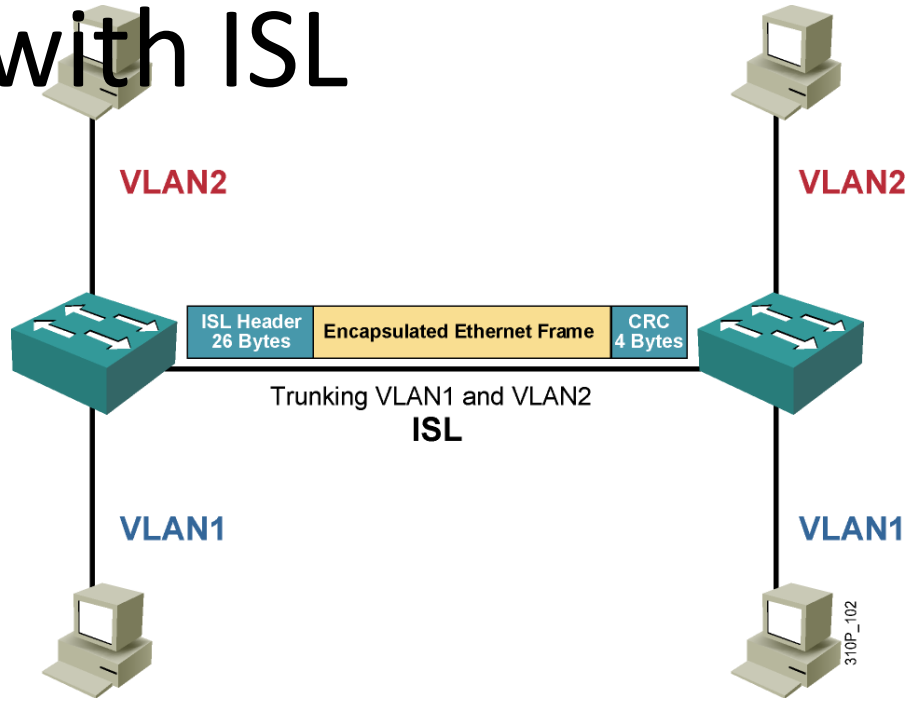
ISL (Inter-Switch Link) is no longer supported by Cisco, opting for 802.1 Q.

Note: Not all switches support both protocols.



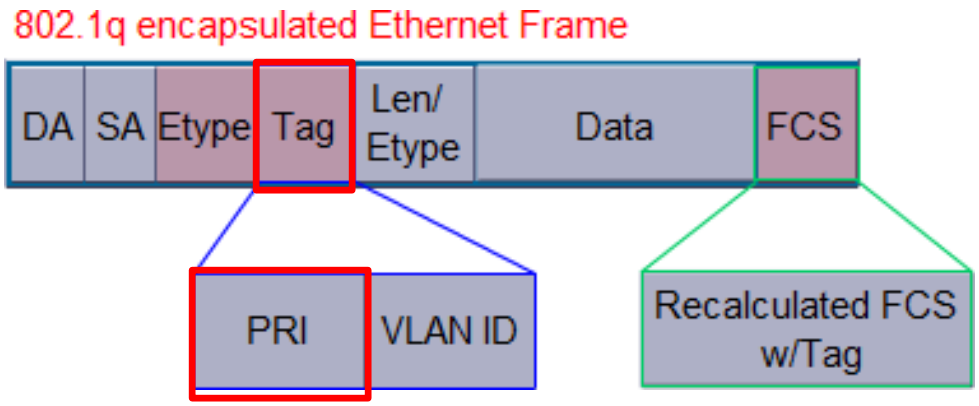
Trunking with ISL

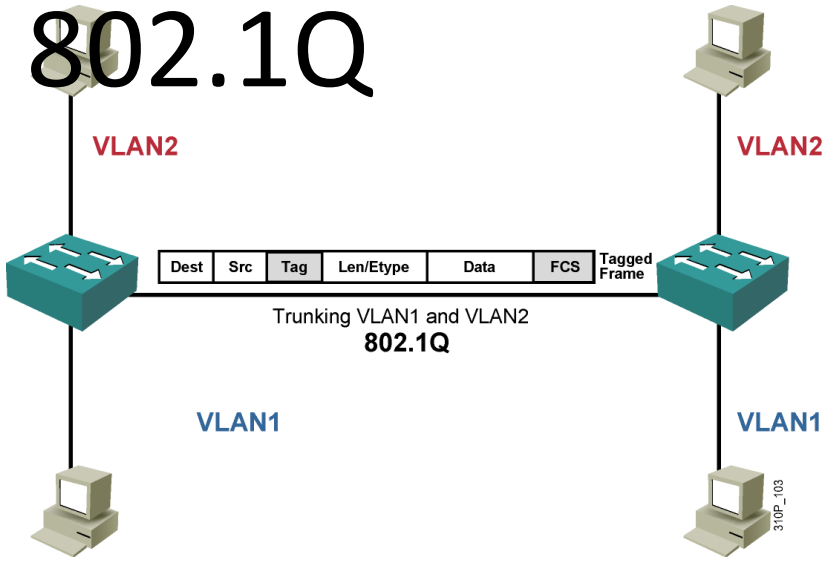




- Is a Cisco proprietary protocol
- Uses an encapsulation process
- Does not modify the original frame

Trunking with 802.1Q





- An IEEE standard
- Adds a 4-byte tag to the original frame
- Additional tag includes a priority field
- More in Part 2

DTP and Switchport Mode Interactions

Note: Table assumes DTP is enabled at both ends.

	Default Dynamic Auto	Dynamic Desirable	Trunk	Access
Default Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

```
ALS1(config-if)# switchport mode ?
  access    Set trunking mode to ACCESS unconditionally
  dynamic   Set trunking mode to dynamically negotiate access or trunk mode
  trunk     Set trunking mode to TRUNK unconditionally

ALS1(config-if)# switchport mode dynamic ?
  auto       Set trunking mode dynamic negotiation parameter to AUTO
  desirable  Set trunking mode dynamic negotiation parameter to DESIRABLE
```

Configure DLS1 for Trunking

```
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
ALS1(config-if-range)#
```

- What will this do to these two links?
- Does ALS2 need to be configured as a trunk?

	Default Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access

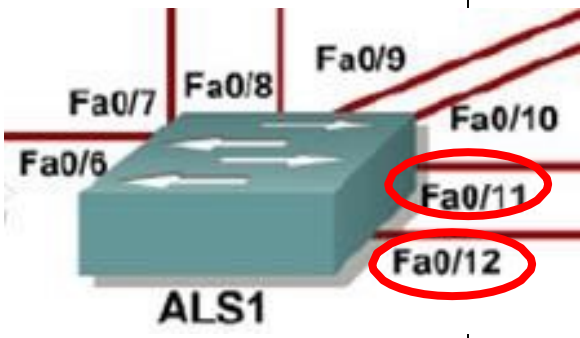

```
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
```

Trunking! We will verify this on ALS1 in a moment.

```
ALS1# show interface trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      on           802.1q         trunking      1
Fa0/12      on           802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/11      1-4094
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1
Fa0/12      1

Port        Vlans in spanning tree forwarding state and not
   pruned
Fa0/11      1
Fa0/12      1
ALS1#
```

ALS1 – Manually Configured Trunk

```
ALS1# show inter fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
<output omitted>
```



- Why is the administrative mode "trunk"?
  - Because we configured the port(s) as trunking:

```
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
```

ALS2 – Default Dynamic A

```
ALS2# show inter fa 0/11 switchport
Name: Fa0/11
Switchport: Enabled
Administrative Mode: dynamic auto
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
```

	Dynamic Auto
Dynamic Auto	Access
Dynamic Desirable	Trunk
Trunk	Trunk
Access	Access

What is the DTP setting on ALS2? (This did not change.)

Is this the default on a 3560 switch? ***Yes***

Notice it is now trunking because the other end is set to trunk.

ALS2 – Default Dynamic Auto

```
ALS2#show interfaces trunk

Port        Mode         Encapsulation  Status        Native vlan
Fa0/11      auto         802.1q         trunking      1
Fa0/12      auto         802.1q         trunking      1

Port        Vlans allowed on trunk
Fa0/11      1-4094
Fa0/12      1-4094

Port        Vlans allowed and active in management domain
Fa0/11      1
Fa0/12      1

Port        Vlans in spanning tree forwarding state and not pruned
Fa0/11      1
Fa0/12      none
```

- Verifying trunks on ALS2

Status

	Default Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not recommended
Access	Access	Access	Not recommended	Access


```
ALS1(config)# interface range fastethernet 0/11 - 12
ALS1(config-if-range)# switchport mode trunk
```

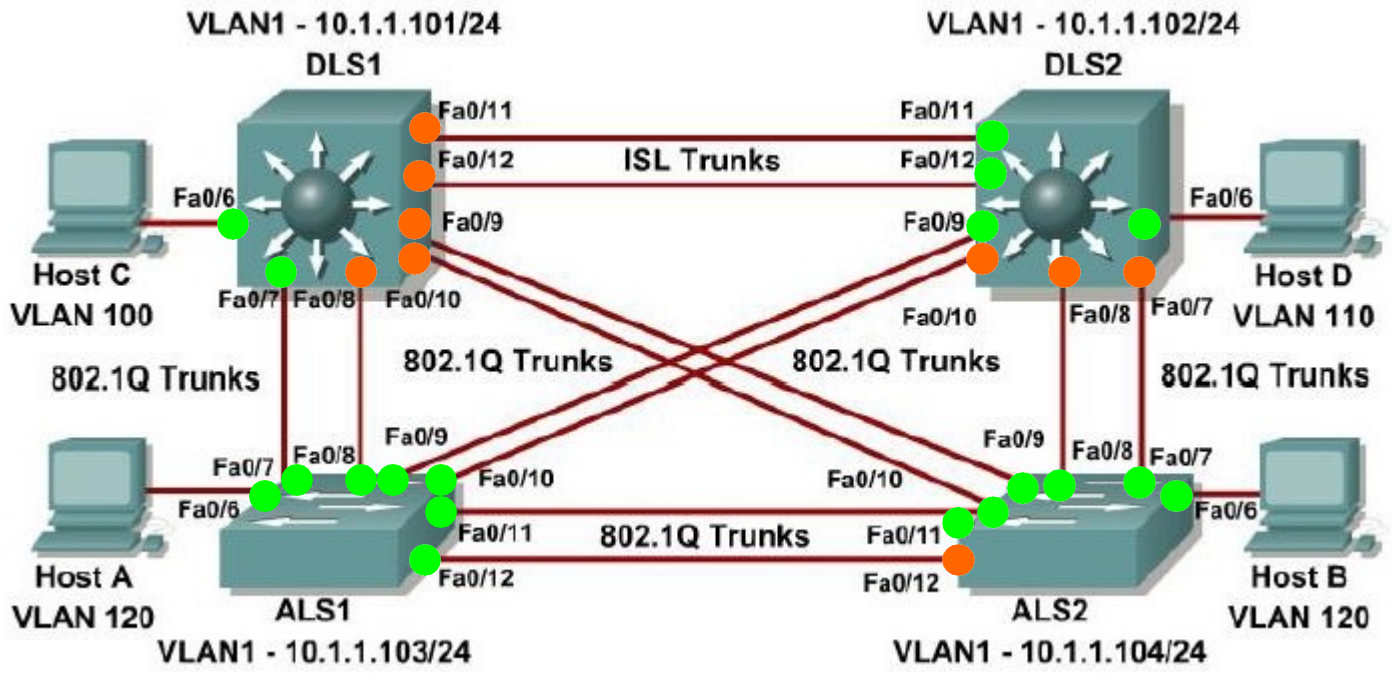
No additional configuration needed on ALS2.

Switches that support both ISL and 802.1Q

```
Switch(config)# interface range fastethernet 0/1 - 4
Switch(config-if-range)# switchport mode trunk
Command rejected: An interface whose trunk encapsulation is
   "Auto" can not be configured to "trunk" mode.
Switch(config-if-range)# switchport trunk encapsulation dot1q
Switch(config-if-range)# switchport mode trunk
```

- What happens when we use the switchport mode trunk command without specifying the encapsulation on switches that support both protocols?
  - On switches that support multiple trunking encapsulations (802.1Q and ISL), you must first configure the trunking encapsulation before setting the interface to trunk mode.
  - The switchport trunk encapsulation command must be configured before the switchport mode trunk.

Configure the rest of the trunk links



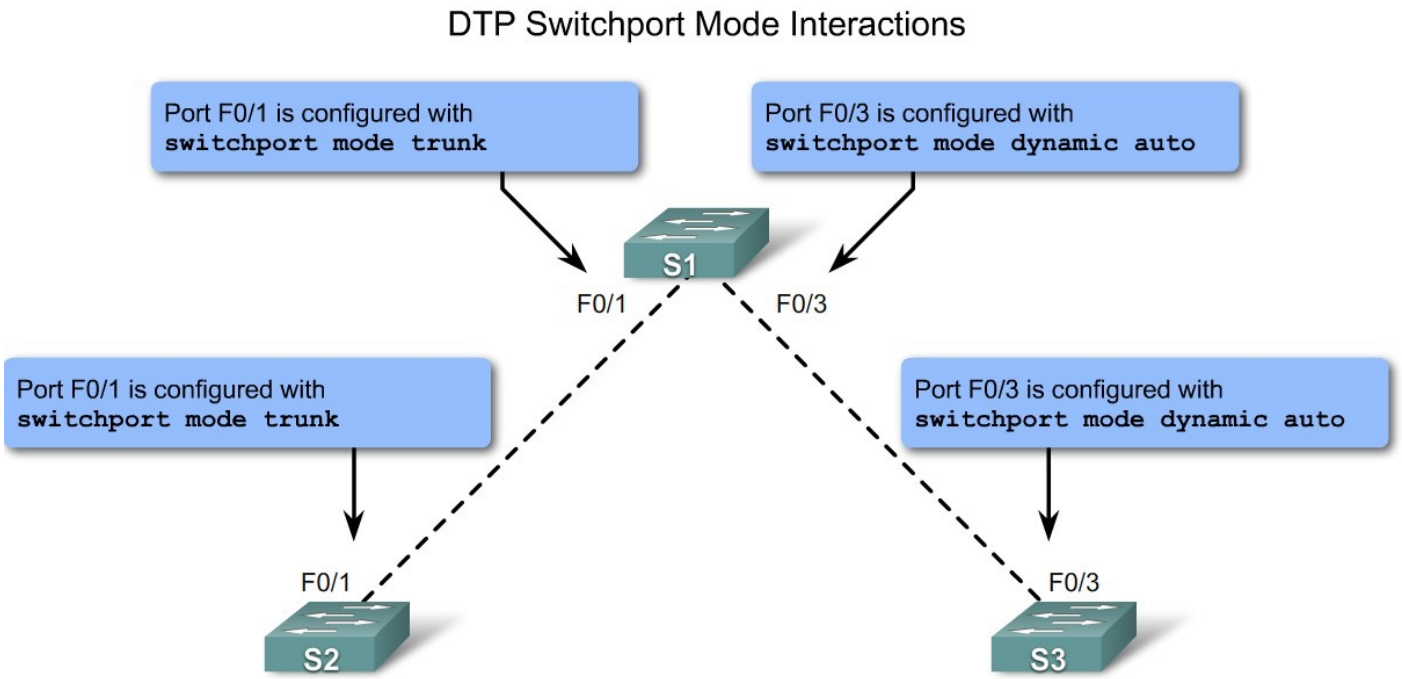
- What about the VTP domain names on DLS1 and DLS2?
  - No other trunk links configured so DLS1 and DLS2 still have no VTP domain name.
- Trunking only configured between ALS1 and ALS2.
- Configure the rest if the trunk links as shown in the topology.
- Packet Tracer only supports 802.1Q trunks, not ISL.

Trunking Modes

- A switch port on a Cisco switch supports a number of trunking modes.
- The trunking mode defines how the port negotiates using DTP to set up a trunk link with its peer port.
- The available trunking modes are:
  - On (default)
  - Dynamic auto
  - Dynamic desirable
  - Off

Explain the Role of Trunking VLANs in a Converged Network

- Describe the switch port trunking modes



Trunking Mode On

- The switch port periodically sends DTP frames, called advertisements, to the remote port.
- The command to enable trunking is **switchport mode trunk**. The local switch port advertises to the remote port that it is dynamically changing to a trunking state.
- The local port then, regardless of what DTP information the remote port sends as a response to the advertisement, changes to a trunking state. The local port is considered to be in an unconditional (always on) trunking state.

Dynamic Auto

- The switch port periodically sends DTP frames to the remote port.
- The command used is **switchport mode dynamic auto**.
- The local switch port advertises to the remote switch port that it is able to trunk but does not request to go to the trunking state.
- After a DTP negotiation, the local port ends up in trunking state only if the remote port trunk mode has been configured to be on or desirable.
- If both ports on the switches are set to auto, they do not negotiate to be in a trunking state. They negotiate to be in the access (non-trunk) mode state.

Dynamic Desirable

- DTP frames are sent periodically to the remote port.
- The command used is **switchport mode dynamic desirable**.
- The local switch port advertises to the remote switch port that it is able to trunk and asks the remote switch port to go to the trunking state.
- If the local port detects that the remote has been configured in on, desirable, or auto mode, the local port ends up in trunking state.
- If the remote switch port is in the nonegotiate mode, the local switch port remains as a nontrunking port.

DTP Switch Modes

	Dynamic Auto	Dynamic Desireable	Trunk	Access
Dynamic Auto	Access	Trunk	Trunk	Access
Dynamic Desireable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	Trunk	Not Recommended
Access	Access	Access	Not Recommended	Access

Note: Table assumes DTP is enabled at both ends.

* `show dtp interface` - to determine current settings

What is a VLAN trunk?

- A trunk is a point-to-point link between two network devices that carries more than one VLAN.
- A VLAN trunk allows you to extend the VLANs across an entire network.
- Cisco supports IEEE 802.1Q for coordinating trunks on Fast Ethernet and Gigabit Ethernet interfaces. You will learn about 802.1Q later in this section.
- A VLAN trunk does NOT belong to a specific VLAN, rather it is a conduit for VLANs between switches and routers.

VLAN Deletion

- The global configuration command **no vlan vlan-id** removes VLANs from the system. The show vlan brief command verifies that VLAN 20 is no longer in the vlan.dat file.
- Alternatively, the entire vlan.dat file can be deleted using the command **delete flash:vlan.dat** from privileged EXEC mode. After the switch is reloaded, the previously configured VLANs will no longer be present. This effectively places the switch into is "factory default" concerning VLAN configurations.
- **Note:** Before deleting a VLAN, be sure to first reassign all member ports to a different VLAN. Any ports that are not moved to an active VLAN are unable to communicate with other stations after you delete the VLAN.

802.1Q Trunk Configuration

```
S1#config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
S1(config)#interface f0/1
S1(config-if)#switchport mode trunk
S1(config-if)#switchport trunk native vlan 99
S1(config-if)#end
```

802.1Q Trunk Verification

```
S1#show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 99 (management)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
Administrative private-vlan host-association: none
Administrative private-vlan mapping: none
Administrative private-vlan trunk native VLAN: none
Administrative private-vlan trunk Native VLAN tagging: enabled
Administrative private-vlan trunk encapsulation: dot1q
Administrative private-vlan trunk normal VLANs: none
Administrative private-vlan trunk private VLANs: none
Operational private-vlan: none
Trunking VLANs Enabled: 10,20,30
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

Common VLAN and Trunk Problems

- **Native VLAN mismatches** - Trunk ports are configured with different native VLANs. This configuration error generates console notifications, causes control and management traffic to be misdirected, and poses a security risk.
- **Trunk mode mismatches** - One trunk port is configured with trunk mode "off" and the other with trunk mode "on". This configuration error causes the trunk link to stop working.
- **VLANs and IP Subnets -** End user devices configured with incorrect IP addresses will not have network connectivity. Each VLAN is a logically separate IP subnetwork. Devices within the VLAN must be configured with the correct IP settings.
- **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.

ISL Trunk Port

- In an ISL trunk port, all received packets are expected to be encapsulated with an ISL header, and all transmitted packets are sent with an ISL header. Native (non-tagged) frames received from an ISL trunk port are dropped. ISL is no longer a recommended trunk port mode, and it is not supported on a number of Cisco switches.

Configure VLANs on the Switches in a Converged Network Topology

- Describe the steps to configure trunks and VLANs

Configuring VLANs and Trunks Overview

Use the following steps to configure and verify VLANs and trunks on a switched network:

1. Create the VLANs.

2. Assign switch ports to VLANs statically

3. Verify VLAN configuration

4. Enable trunking on the inter-switch connections.

5. Verify trunk configuration.

Configure VLANs on the Switches in a Converged Network Topology

- Describe the Cisco IOS commands used to create a trunk on a Cisco Catalyst switch

Configure an 802.1Q Trunk

Cisco IOS CLI Command Syntax	
Enter global configuration mode.	#configure terminal
Enters the interface configuration mode for the defined interface.	(config)#interface *interface id*
Force the link connecting the switches to be a trunk link.	(config-if)#switchport mode trunk
Specify another VLAN as the native VLAN for untagged for IEEE 802.1Q trunks.	(config)#switchport trunk native vlan *vlan-id*
Add the VLANs allowed on this trunk.	(config-if)#switchport trunk allowed vlan add *vlan-list*
Return to privileged EXEC mode.	(config-if)#end

Troubleshoot Common Software or Hardware Misconfigurations Associated with VLANs

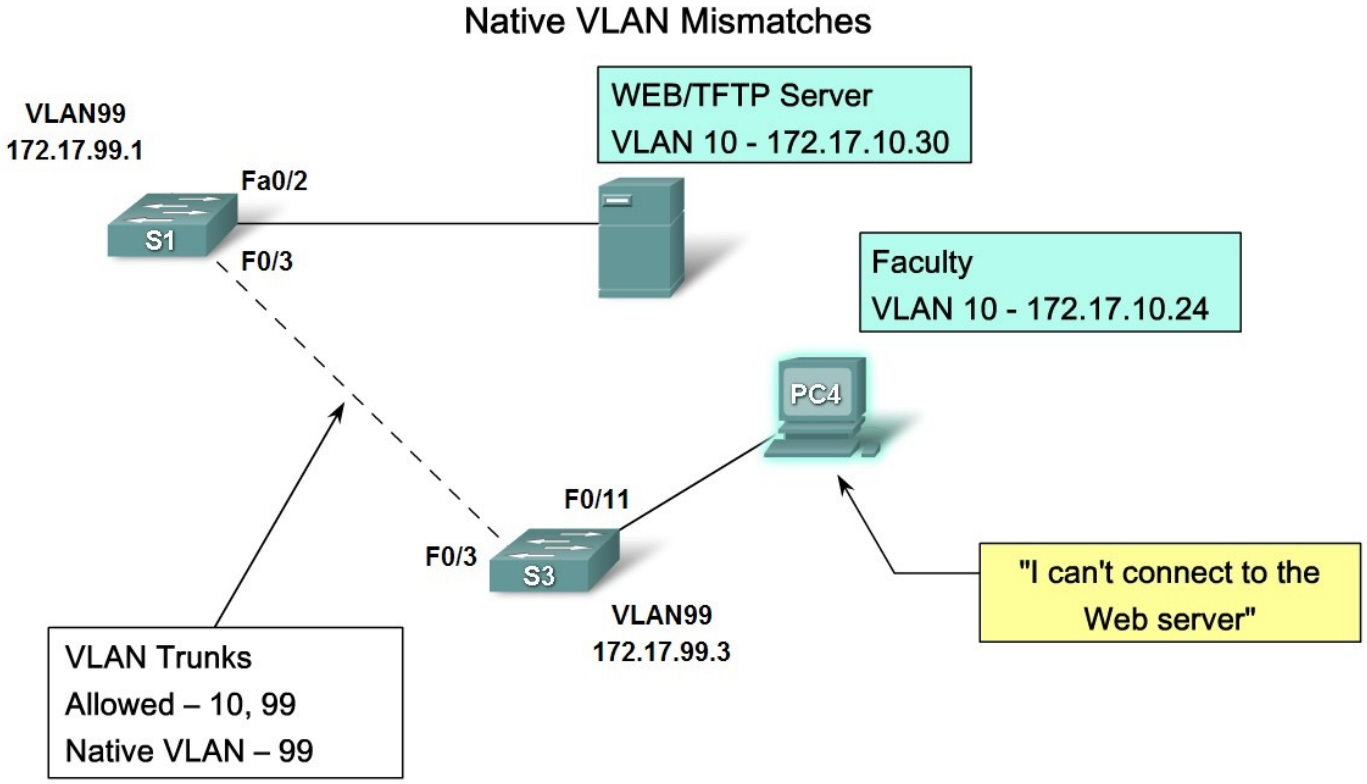
- Describe the common problems with VLANs and trunks

Common Problems with VLANs and Trunks

Problem	Result	Example
Native VLAN mismatches	Pose a security risks and create unintended results	For example one port has defined as VLAN 99, the other defined as VLAN 100
Trunk mode mismatches	Causes loss of network connectivity	For example on port configured as trunk mode "off" and the other as trunk mode "on".
VLANs and IP Subnets	Causes loss of network connectivity	For example user computers may have been configured with the incorrect IP addresses.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic is being sent over the trunk	The list of allowed VLANs does not support current VLAN trunking requirements.

Troubleshoot Common Software or Hardware Misconfigurations Associated with VLANs

- Describe the common problems with VLANs and trunks



Summary

VLANS

- Allows an administrator to logically group devices that act as their own network
- Are used to segment broadcast domains
- Some benefits of VLANs include
- Cost reduction, security, higher performance, better management

Summary

- Types of Traffic on a VLAN include
  - –Data
  - –Voice
  - –Network protocol
  - –Network management
- Communication between different VLANs requires the use of
  - – Routers

Summary

- Trunks

  A common conduit used by multiple VLANS for intra-VLAN communication

- IEEE 802.1Q

  The standard trunking protocol

  Uses frame tagging to identify the VLAN to which a frame belongs

  Does not tag native VLAN traffic