Switch Configuration
and
VLANs

Introduction to Networks v6.0

Chapter 6: VLANs

Pertemuan ke 20

Kompetensi Khusus

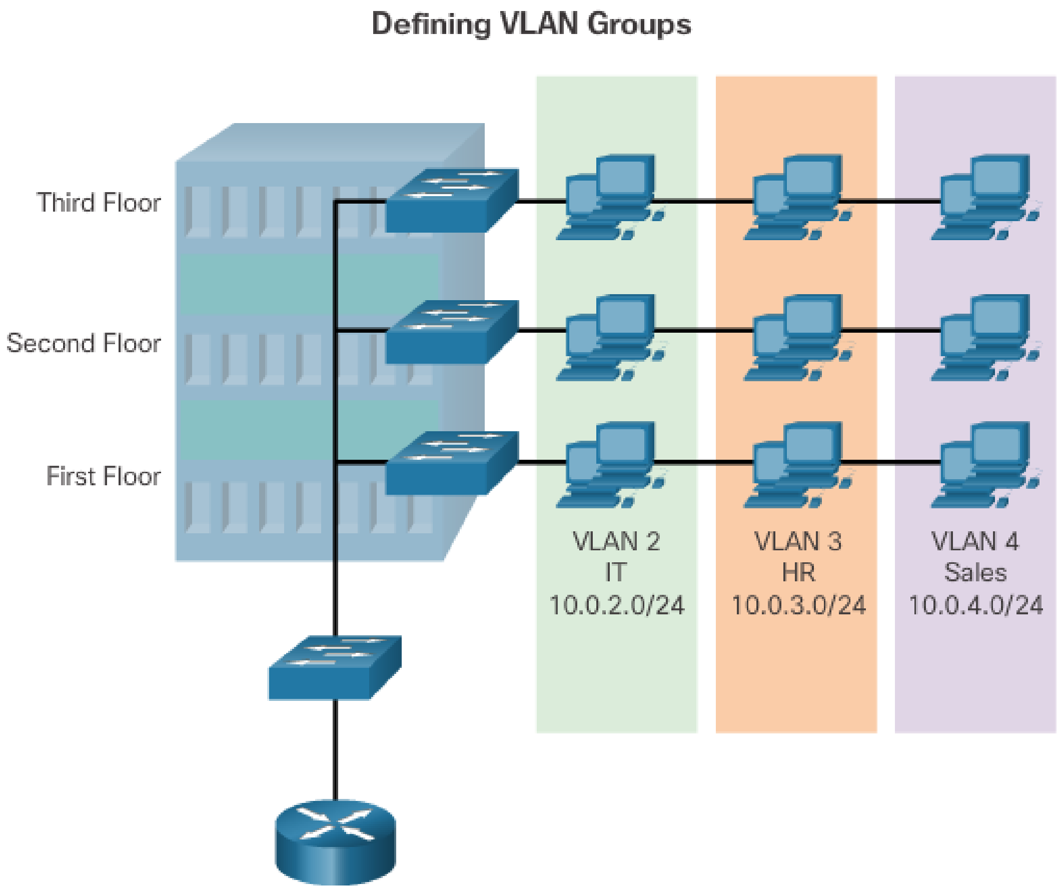
- Mahasiswa dapat melakukan konfigurasi switch dan pembagian VLAN untuk mengatur jalur akses dalam jaringan (C3)

Materi:

1. Basic Switch Configuration
2. Switch Security
3. VLAN Segmentation
4. VLAN Implementations
5. Inter-VLAN Routing Using Routers

1. VLAN Segmentation

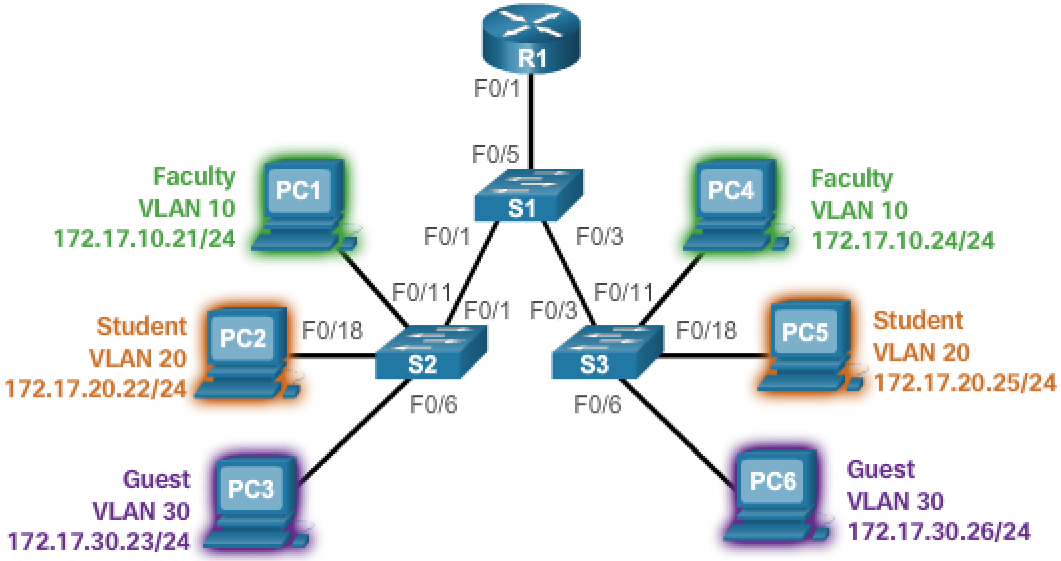
1.1 VLAN Definitions



1.1 VLAN Definitions

- VLANs allow an administrator to segment networks based on factors such as function, project team, or application, without regard for the physical location of the user or device.
- VLANs enable the implementation of access and security policies according to specific groupings of users.
- A VLAN is a logical partition of a Layer 2 network.
- Multiple partitions can be created, allowing for multiple VLANs to co-exist.
- Each VLAN is a broadcast domain, usually with its own IP network.
- VLANs are mutually isolated, and packets can only pass between them via a router.
- The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
- The hosts grouped within a VLAN are unaware of the VLAN’s existence.

1.2 Benefits of VLANs



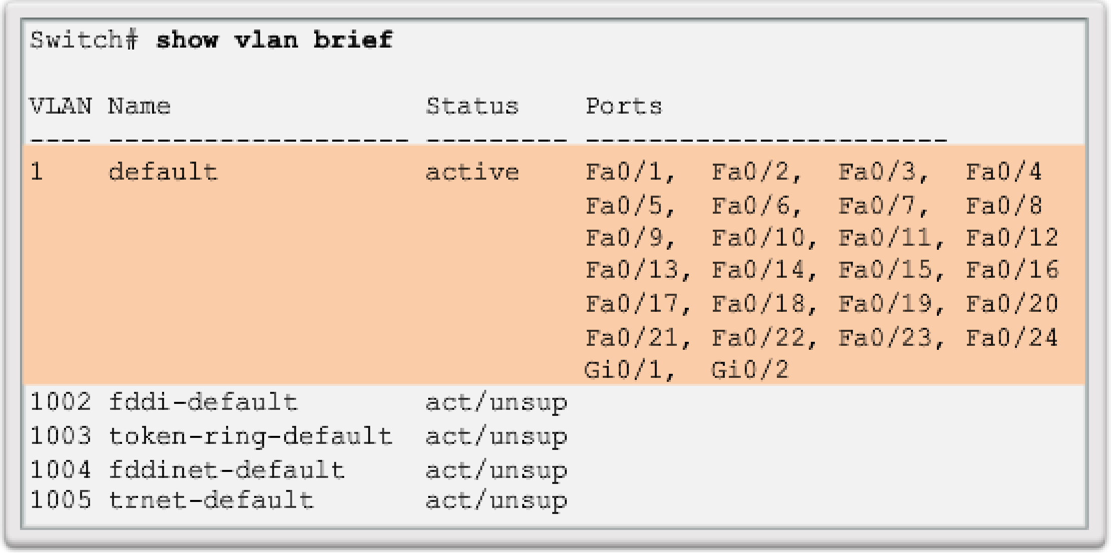
- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency
- Simpler Project and Application Management

1.3 Types of VLANs

- Data VLAN – user generated traffic
- Default VLAN – all switch ports become part of this VLAN until switch is configured, **`show vlan brief`**
- Native VLAN – used for untagged traffic
- Management VLAN – used to access management capabilities

1.3 Types of VLANs

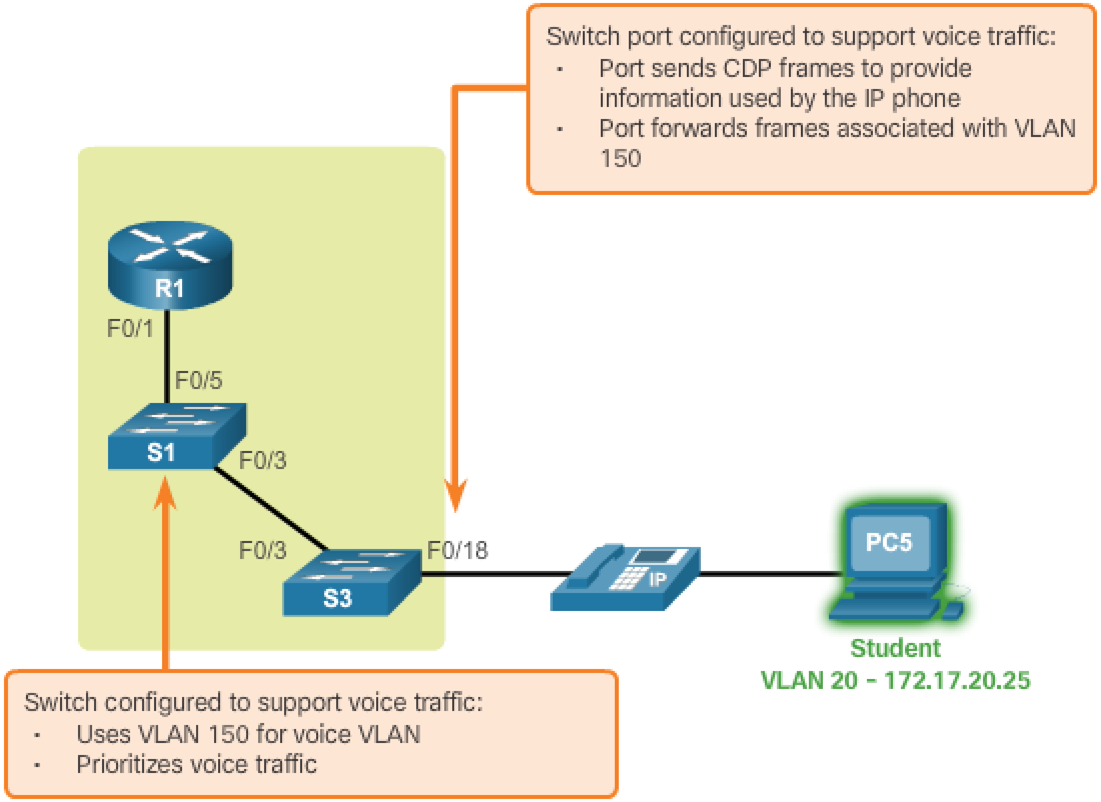
VLAN 1



```
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
```

- All ports assigned to VLAN 1 by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.

1.4 Voice VLANs



Switch port configured to support voice traffic:
- Port sends CDP frames to provide information used by the IP phone
- Port forwards frames associated with VLAN 150

Switch configured to support voice traffic:
- Uses VLAN 150 for voice VLAN
- Prioritizes voice traffic

1.4 Voice VLANs

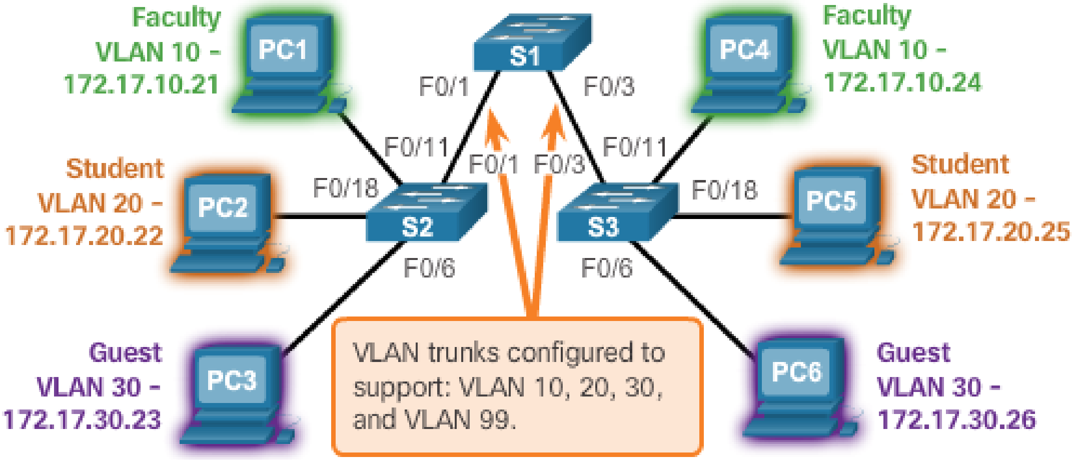
- VoIP traffic is time-sensitive and requires:
  - Assured bandwidth to ensure voice quality.
  - Transmission priority over other types of network traffic.
  - Ability to be routed around congested areas on the network.
  - Delay of less than 150 ms across the network.
- The voice VLAN feature enables access ports to carry IP voice traffic from an IP phone.

1.5 VLAN Trunks

The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network. This network could not function without VLAN trunks.

VLAN 10 Faculty/Staff - 172.17.10.0/24
VLAN 20 Students - 172.17.20.0/24
VLAN 30 Guest - 172.17.30.0/24
VLAN 99 Management and Native - 172.17.99.0/24

F0/1-5 are 802.1Q trunk interfaces with native VLAN 99.
F0/11-17 are in VLAN 10.
F0/18-24 are in VLAN 20.
F0/6-10 are in VLAN 30.



VLAN trunks configured to support: VLAN 10, 20, 30, and VLAN 99.

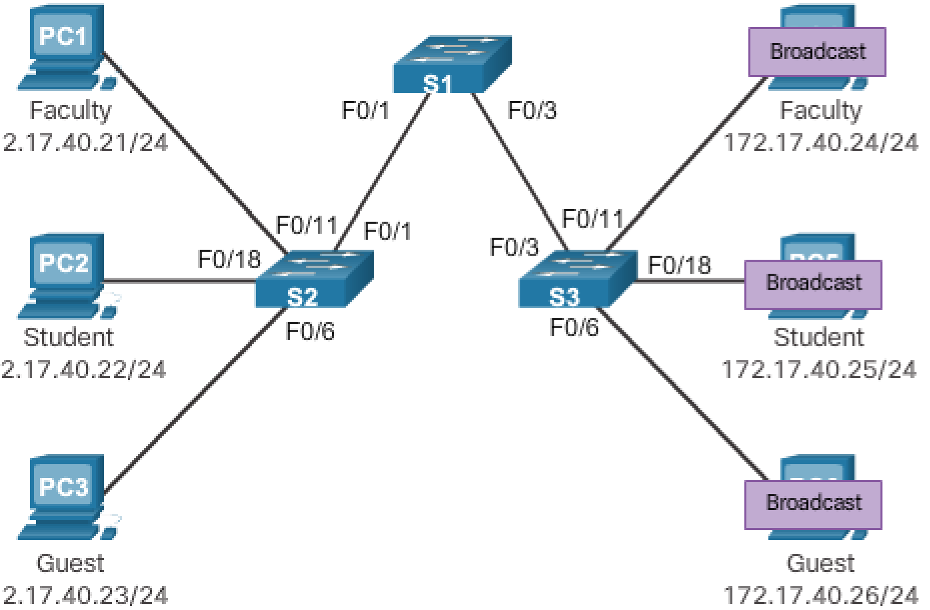
1.5 VLAN Trunks

- A VLAN trunk is a point-to-point link that carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco IOS supports IEEE802.1q, a popular VLAN trunk protocol.

1.6 Controlling Broadcast Domains with VLANs

No VLAN Segmentation

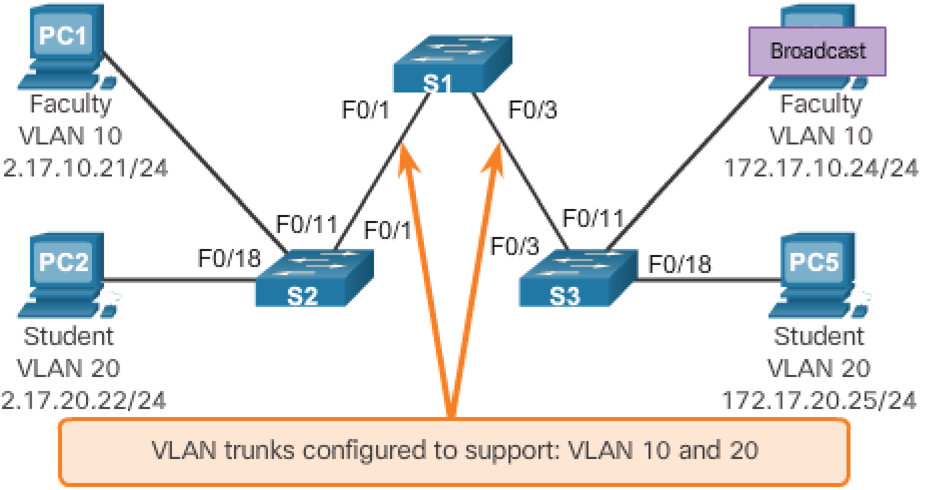
PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame out all available ports.



1.6 Controlling Broadcast Domains with VLANs

With VLAN Segmentation

PC1 sends out a local Layer 2 broadcast. The switches forward the broadcast frame only out ports configured for VLAN10.



1.6 Controlling Broadcast Domains with VLANs

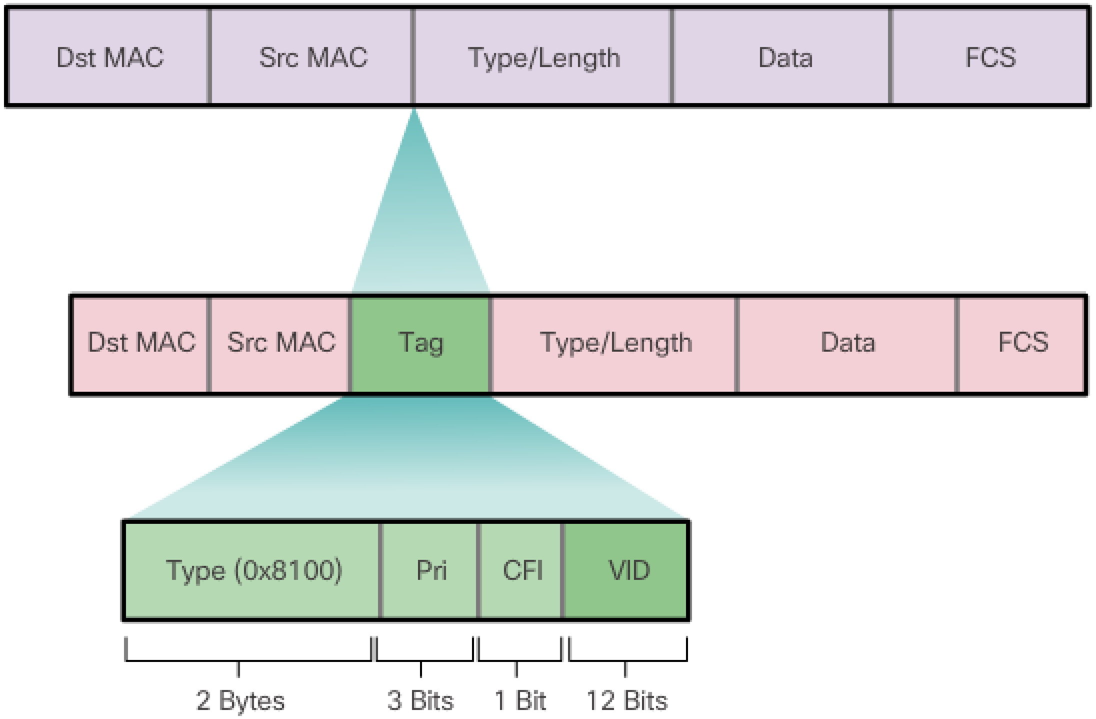
- VLANs can be used to limit the reach of broadcast frames.
- A VLAN is a broadcast domain of its own.
- A broadcast frame sent by a device in a specific VLAN is forwarded within that VLAN only.
- VLANs help control the reach of broadcast frames and their impact in the network.
- Unicast and multicast frames are forwarded within the originating VLAN.

1.7 Tagging Ethernet Frames for VLAN Identification

- Frame tagging is the process of adding a VLAN identification header to the frame.
- It is used to properly transmit multiple VLAN frames through a trunk link.
- Switches tag frames to identify the VLAN to which they belong.
- Different tagging protocols exist; IEEE 802.1Q is a vey popular example.
- The protocol defines the structure of the tagging header added to the frame.
- Switches add VLAN tags to the frames before placing them into trunk links and remove the tags before forwarding frames through non-trunk ports.
- When properly tagged, the frames can transverse any number of switches via trunk links and still be forwarded within the correct VLAN at the destination.

1.7 Tagging Ethernet Frames for VLAN Identification

Fields in an Ethernet 802.1Q Frame



1.8 Native VLANs and 802.1Q Tagging

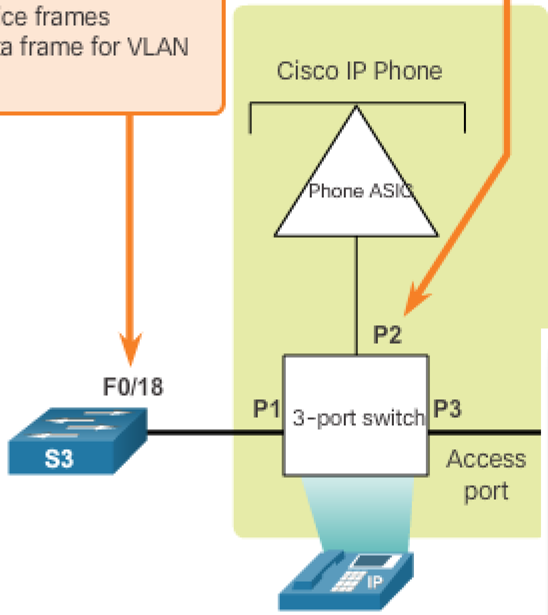
- Control traffic sent on the native VLAN should not be tagged.
- Frames received untagged, remain untagged and are placed in the native VLAN when forwarded.
- If there are no ports associated to the native VLAN and no other trunk links, an untagged frame is dropped.
- When configuring a switch port on a Cisco switch, configure devices so that they do not send tagged frames on the native VLAN.
- In Cisco switches, the native VLAN is VLAN 1, by default.

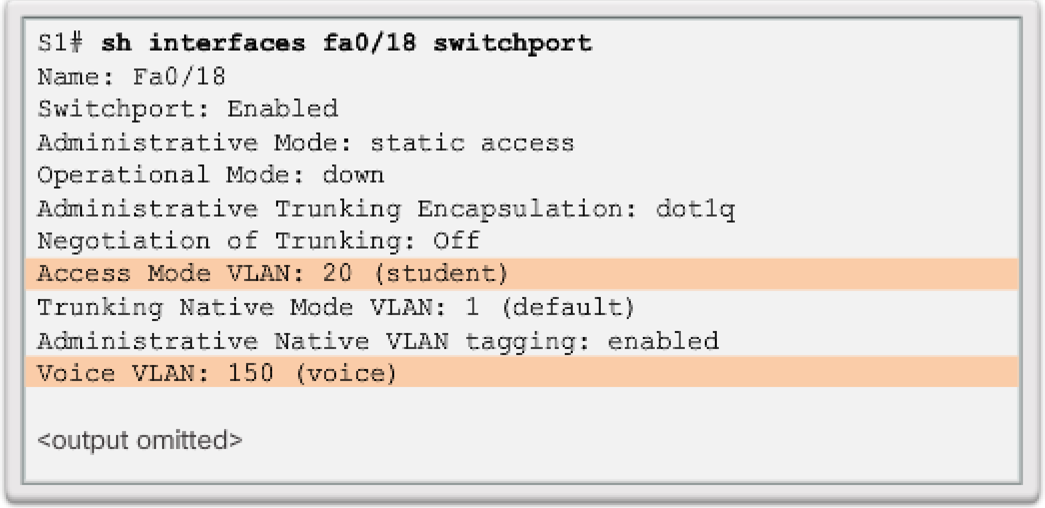
1.9 Voice VLAN Tagging

Switch port configured to support voice traffic:

- Instructs phone to tag voice frames with VLAN 150
- Prioritizes voice frames
- Forwards data frame for VLAN 20

Configured to tag voice traffic frames with VLAN 150.

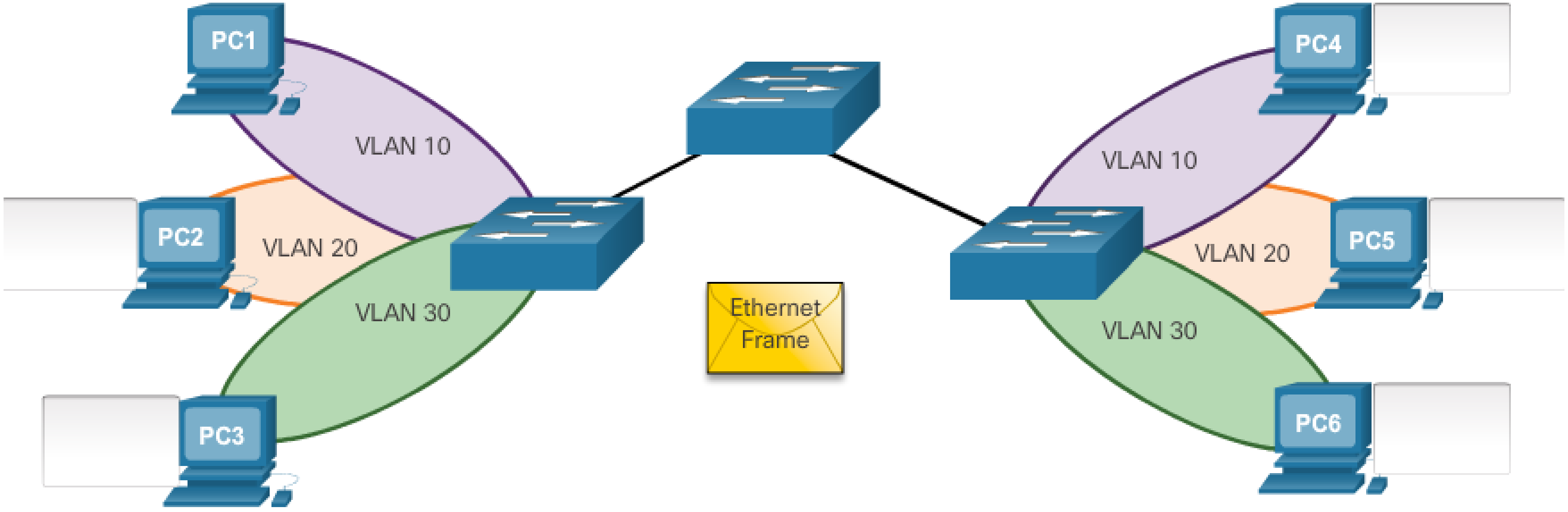




```
S1# sh interfaces fa0/18 switchport
Name: Fa0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 20 (student)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: 150 (voice)

<output omitted>
```

1.10 Activity – Predict Switch Behavior

- Scenario 1: PC 1 sends a broadcast.
- Scenario 2: PC 2 sends a broadcast.
- Scenario 3: PC 3 sends a broadcast.



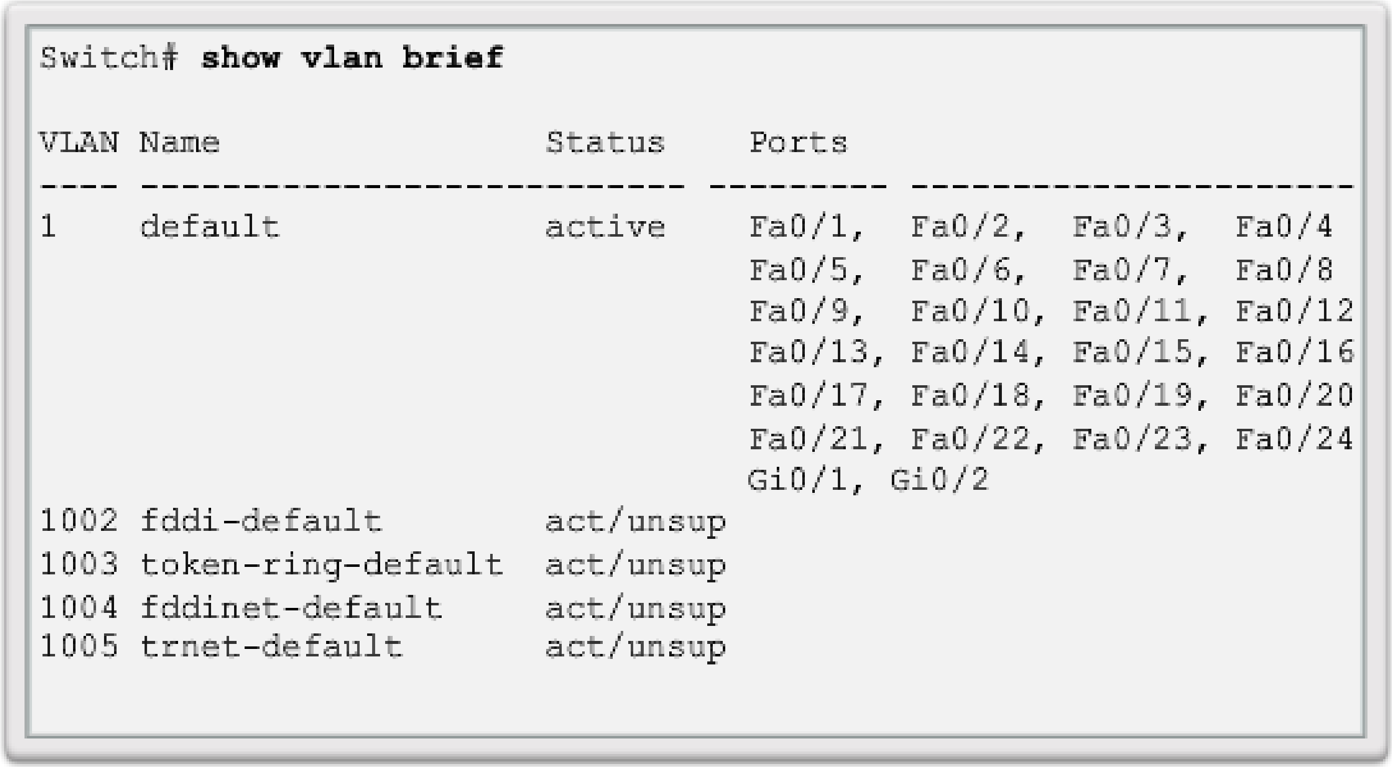
2. VLAN Implementations

2.1 VLAN Ranges on Catalyst Switches

- Cisco Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.
- VLANs are split into two categories:
  - Normal range VLANs
    - VLAN numbers from 1 to 1,005
    - Configurations stored in the vlan.dat (in the flash memory)
    - IDs 1002 through 1005 are reserved for Token Ring and Fiber Distributed Data Interface (FDDI) VLANs, automatically created and cannot be removed
  - Extended Range VLANs
    - VLAN numbers from 1,006 to 4,096
    - Configurations stored in the running configuration (NVRAM)
    - VLAN Trunking Protocol (VTP) does not learn extended VLANs

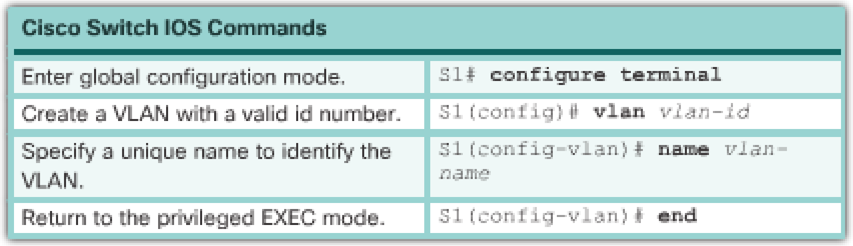
2.1 VLAN Ranges on Catalyst Switches

- Normal Range VLANs



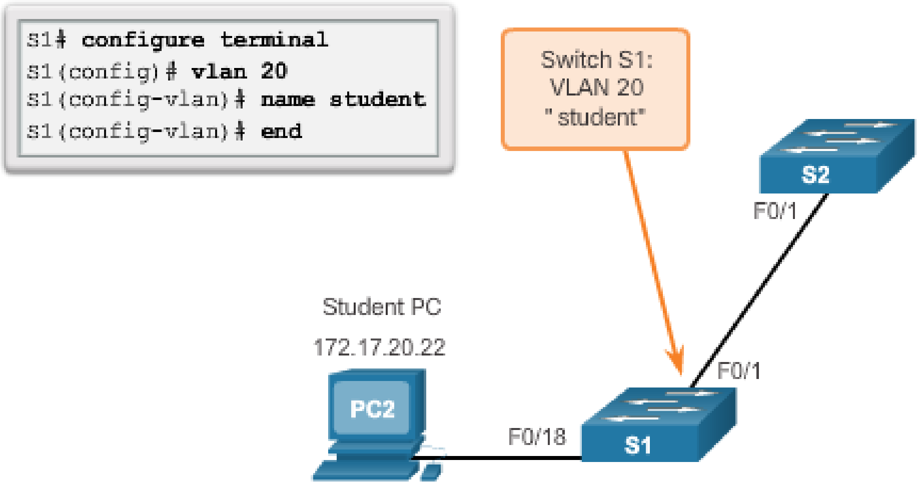
```
Switch# show vlan brief

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
```

2.2 Creating a VLAN



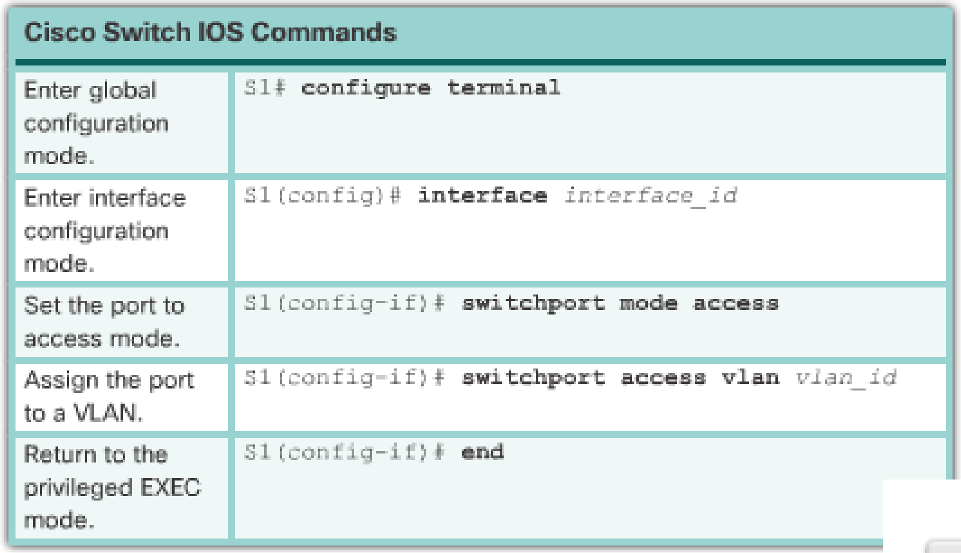
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan-id`
Specify a unique name to identify the VLAN.	`S1(config-vlan)# name vlan-name`
Return to the privileged EXEC mode.	`S1(config-vlan)# end`

Sample Configuration

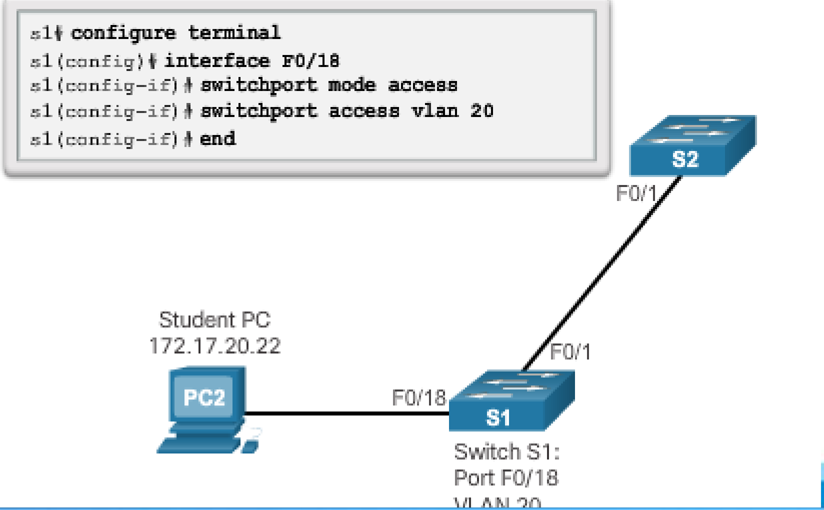


```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

2.3 Assigning Ports to VLANs

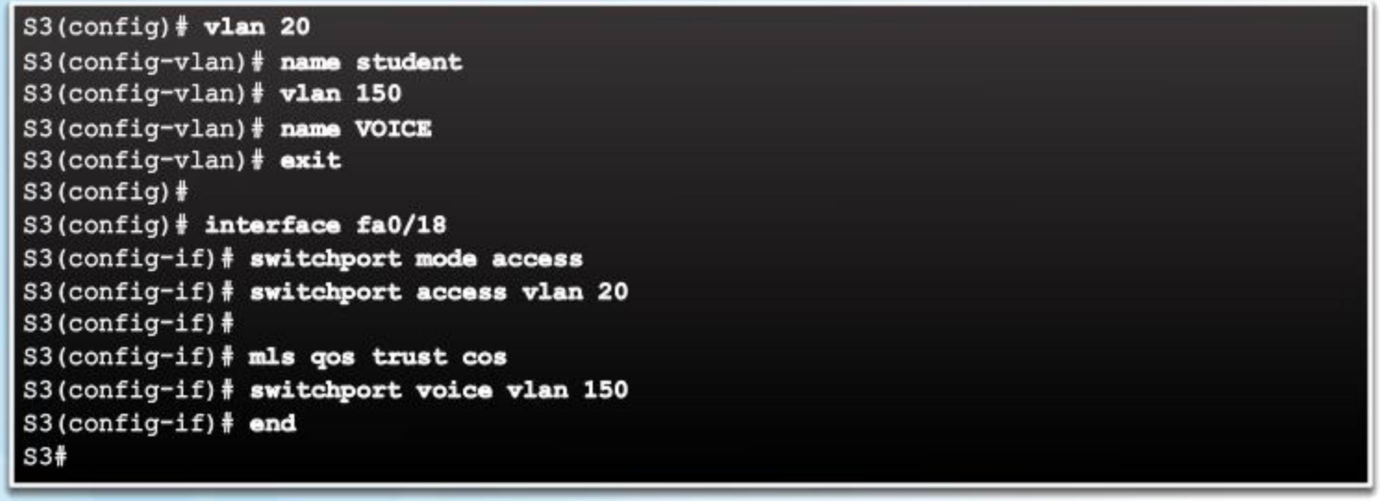


Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`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

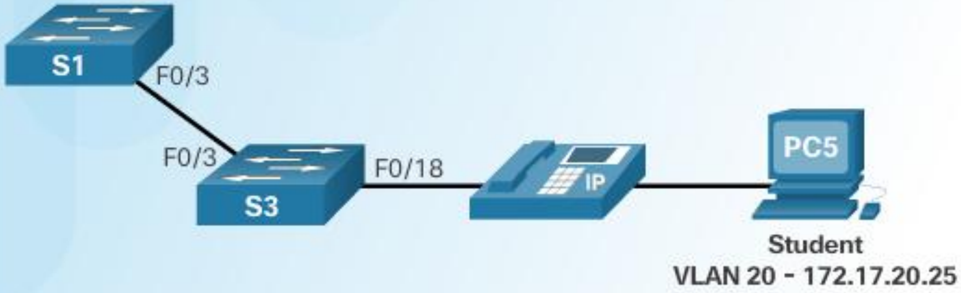


```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

2.3 Assigning Ports to VLANs

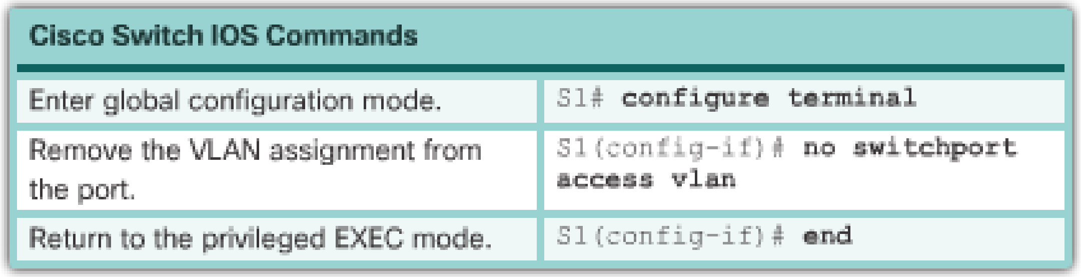


```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)#
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)#
S3(config-if)# mls qos trust cos
S3(config-if)# switchport voice vlan 150
S3(config-if)# end
S3#
```



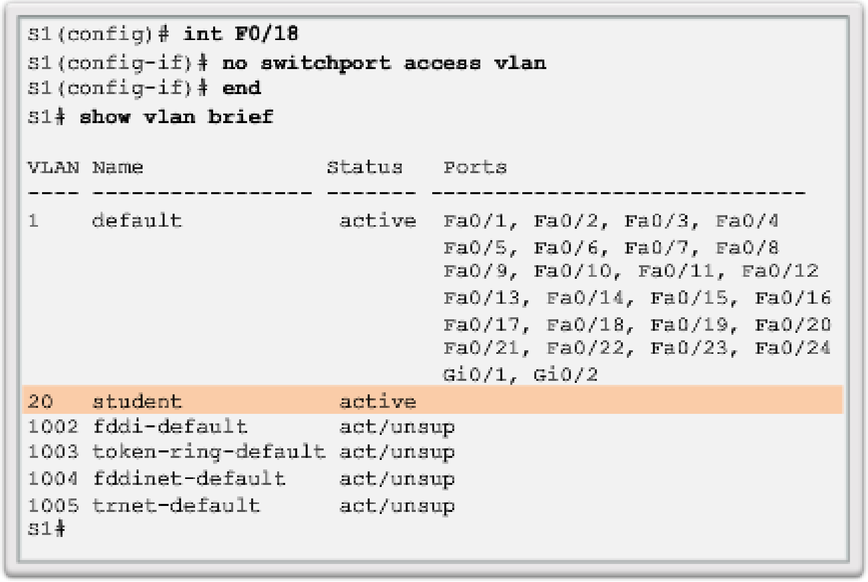
2.4 Changing VLAN Port Membership

- Remove VLAN Assignment



Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Remove the VLAN assignment from the port.	`S1(config-if)# no switchport access vlan`
Return to the privileged EXEC mode.	`S1(config-if)# end`

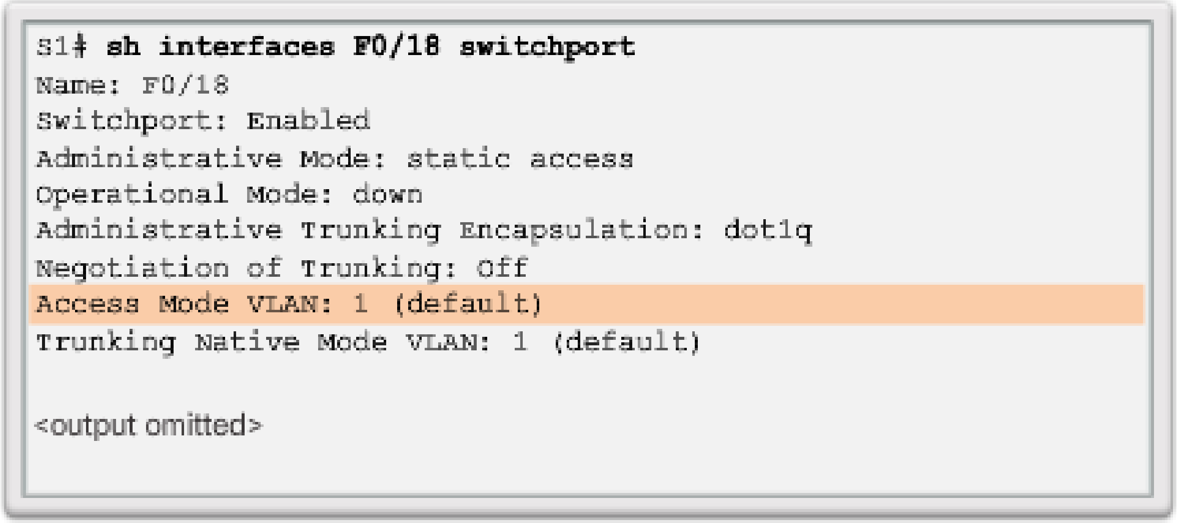
- Interface F0/18 was previously assigned to VLAN 20 which is still active, F0/18 reset to VLAN1



```
S1(config)# int F0/18
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, Fa0/4
                                     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#
```

2.4 Changing VLAN Port Membership

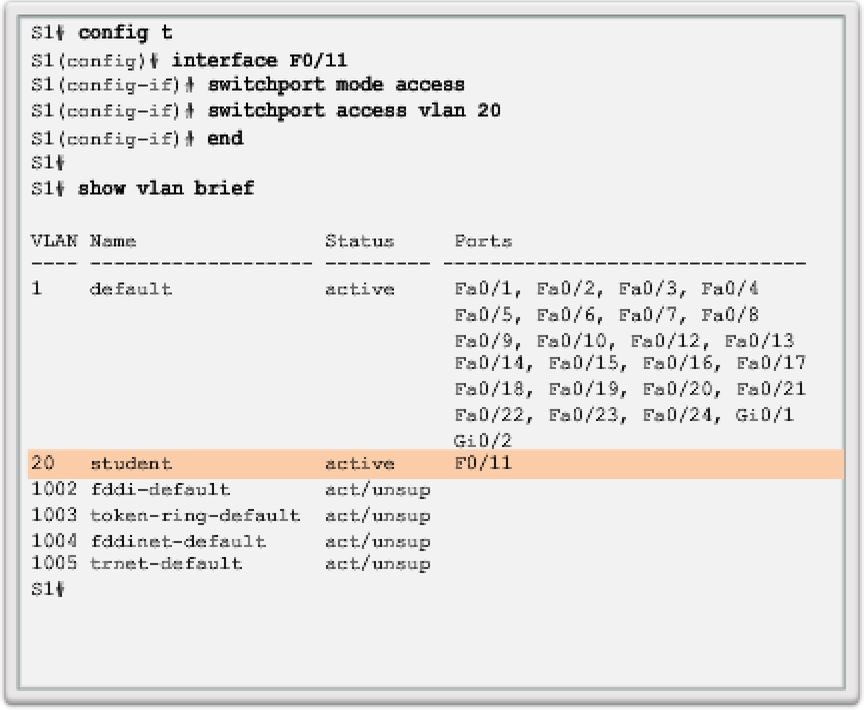
Verification



```
S1# sh interfaces F0/18 switchport
Name: F0/18
Switchport: Enabled
Administrative Mode: static access
Operational Mode: down
Administrative Trunking Encapsulation: dot1q
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)


<output omitted>
```

2.4 Changing VLAN Port Membership

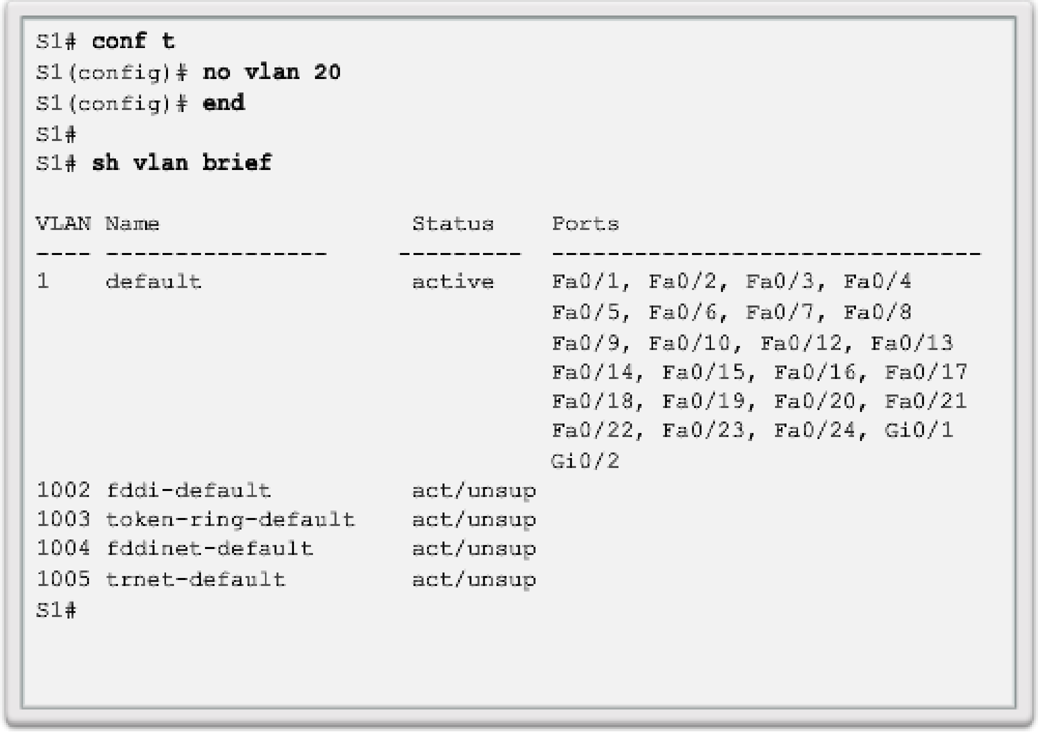
Assign Port to VLAN



```
S1# config t
S1(config)# interface F0/11
S1(config-if)# switchport mode access
S1(config-if)# switchport access vlan 20
S1(config-if)# end
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, Fa0/12, 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    F0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```

2.5 Deleting VLANs

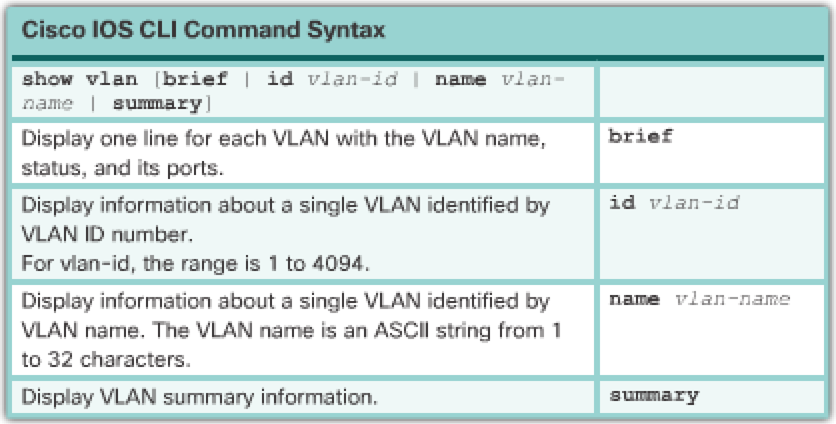
- The entire vlan.dat file can be deleted using the **delete flash:vlan.dat** privileged EXEC mode command
- Abbreviated command version (**delete vlan.dat**) can be used if the vlan.dat file has not been moved from its default location



```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh 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, Fa0/12, 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
S1#
```

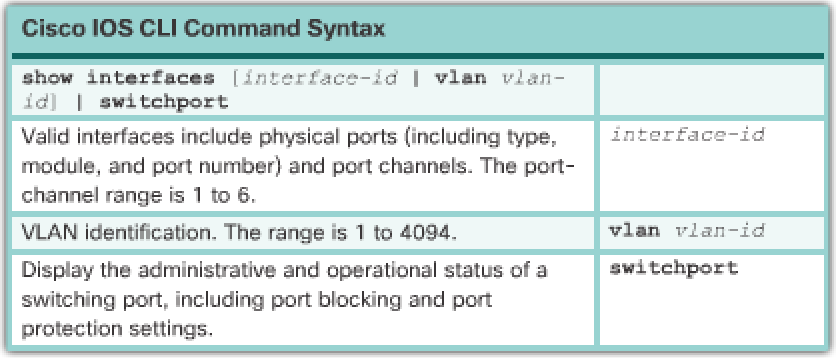
2.6 Verifying VLAN Information

`show vlan` Command



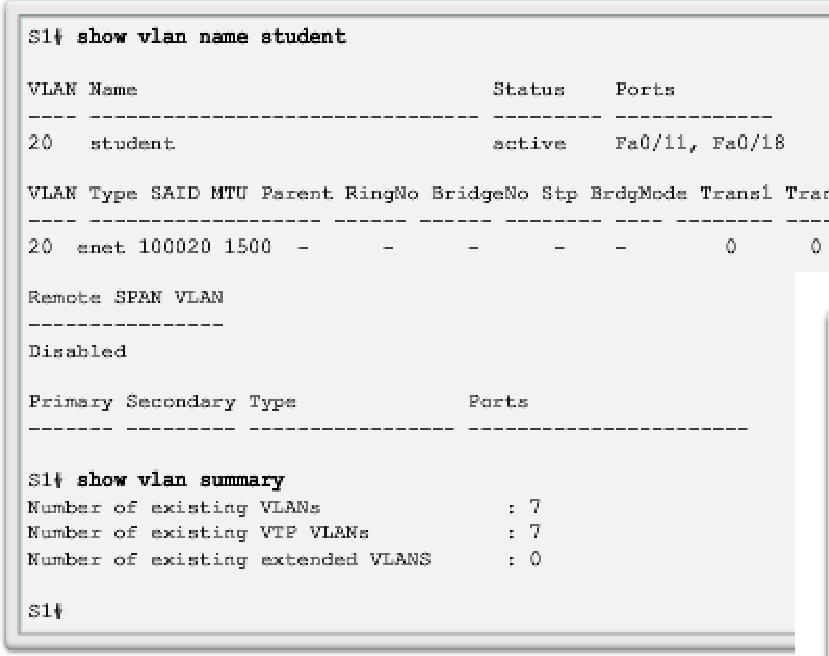
Cisco IOS CLI Command Syntax	
show vlan [**brief** | **id** *vlan-id* | **name** *vlan-name* | **summary**]	
Display one line for each VLAN with the VLAN name, status, and its ports.	**brief**
Display information about a single VLAN identified by VLAN ID number. For vlan-id, the range is 1 to 4094.	**id** *vlan-id*
Display information about a single VLAN identified by VLAN name. The VLAN name is an ASCII string from 1 to 32 characters.	**name** *vlan-name*
Display VLAN summary information.	**summary**

`show interfaces` Command

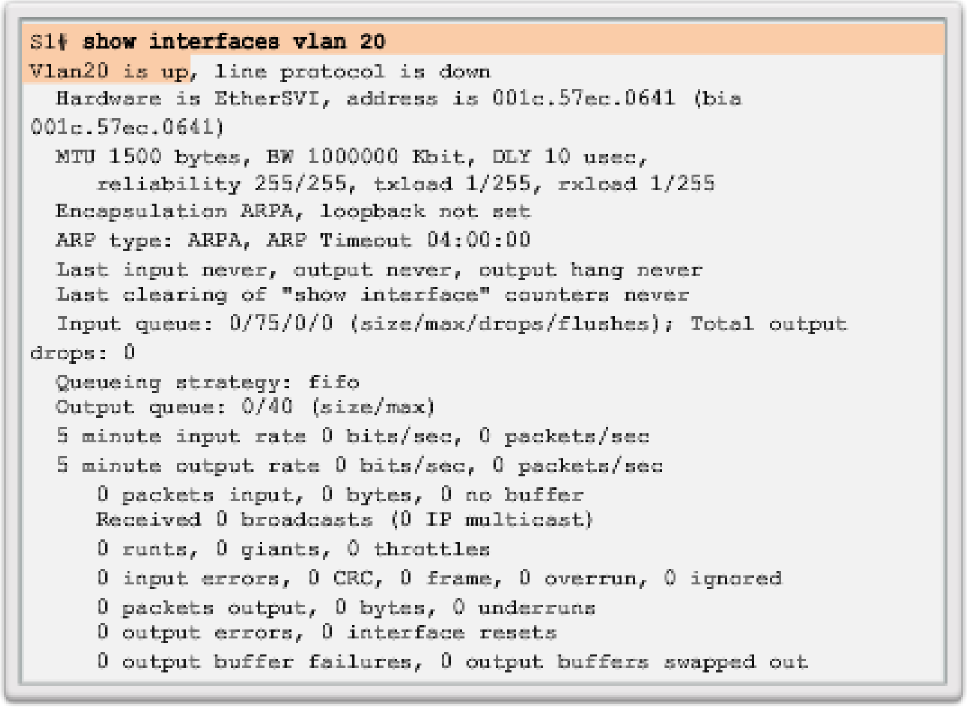


Cisco IOS CLI Command Syntax	
show interfaces [*interface-id* | **vlan** *vlan-id*] | **switchport**	
Valid interfaces include physical ports (including type, module, and port number) and port channels. The port-channel range is 1 to 6.	*interface-id*
VLAN identification. The range is 1 to 4094.	**vlan** *vlan-id*
Display the administrative and operational status of a switching port, including port blocking and port protection settings.	**switchport**

2.6 Verifying VLAN Information



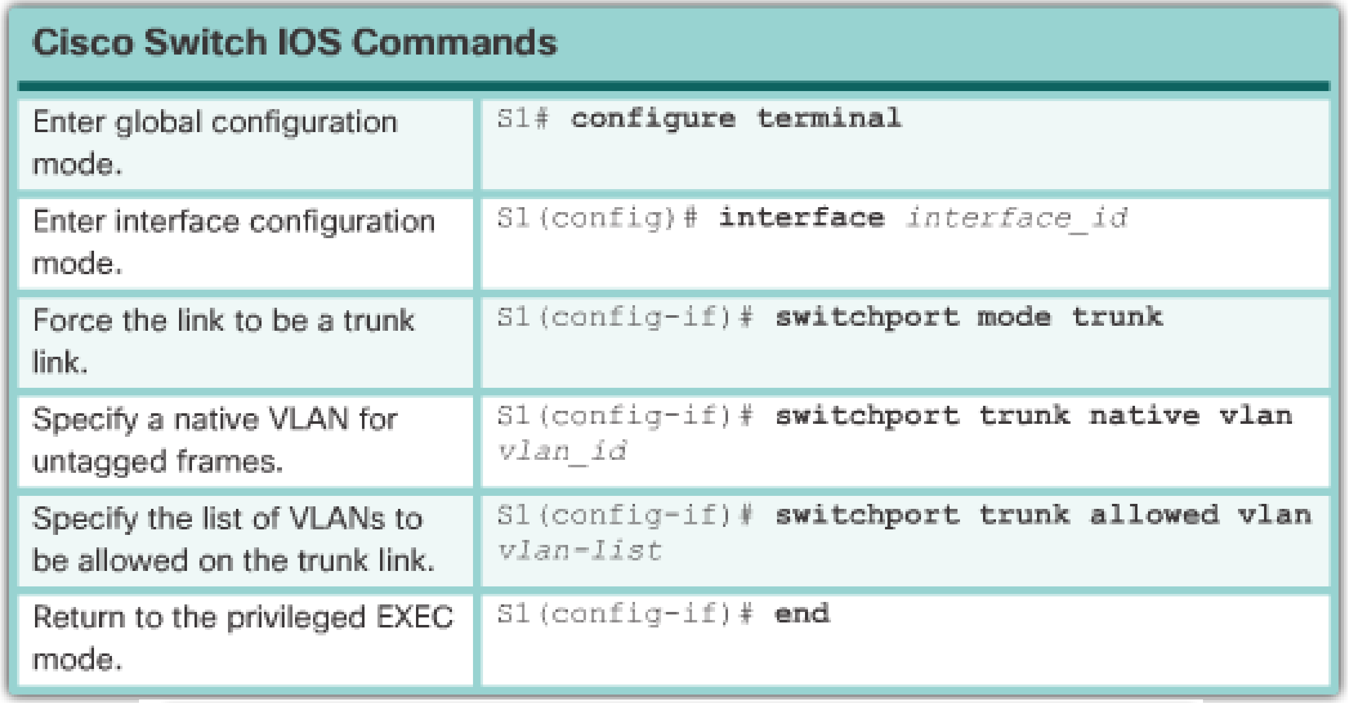
```
S1# show vlan name student

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#
```



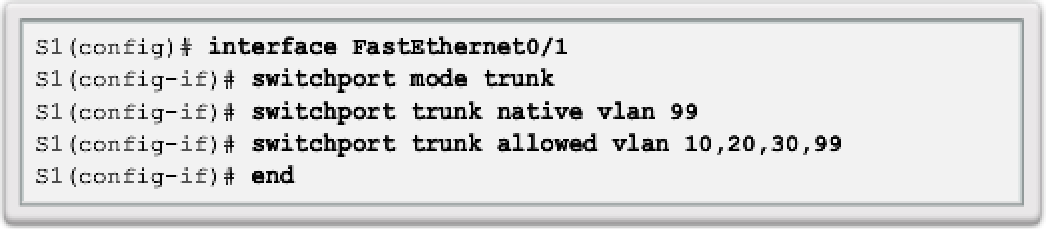
```
S1# show interfaces vlan 20
Vlan20 is up, line protocol is down
  Hardware is EtherSVI, address is 001c.57ec.0641 (bia
001c.57ec.0641)
  MTU 1500 bytes, BW 1000000 Kbit, DLY 10 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  ARP type: ARPA, ARP 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
     0 output errors, 0 interface resets
     0 output buffer failures, 0 output buffers swapped out
```

2.7 Configuring IEEE 802.1q Trunk Links

Trunk Configuration



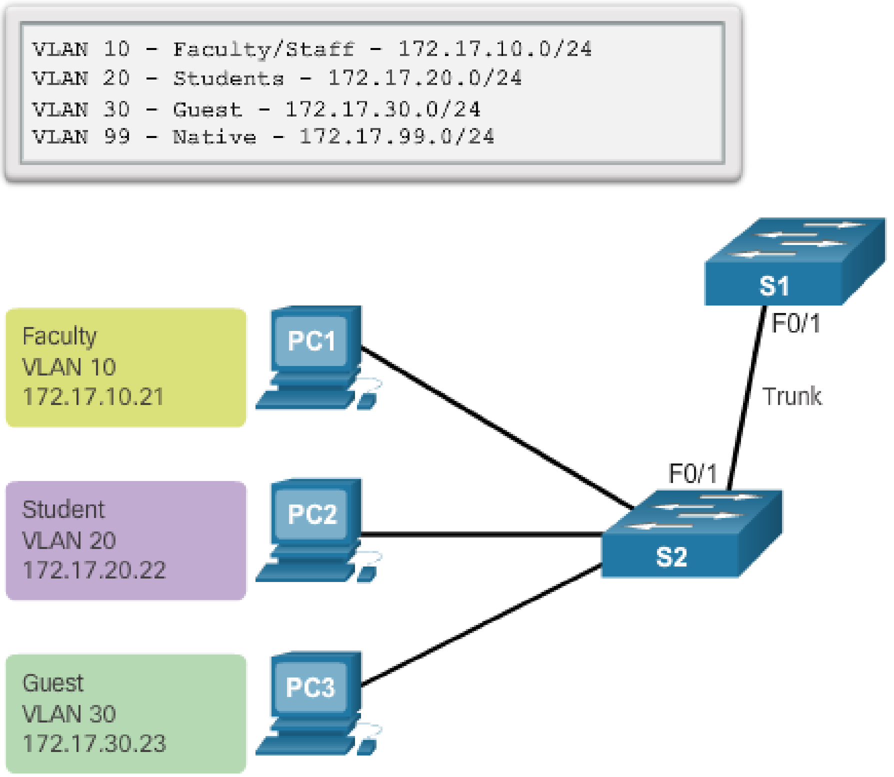
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged frames.	`S1(config-if)# switchport trunk native vlan vlan_id`
Specify the list of VLANs to be allowed on the trunk link.	`S1(config-if)# switchport trunk allowed vlan vlan-list`
Return to the privileged EXEC mode.	`S1(config-if)# end`



```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

2.7 Configuring IEEE 802.1q Trunk Links

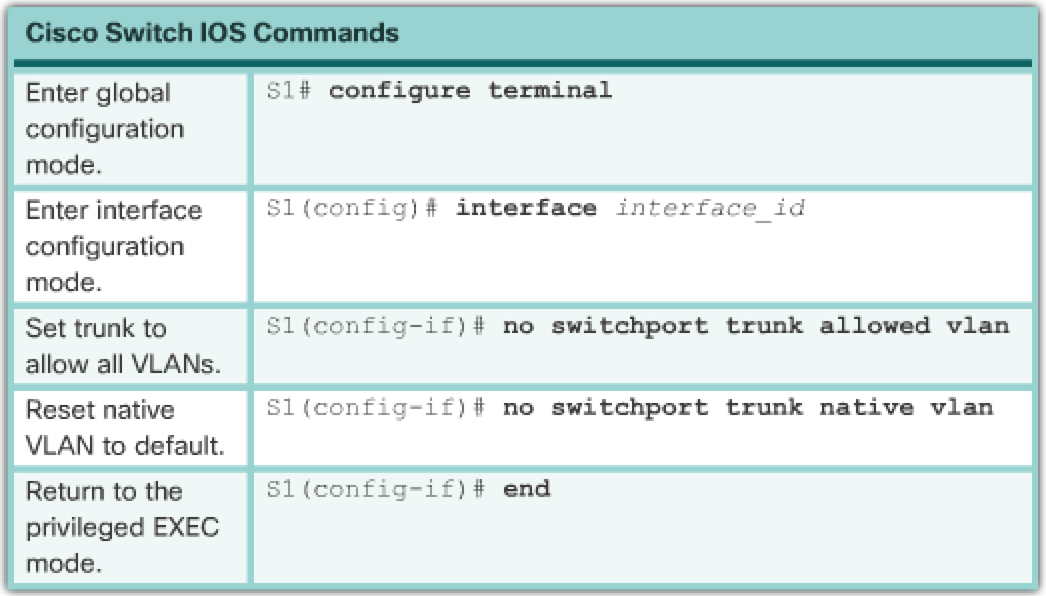
Example Topology



```
VLAN 10 - Faculty/Staff - 172.17.10.0/24
VLAN 20 - Students - 172.17.20.0/24
VLAN 30 - Guest - 172.17.30.0/24
VLAN 99 - Native - 172.17.99.0/24
```

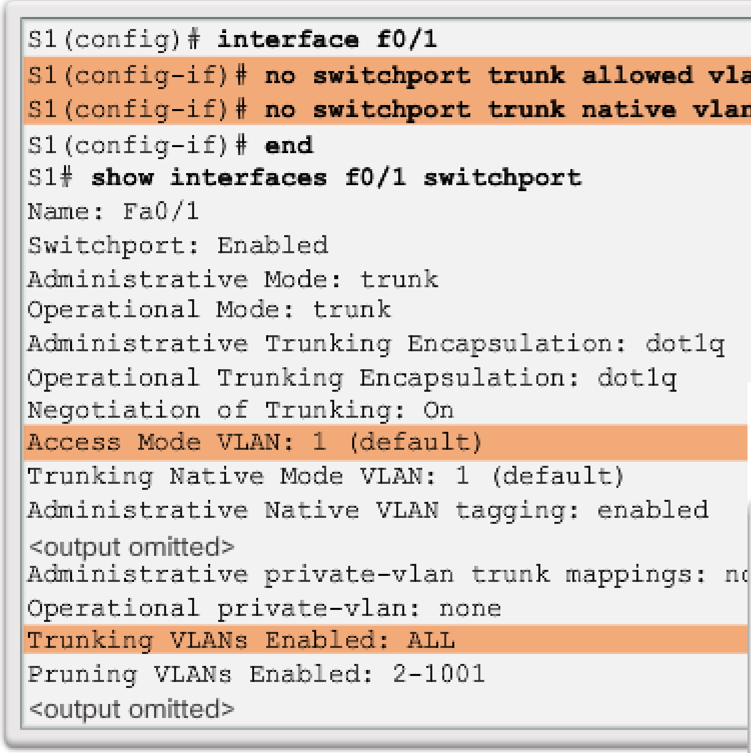
2.8 Resetting the Trunk to Default State

Resetting Configured Values on Trunk Links



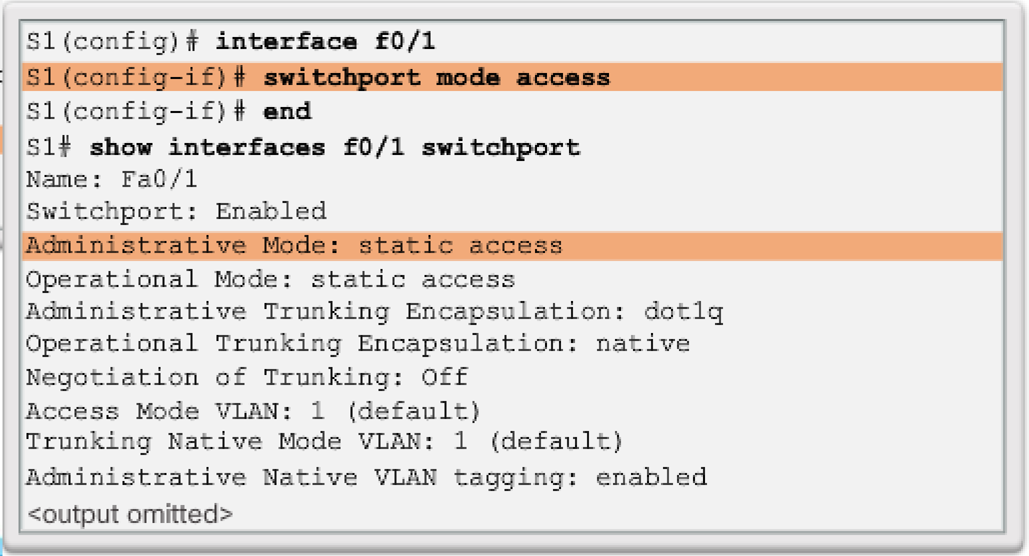
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set trunk to allow all VLANs.	`S1(config-if)# no switchport trunk allowed vlan`
Reset native VLAN to default.	`S1(config-if)# no switchport trunk native vlan`
Return to the privileged EXEC mode.	`S1(config-if)# end`

2.8 Resetting the Trunk to Default State



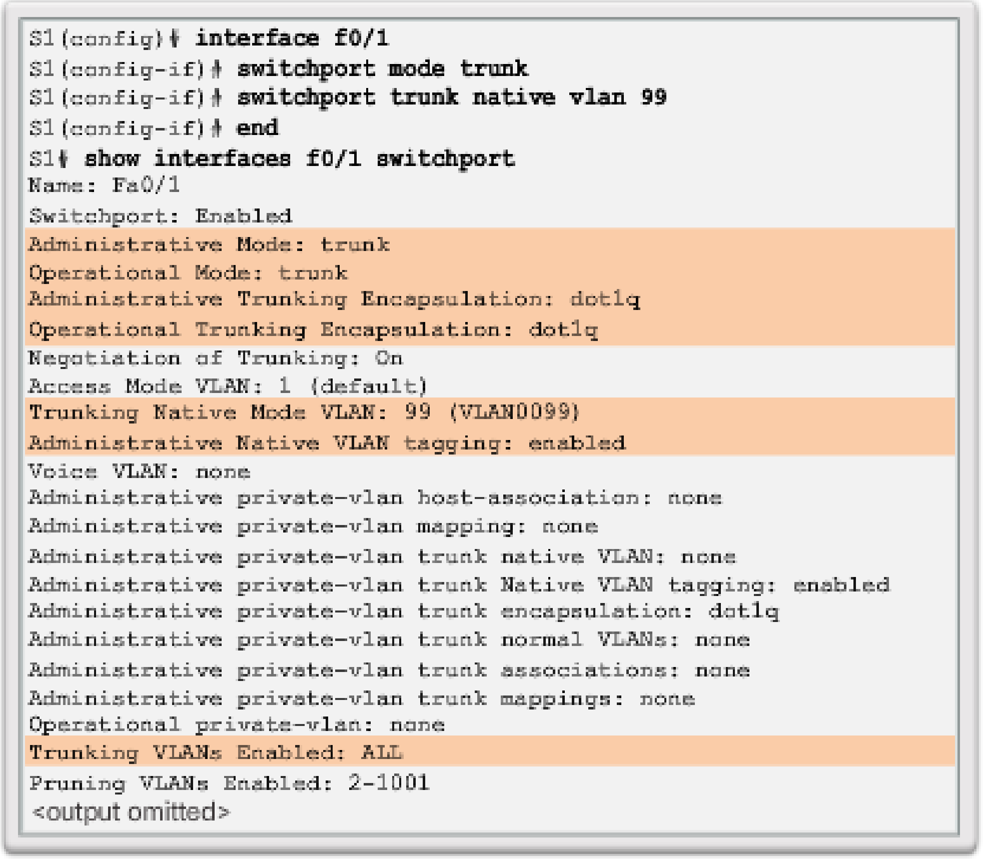
```
S1(config)# interface f0/1
S1(config-if)# no switchport trunk allowed vlan
S1(config-if)# no switchport trunk native vlan
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: trunk
Operational Mode: trunk
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: dot1q
Negotiation of Trunking: On
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
Administrative private-vlan trunk mappings: n
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

Return Port to Access Mode



```
S1(config)# interface f0/1
S1(config-if)# switchport mode access
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
<output omitted>
```

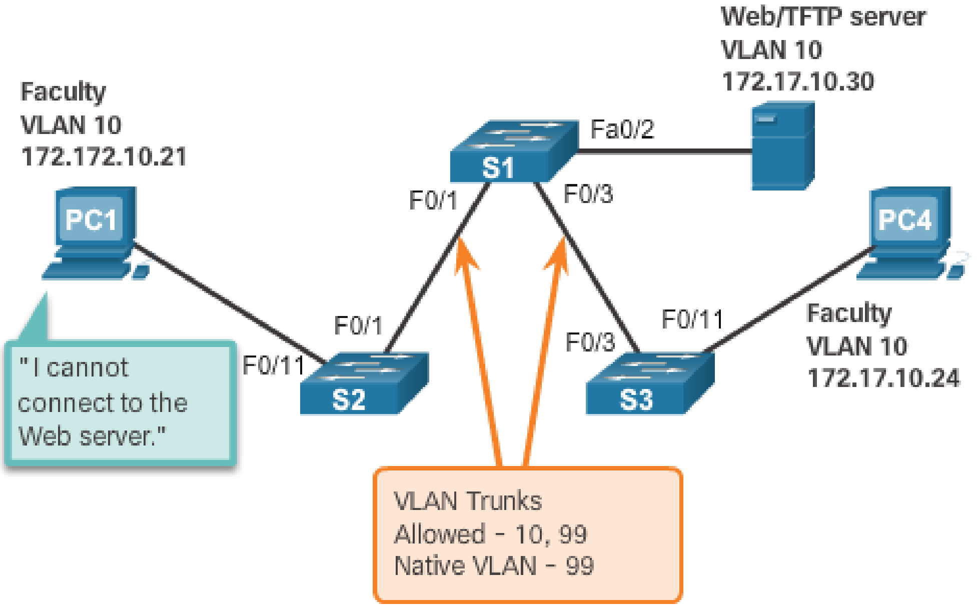
2.9 Verifying Trunk Configuration



```
S1(config)# interface f0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# end
S1# show interfaces f0/1 switchport
Name: Fa0/1
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)
Trunking Native Mode VLAN: 99 (VLAN0099)
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 associations: none
Administrative private-vlan trunk mappings: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

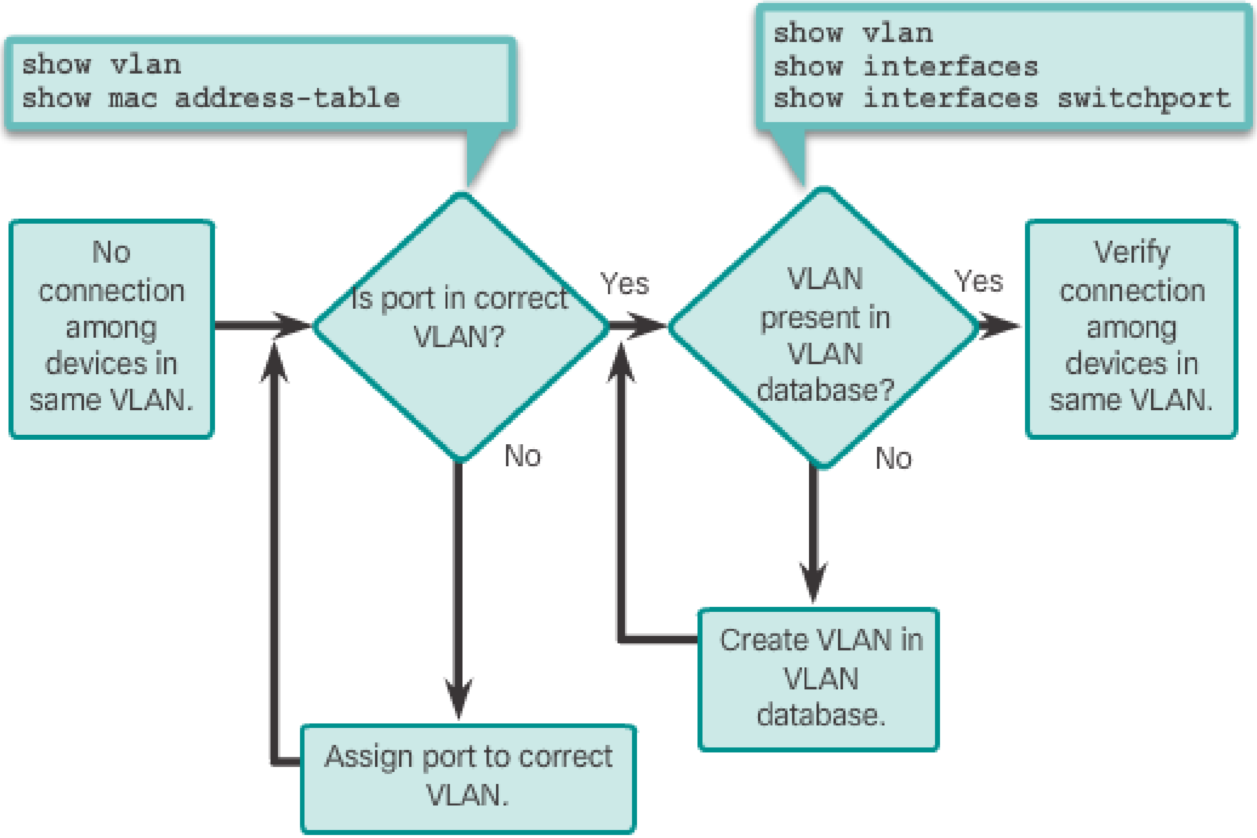
2.10 IP Addressing Issues with VLANs

- It is a common practice to associate a VLAN with an IP network.
- Because different IP networks only communicate through a router, all devices within a VLAN must be part of the same IP network to communicate.
- The figure displays that PC1 cannot communicate to the server because it has a wrong IP address configured.



2.11 Missing VLANs

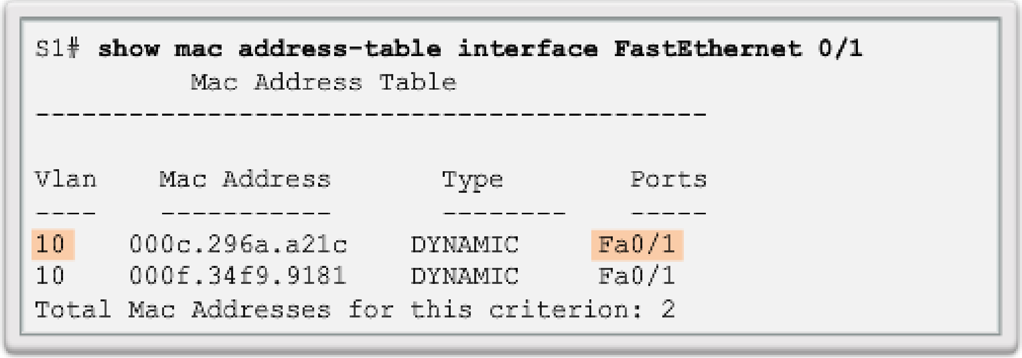
- If all the IP address mismatches have been solved, but the device still cannot connect, check if the VLAN exists in the switch.


show vlan
show mac address-table
show vlan
show interfaces
show interfaces switchport
No connection among devices in same VLAN.
Is port in correct VLAN?
Yes
VLAN present in VLAN database?
Yes
Verify connection among devices in same VLAN.
No
No
Create VLAN in VLAN database.
Assign port to correct VLAN.

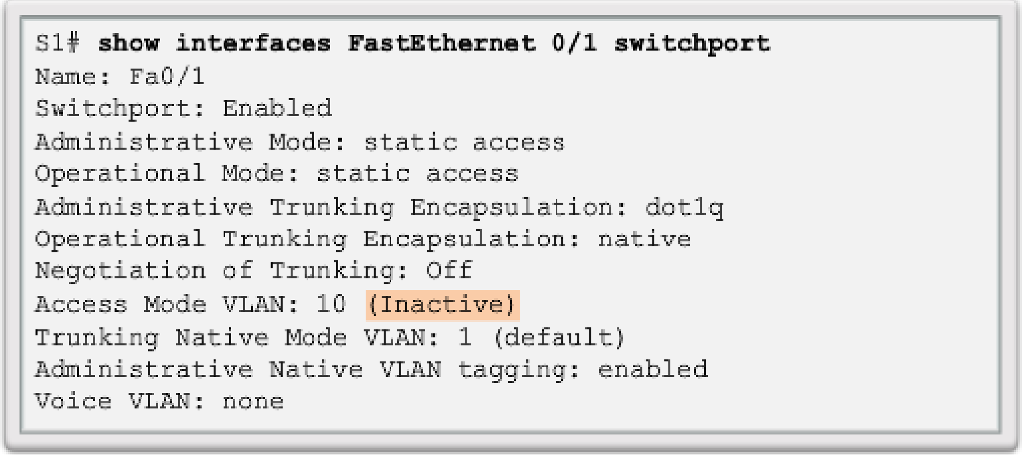
2.11 Missing VLANs

- If the VLAN to which a port belongs is deleted, the port becomes inactive. All ports belonging to the VLAN that was deleted are unable to communicate with the rest of the network.

- Not functional until the missing VLAN is created using the **vlan** *vlan_id* global configuration.



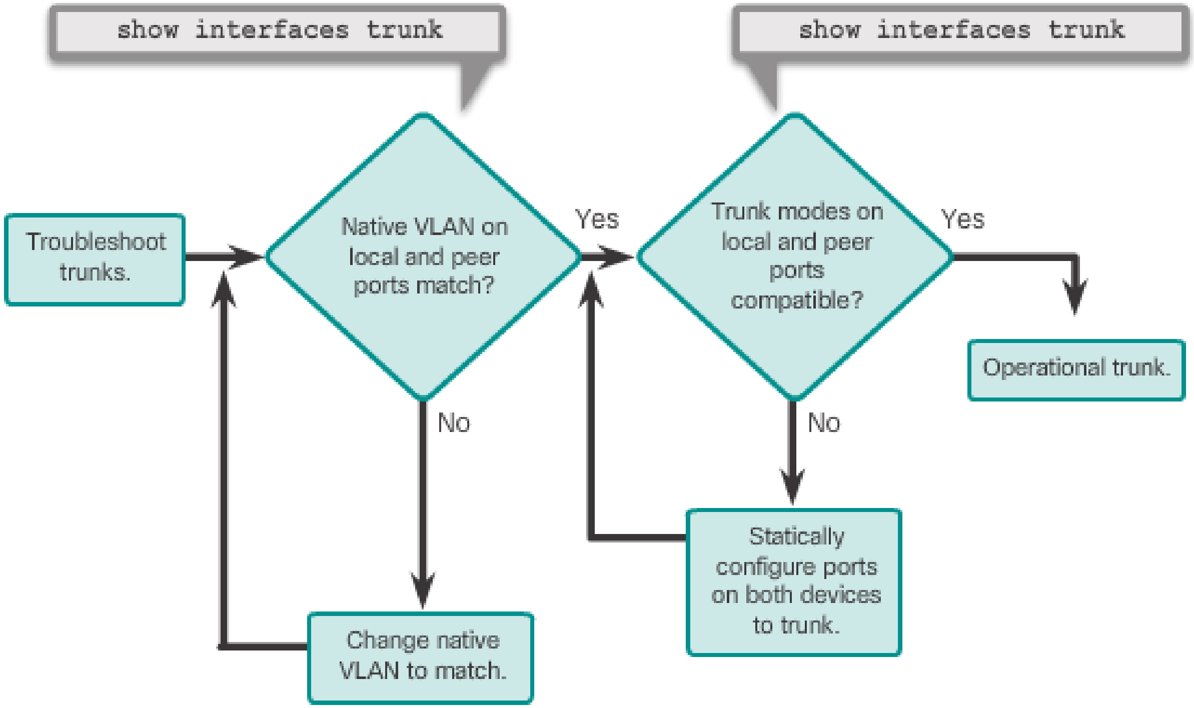
```
S1# show mac address-table interface FastEthernet 0/1
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----
10    000c.296a.a21c    DYNAMIC     Fa0/1
10    000f.34f9.9181    DYNAMIC     Fa0/1
Total Mac Addresses for this criterion: 2
```

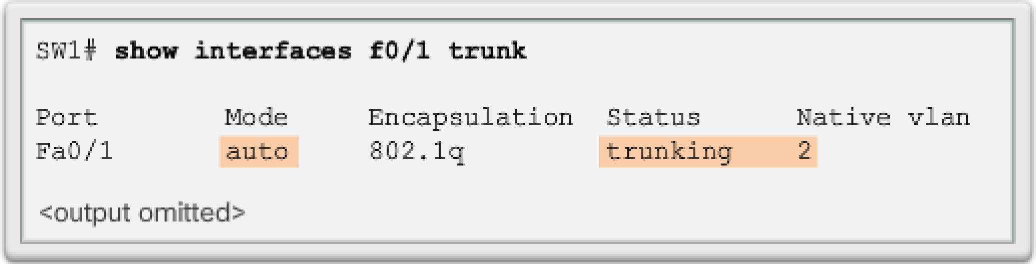


```
S1# show interfaces FastEthernet 0/1 switchport
Name: Fa0/1
Switchport: Enabled
Administrative Mode: static access
Operational Mode: static access
Administrative Trunking Encapsulation: dot1q
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 10 (Inactive)
Trunking Native Mode VLAN: 1 (default)
Administrative Native VLAN tagging: enabled
Voice VLAN: none
```

2.12 Introduction to Troubleshooting Trunks

- **Note:** To solve a native VLAN mismatch, configure the native VLAN to be the same VLAN on both sides of the link.


show interfaces trunk
show interfaces trunk
Troubleshoot trunks.
Native VLAN on local and peer ports match?
Yes
No
Change native VLAN to match.
Trunk modes on local and peer ports compatible?
Yes
No
Statically configure ports on both devices to trunk.
Operational trunk.

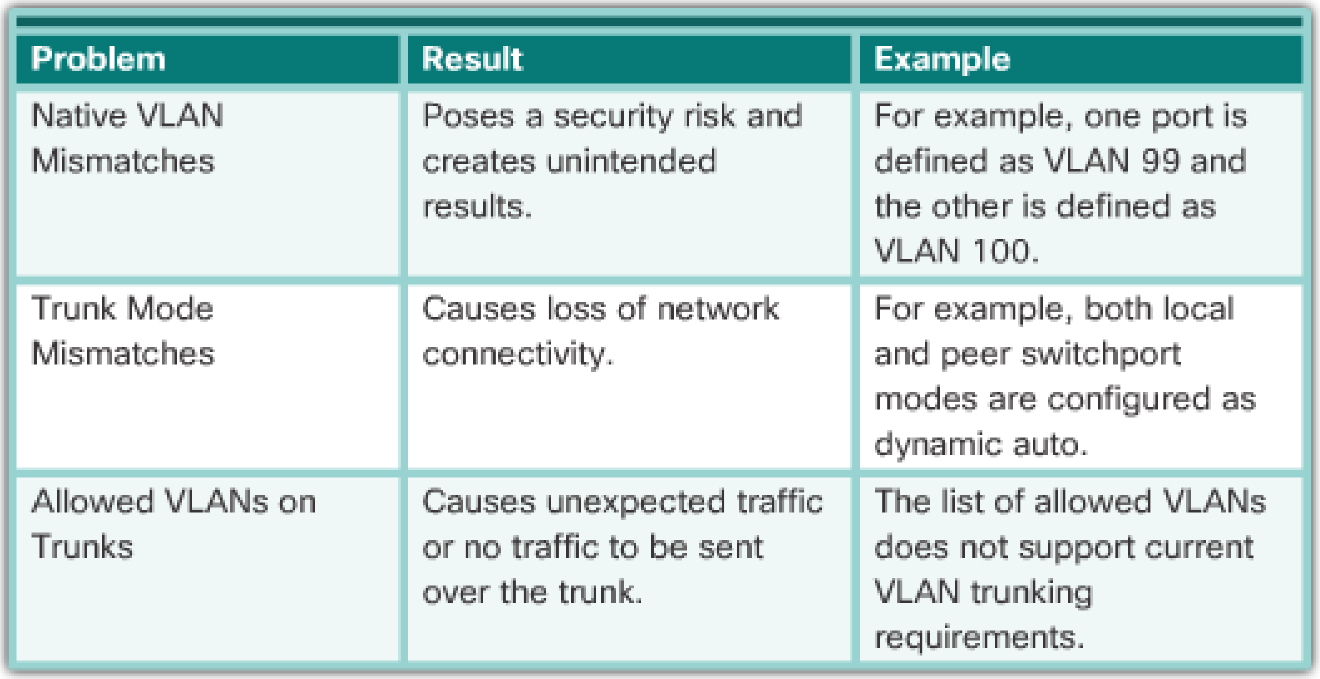


```
SW1# show interfaces f0/1 trunk

Port        Mode        Encapsulation  Status       Native vlan
Fa0/1       auto        802.1q         trunking     2

<output omitted>
```

2.13 Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations.
- The most common type of trunk configuration errors are:
  - Native VLAN mismatches
  - Trunk mode mismatches
  - Allowed VLANs on trunks
- If a trunk problem is detected, the best practice guidelines recommend to troubleshoot in the order shown above.

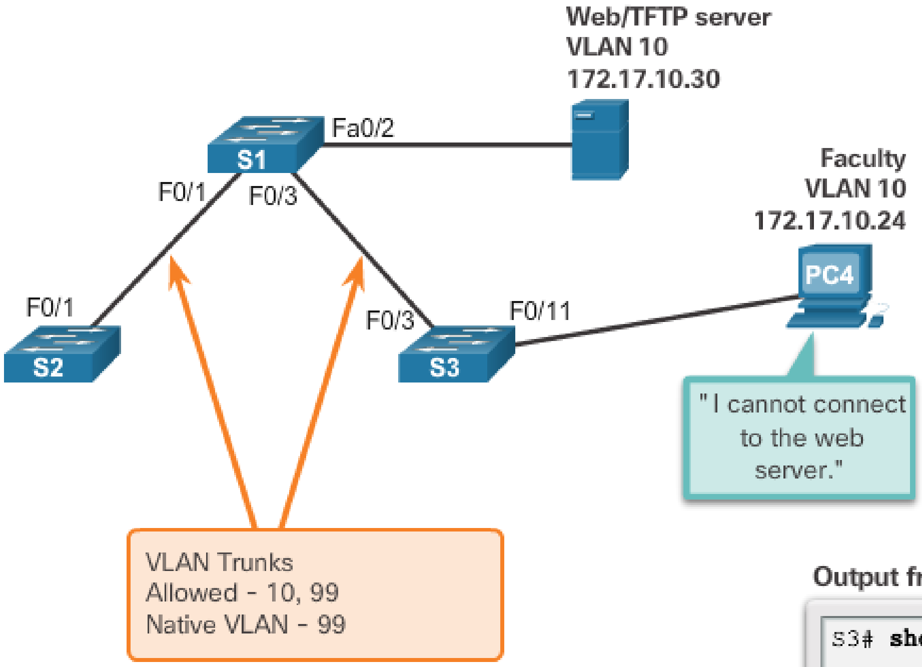
2.13 Common Problems with Trunks



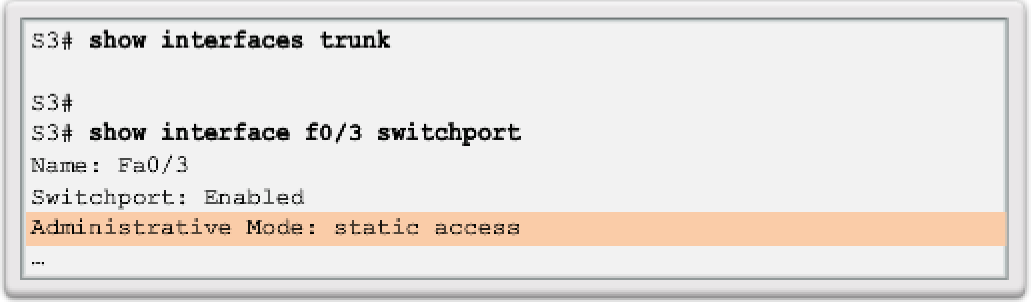
Problem	Result	Example
Native VLAN Mismatches	Poses a security risk and creates unintended results.	For example, one port is defined as VLAN 99 and the other is defined as VLAN 100.
Trunk Mode Mismatches	Causes loss of network connectivity.	For example, both local and peer switchport modes are configured as dynamic auto.
Allowed VLANs on Trunks	Causes unexpected traffic or no traffic to be sent over the trunk.	The list of allowed VLANs does not support current VLAN trunking requirements.

2.14 Incorrect Port Mode

Scenario Topology



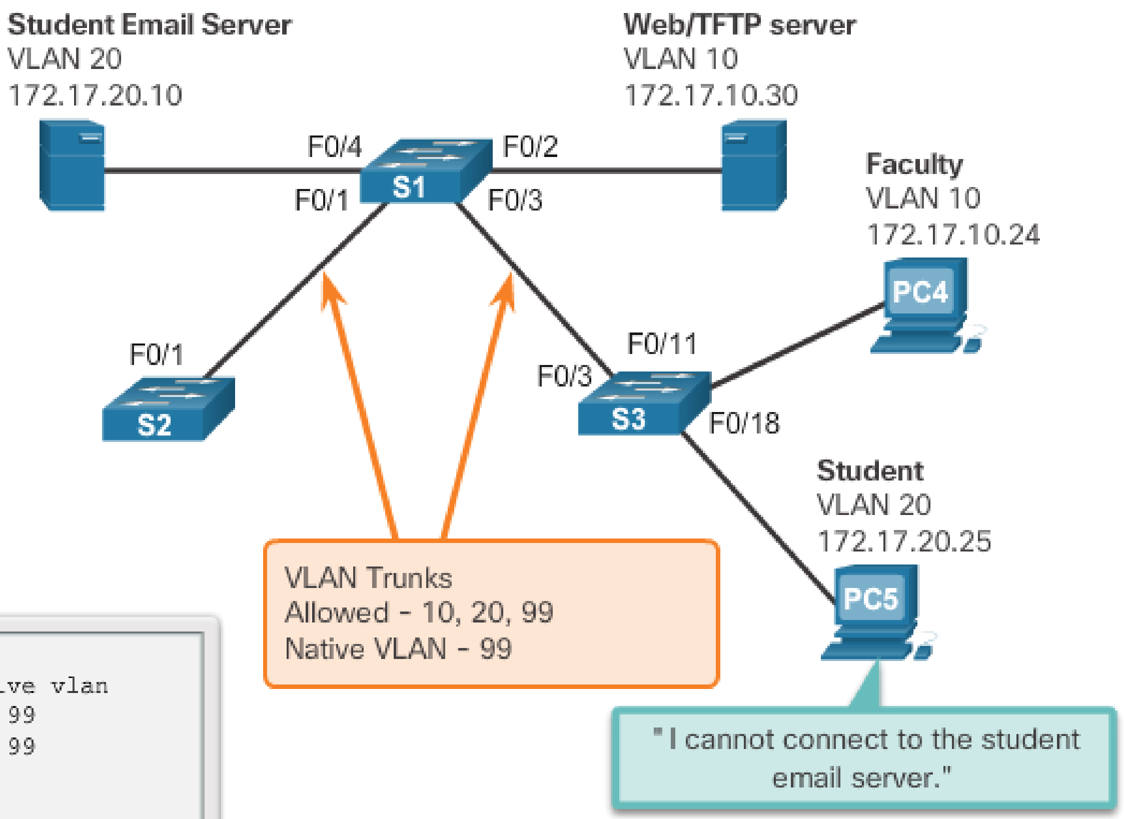
Output from Switch S3



```
S3# show interfaces trunk

S3#
S3# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: static access
...
```

2.15 Incorrect VLAN List

Scenario Topology



VLAN Trunks
Allowed - 10, 20, 99
Native VLAN - 99

"I cannot connect to the student email server."

Output from Switch S1

```
S1# show interfaces trunk
Port        Mode      Encapsulation  Status      Native vlan
Fa0/1       on          802.1q       trunking       99
Fa0/3       on          802.1q       trunking       99
Port        Vlans allowed on trunk
Fa0/1       10,99
Fa0/3       10,99
…
S1#
```

2.15 Incorrect VLAN List

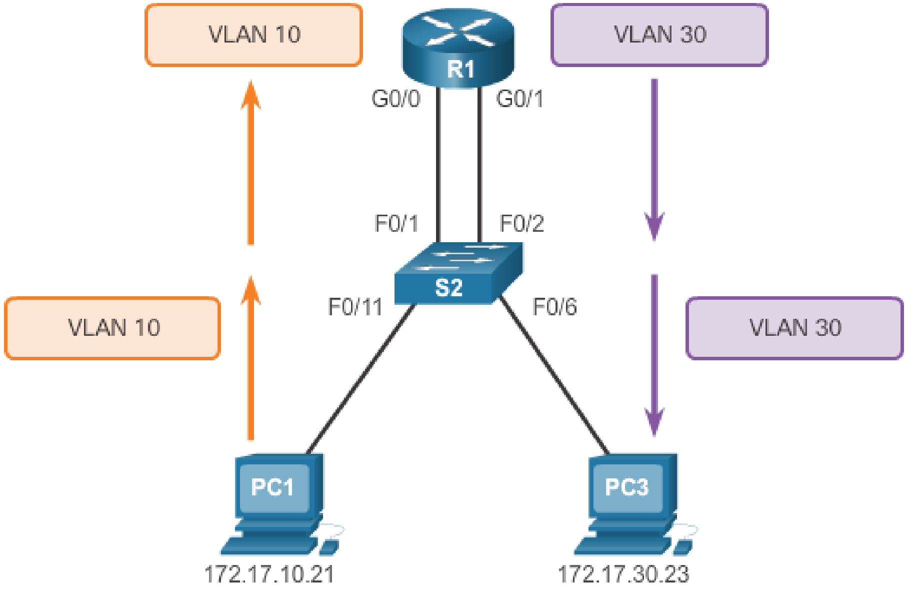
- VLANs must be allowed in the trunk before their frames can be transmitted across the link.
- Use the **switchport trunk allowed vlan** command to specify which VLANs are allowed in a trunk link.
- Use the **show interfaces trunk** command to ensure the correct VLANs are permitted in a trunk.

3. Inter-VLAN Routing Using Routers

3.1 What is Inter-VLAN Routing?

- Layer 2 switches cannot forward traffic between VLANs without the assistance of a router.
- Inter-VLAN routing is a process for forwarding network traffic from one VLAN to another, using a router.

What is Inter-VLAN Routing?



3.2 Legacy Inter-VLAN Routing

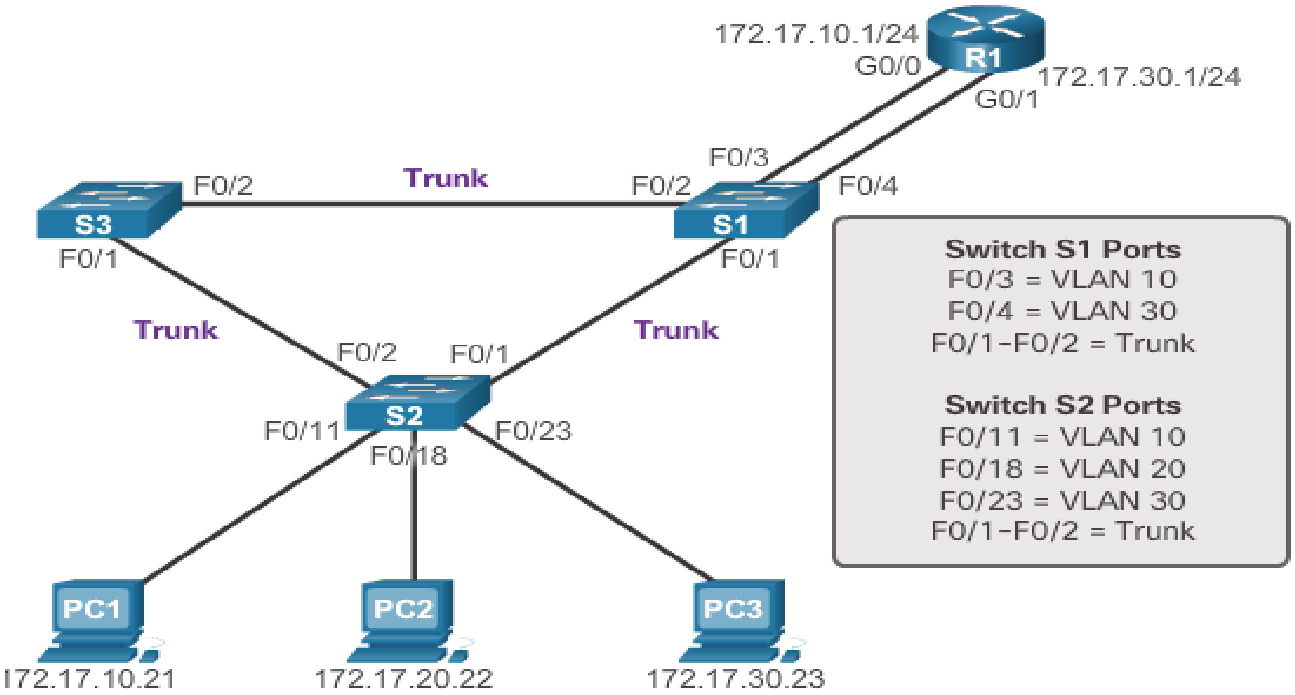
In the past:

- Actual routers were used to route between VLANs.
- Each VLAN was connected to a different physical router interface.
- Packets would arrive on the router through one interface, be routed and leave through another.
- Because the router interfaces were connected to VLANs and had IP addresses from that specific VLAN, routing between VLANs was achieved.
- Large networks with large number of VLANs required many router interfaces.

3.2 Legacy Inter-VLAN Routing

- In this example, the router was configured with two separate physical interfaces to interact with the different VLANs and perform the routing.

Legacy Inter-VLAN Routing



Switch S1 Ports
F0/3 = VLAN 10
F0/4 = VLAN 30
F0/1-F0/2 = Trunk

Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk

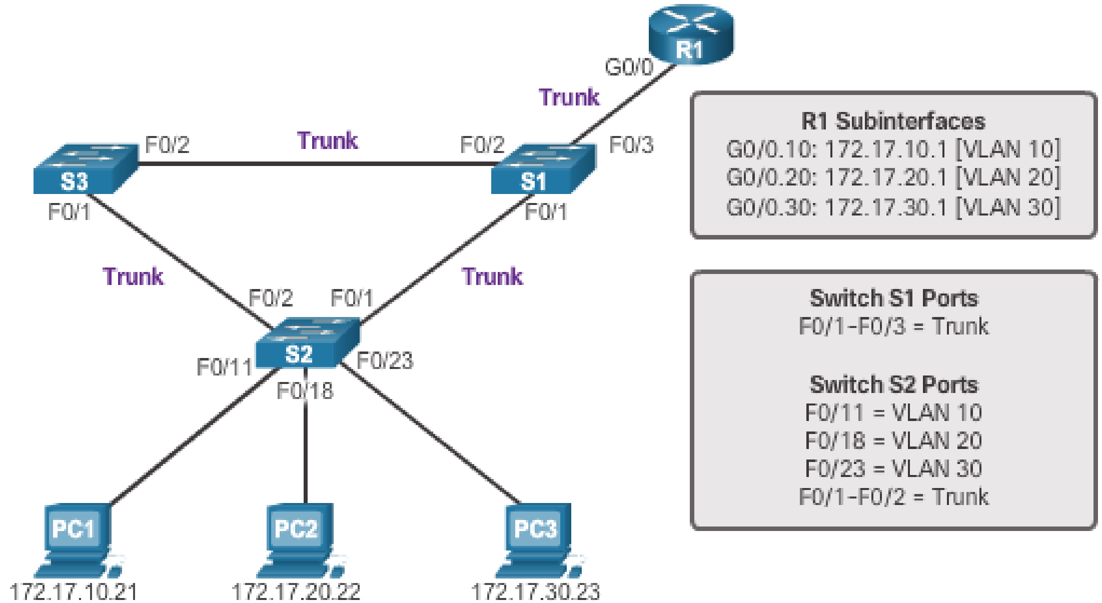
3.3 Router-on-a-Stick Inter-VLAN Routing

- The router-on-a-stick approach uses only one of the router’s physical interface.
- One of the router’s physical interfaces is configured as a 802.1Q trunk port so it can understand VLAN tags.
- Logical subinterfaces are created; one subinterface per VLAN.
- Each subinterface is configured with an IP address from the VLAN it represents.
- VLAN members (hosts) are configured to use the subinterface address as a default gateway.

3.3 Router-on-a-Stick Inter-VLAN Routing

Router interface configured to operate as a trunk link and is connected to a trunked switch port. The router performs inter-VLAN routing by accepting VLAN-tagged traffic on the trunk interface coming from the adjacent switch, and then, internally routing between the VLANs using subinterfaces. The router then forwards the routed traffic, VLAN-tagged for the destination VLAN, out the same physical interface as it used to receive the traffic.

'Router-on-a-Stick' Inter-VLAN Routing



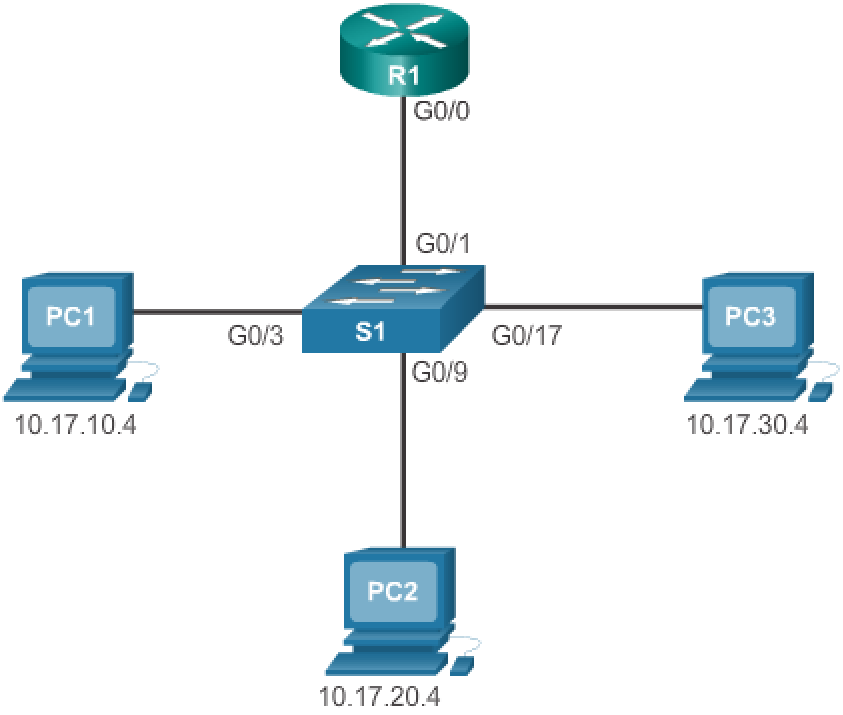
R1 Subinterfaces
G0/0.10: 172.17.10.1 [VLAN 10]
G0/0.20: 172.17.20.1 [VLAN 20]
G0/0.30: 172.17.30.1 [VLAN 30]

Switch S1 Ports
F0/1-F0/3 = Trunk

Switch S2 Ports
F0/11 = VLAN 10
F0/18 = VLAN 20
F0/23 = VLAN 30
F0/1-F0/2 = Trunk

3.4 Identify the Types of Inter-VLAN Routing Activity

- Legacy or Router-on-a-Stick?



R1 Interface
G0/0 Trunk Link

R1 Subinterfaces

G0/0.10	10.17.10.1/28
G0/0.20	10.17.20.1/28
G0/0.30	10.17.30.1/28

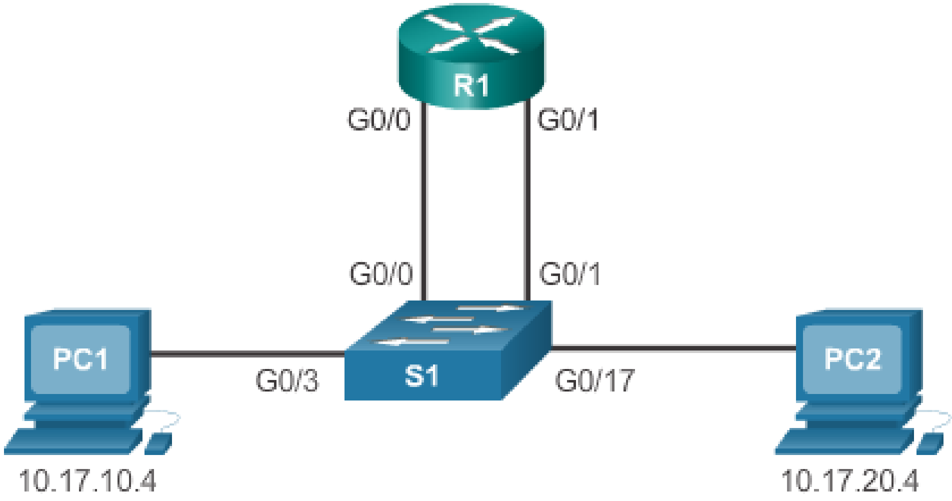
S1 Ports
G0/1 Trunk Link
G0/3 = VLAN 10
G0/9 = VLAN 20
G0/17 = VLAN 30

End Devices

PC1 – VLAN 10	10.17.10.4/28
PC2 – VLAN 20	10.17.20.4/28
PC3 – VLAN 30	10.17.30.4/28

3.4 Identify the Types of Inter-VLAN Routing Activity

- Legacy or Router-on-a-Stick?



R1 Interface
G0/0 10.17.10.1/28
G0/1 10.17.20.1/28

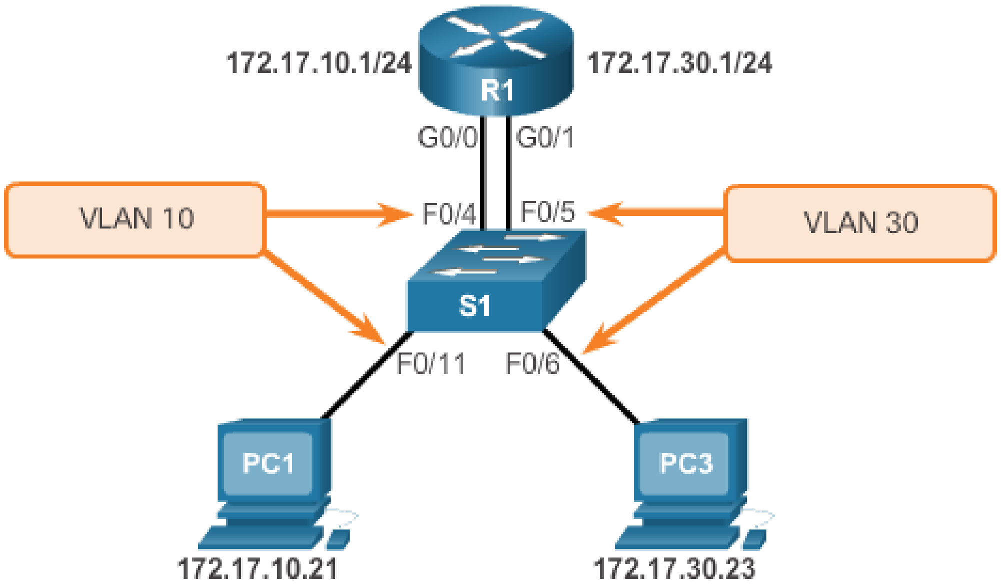
S1 Ports
G0/3 = VLAN 10
G0/17 = VLAN 20

End Devices
PC1 – VLAN 10
10.17.10.4/28

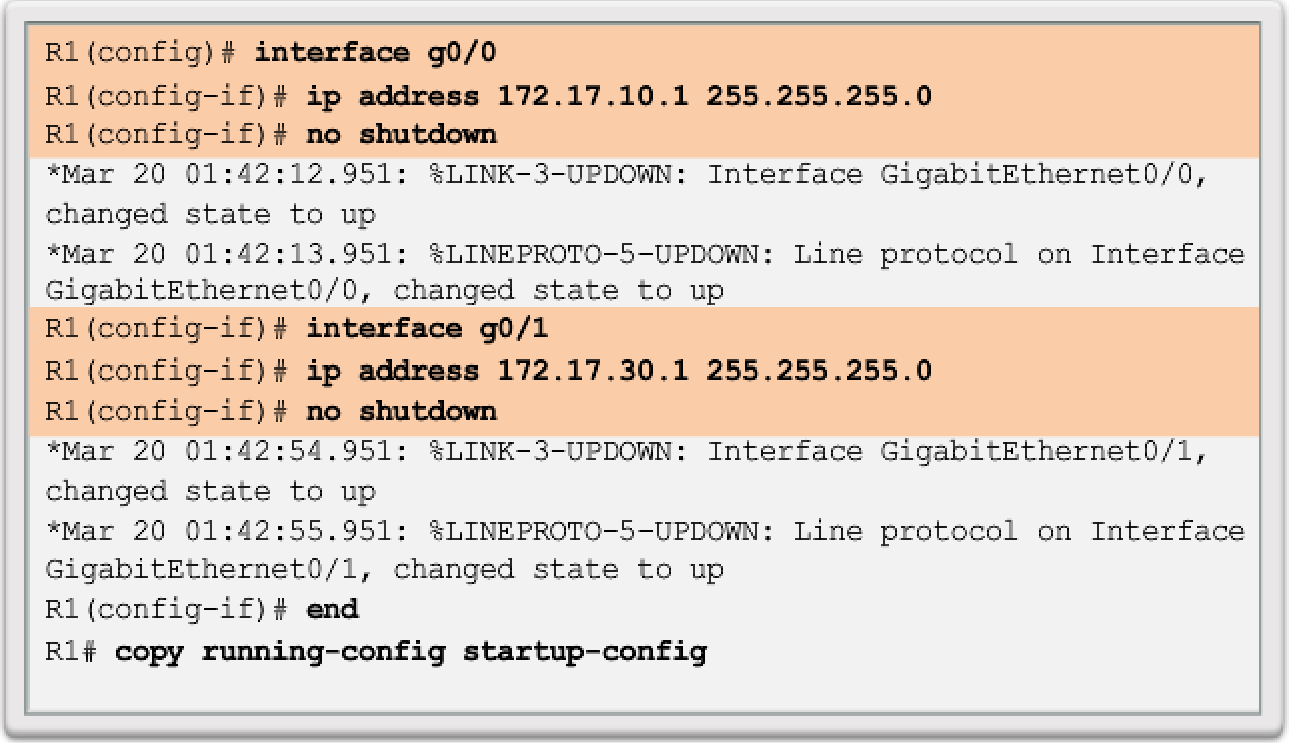
PC2 – VLAN 20
10.17.20.4/28

3.5 Configure Legacy Inter-VLAN Routing: Preparation

- Legacy inter-VLAN routing requires routers to have multiple physical interfaces.
- Each one of the router’s physical interfaces is connected to a unique VLAN.
- Each interface is also configured with an IP address for the subnet associated with the particular VLAN.
- Network devices use the router as a gateway to access the devices connected to the other VLANs.

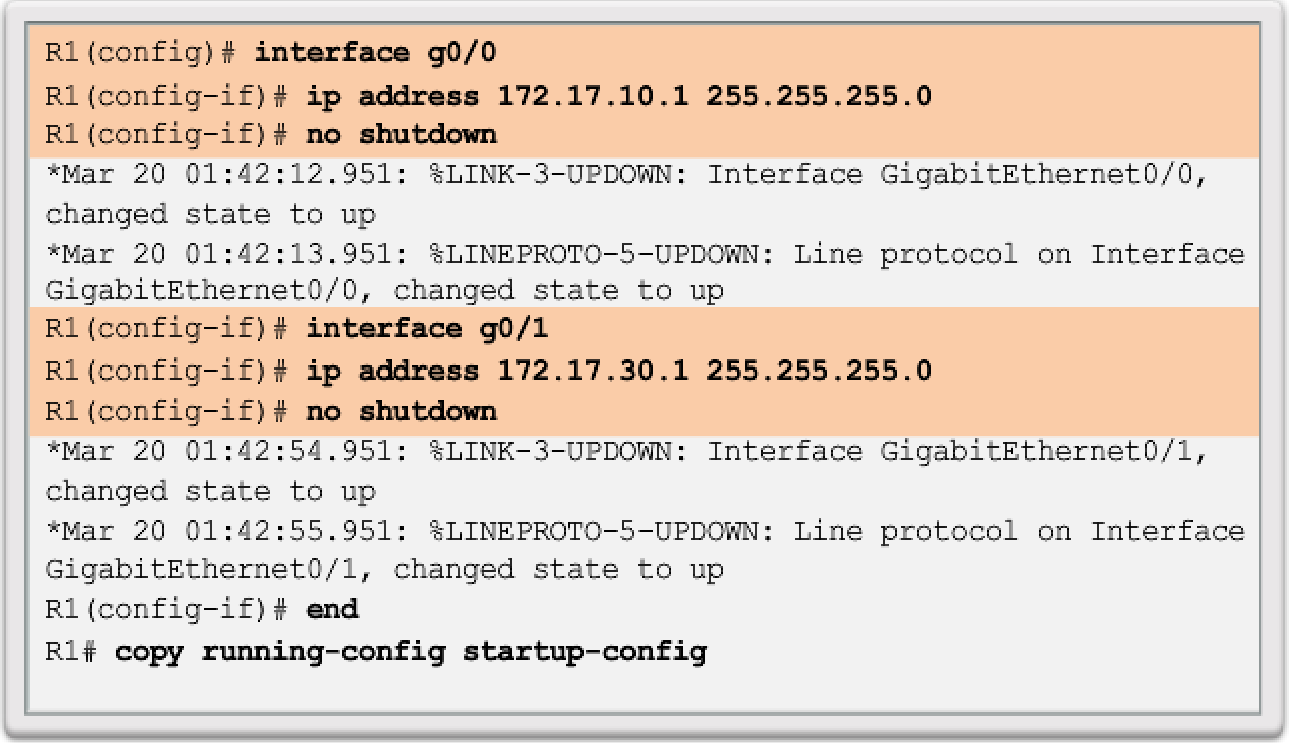


3.6 Configure Legacy Inter-VLAN Routing: Switch Configuration



```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

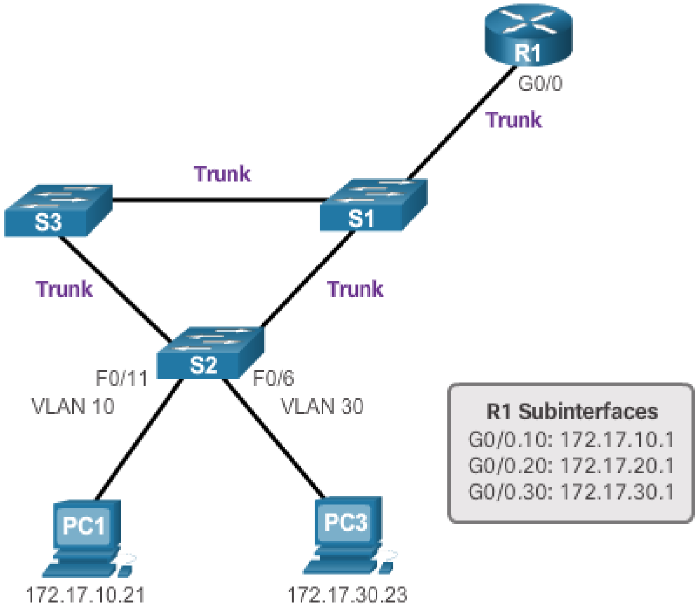
3.7 Configure Legacy Inter-VLAN Routing: Router Interface Configuration



```
R1(config)# interface g0/0
R1(config-if)# ip address 172.17.10.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:12.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
changed state to up
*Mar 20 01:42:13.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/0, changed state to up
R1(config-if)# interface g0/1
R1(config-if)# ip address 172.17.30.1 255.255.255.0
R1(config-if)# no shutdown
*Mar 20 01:42:54.951: %LINK-3-UPDOWN: Interface GigabitEthernet0/1,
changed state to up
*Mar 20 01:42:55.951: %LINEPROTO-5-UPDOWN: Line protocol on Interface
GigabitEthernet0/1, changed state to up
R1(config-if)# end
R1# copy running-config startup-config
```

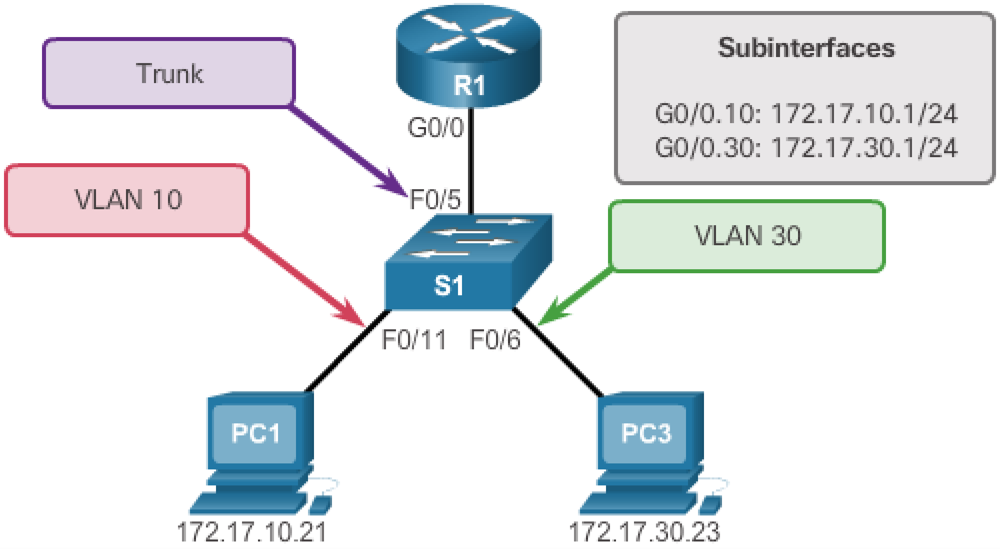
3.8 Configure Router-on-a Stick: Preparation

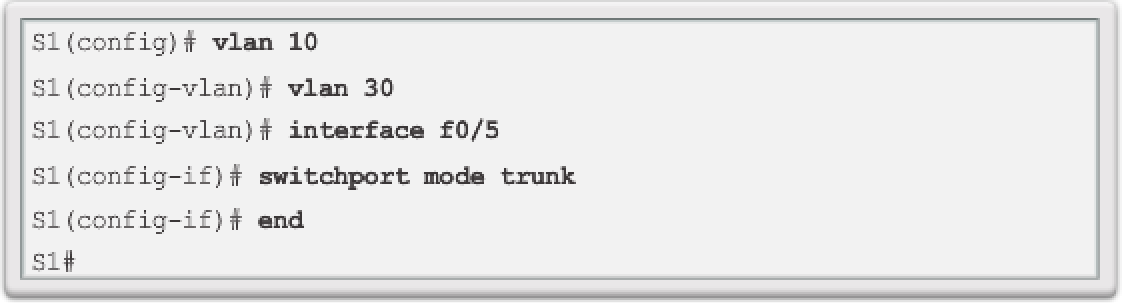
- An alternative to legacy inter-VLAN routing is to use VLAN trunking and subinterfaces.
- VLAN trunking allows a single physical router interface to route traffic for multiple VLANs.
- The physical interface of the router must be connected to a trunk link on the adjacent switch.
- On the router, subinterfaces are created for each unique VLAN.
- Each subinterface is assigned an IP address specific to its subnet or VLAN and is also configured to tag frames for that VLAN.



R1 Subinterfaces
G0/0.10: 172.17.10.1
G0/0.20: 172.17.20.1
G0/0.30: 172.17.30.1

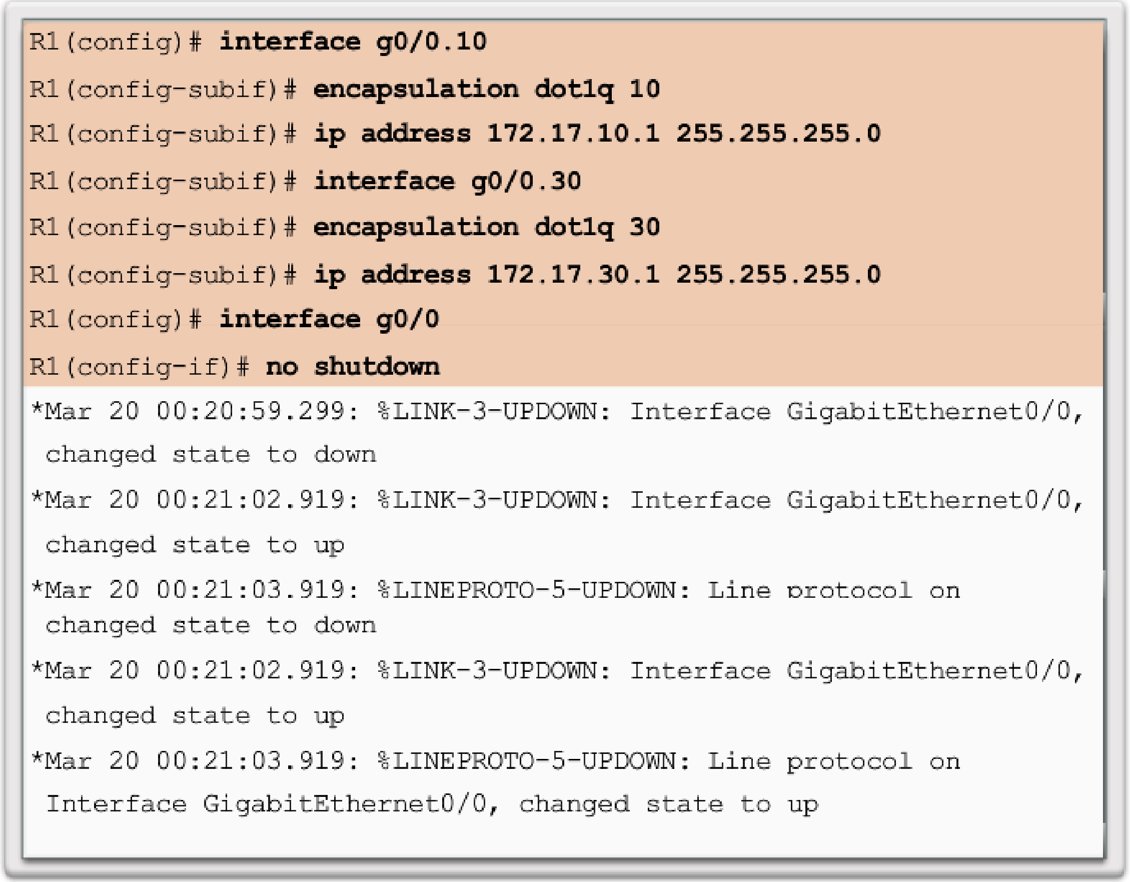
3.9 Configure Router-on-a Stick: Switch Configuration





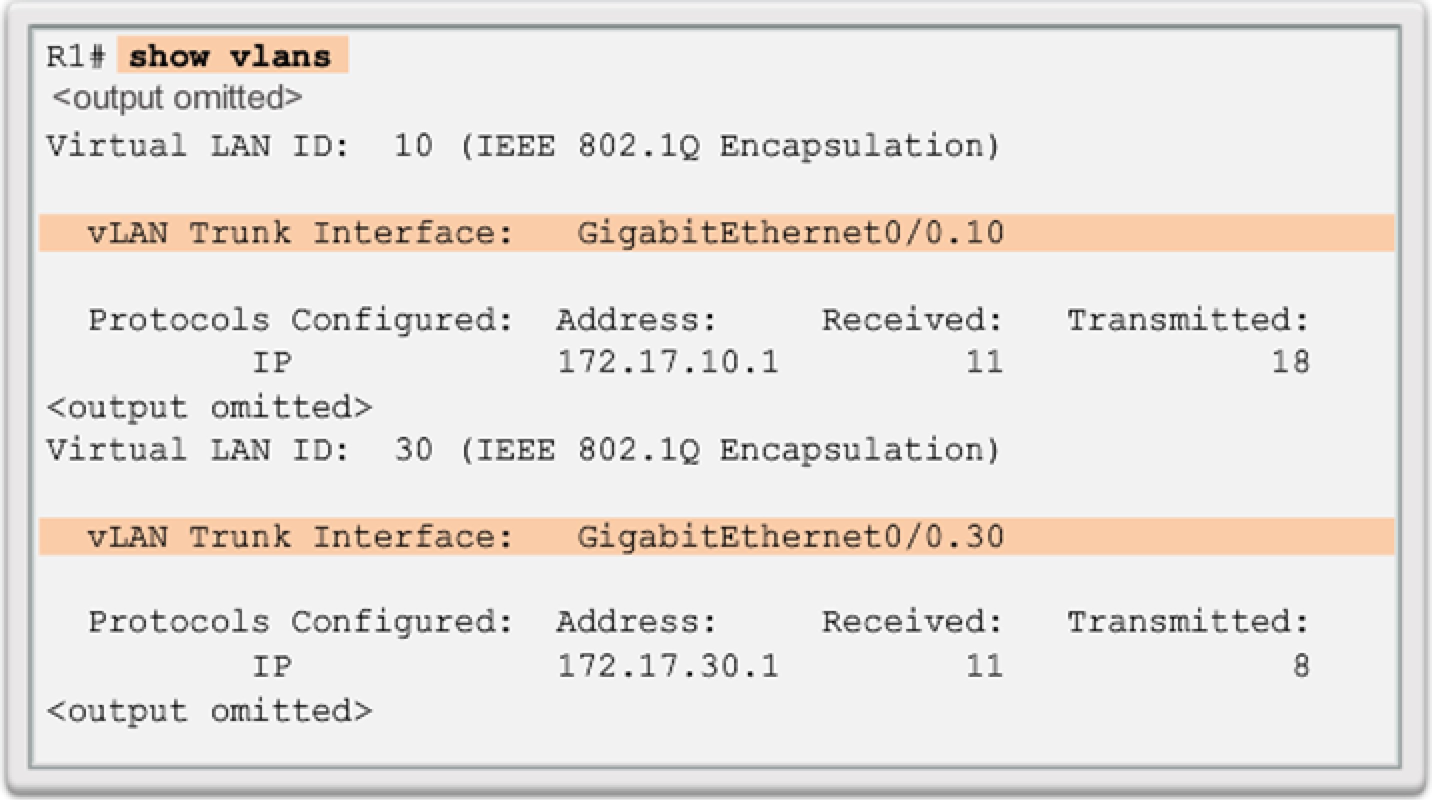
```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

3.10 Configure Router-on-a Stick: Router Subinterface Configuration



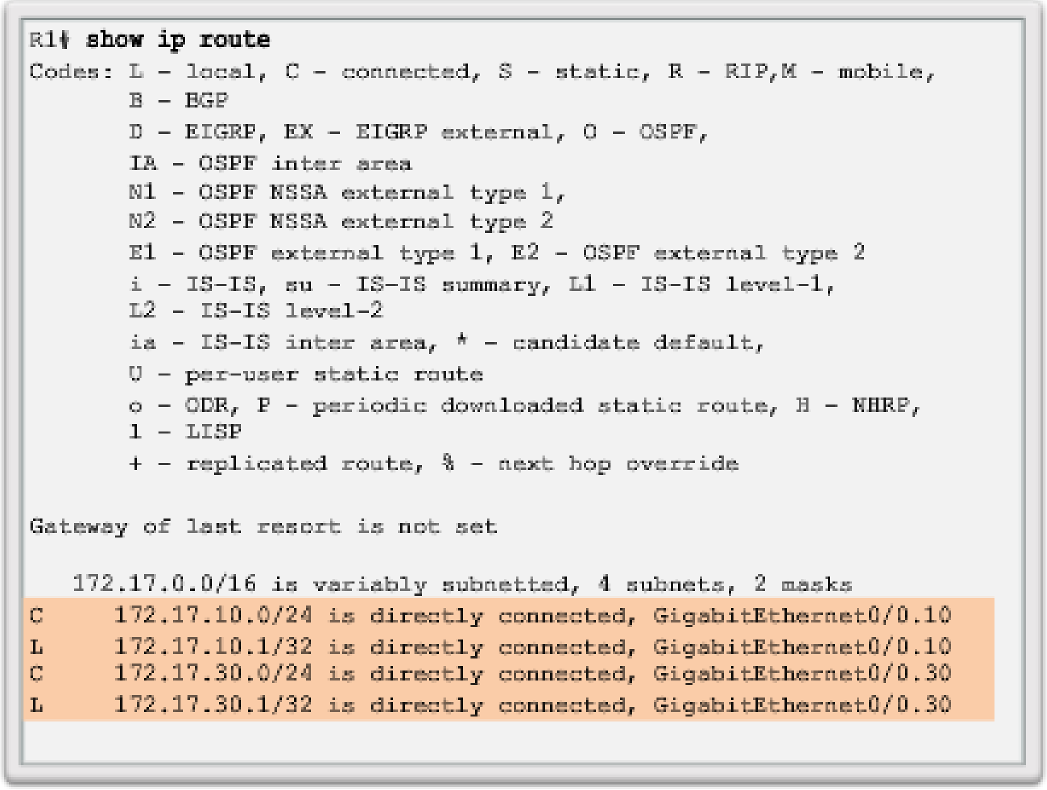
```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# no shutdown
*Mar 20 00:20:59.299: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 changed state to down
*Mar 20 00:21:02.919: %LINK-3-UPDOWN: Interface GigabitEthernet0/0,
 changed state to up
*Mar 20 00:21:03.919: %LINEPROTO-5-UPDOWN: Line protocol on
 Interface GigabitEthernet0/0, changed state to up
```

3.11 Configure Router-on-a Stick: Verifying Subinterfaces



```
R1# show vlans
<output omitted>
Virtual LAN ID:  10 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.10

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.10.1          11             18
<output omitted>
Virtual LAN ID:  30 (IEEE 802.1Q Encapsulation)

  vLAN Trunk Interface:   GigabitEthernet0/0.30

  Protocols Configured:  Address:      Received:   Transmitted:
          IP             172.17.30.1          11              8
<output omitted>
```

3.11 Configure Router-on-a Stick: Verifying Subinterfaces



```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile,
       B - BGP
       D - EIGRP, EX - EIGRP external, O - OSPF,
       IA - OSPF inter area
       N1 - OSPF NSSA external type 1,
       N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2
       i - IS-IS, su - IS-IS summary, L1 - IS-IS level-1,
       L2 - IS-IS level-2
       ia - IS-IS inter area, * - candidate default,
       U - per-user static route
       o - ODR, P - periodic downloaded static route, H - NHRP,
       l - LISP
       + - replicated route, % - next hop override

Gateway of last resort is not set

   172.17.0.0/16 is variably subnetted, 4 subnets, 2 masks
C      172.17.10.0/24 is directly connected, GigabitEthernet0/0.10
L      172.17.10.1/32 is directly connected, GigabitEthernet0/0.10
C      172.17.30.0/24 is directly connected, GigabitEthernet0/0.30
L      172.17.30.1/32 is directly connected, GigabitEthernet0/0.30
```

3.12 Configure Router-on-a Stick: Verifying Routing

- Access to devices on remote VLANs can be tested using the **`ping`** command.
- The **`ping`** command sends an ICMP echo request to the destination address.
- When a host receives an ICMP echo request, it responds with an ICMP echo reply.
- **`Tracert`** is a useful utility for confirming the routed path taken between two devices.

Chapter Summary

Summary

- Explain the purpose of VLANs in a switched network.
- Explain how a switch forwards frames based on VLAN configuration in a multi-switch environment.
- Configure a switch port to be assigned to a VLAN based on requirements.
- Configure a trunk port on a LAN switch.
- Troubleshoot VLAN and trunk configurations in a switched network.
- Describe the two options for configuring inter-VLAN routing.
- Configure Legacy Inter-VLAN Routing.
- Configure Router-on-a-Stick Inter-VLAN Routing

TERIMA KASIH

CISCO™