# VLANs

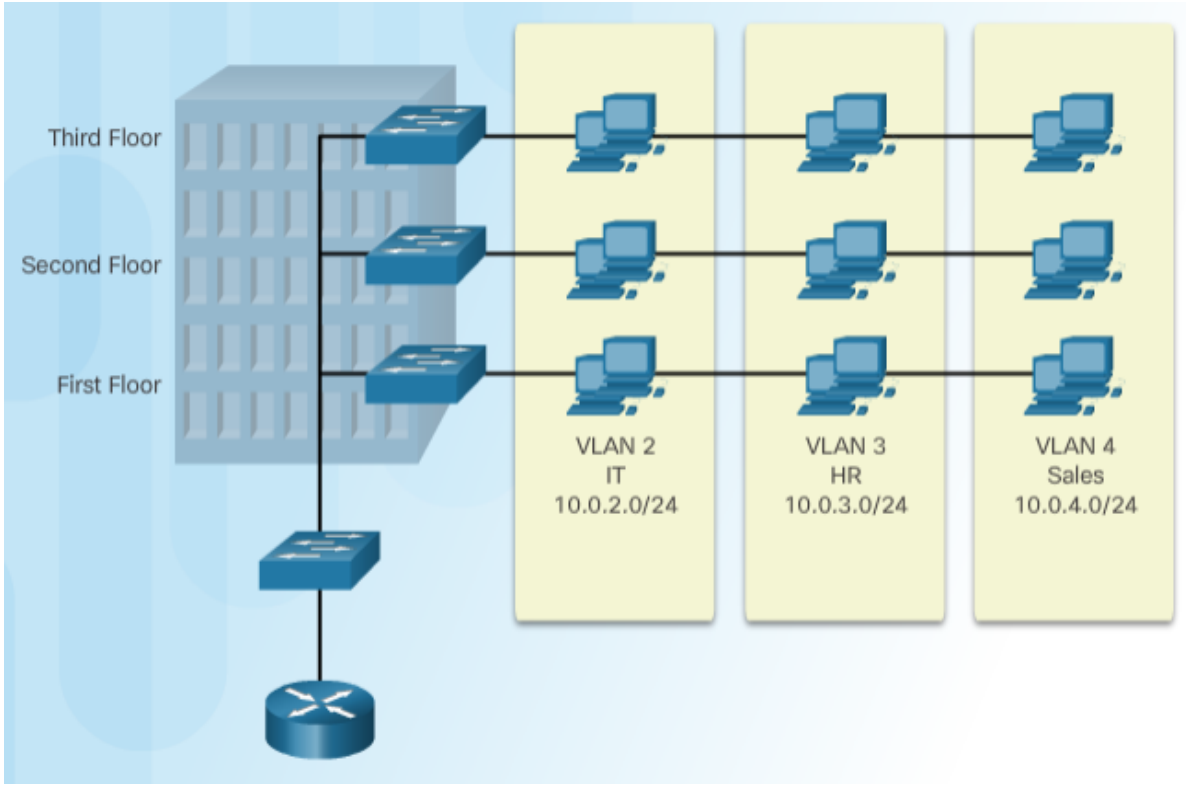
Faculty of Technology

University of Sri Jayewardenepura

2020

# Overview of VLANs

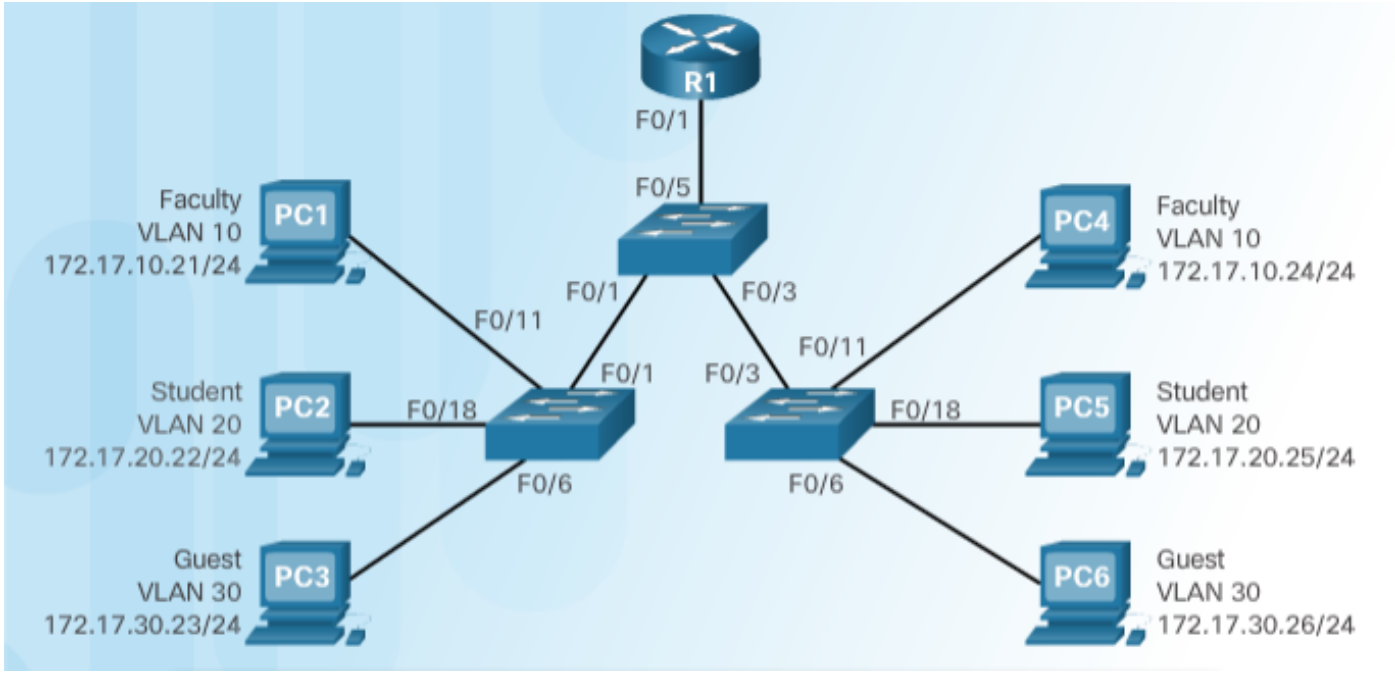
- VLANs can segment LAN devices without regard for the physical location of the user or device.
  - In the figure, IT users on the first, second, and third floors are all on the same LAN segment. The same is true for HR and Sales users.
- A VLAN is a logical partition of a Layer 2 network.
  - Multiple partitions can be created and multiple VLANs can co-exist.
  - The partitioning of the Layer 2 network takes place inside a Layer 2 device, usually via a switch.
  - Each VLAN is a broadcast domain that can span multiple physical LAN segments.
  - Hosts on the same VLAN are unaware of the VLAN's existence.




VLANs are mutually isolated and packets can only pass between VLANs via a router.

# Benefits of VLANs

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



# Types of VLANs

- **Default VLAN** – Also known as VLAN 1. All switch ports are members of VLAN 1 by default.
- **Data VLAN** – Data VLANs are commonly created for specific groups of users or devices. They carry user generated traffic.
- **Native VLAN** – This is the VLAN that carries all untagged traffic. This is traffic that does not originate from a VLAN port (e.g., STP BPDU traffic exchanged between STP enabled switches). The native VLAN is VLAN 1 by default.
- **Management VLAN** – This is a VLAN that is created to carry network management traffic including SSH, SNMP, Syslog, and more. VLAN 1 is the default VLAN used for network management.

## Default VLAN Assignment

```
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
```

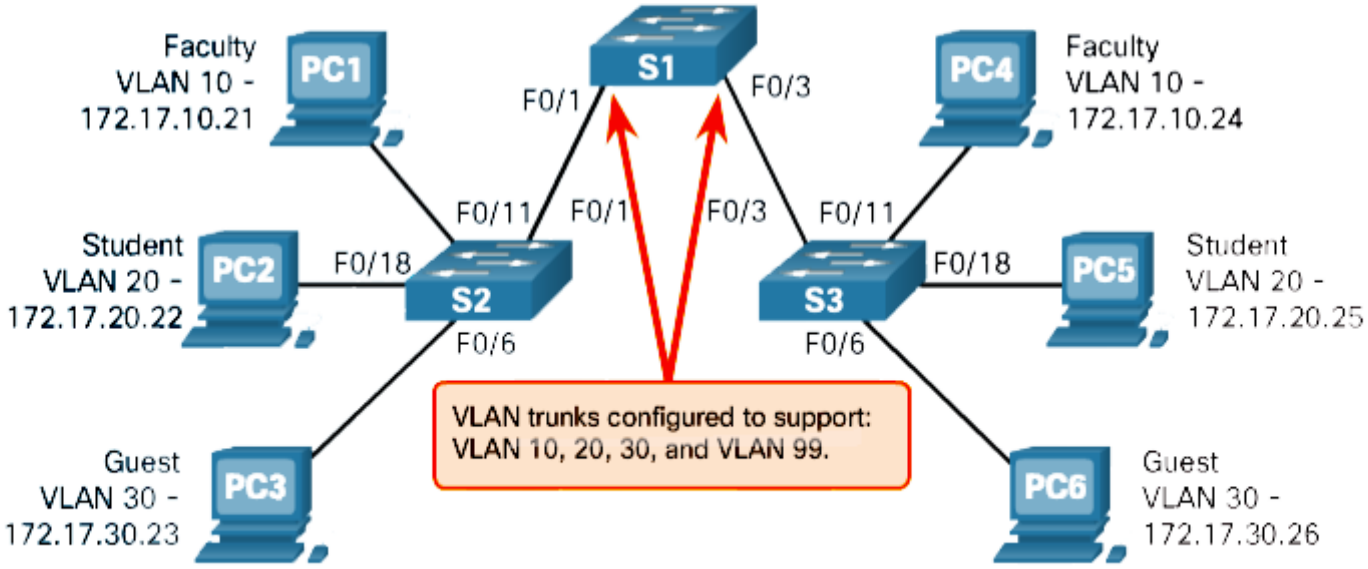
Initially, all switch ports are members of VLAN 1.

# 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.

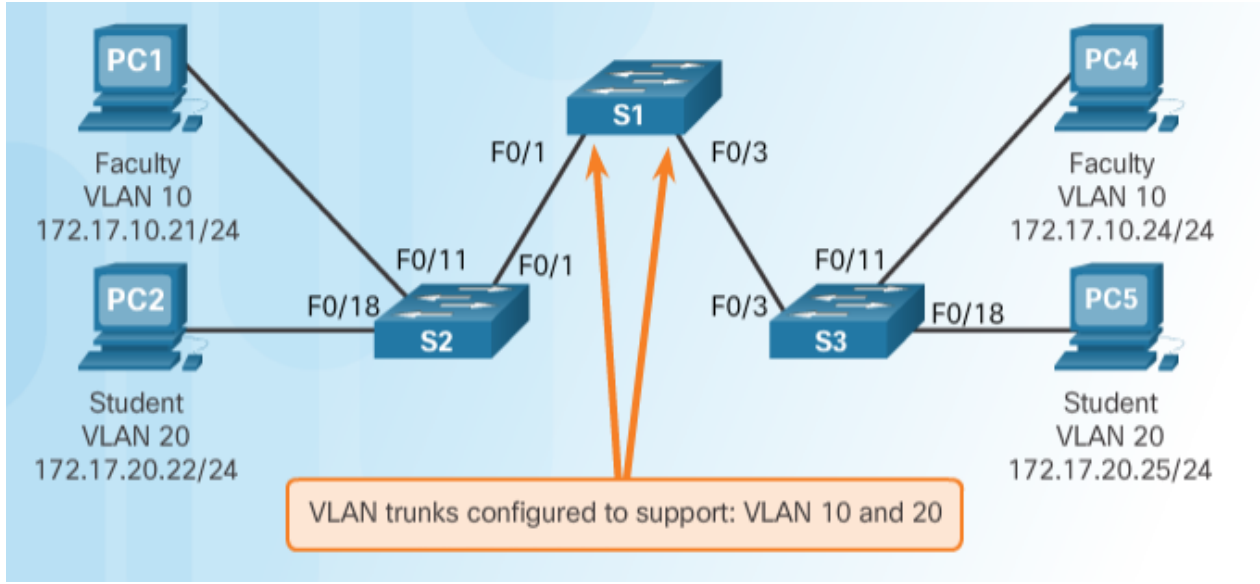
- A VLAN trunk is a point-to-point link that carries more than one VLAN.
  - Usually established between switches to support intra VLAN communication.
  - A VLAN trunk or trunk ports are not associated to any VLANs.
- Cisco IOS supports IEEE 802.1q, a popular VLAN trunk protocol.




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.

# Controlling Broadcast Domains with VLANs

- If a switch port receives a broadcast frame, it forwards it out all ports except the originating port.
  - Eventually the entire network receives the broadcast because the network is one broadcast domain.
- VLANs can be used to limit the reach of broadcast frames because each VLAN is a broadcast domain.
  - VLANs help control the reach of broadcast frames and their impact in the network.

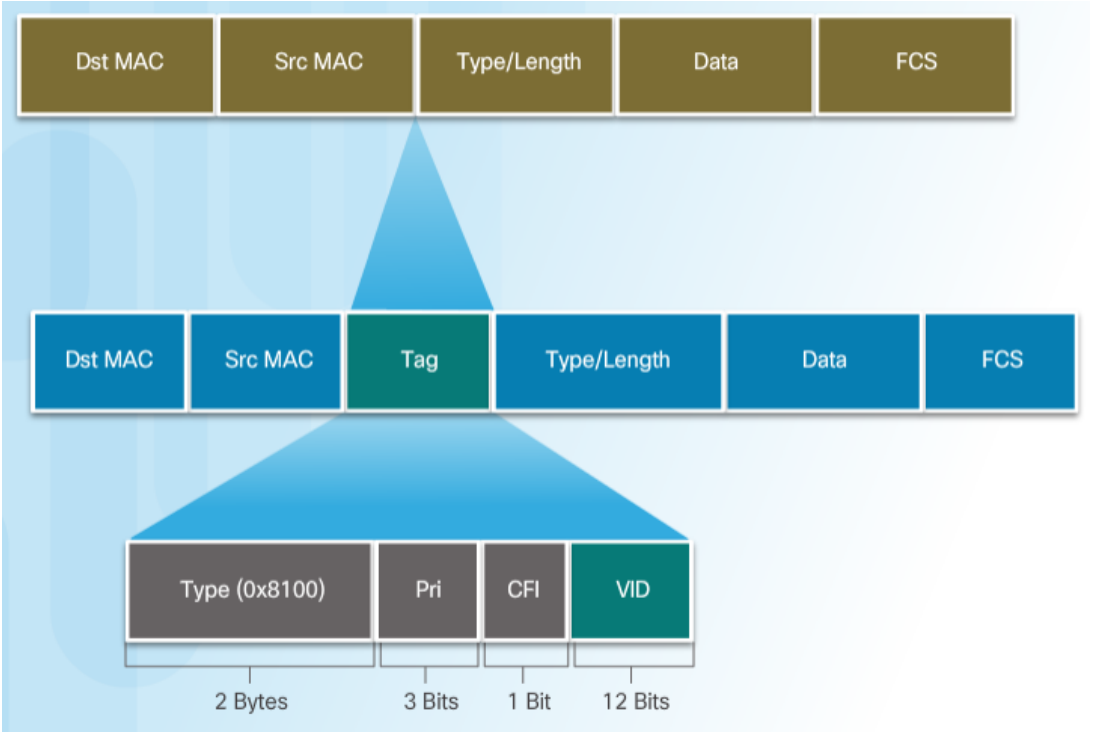



In the figure, PC1 on VLAN 10 sends a broadcast frame. Only devices in the same VLAN receive the broadcast therefore, PC4 would receive the broadcast.

# Tagging Ethernet Frames for VLAN Identification

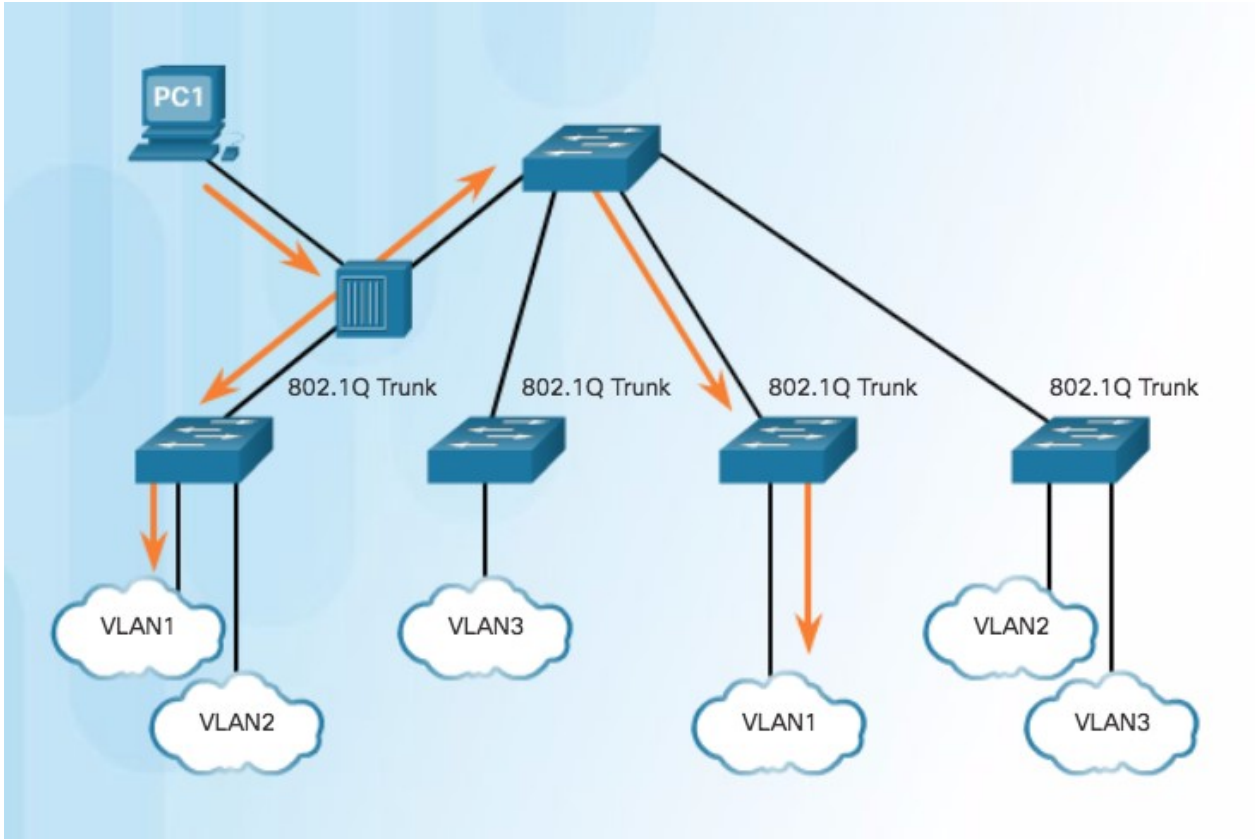
- Before a frame is forwarded across a trunk link, it must be tagged with its VLAN information.
  - Frame tagging is the process of adding a VLAN identification header to the frame.
  - It is used to properly transmit multiple VLAN frames through a trunk link.
- Switches add VLAN tagging information after the Source MAC address field.
- IEEE 802.1Q is a vey popular VLAN trunking protocol that defines the structure of the tagging header added to the frame.
- The fields in the 802.1Q VLAN tag includes VLAN ID (VID).

- Trunk links add the tag information before sending the frame and then remove the tags before forwarding frames through non-trunk ports.



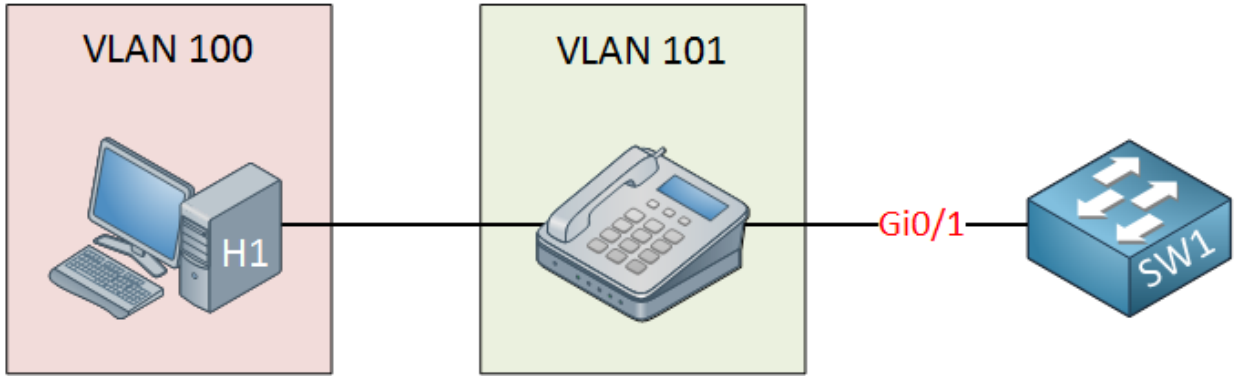
# Native VLANs and 802.1Q Tagging

- 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.



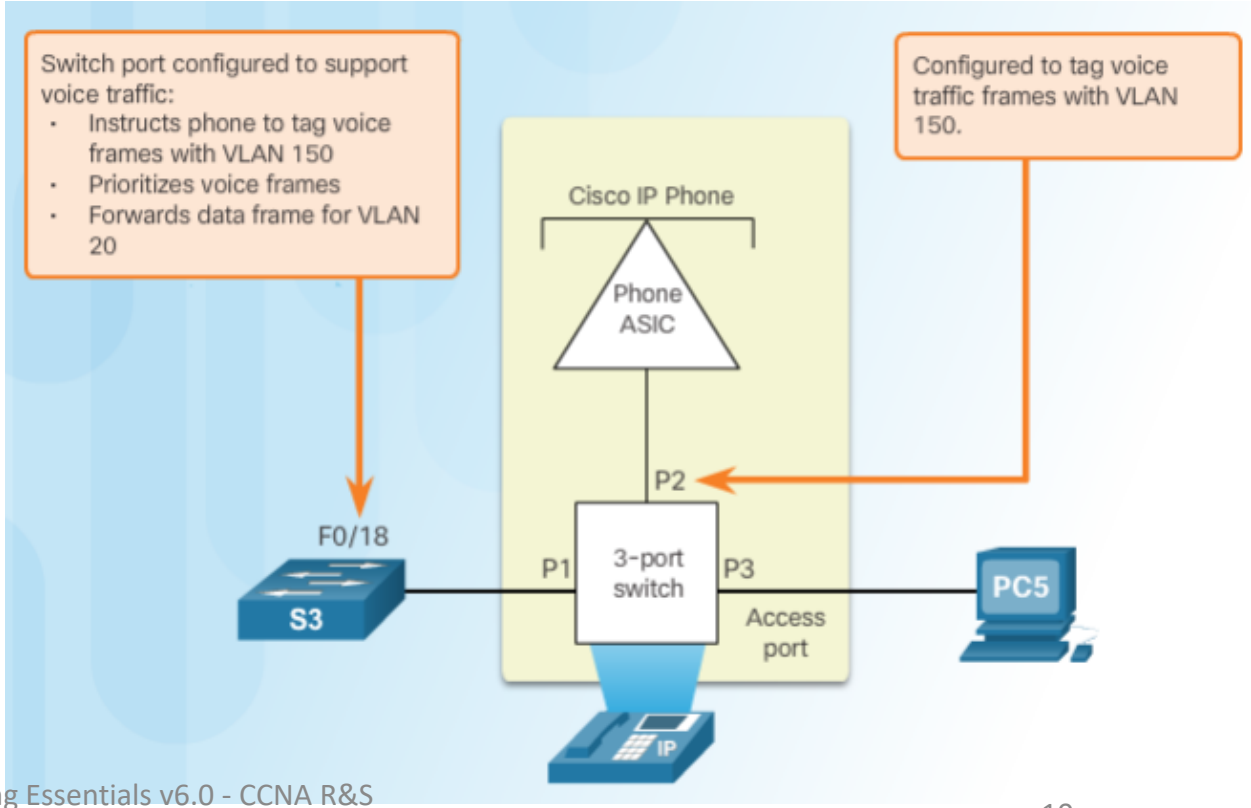
# Voice VLANs (Auxiliary VLANs)

- To support time-sensitive voice traffic, a voice VLAN requires:
  - Assured bandwidth
  - Delay of less than 150 ms across the network to ensure voice quality
  - Transmission priority over other types of network traffic
  - Ability to be routed around congested areas on the network.
- The voice VLAN feature enables access ports to carry user and IP voice traffic.
- The computer will be in a **data VLAN**, the IP phone will be in the **voice VLAN**.



# Voice VLAN Tagging

- An access port connecting a Cisco IP phone can be configured to use two separate VLANs:
  - A VLAN for voice traffic
  - A VLAN for data traffic from a device attached to the phone.
- Cisco IP Phone contains an integrated three-port 10/100 switch dedicated to these devices:
  - Port 1 connects to the switch or other VoIP device.
  - Port 2 is an internal 10/100 interface that carries the IP phone traffic.
  - Port 3 (access port) connects to a PC or other device.
- The link between the switch and the IP phone behaves like a trunk to carry traffic from both VLANs.



# VLAN Implementation

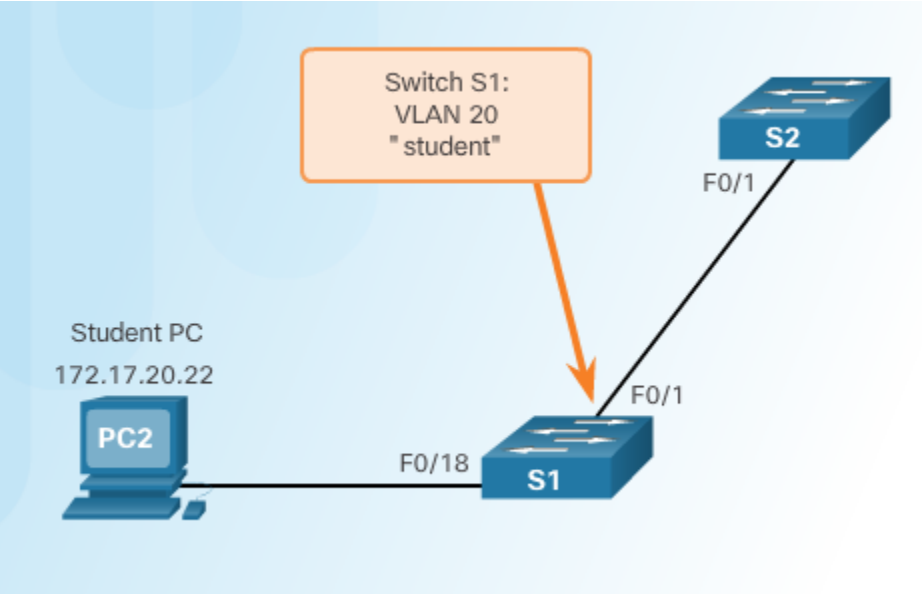
# VLAN Assignment

- 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 legacy 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

```
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
```

# 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** |



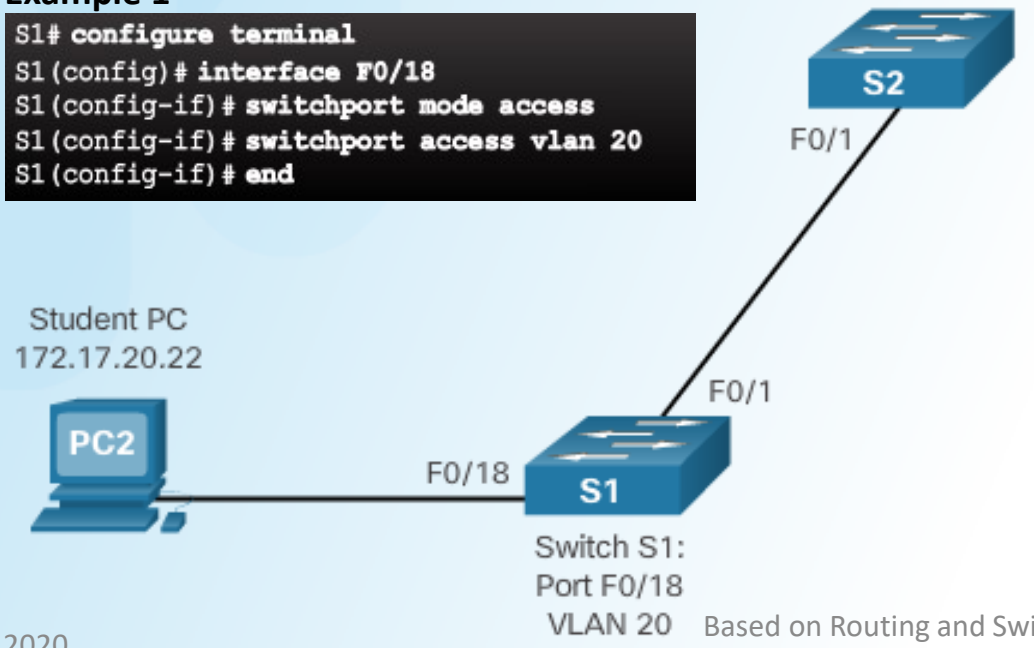

```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

# 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 |

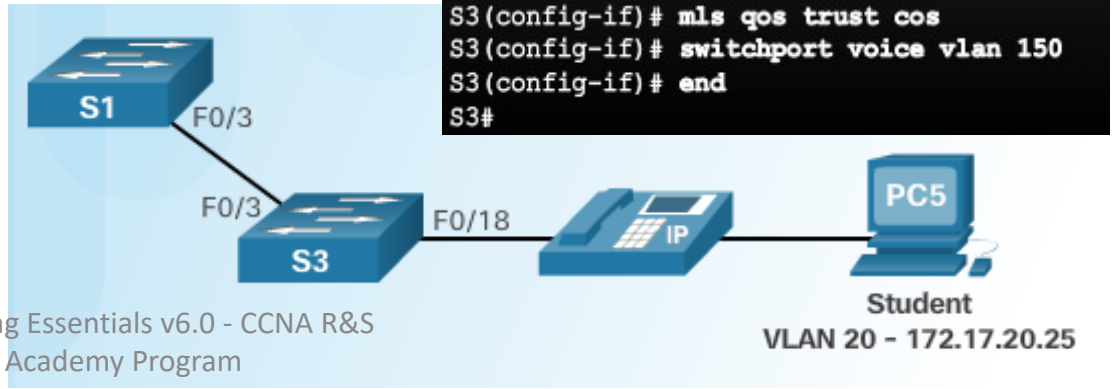
**Example 1**

```
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
```




**Example 2**

```
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#
```



# Changing VLAN Port Membership

- Remove VLAN Assignment

| Cisco Switch IOS Commands | |
|---|---|
| Enter global configuration mode. | `S1# configure terminal` |
| Enter interface configuration mode | `S1(config)# interface F0/18` |
| Remove the VLAN assignment from the port. | `S1(config-if)# no switchport access vlan` |
| Return to the privileged EXEC mode. | `S1(config-if)# end` |

- Deleting VLANs
  - To remove VLAN, use the **`no vlan`** *`vlan-id`* global configuration mode command.
  - To delete the entire vlan.dat file, use the **`delete flash:vlan.dat`** privileged EXEC mode command.
    - **`delete vlan.dat`** can be used if the vlan.dat file has not been moved from its default location.

# Verifying VLAN Information

- VLAN configurations can be validated using the Cisco IOS `show vlan` and `show interfaces` command options.

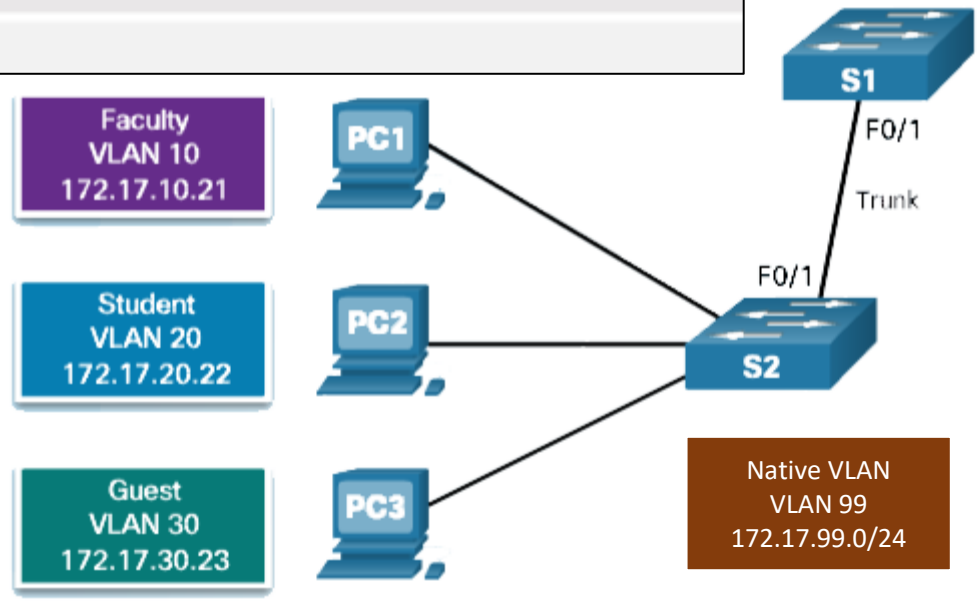
```
S1# show vlan name student

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# 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
```

# Configuring IEEE 802.1q Trunk Links

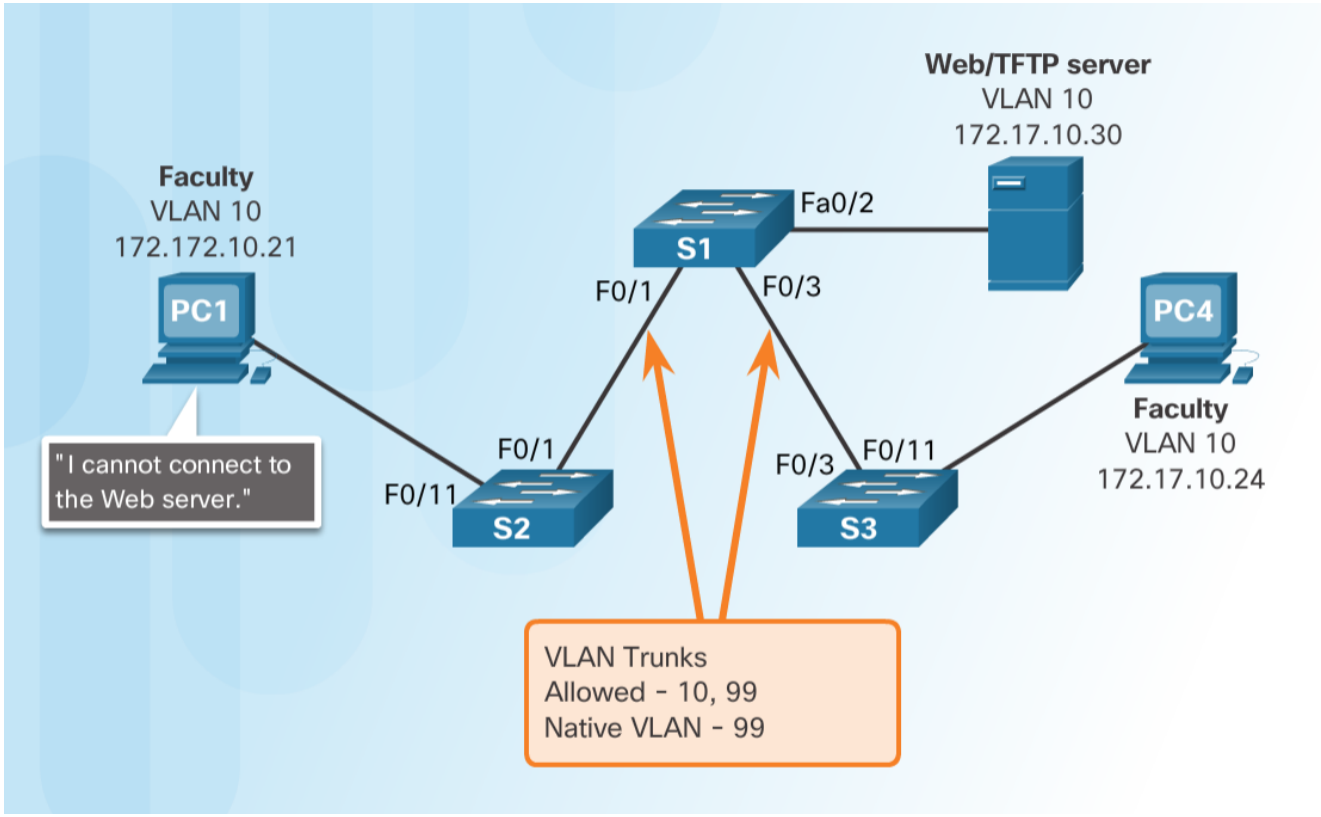
| Cisco Switch IOS Commands | |
|---|---|
| Enter global configuration mode. | `S1# configure terminal` |
| Enter interface configuration mode. | `S1(config)# interface` *interface_id* |
| Force the link to be a trunk link. | `S1(config-if)# switchport mode trunk` |
| Specify a native VLAN for untagged 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
```



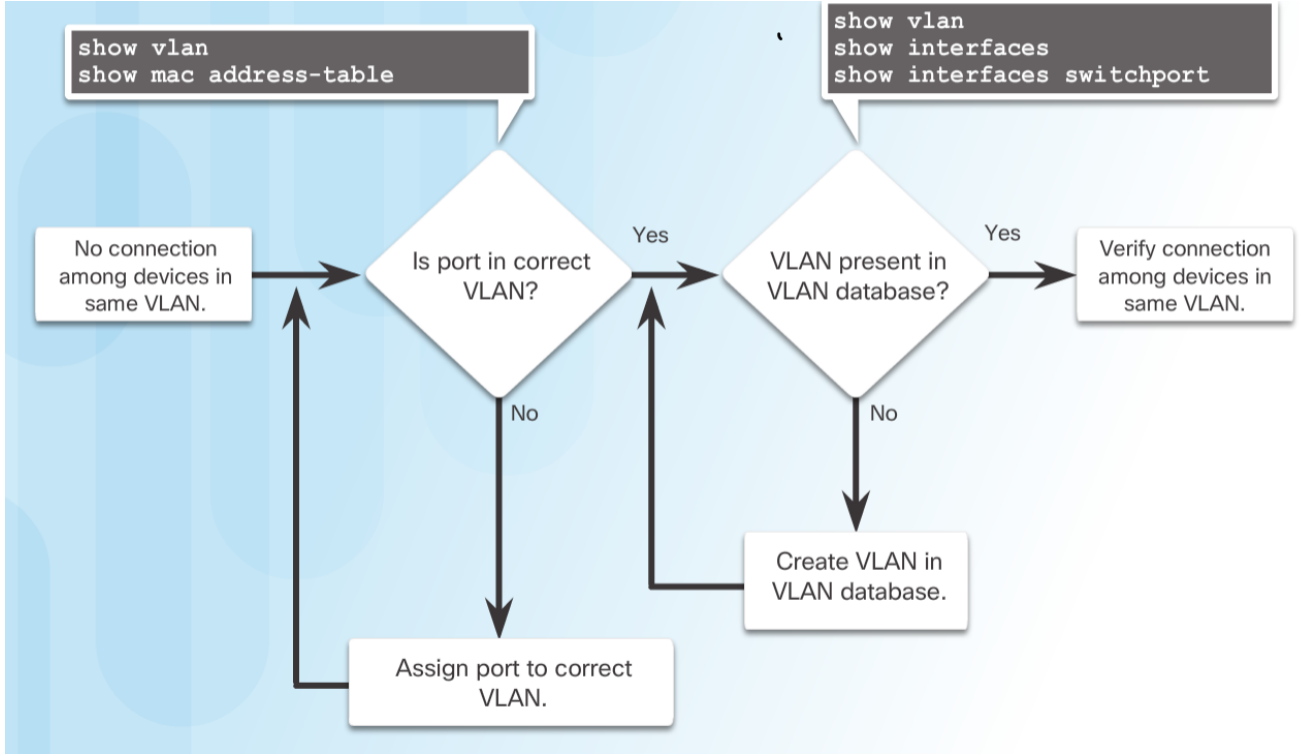
# Troubleshooting VLANs

- Common practice to associate a VLAN with an IP network.
  - Different IP networks must communicate through a router.
  - All devices within a VLAN must be part of the same IP network to communicate.
  - In the figure, PC1 cannot communicate to the server because it has a wrong IP address configured.



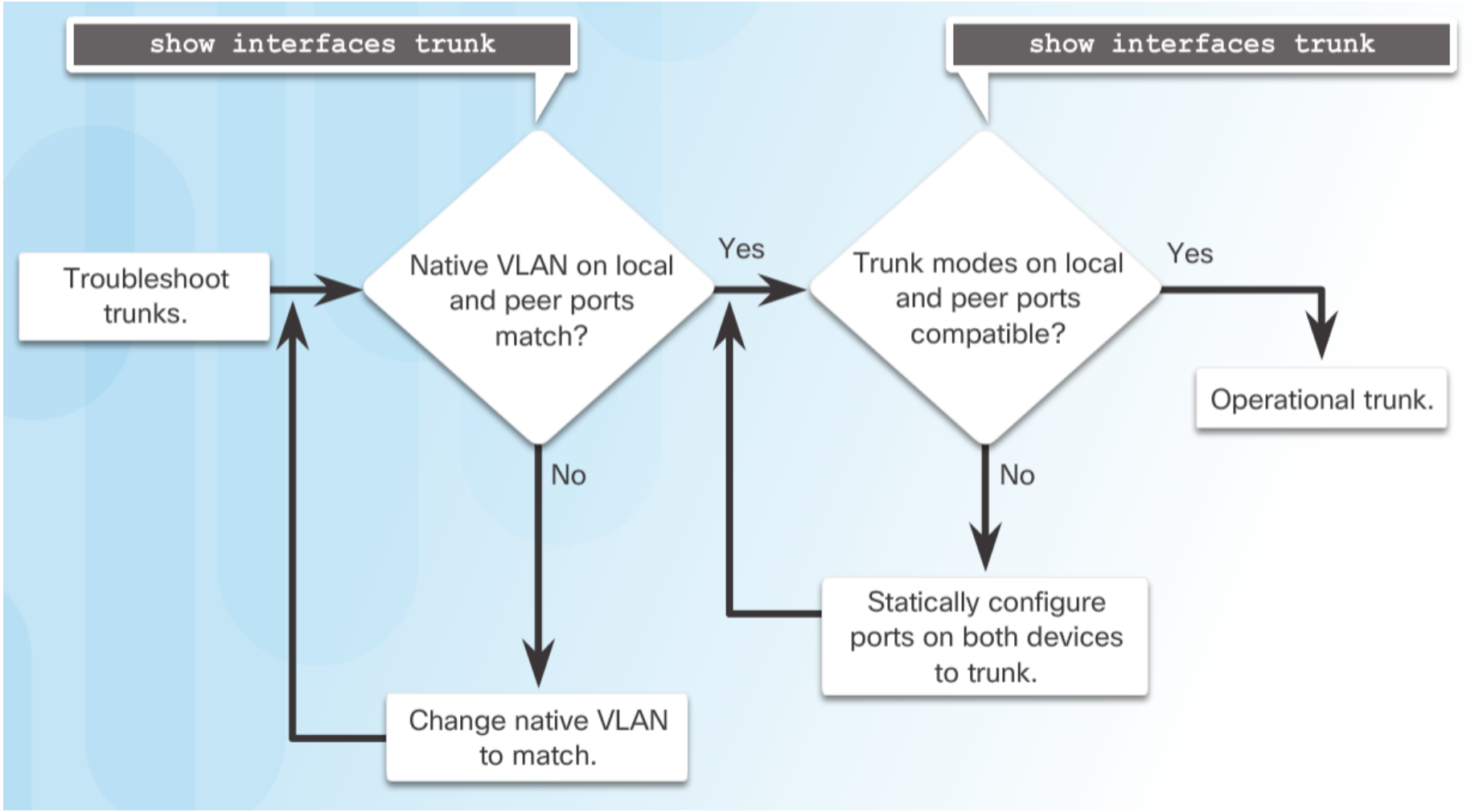
# Missing VLANs

- If all the IP address mismatches have been solved, but the device still cannot connect, check if the VLAN exists in the switch.
- If the VLAN to which the port belongs is deleted, the port becomes inactive and is unable to communicate with the rest of the network.
  - It is not functional until the missing VLAN is created or the VLAN is removed from the port.




```
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
```

# Troubleshooting Trunks



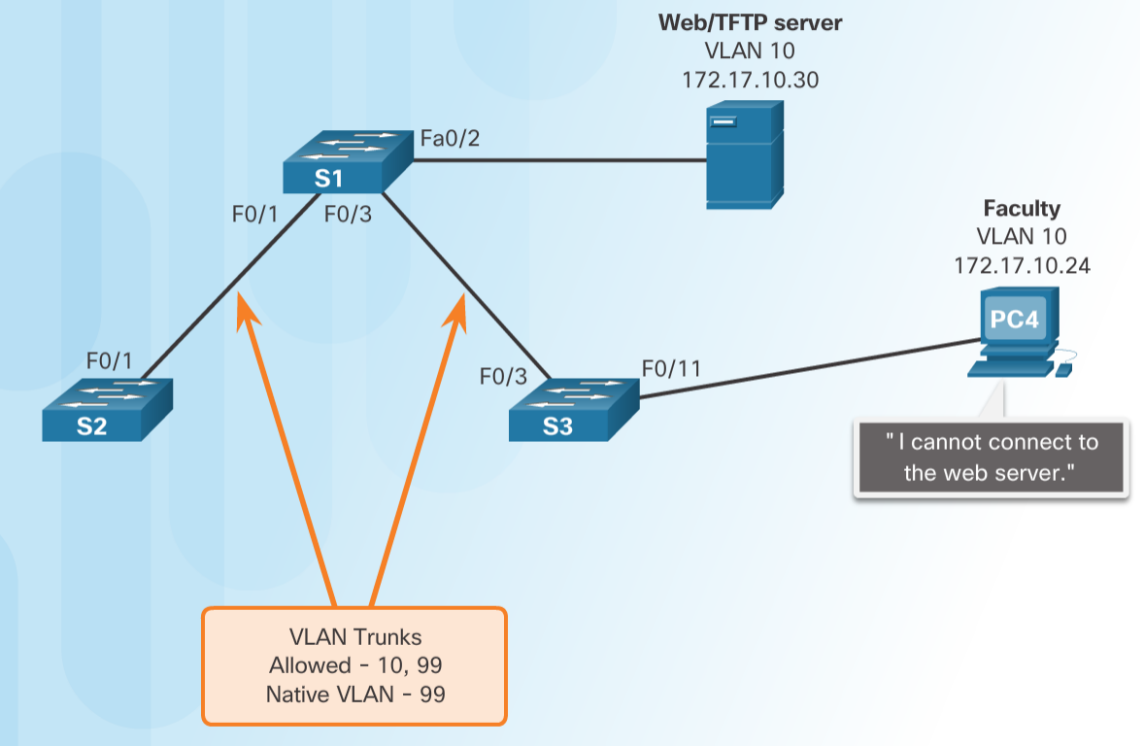
# Common Problems with Trunks

- Trunking issues are usually associated with incorrect configurations.
- The most common type of trunk configuration errors are:

| 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, one side of the trunk is configured as an access port. |
| 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. |

- When a trunk problem is suspected, it is recommended to troubleshoot in the order shown above.

# Incorrect Port Mode




- In this example, PC4 cannot reach the Web server.
  - The trunk links on S1 and S3 are verified and reveal that the S3 trunk port has been configured as an access port.
- To resolve the issue, the S3 F03 port is configured as a trunk link.

```
S1# show interface f0/3 switchport
Name: Fa0/3
Switchport: Enabled
Administrative Mode: trunk
```

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

```
S3# config terminal
S3(config)# interface f0/3
S3(config-if)# switchport mode trunk
S3(config-if)# end
```

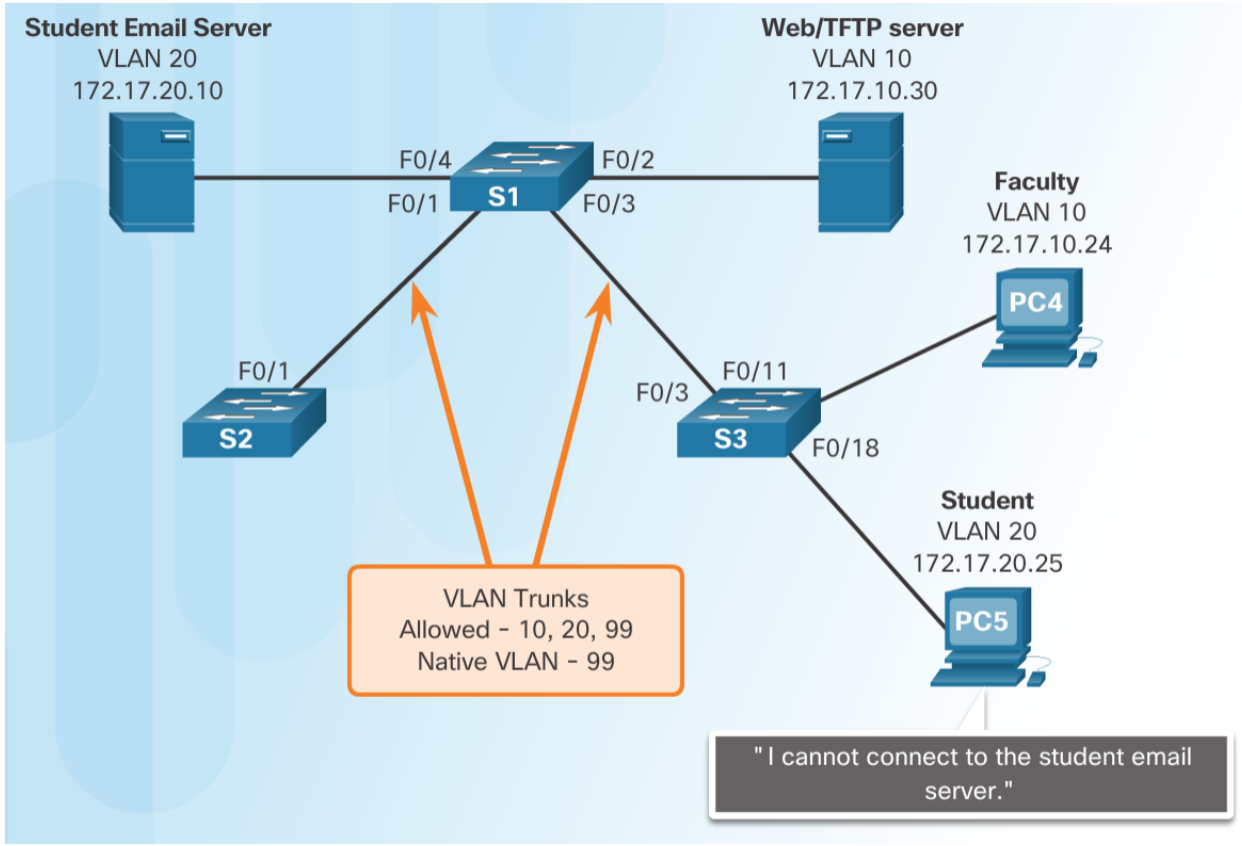
# Incorrect VLAN List

```
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#
```

- In this example, PC5 cannot reach the Student Email server.
  - The output of the switchport trunk allowed vlan command reveals S1 is not allowing VLAN 20.

To resolve the issue, the S1 F0/1 port is configured to allow VLANs 10, 20, and 99.

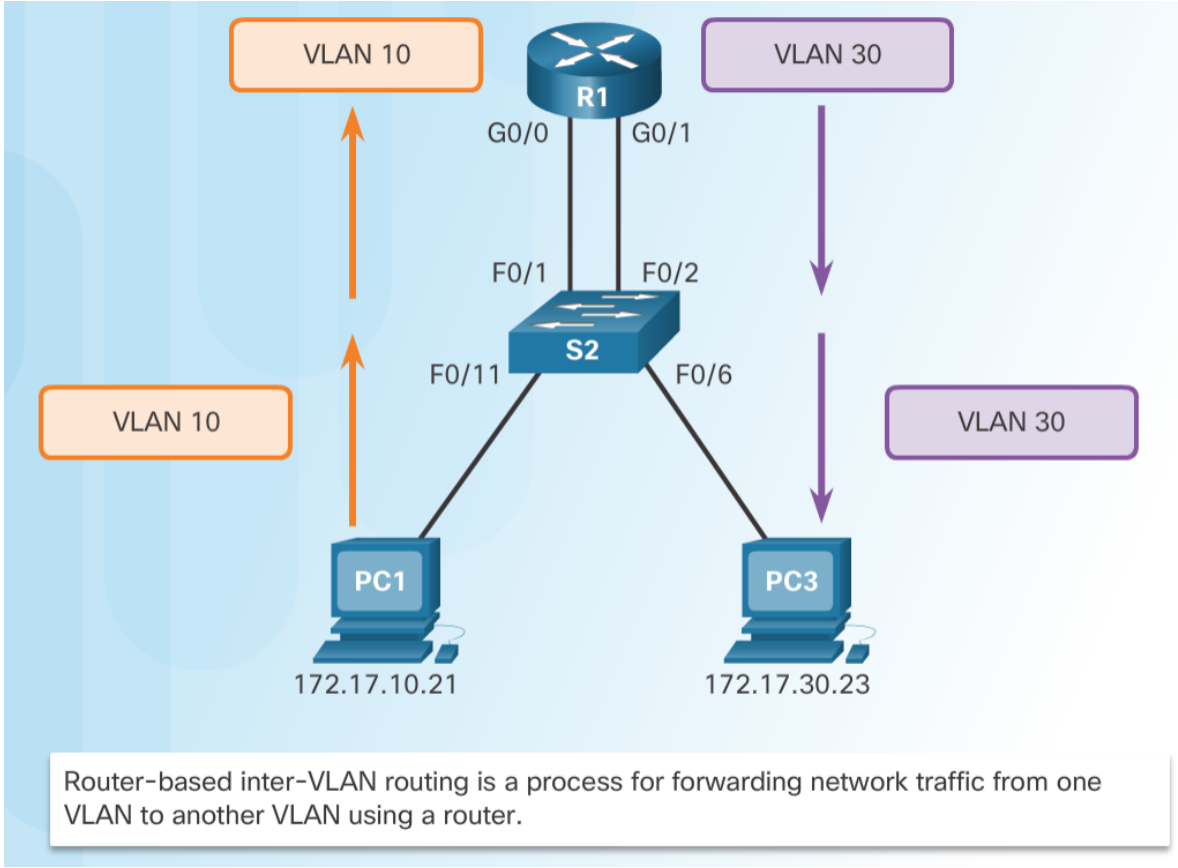
```
S1# config terminal
S1(config)# interface f0/1
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1(config-if)# interface f0/3
S1(config-if)# switchport trunk allowed vlan 10,20,99
S1# show interfaces trunk
Port        Mode     Encapsulation  Status     Native vlan
Fa0/1       on         802.1q       trunking       99
Fa0/3       on         802.1q       trunking       99
Port        Vlans allowed on trunk
Fa0/1       10,20,99
Fa0/3       10,20,99
…
```



# Inter-VLAN Routing Using Routers

# Inter-VLAN Routing Operation

- 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.
- There are three options for inter-VLAN routing:
  - Legacy inter-VLAN routing
  - Router-on-a-Stick
  - Layer 3 switching using SVIs

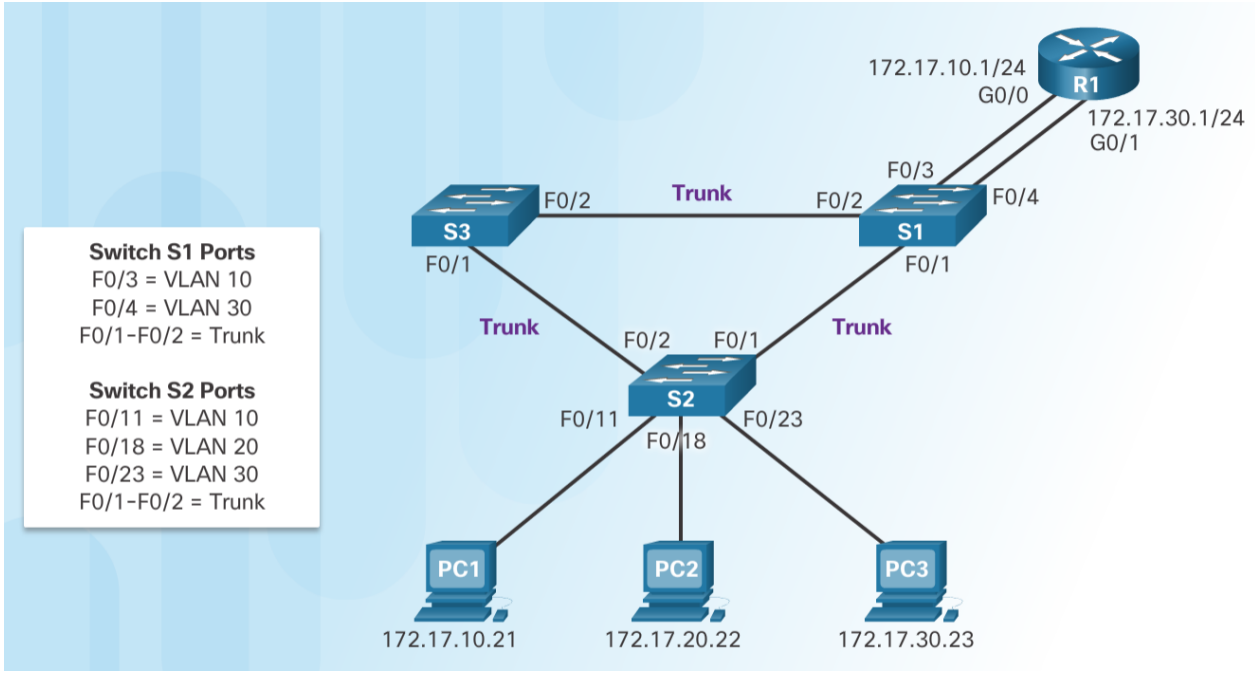



Router-based inter-VLAN routing is a process for forwarding network traffic from one VLAN to another VLAN using a router.

# Legacy Inter-VLAN Routing

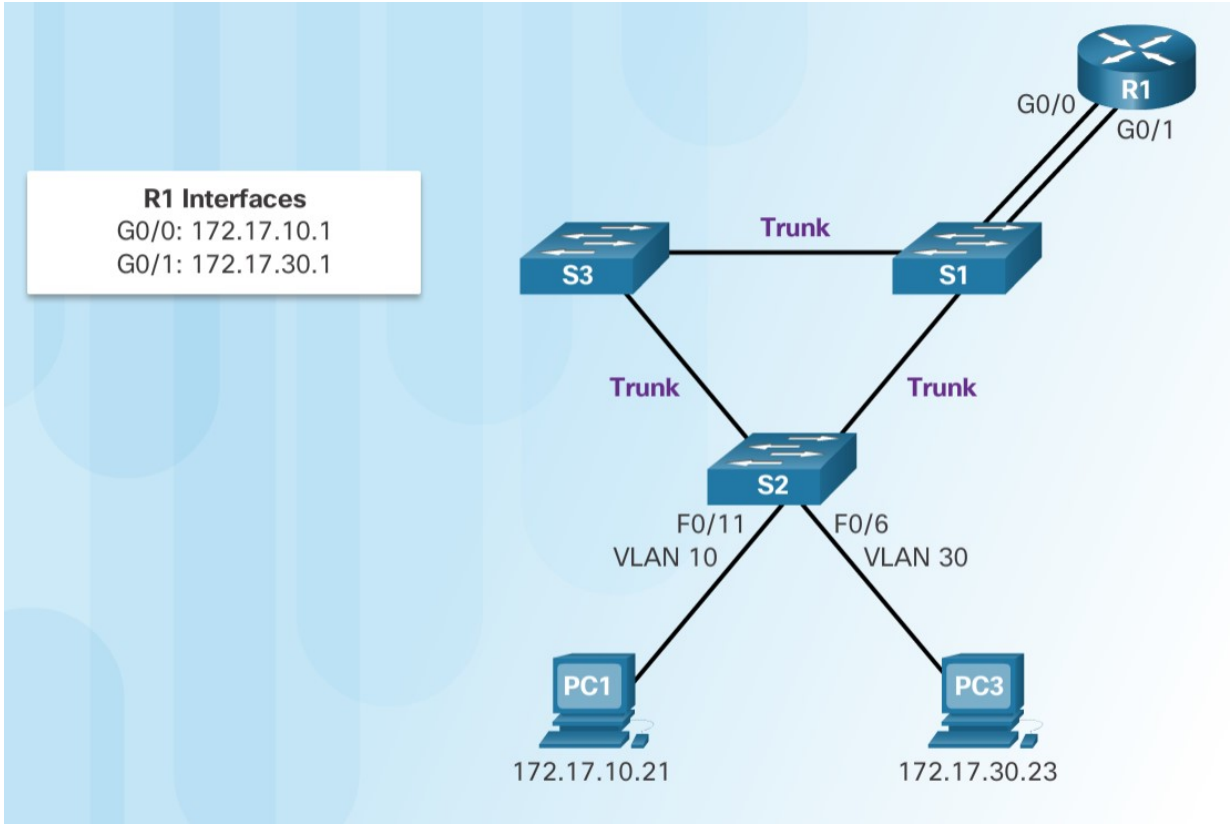
- Router interfaces were used to route between VLANs.
- Each VLAN was connected to a different physical router interface.
- Packets would arrive on the router through one interface, be routed and leave through another.
- Because the router interfaces were connected to VLANs and had IP addresses from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

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



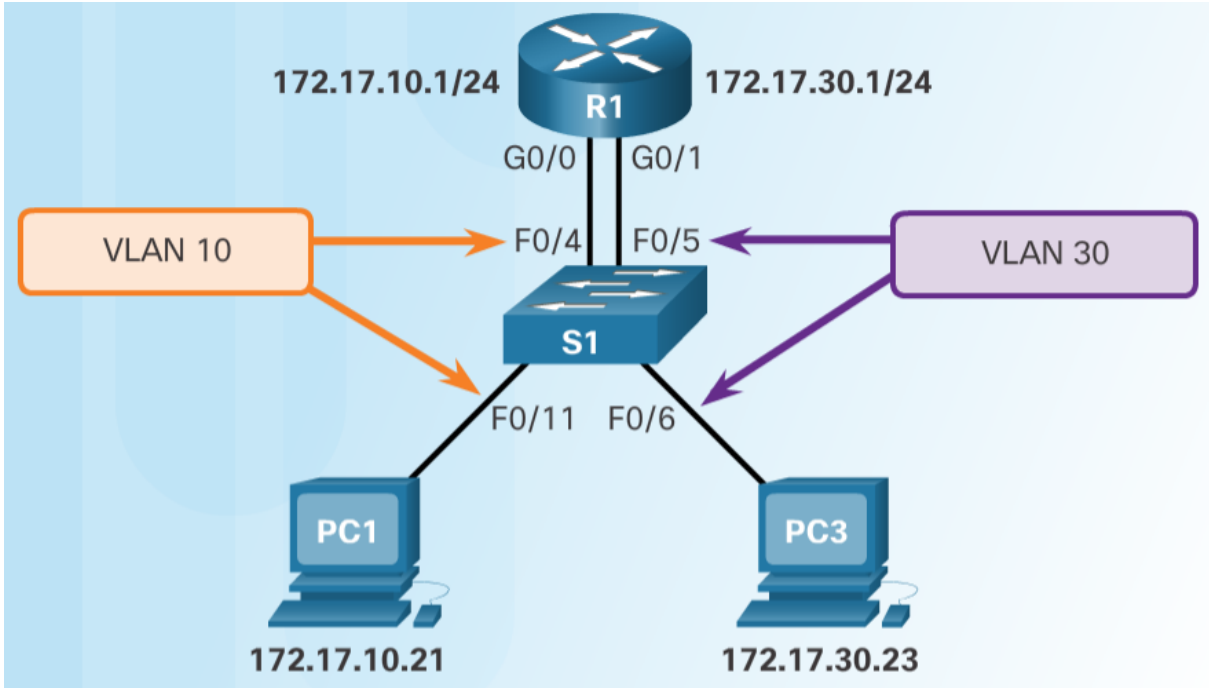
# Configure Legacy Inter-VLAN Routing:
# Preparation

- 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.



# Configure Legacy Inter-VLAN Routing:
# Switch Configuration

- Configure the VLANs on the switch and then assign the ports to their respective VLANs.
- In this example, the S1 ports are configured as follows:
  - Ports F0/4 and F0/11 of S1 are on VLAN 10
  - Ports F0/5 and F0/16 ports are on VLAN 30.

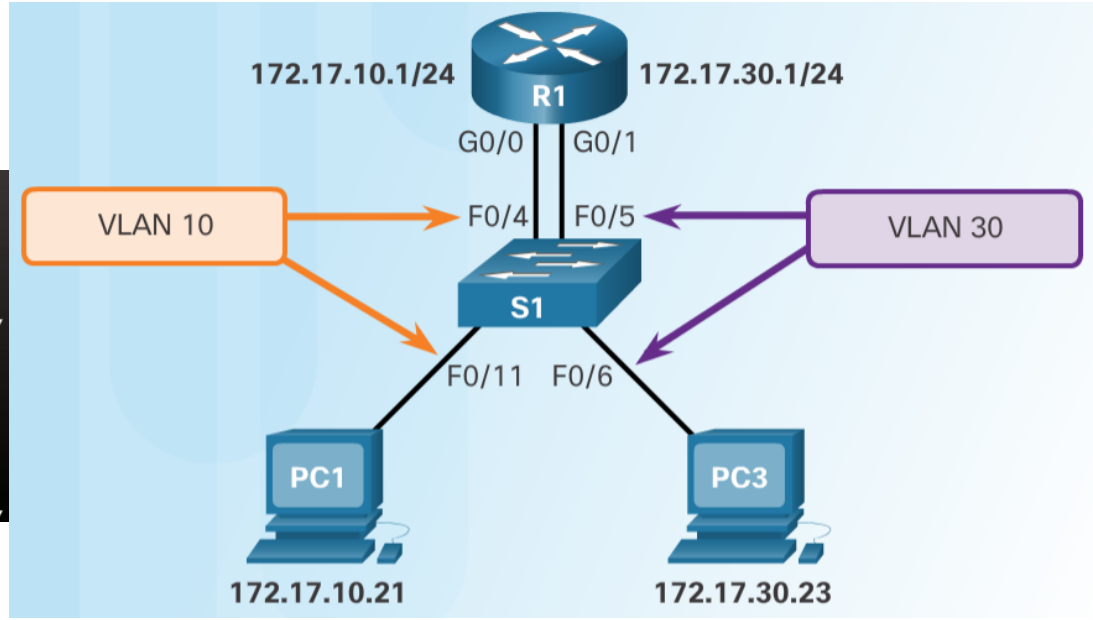



```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/11
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/4
S1(config-if)# switchport access vlan 10
S1(config-if)# interface f0/6
S1(config-if)# switchport access vlan 30
S1(config-if)# interface f0/5
S1(config-if)# switchport access vlan 30
S1(config-if)# end
```

# Configure Legacy Inter-VLAN Routing:
# Router Interface Configuration

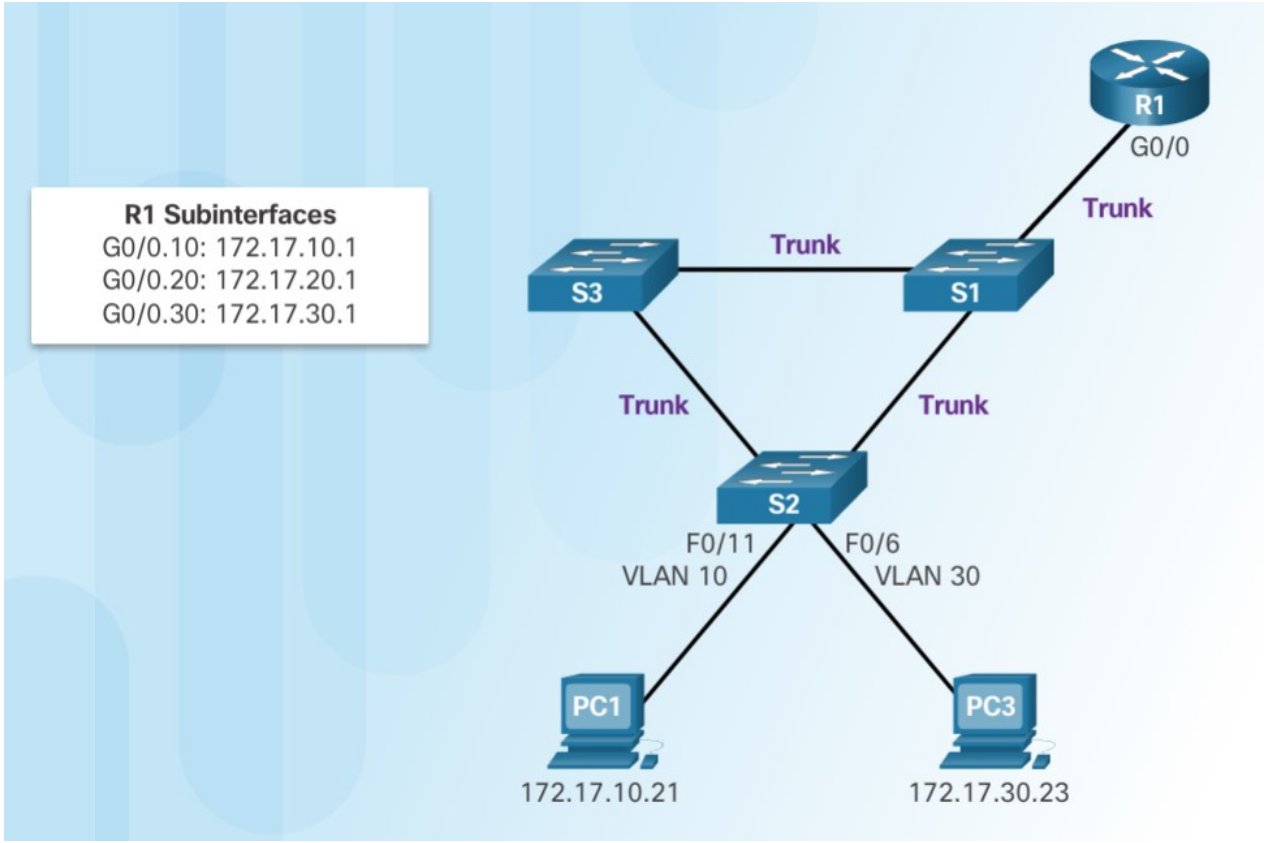
- Next configure the router interfaces.

```
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,
```



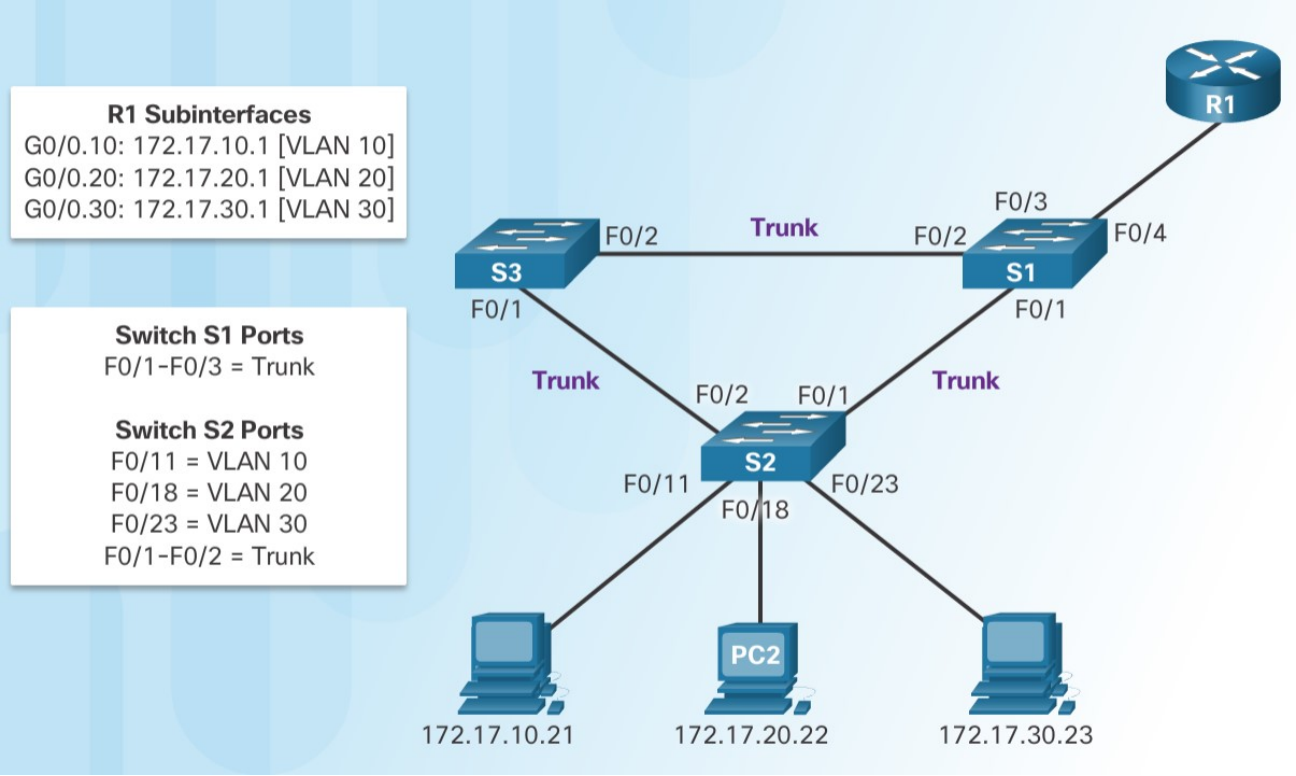
# Router-on-a-Stick Inter-VLAN Routing

- 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.



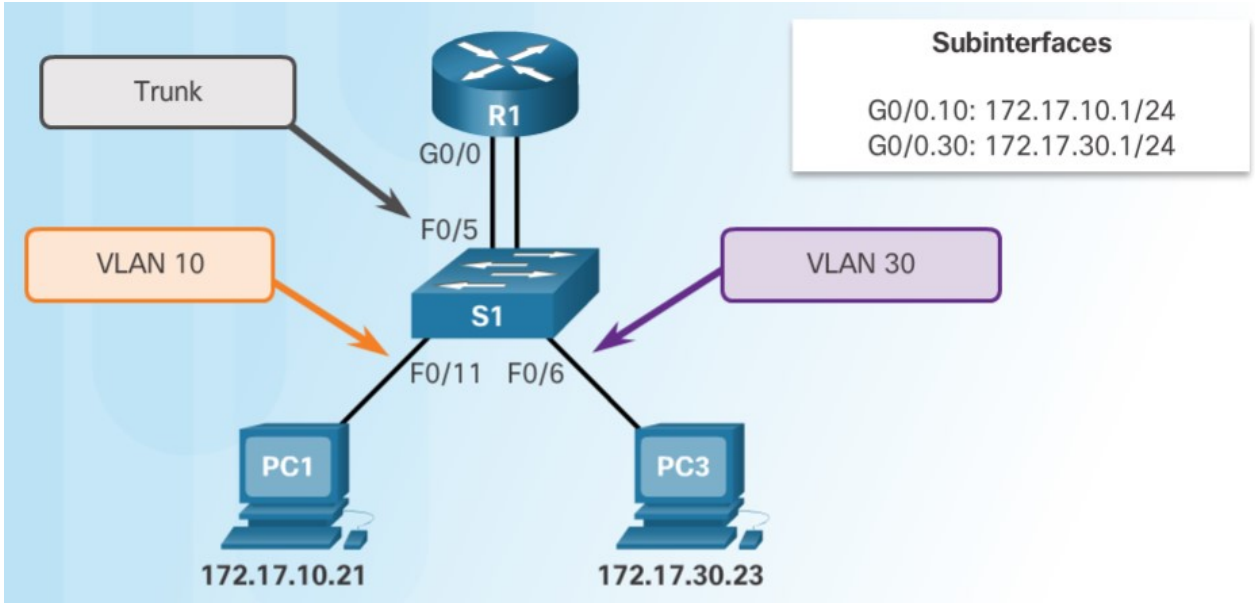
# Configure Router-on-a Stick:
# Preparation

- 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.



# Configure Router-on-a Stick: Switch Configuration

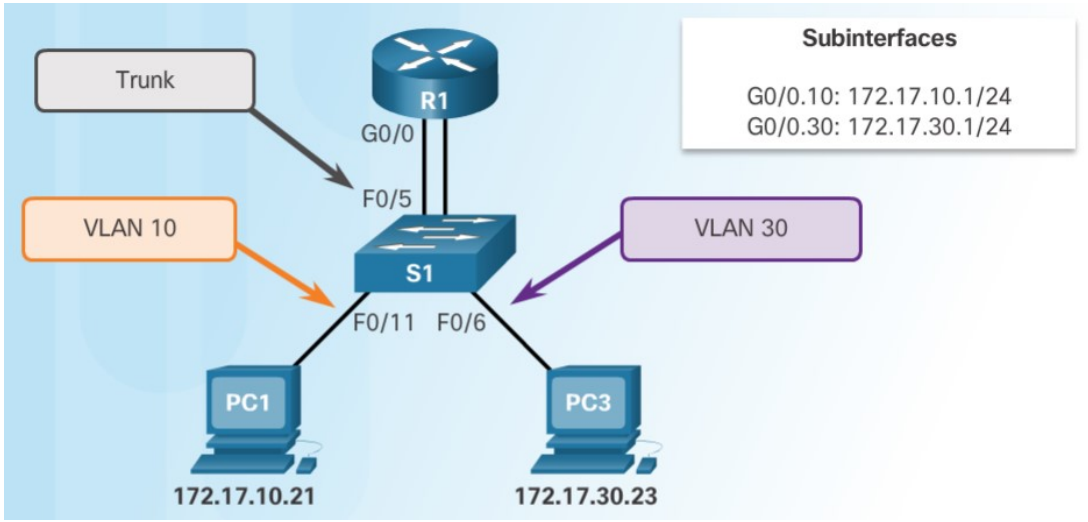
- To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.




```
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#
```

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

- The router-on-a-stick method requires subinterfaces to be configured for each routable VLAN.
  - The subinterfaces must be configured to support VLANs using the encapsulation dot1Q VLAN-ID interface configuration command.




```
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 Interface GigabitEthernet0/0,
changed state to up
```

# Configure Router-on-a Stick:
# Verifying Subinterfaces

- By default, Cisco routers are configured to route traffic between local subinterfaces.
  - As a result, routing does not specifically need to be enabled.
- Use the show vlan and show ip route commands to verify the subinterface configurations.
- The **show vlan** command displays information about the Cisco IOS VLAN subinterfaces.
- The **show ip route** command displays the routing table containing the networks associated with outgoing subinterfaces.

```
R1# show vlan
<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>
```

```
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
```

# Configure Router-on-a Stick:
# Verifying Routing

- Remote VLAN device connectivity can be tested using the ping command.
  - The command sends an ICMP echo request and when a host receives an ICMP echo request, it responds with an ICMP echo reply.

```
PC1> ping 172.17.30.23

Pinging 172.17.30.23 with 32 bytes of data:

Reply from 172.17.30.23: bytes=32 time=17ms TTL=127
Reply from 172.17.30.23: bytes=32 time=15ms TTL=127
Reply from 172.17.30.23: bytes=32 time=18ms TTL=127
Reply from 172.17.30.23: bytes=32 time=19ms TTL=127

Ping statistics for 172.17.30.23:
   Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
```

- Tracert is a useful utility for confirming the routed path taken between two devices.

```
Approximate round trip times in milli-seconds:
   Minimum = 15ms, Maximum = 19ms, Average = 17ms

PC1> tracert 172.17.30.23

Tracing route to 172.17.30.23 over a maximum of 30 hops:

 1    9 ms      7 ms      9 ms      172.17.10.1
 2    16 ms     15 ms     16 ms     172.17.30.23

Trace complete.
```

# Summary

- VLAN Segmentation
  - The purpose of VLANs in a switched network.
  - How a switch forwards frames based on VLAN configuration in a multi-switch environment.
- VLAN Implementations
  - 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.
- Inter-VLAN Routing Using Routers
  - Two options for configuring Inter-VLAN routing.
  - Configure legacy Inter-VLAN Routing.
  - Configure Router-on-a-Stick Inter-VLAN Routing