Computer Networks
Day 1
Switching

Outline

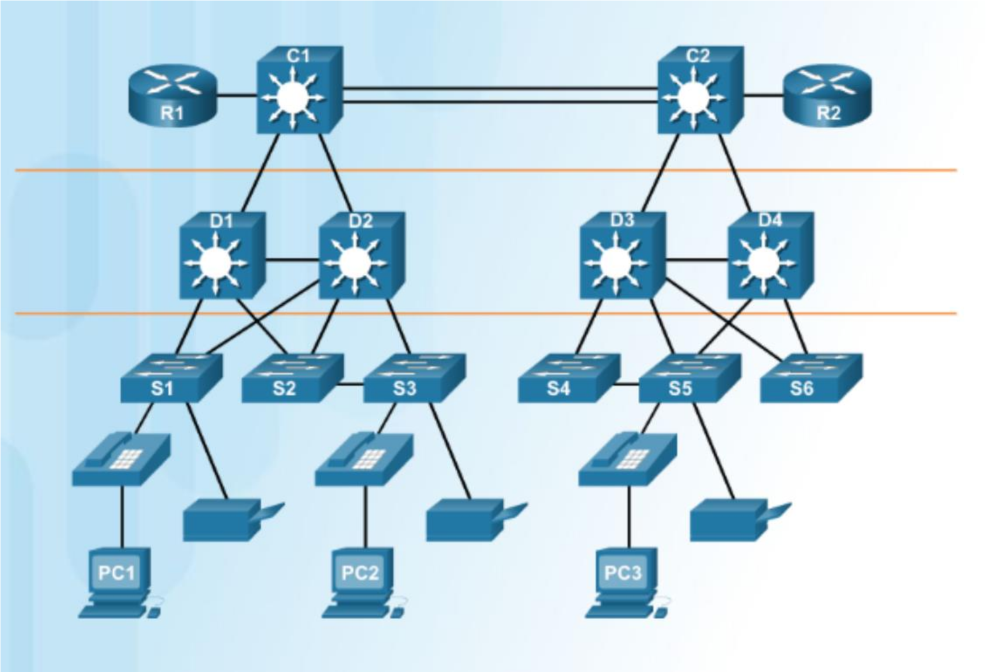
1. The Switched Environment.
2. Configure a Switch with Initial Settings.
3. VLAN
4. Summary.

1. The Switched Environment

Converged Networks

Access, Distribution, and Core Layers

- Access Layer – provides network access to the user.
- Distribution Layer – interfaces between the access layer and the core layer. Provides functions such as:
  - aggregating Layer 2 broadcast domains and Layer 3 routing boundaries.
  - providing intelligent switching, routing, and network access policy functions to access the rest of the network.
- Core Layer – is the network backbone. It provides fault isolation and high-speed backbone connectivity.



Switched Networks

Form Factors

Fixed Configuration

Stackable Configuration

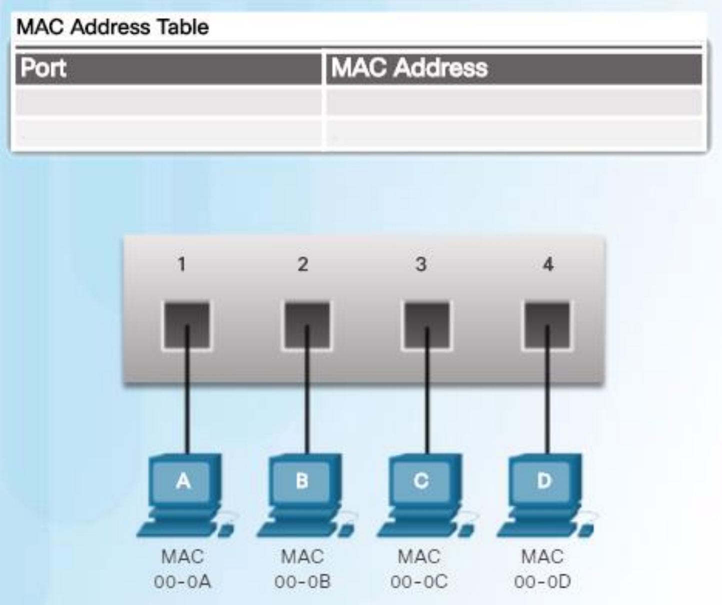
Modular Configuration

- Considerations when selecting switches:
  - Cost
  - Port Density
  - Power
  - Reliability
  - Port Speed
  - Frame buffers
  - Scalability

The MAC Address Table

Switch Fundamentals

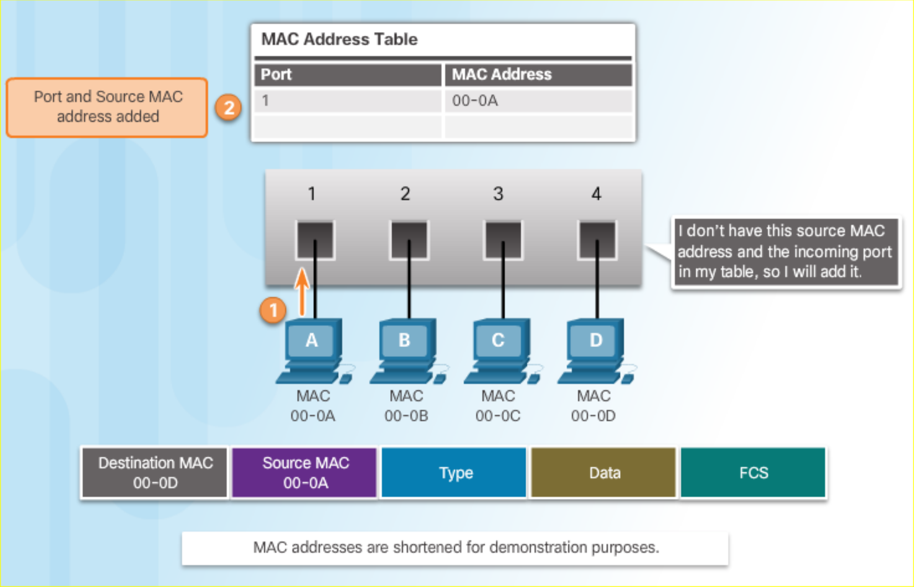
- The switch is a layer 2 device.
- A Layer 2 Ethernet switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.
- A switch that is powered on, will have an empty MAC address table as it has not yet learned the MAC addresses for the four attached PCs.
- Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.



The MAC Address Table

Learning MAC Addresses

- The switch dynamically builds the MAC address table. The process to learn the Source MAC Address is:
  - Switches examine all incoming frames for new source MAC address information to learn.
  - If the source MAC address is unknown, it is added to the table along with the port number.
  - If the source MAC address does exist, the switch updates the refresh timer for that entry.
  - By default, most Ethernet switches keep an entry in the table for 5 minutes.



MAC Address Table

Port	MAC Address
1	00-0A

Port and Source MAC address added

I don't have this source MAC address and the incoming port in my table, so I will add it.

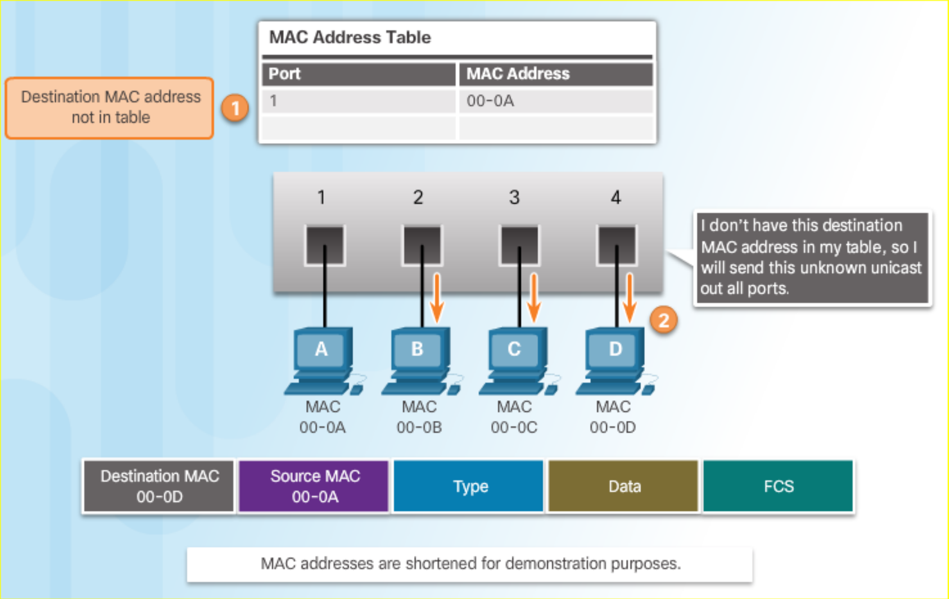
Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS

MAC addresses are shortened for demonstration purposes.

The MAC Address Table

Learning MAC Addresses (Cont.)

- The process to forward the Destination MAC Address is:
  - If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
  - If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
  - If the destination MAC address is in the table, it will forward the frame out the specified port.
  - If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.



MAC Address Table

Port	MAC Address
1	00-0A

1 Destination MAC address not in table

2 I don't have this destination MAC address in my table, so I will send this unknown unicast out all ports.

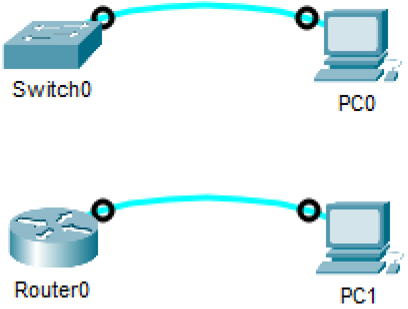
MAC addresses are shortened for demonstration purposes.

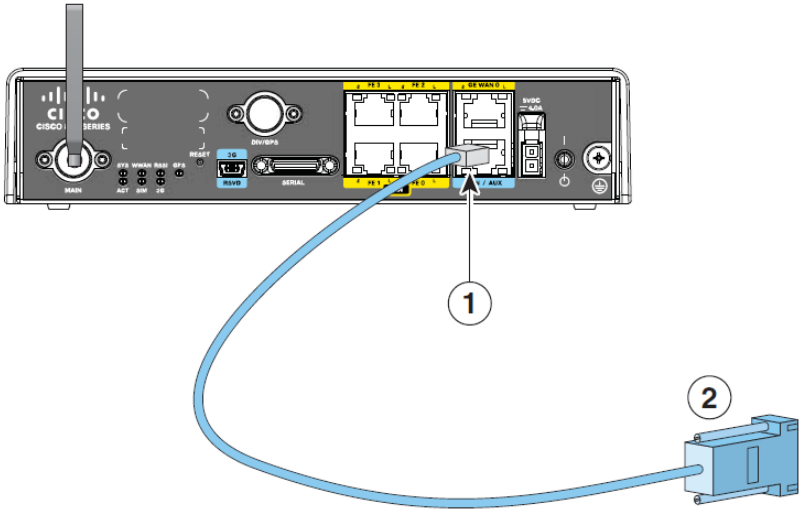
2. Configure a Switch with Initial Settings

Configure a Switch with Initial Settings

Preparing for Basic Switch Management

- Every Cisco Router/Switch has a Console port.
- Console port is used to configure new devices.

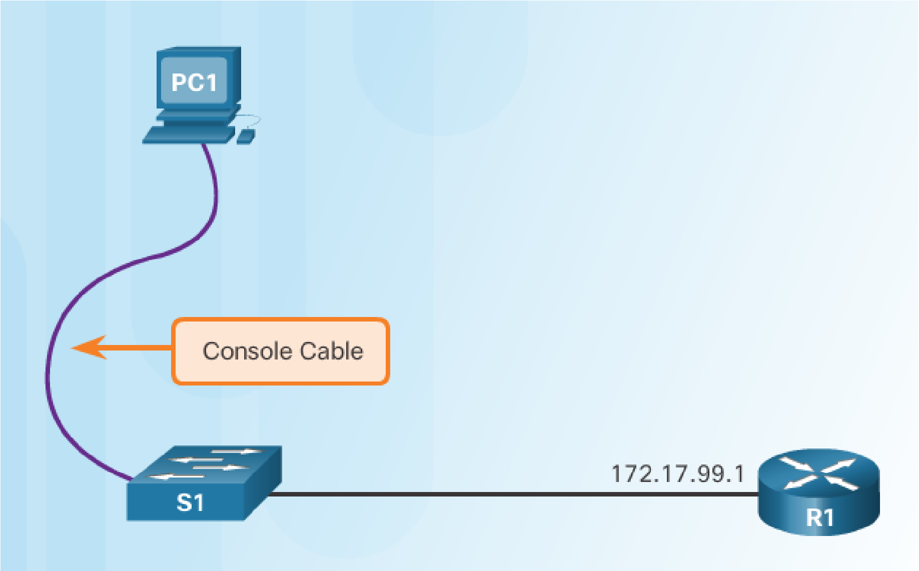




Configure a Switch with Initial Settings

Preparing for Basic Switch Management

- To configure a switch for remote access, the switch must be configured with an IP address, subnet mask, and default gateway.
- One particular switch virtual interface (SVI) is used to manage the switch:
  - A switch IP address is assigned to an SVI.
  - By default the management SVI is controlled and configured through VLAN 1.
  - The management SVI is commonly called the management VLAN.

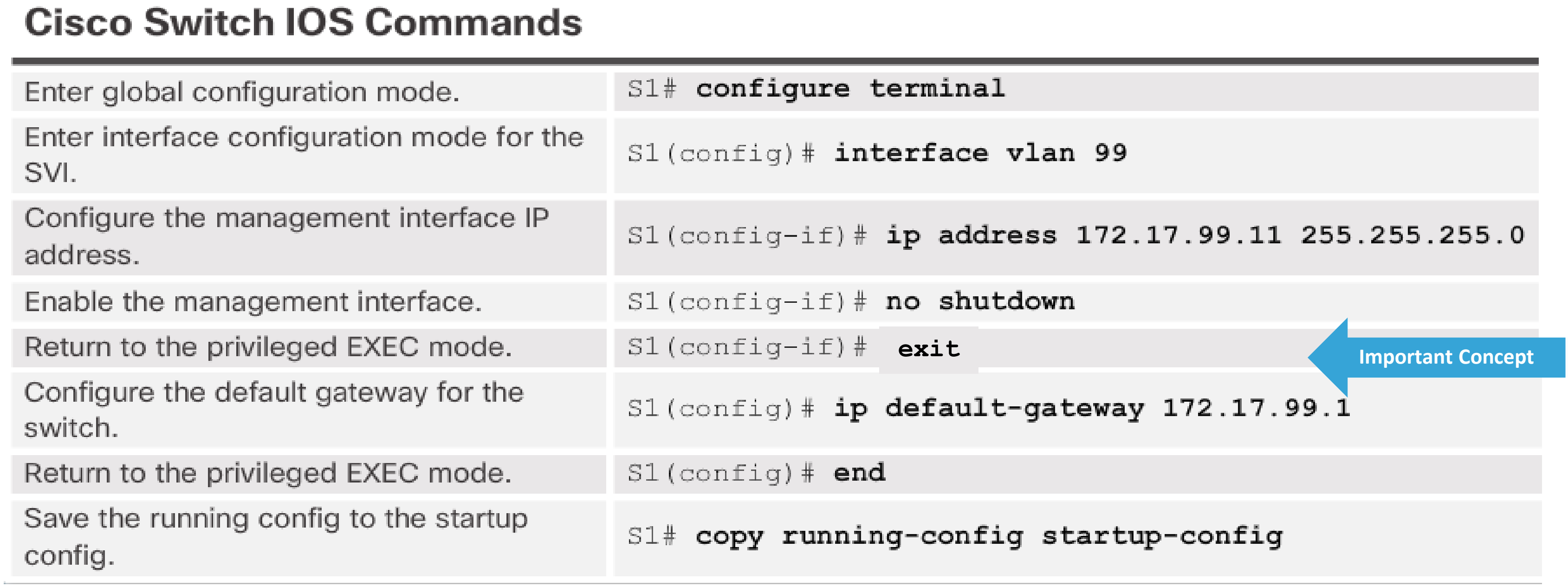


Remember that the switch console port is on the back of the switch.

For security reasons, it is best practice to use a VLAN other than VLAN 1 for the management VLAN.

Configure a Switch with Initial Settings

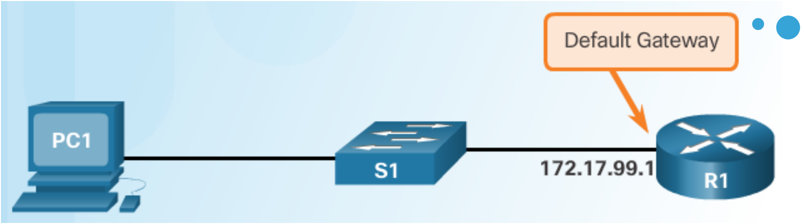
Configuring Basic Switch Management Access with IPv4



Cisco Switch IOS Commands

Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode for the SVI.	`S1(config)# interface vlan 99`
Configure the management interface IP address.	`S1(config-if)# ip address 172.17.99.11 255.255.255.0`
Enable the management interface.	`S1(config-if)# no shutdown`
Return to the privileged EXEC mode.	`S1(config-if)# exit`
Configure the default gateway for the switch.	`S1(config)# ip default-gateway 172.17.99.1`
Return to the privileged EXEC mode.	`S1(config)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Important Concept

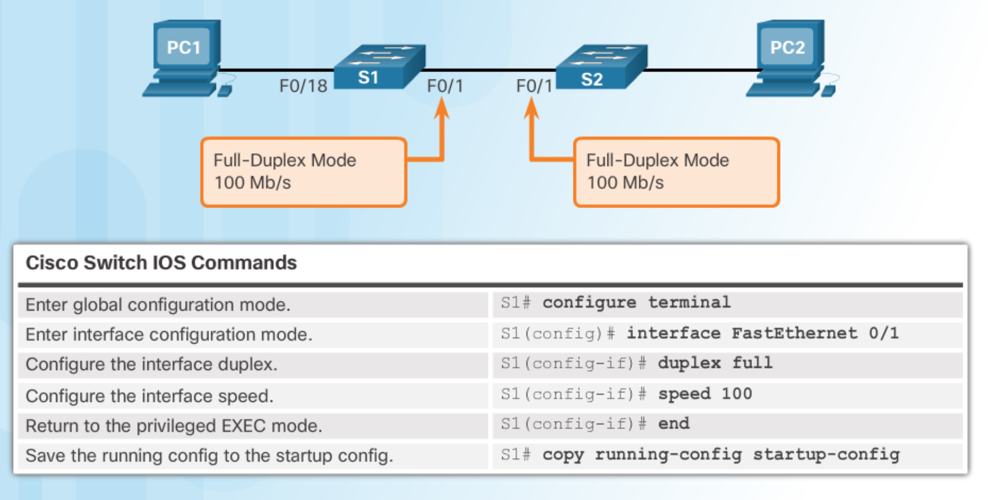


The default gateway is the router address and is used by the switch to communicate with other networks.

Configure Switch Ports

Configure Switch Ports at the Physical Layer

- Some switches have the default setting of auto for both duplex and speed.
- Mismatched duplex and/or speed settings can cause connectivity issues.
- Always check duplex and speed settings using the **show interface** *interface_id* command.
- All fiber ports operate at one speed and are always full-duplex.



Full-Duplex Mode
100 Mb/s

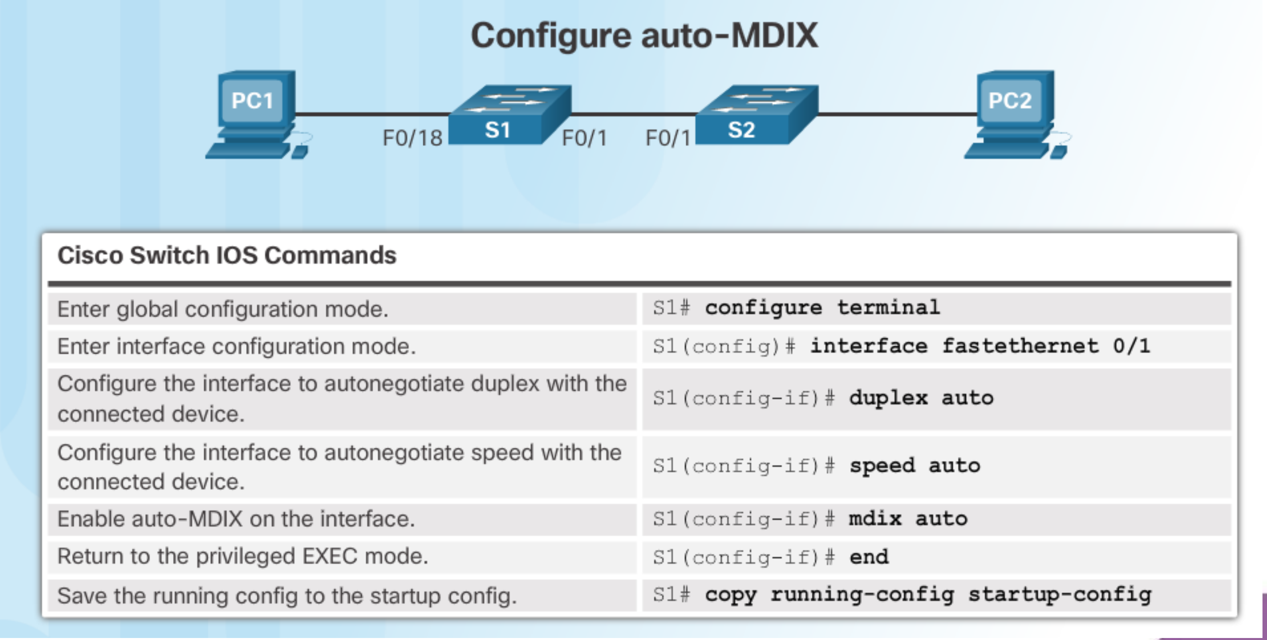
Full-Duplex Mode
100 Mb/s

Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface FastEthernet 0/1`
Configure the interface duplex.	`S1(config-if)# duplex full`
Configure the interface speed.	`S1(config-if)# speed 100`
Return to the privileged EXEC mode.	`S1(config-if)# end`
Save the running config to the startup config.	`S1# copy running-config startup-config`

Configure Switch Ports

Auto-MDIX

- Some switches have the automatic medium-dependent interface crossover (auto-MDIX) feature that allows an interface to detect the required cable connection type (straight-through or crossover) and configure the connection appropriately.



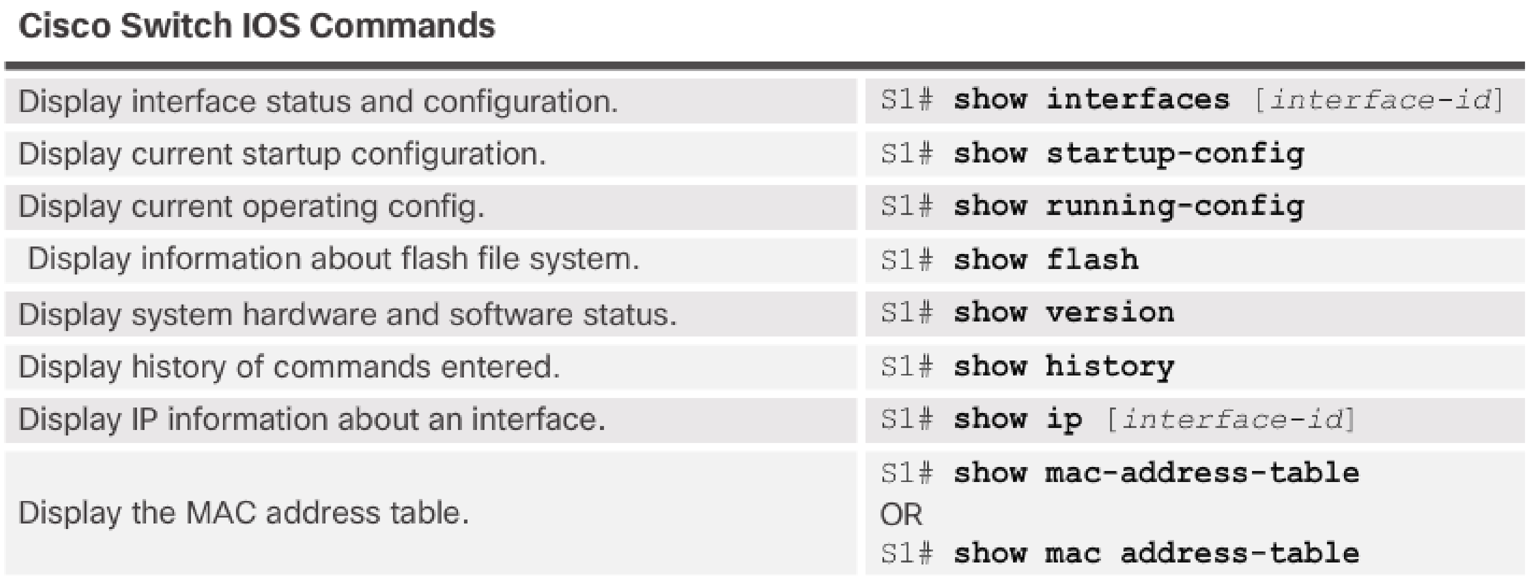
Configure auto-MDIX

Cisco Switch IOS Commands

Enter global configuration mode.	S1# **configure terminal**
Enter interface configuration mode.	S1(config)# **interface fastethernet 0/1**
Configure the interface to autonegotiate duplex with the connected device.	S1(config-if)# **duplex auto**
Configure the interface to autonegotiate speed with the connected device.	S1(config-if)# **speed auto**
Enable auto-MDIX on the interface.	S1(config-if)# **mdix auto**
Return to the privileged EXEC mode.	S1(config-if)# **end**
Save the running config to the startup config.	S1# **copy running-config startup-config**

Configure Switch Ports

Verifying Switch Port Configuration

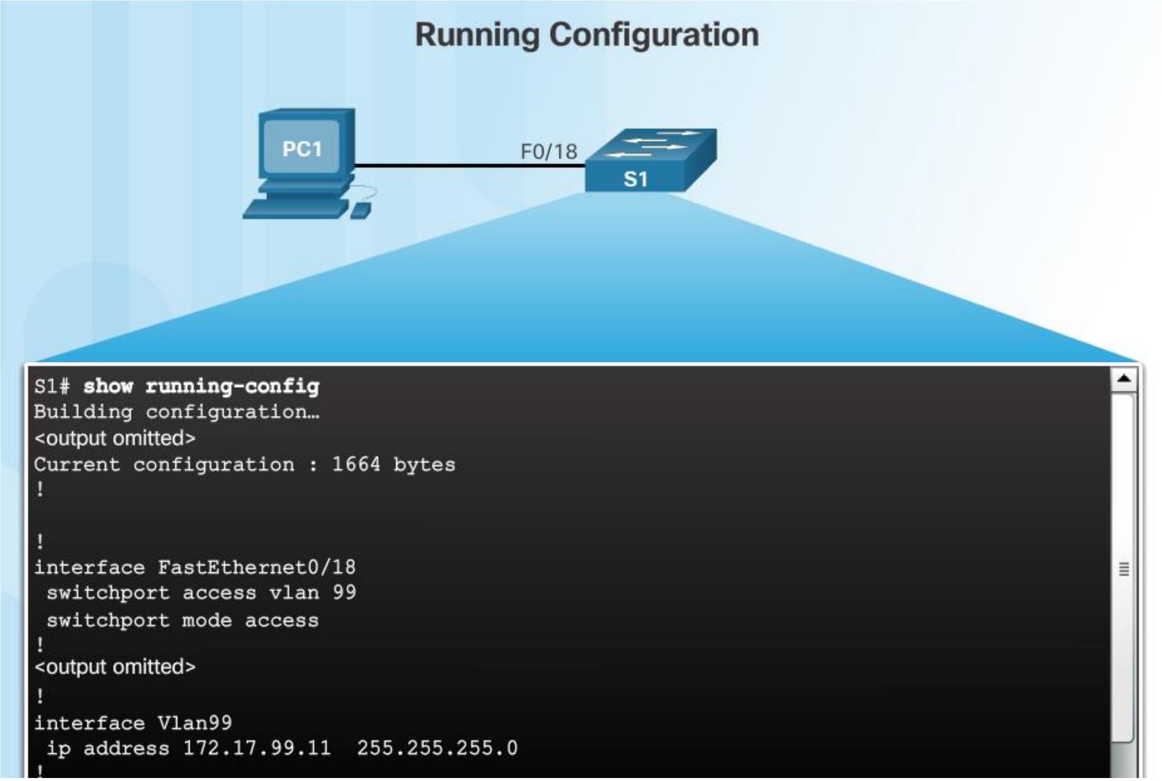


Cisco Switch IOS Commands

Display interface status and configuration.	S1# **show interfaces** [*interface-id*]
Display current startup configuration.	S1# **show startup-config**
Display current operating config.	S1# **show running-config**
Display information about flash file system.	S1# **show flash**
Display system hardware and software status.	S1# **show version**
Display history of commands entered.	S1# **show history**
Display IP information about an interface.	S1# **show ip** [*interface-id*]
Display the MAC address table.	S1# **show mac-address-table** OR S1# **show mac address-table**

Configure Switch Ports

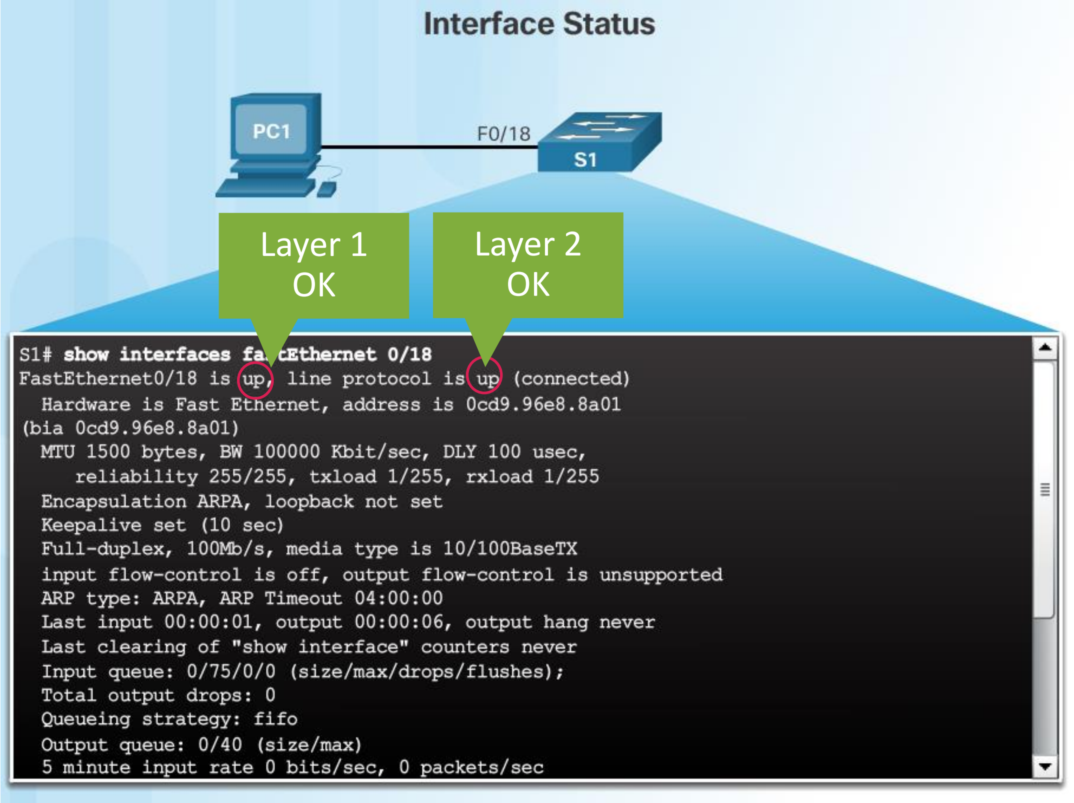
Verifying Switch Port Configuration (Cont.)


Running Configuration

```
S1# show running-config
Building configuration…
<output omitted>
Current configuration : 1664 bytes
!

!
interface FastEthernet0/18
 switchport access vlan 99
 switchport mode access
!
<output omitted>
!
interface Vlan99
 ip address 172.17.99.11  255.255.255.0
!
```

Configure Switch Ports

Verifying Switch Port Configuration (Cont.)



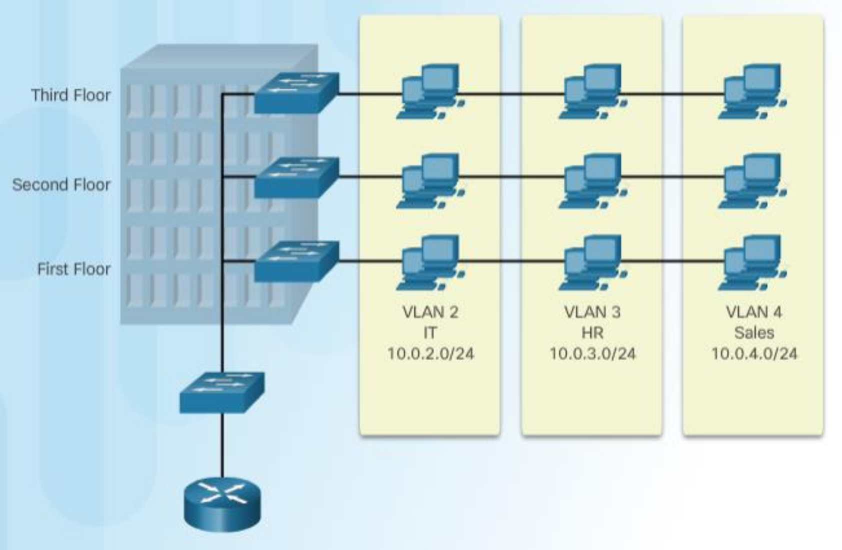
```
S1# show interfaces fastEthernet 0/18
FastEthernet0/18 is up, line protocol is up (connected)
  Hardware is Fast Ethernet, address is 0cd9.96e8.8a01
(bia 0cd9.96e8.8a01)
  MTU 1500 bytes, BW 100000 Kbit/sec, DLY 100 usec,
     reliability 255/255, txload 1/255, rxload 1/255
  Encapsulation ARPA, loopback not set
  Keepalive set (10 sec)
  Full-duplex, 100Mb/s, media type is 10/100BaseTX
  input flow-control is off, output flow-control is unsupported
  ARP type: ARPA, ARP Timeout 04:00:00
  Last input 00:00:01, output 00:00:06, 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
```

3. VLANs

Overview of VLANs

VLAN Definitions

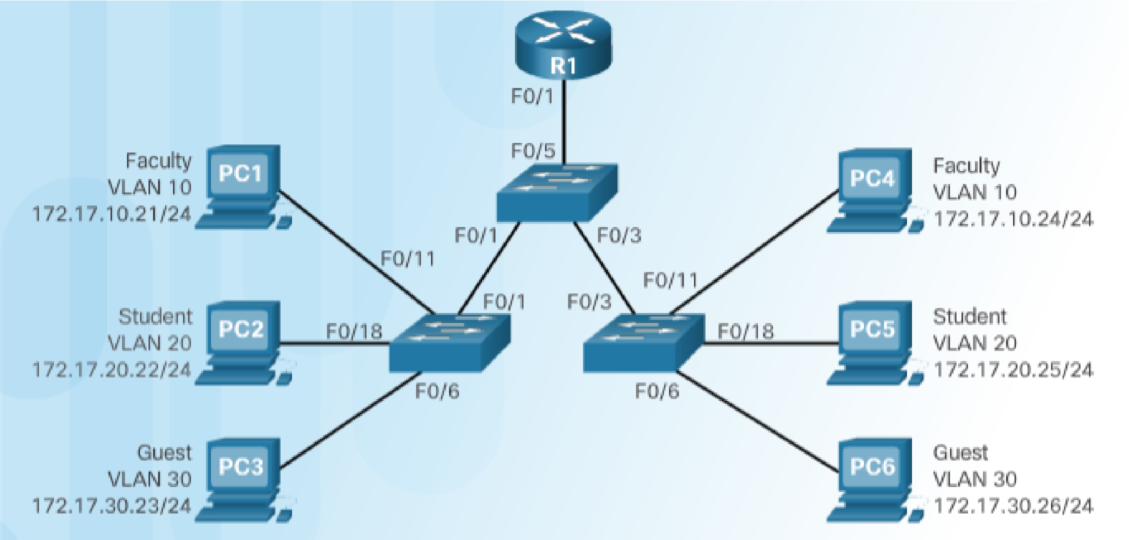
- VLANs can segment LAN devices without regard for the physical location of the user or device.
  - In the figure, IT users on the first, second, and third floors are all on the same LAN segment. The same is true for HR and Sales users.
- A VLAN is a logical partition of a Layer 2 network.
  - Multiple 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.

Overview of VLANs

Benefits of VLANs



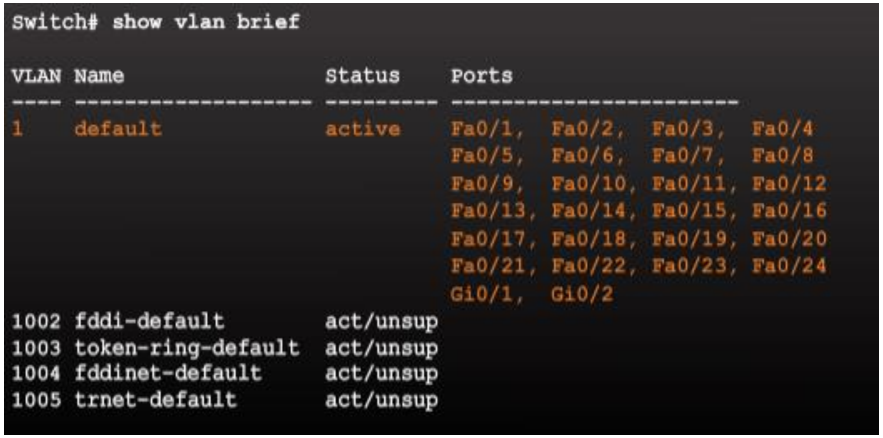
- Improved Security
- Reduced Cost
- Better Performance
- Smaller Broadcast Domains
- IT Efficiency
- Management Efficiency
- Simpler Project and Application Management

Overview of VLANs

Types of VLANs

- Common 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
```

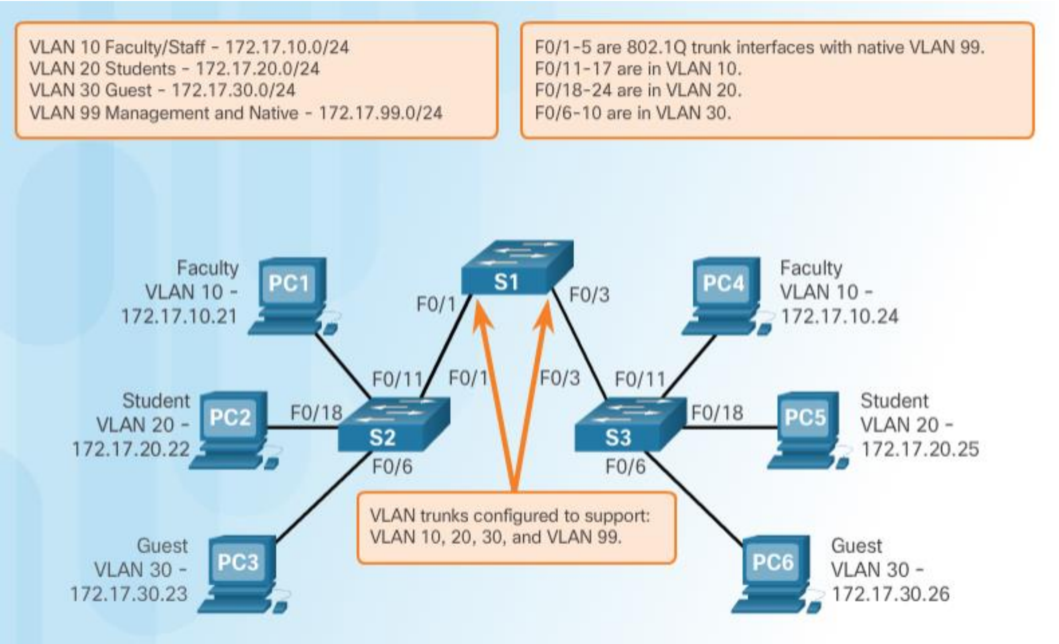
Initially, all switch ports are members of VLAN 1.

VLANs in a Multi-Switched Environment

VLAN Trunks

- 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.



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.

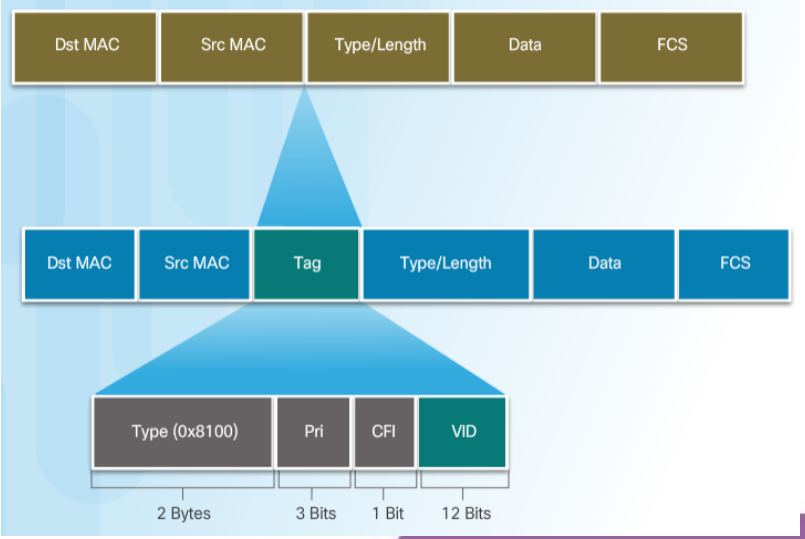
The links between switches S1 and S2, and S1 and S3 are configured to transmit traffic coming from VLANs 10, 20, 30, and 99 across the network.

VLANs in a Multi-Switched Environment

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.

- IEEE 802.1Q is a vey popular VLAN trunking protocol that defines the structure of the tagging header added to the frame.



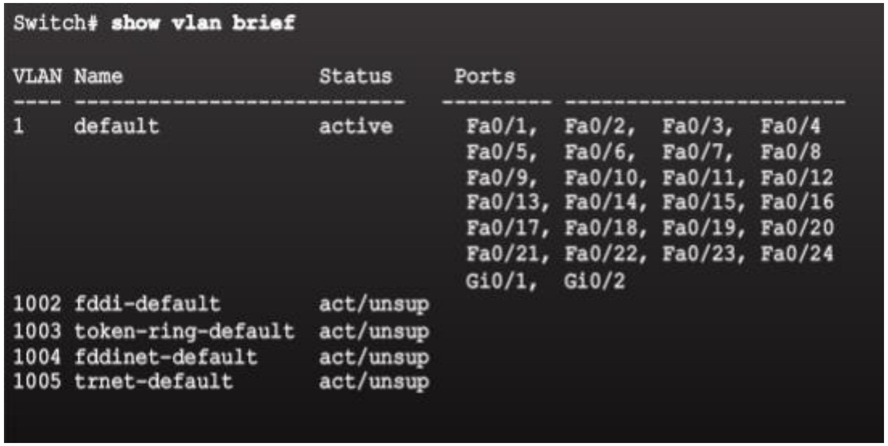
- Switches add VLAN tagging information after the Source MAC address field.
- The fields in the 802.1Q VLAN tag includes VLAN ID (VID).
- Trunk links add the tag information before sending the frame and then remove the tags before forwarding frames through non-trunk ports.

VLAN Assignment

VLAN Ranges on Catalyst Switches

- 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

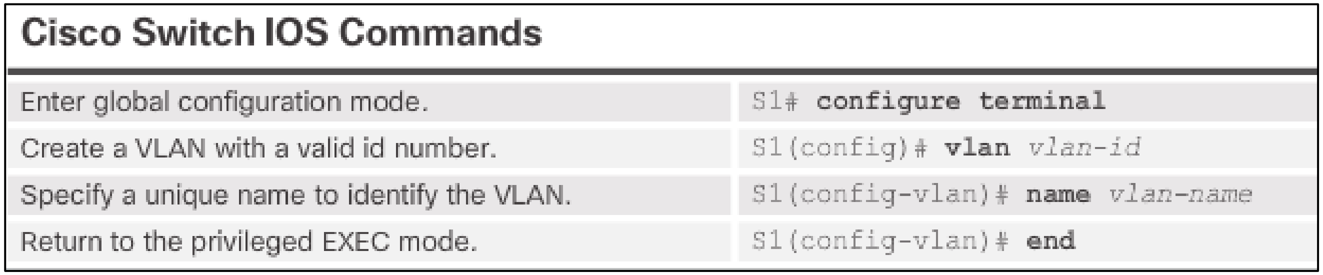
- Cisco Catalyst 2960 and 3560 Series switches support over 4,000 VLANs.



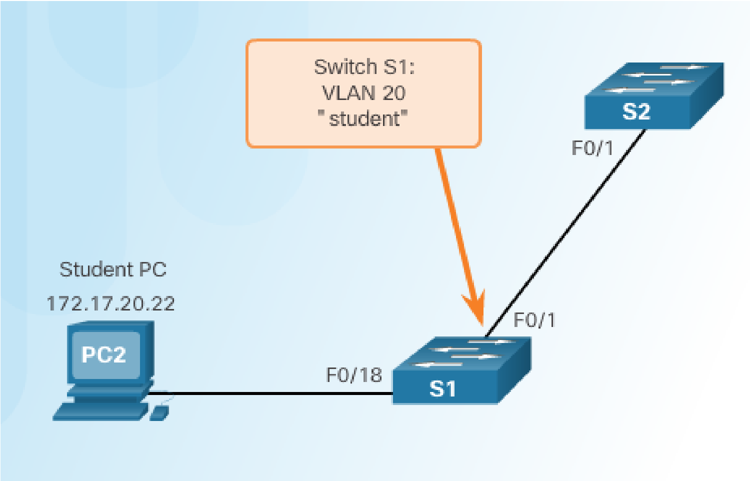
```
Switch# show vlan brief

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
```

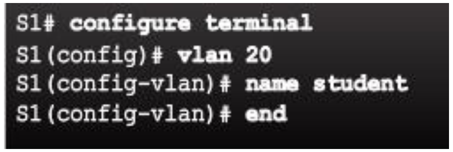
VLAN Assignment

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`

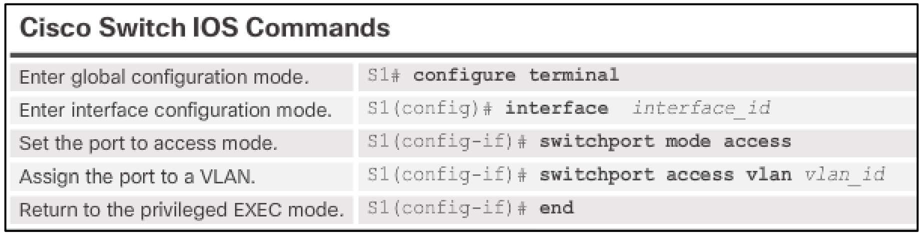




```
S1# configure terminal
S1(config)# vlan 20
S1(config-vlan)# name student
S1(config-vlan)# end
```

VLAN Assignment

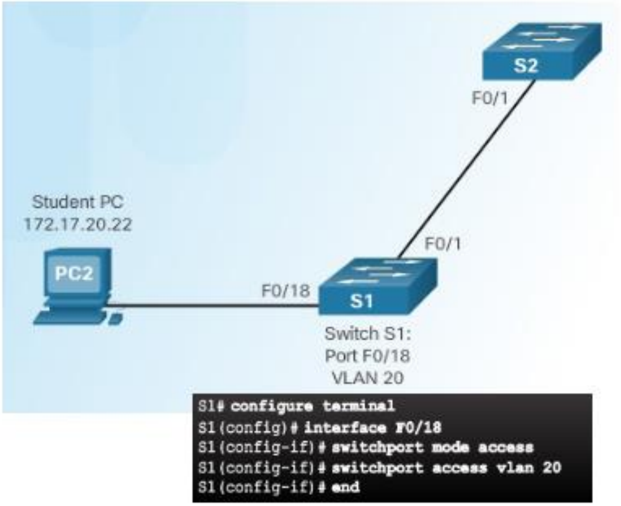
Assigning Ports to VLANs



Cisco Switch IOS Commands

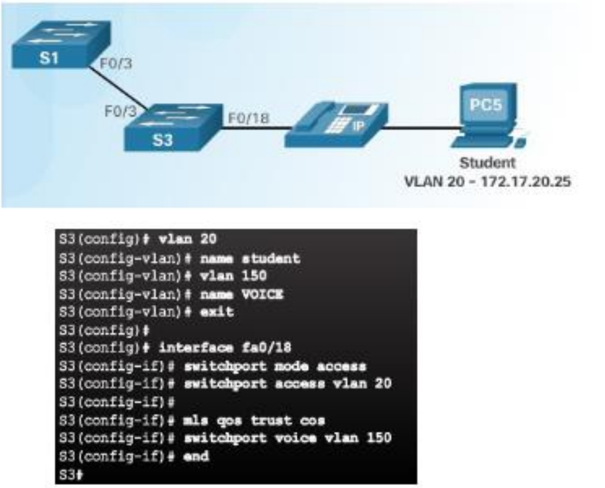
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set the port to access mode.	`S1(config-if)# switchport mode access`
Assign the port to a VLAN.	`S1(config-if)# switchport access vlan vlan_id`
Return to the privileged EXEC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

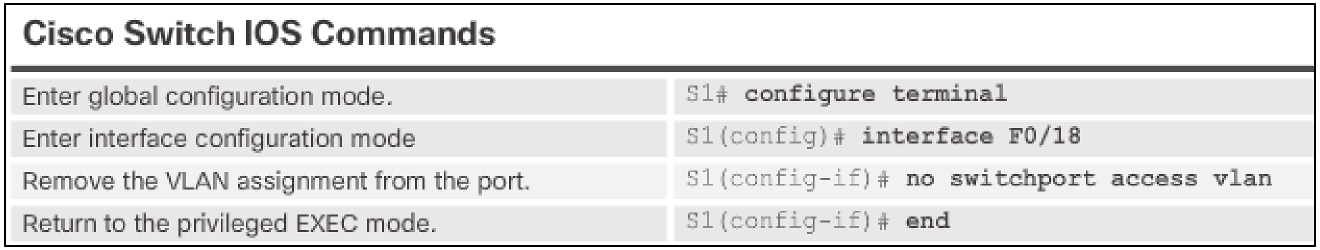


```
S3(config)# vlan 20
S3(config-vlan)# name student
S3(config-vlan)# vlan 150
S3(config-vlan)# name VOICE
S3(config-vlan)# exit
S3(config)#
S3(config)# interface fa0/18
S3(config-if)# switchport mode access
S3(config-if)# switchport access vlan 20
S3(config-if)#
S3(config-if)# mls qos trust cos
S3(config-if)#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

VLAN Assignment

Changing VLAN Port Membership

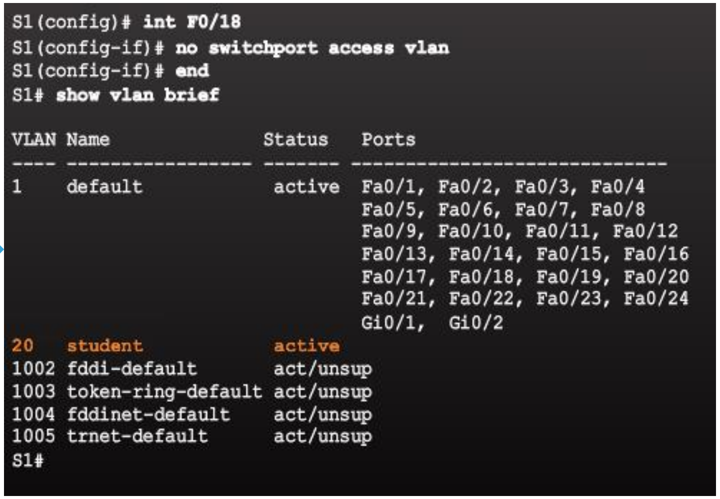
- Remove VLAN Assignment



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`

Even though interface F0/18 was previously assigned to VLAN 20, it reset to the default VLAN1.

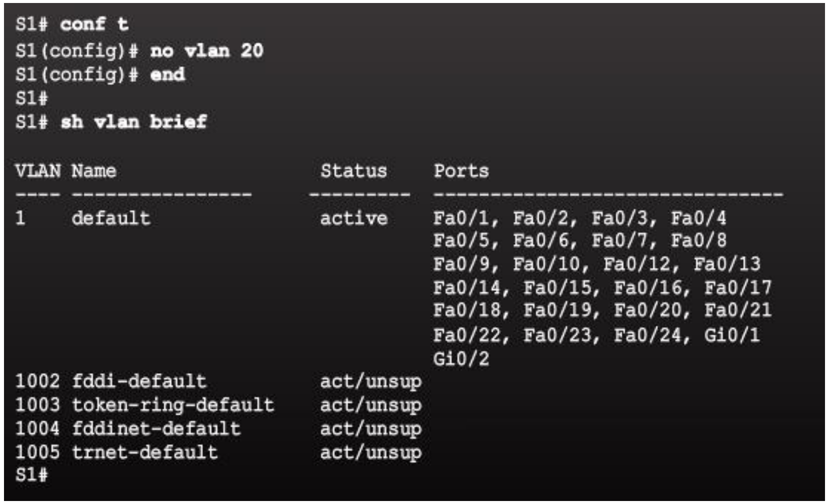


```
S1(config)# int F0/18
S1(config-if)# no switchport access vlan
S1(config-if)# end
S1# show vlan brief

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#
```

VLAN Assignment

Deleting VLANs

- Use the **no vlan** *vlan-id* global configuration mode command to remove VLAN.

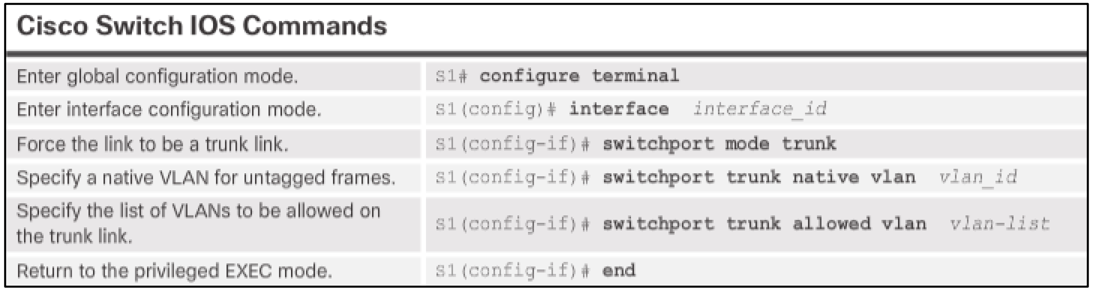


```
S1# conf t
S1(config)# no vlan 20
S1(config)# end
S1#
S1# sh vlan brief

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#
```

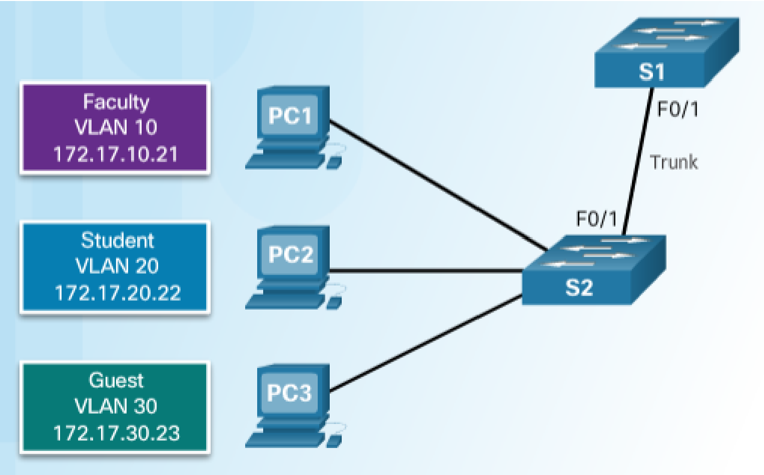
- To delete the entire vlan.dat file, use the **delete flash:vlan.dat** privileged EXEC mode command.
  - **delete vlan.dat** can be used if the vlan.dat file has not been moved from its default location.

VLAN Trunks

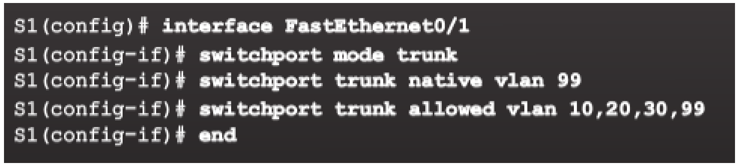
Configuring IEEE 802.1q Trunk Links



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`



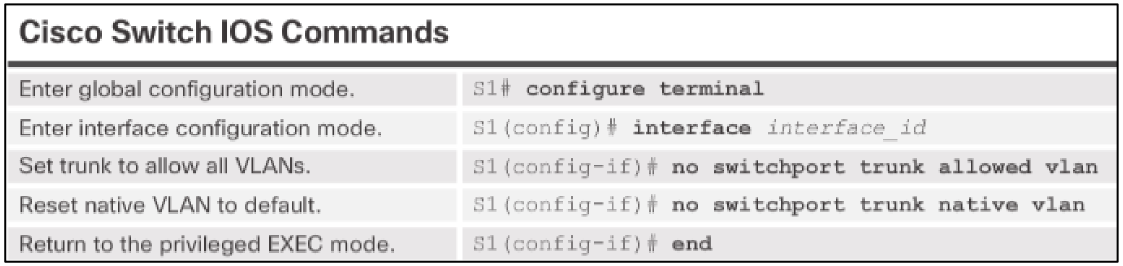
Native VLAN
VLAN 99
172.17.99.0/24



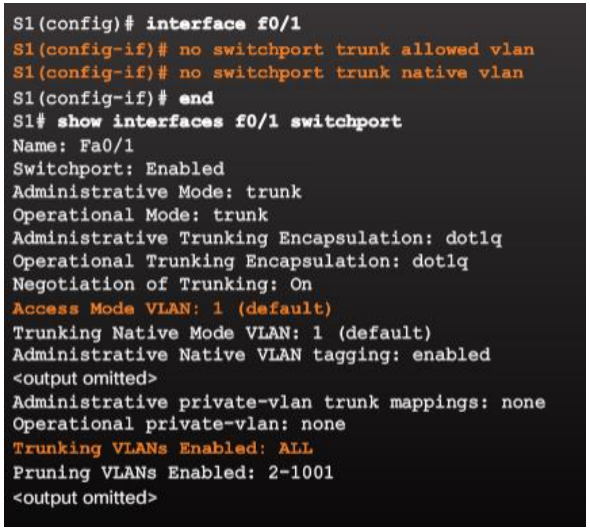
```
S1(config)# interface FastEthernet0/1
S1(config-if)# switchport mode trunk
S1(config-if)# switchport trunk native vlan 99
S1(config-if)# switchport trunk allowed vlan 10,20,30,99
S1(config-if)# end
```

VLAN Trunks

Resetting the Trunk to Default State

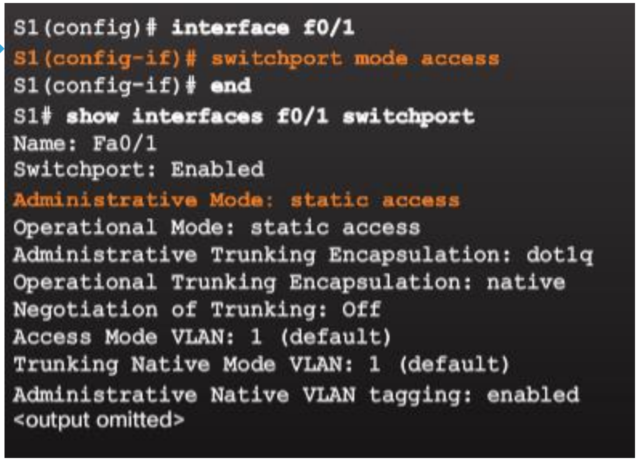


Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Set trunk to allow all VLANs.	`S1(config-if)# no switchport trunk allowed vlan`
Reset native VLAN to default.	`S1(config-if)# no switchport trunk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



```
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: none
Operational private-vlan: none
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
<output omitted>
```

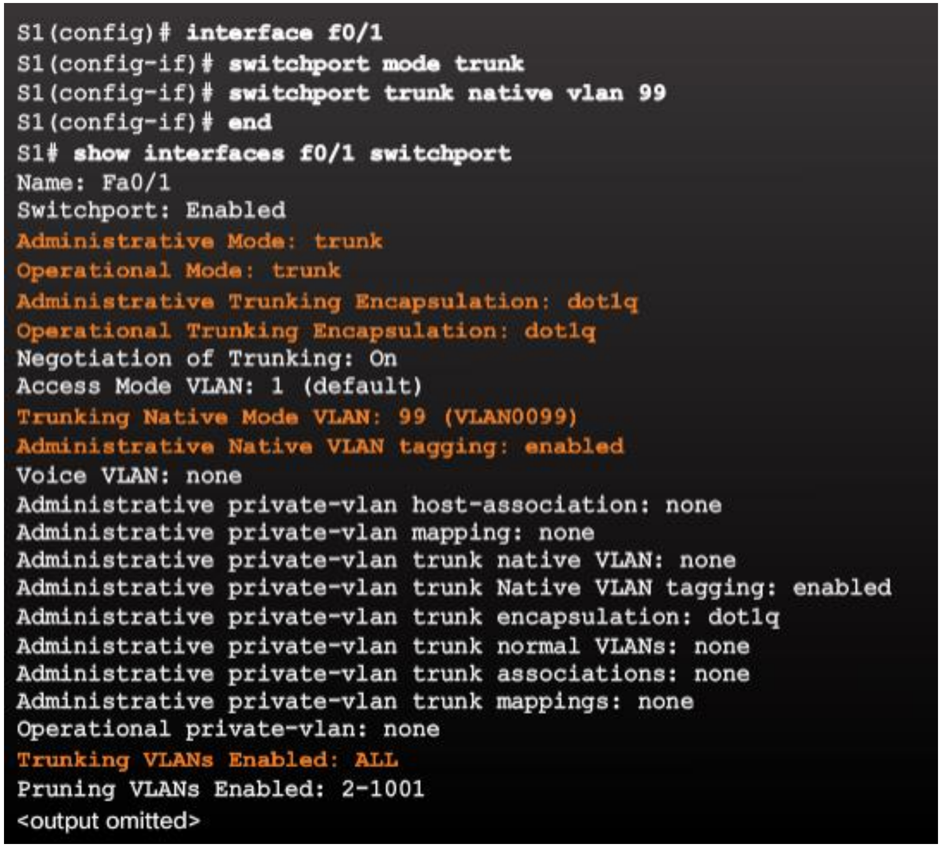
F0/1 is configured as an access port which removes the trunk feature.



```
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>
```

VLAN Trunks

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>
```

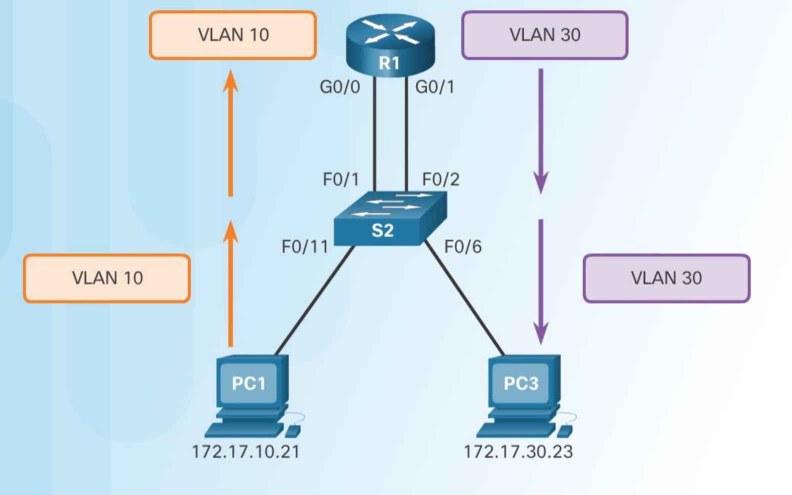
Inter-VLAN Routing Operation

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.

- 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.

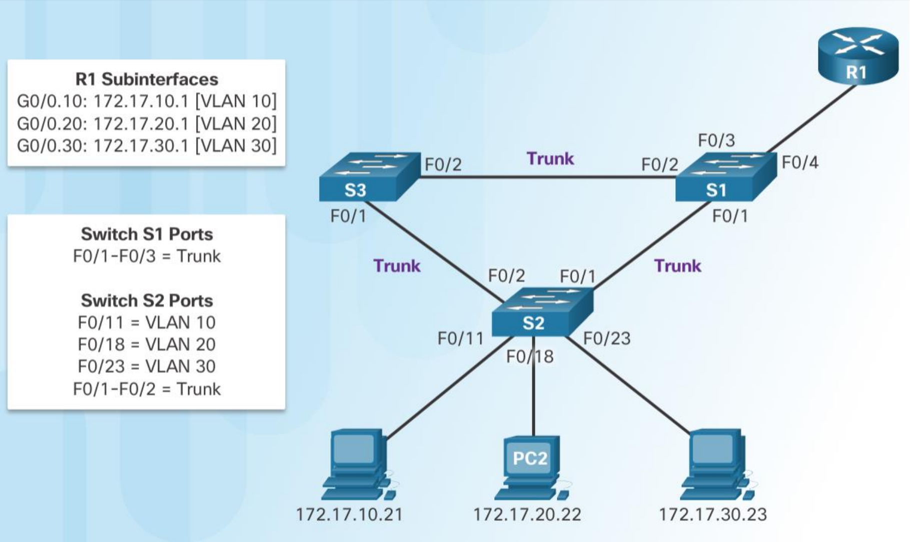
Inter-VLAN Routing Operation

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.

In this example, the R1 interface is configured as a trunk link and connects to the trunk F0/4 port on S1.

- Router accepts VLAN-tagged traffic on the trunk interface
- Router internally routes between the VLANs using subinterfaces.
- Router then forwards the routed traffic as VLAN-tagged for the destination VLAN out the trunk link.



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]

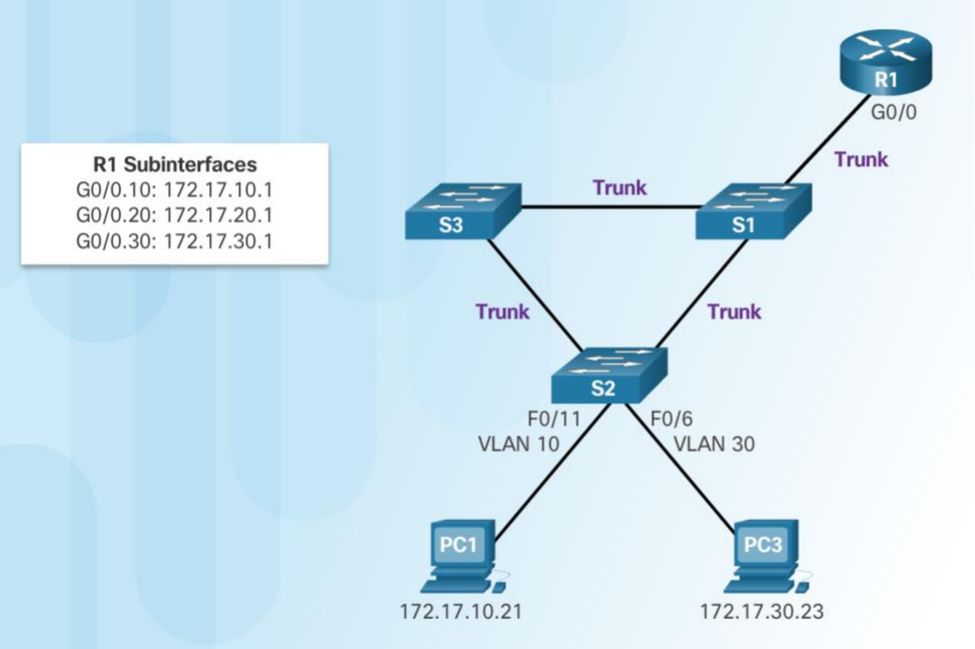
Switch S1 Ports
F0/1-F0/3 = Trunk

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

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

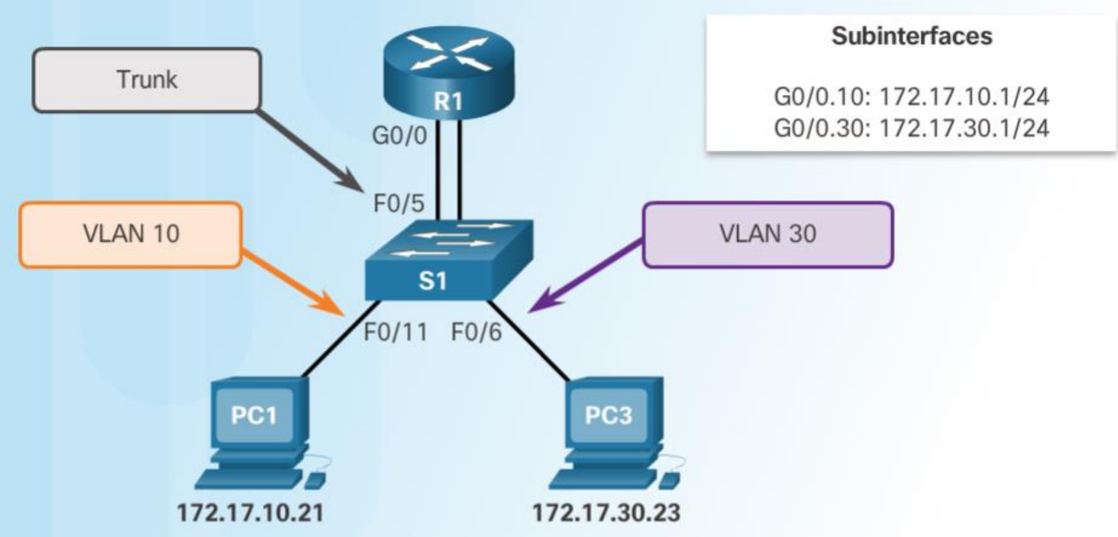
Configure Router-on-a Stick: Preparation

- 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.

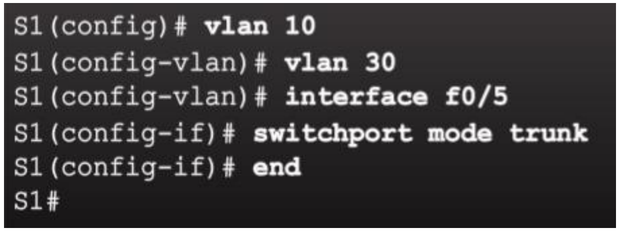

R1 Subinterfaces
G0/0.10: 172.17.10.1
G0/0.20: 172.17.20.1
G0/0.30: 172.17.30.1

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

Configure Router-on-a Stick: Switch Configuration



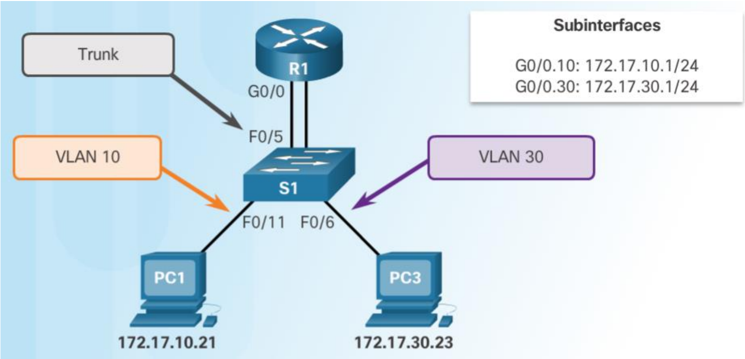
- To enable inter-VLAN routing using router-on-a stick, start by enabling trunking on the switch port that is connected to the router.



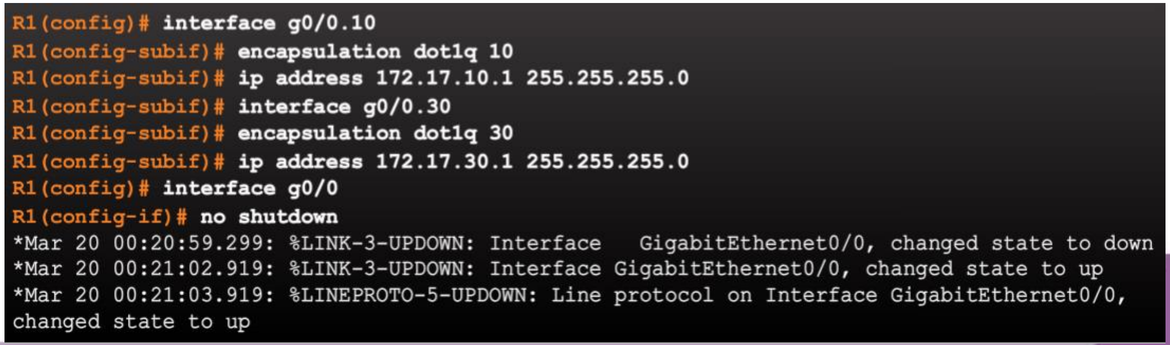
```
S1(config)# vlan 10
S1(config-vlan)# vlan 30
S1(config-vlan)# interface f0/5
S1(config-if)# switchport mode trunk
S1(config-if)# end
S1#
```

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

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.

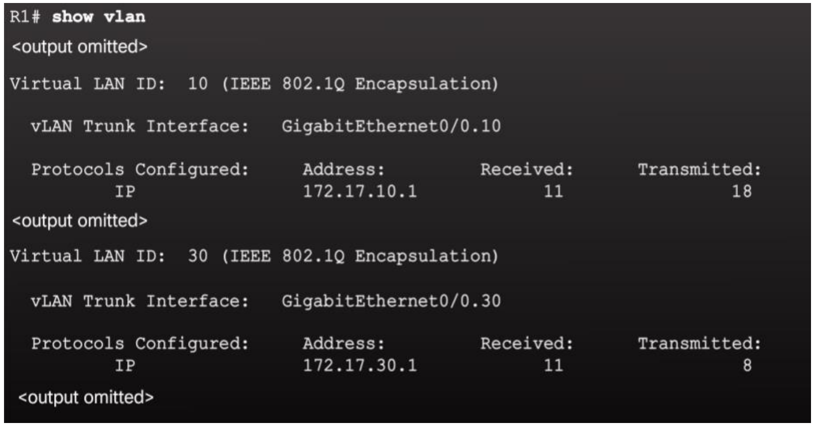


```
R1(config)# interface g0/0.10
R1(config-subif)# encapsulation dot1q 10
R1(config-subif)# ip address 172.17.10.1 255.255.255.0
R1(config-subif)# interface g0/0.30
R1(config-subif)# encapsulation dot1q 30
R1(config-subif)# ip address 172.17.30.1 255.255.255.0
R1(config)# interface g0/0
R1(config-if)# 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 Inter-VLAN Routing

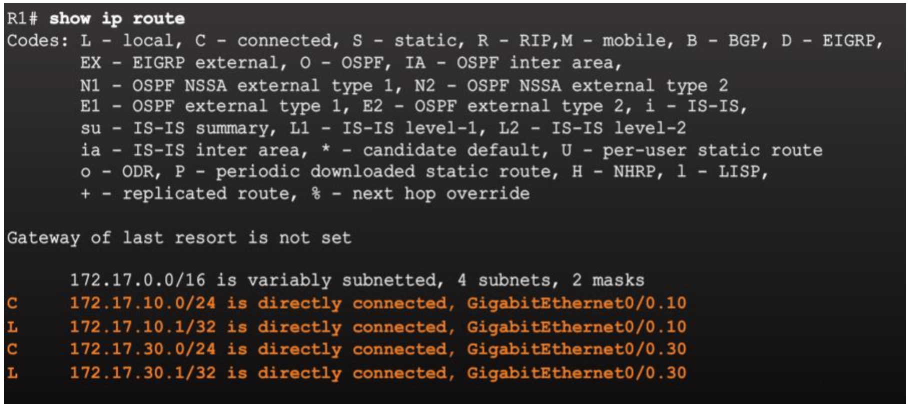
Configure Router-on-a Stick: Verifying Subinterfaces

- 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.



```
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>
```

The **show vlan** command displays information about the Cisco IOS VLAN subinterfaces.



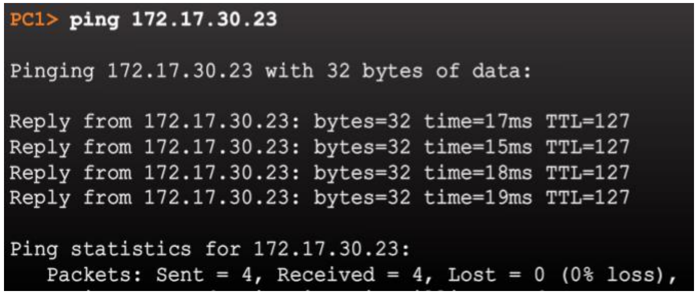
```
R1# show ip route
Codes: L - local, C - connected, S - static, R - RIP,M - mobile, B - BGP, D - EIGRP,
       EX - EIGRP external, O - OSPF, IA - OSPF inter area,
       N1 - OSPF NSSA external type 1, N2 - OSPF NSSA external type 2
       E1 - OSPF external type 1, E2 - OSPF external type 2, i - 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
```

The **show ip route** command displays the routing table containing the networks associated with outgoing subinterfaces.

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

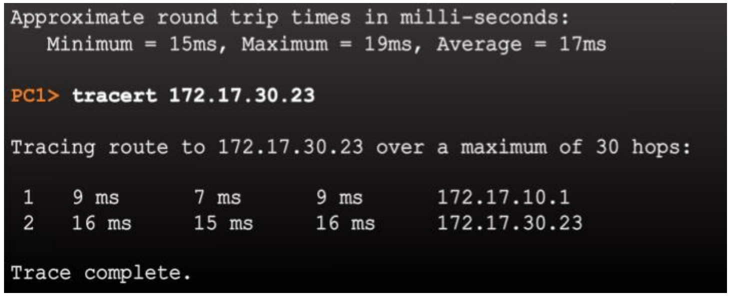
Configure Router-on-a Stick: Verifying Routing

- 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.

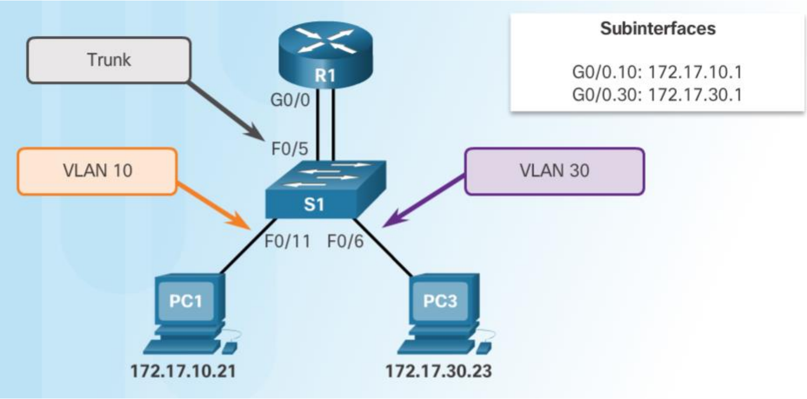


```
PC1> ping 172.17.30.23

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.
```



4. Summary

5. Summary

Summary

- How frames are forwarded in a switched network.
- Configure basic switch settings to meet network requirements.
- Explain how VLANs segment broadcast domains in a small to medium-sized business network.
- Implement VLANs to segment a small to medium-sized business network..
- Configure routing between VLANs in a small to medium-sized business network.

Q&A