Chapter 3: VLANs

Switched Networks

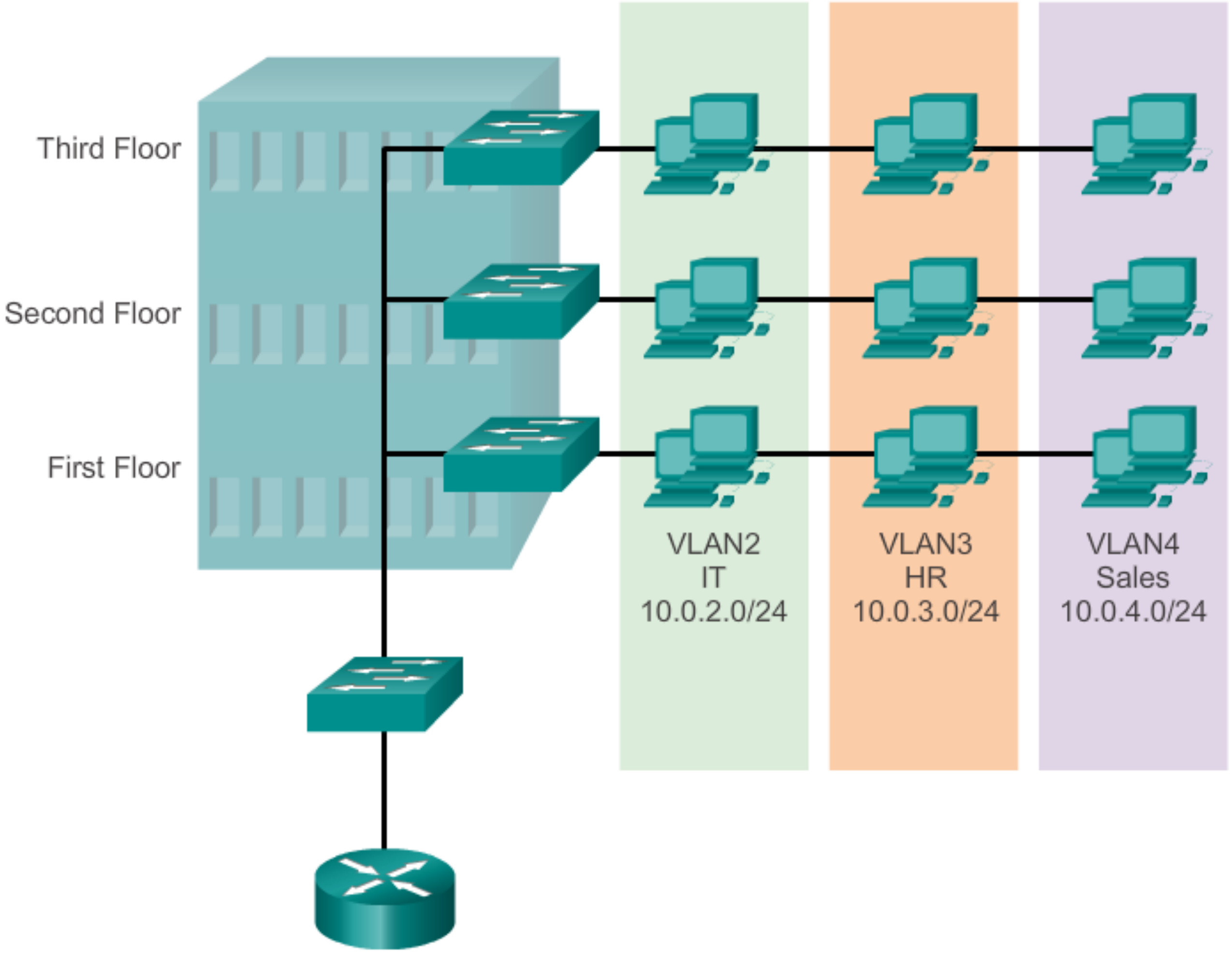
Cisco | Networking Academy®
Mind Wide Open™

3.1 VLAN Segmentation

Cisco | Networking Academy®
Mind Wide Open™

Overview of VLANs

VLAN Definitions (cont.)



Overview of VLANs

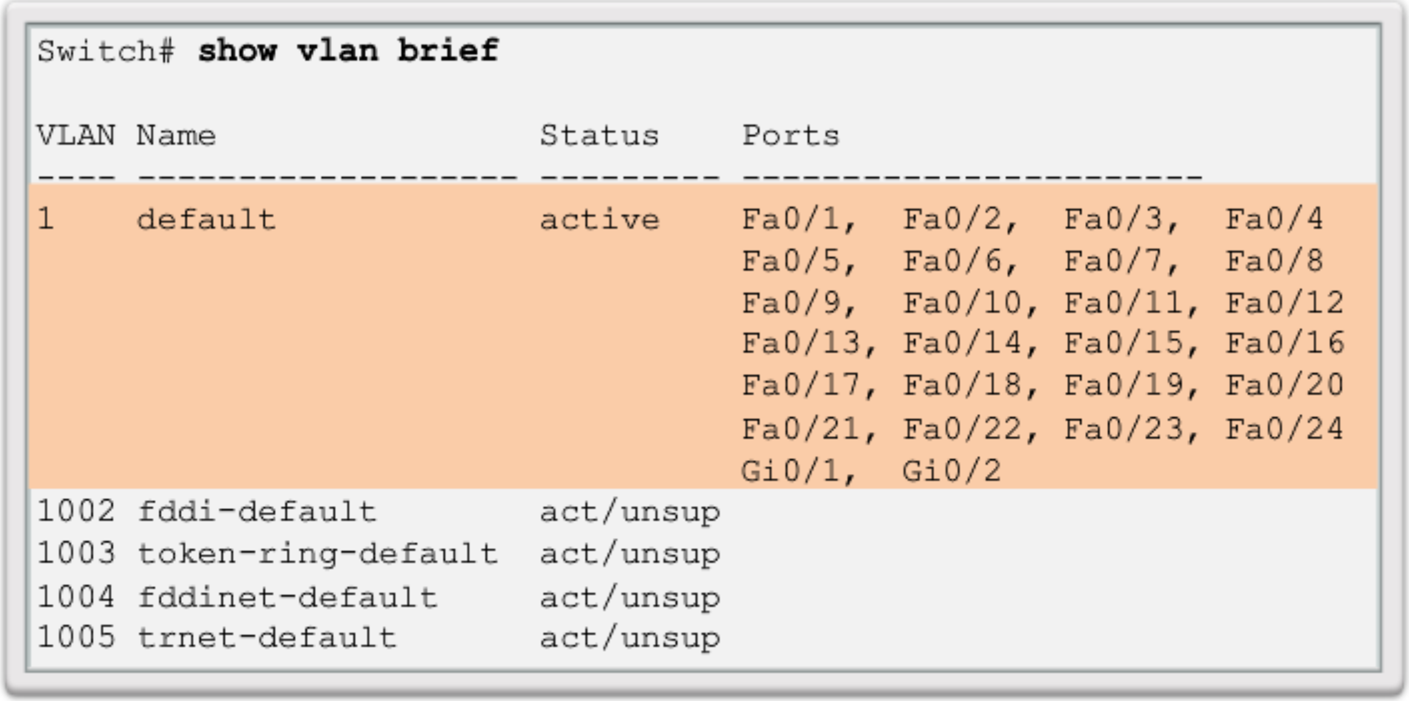
Benefits of VLANs

- Security
- Cost reduction
- Better performance
- Shrink broadcast domains
- Improved IT staff efficiency
- Simpler project and application management

Overview of VLANs

Types of VLANs (cont.)

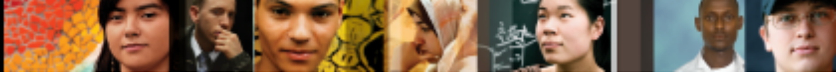
VLAN 1



```
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 to forward data by default.
- Native VLAN is VLAN 1 by default.
- Management VLAN is VLAN 1 by default.
- VLAN 1 cannot be renamed or deleted.



VLANs in a Multi-Switched Environment

VLAN Trunks

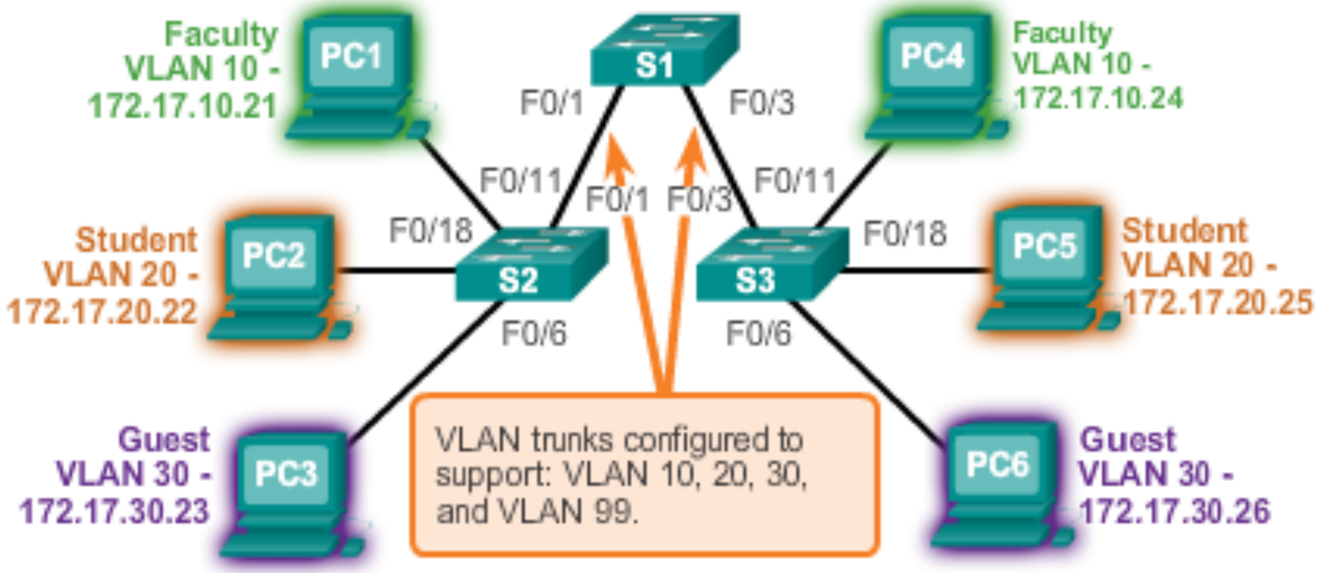
- A VLAN trunk carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco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

VLANs in a Multi-Switched Environment

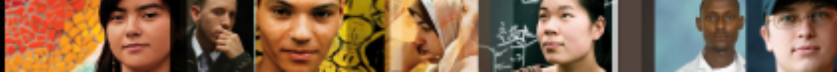
VLAN Trunks (cont.)

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.



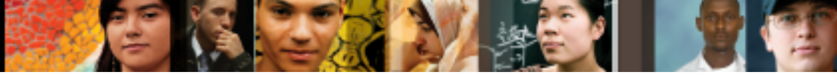
VLAN trunks configured to support: VLAN 10, 20, 30, and VLAN 99.



VLANs in a Multi-Switched Environment

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.



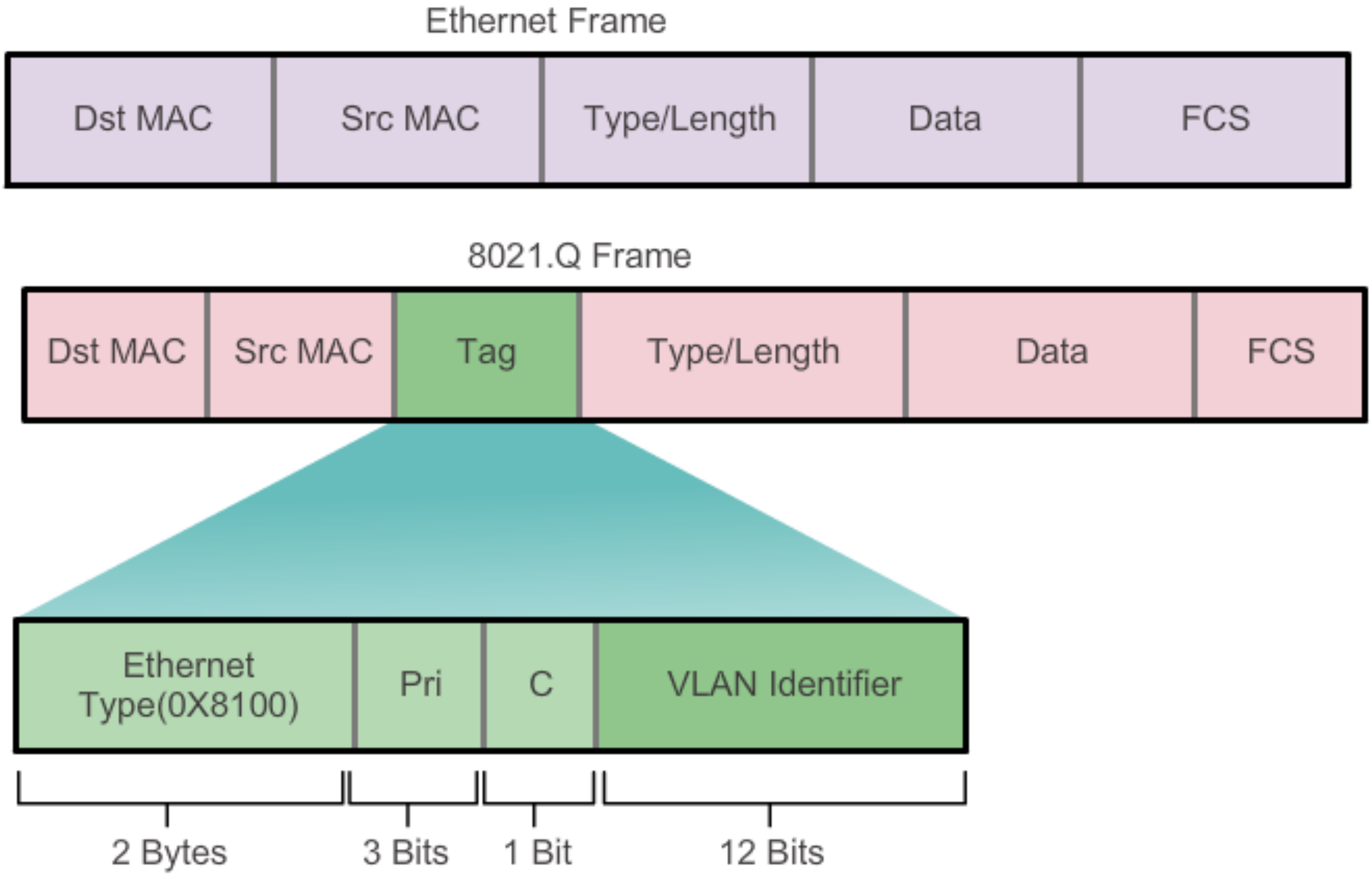
VLANs in a Multi-Switched Environment

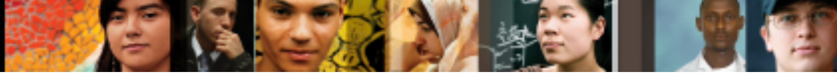
Tagging Ethernet Frames for VLAN Identification

- 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 that 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 nontrunk 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.

VLANs in a Multi-Switched Environment

Tagging Ethernet Frames for VLAN Identification





VLANs in a Multi-Switched Environment

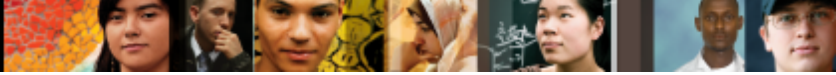
Native VLANs and 802.1Q Tagging

- Frames that belong to the native VLAN are not 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.
- In Cisco switches, the native VLAN is VLAN 1, by default.

VLAN Assignment

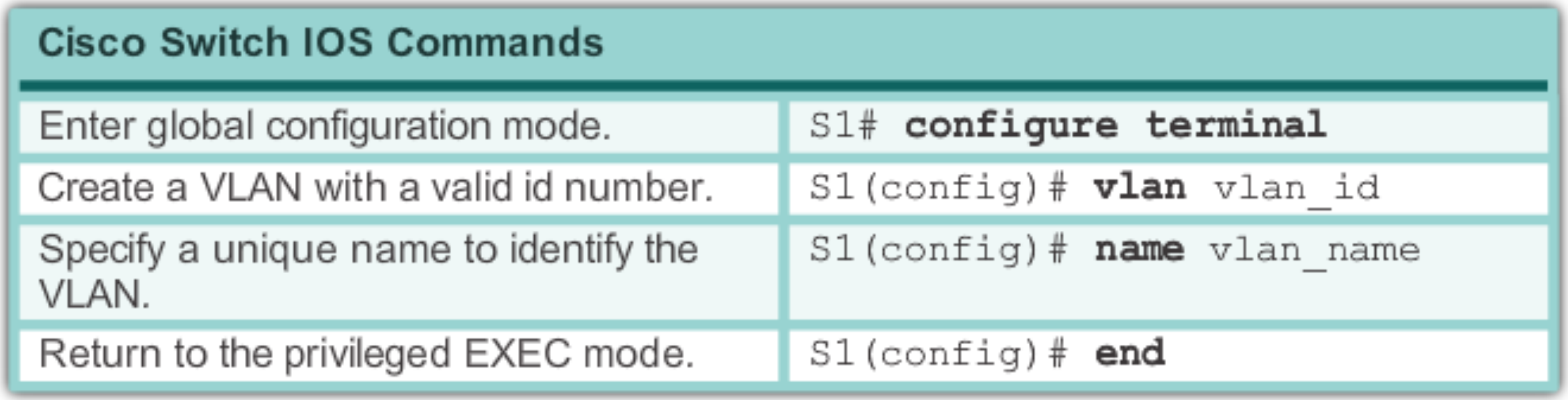
VLAN Ranges on Catalyst Switches

- 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)
    - VTP can only learn and store normal range VLANs
  - Extended Range VLANs
    - VLAN numbers from 1,006 to 4,096
    - Configurations stored in the running configuration (NVRAM)
    - VTP does not learn extended range VLANs

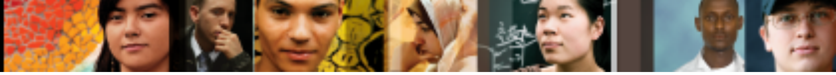


VLAN Assignment

Creating a VLAN

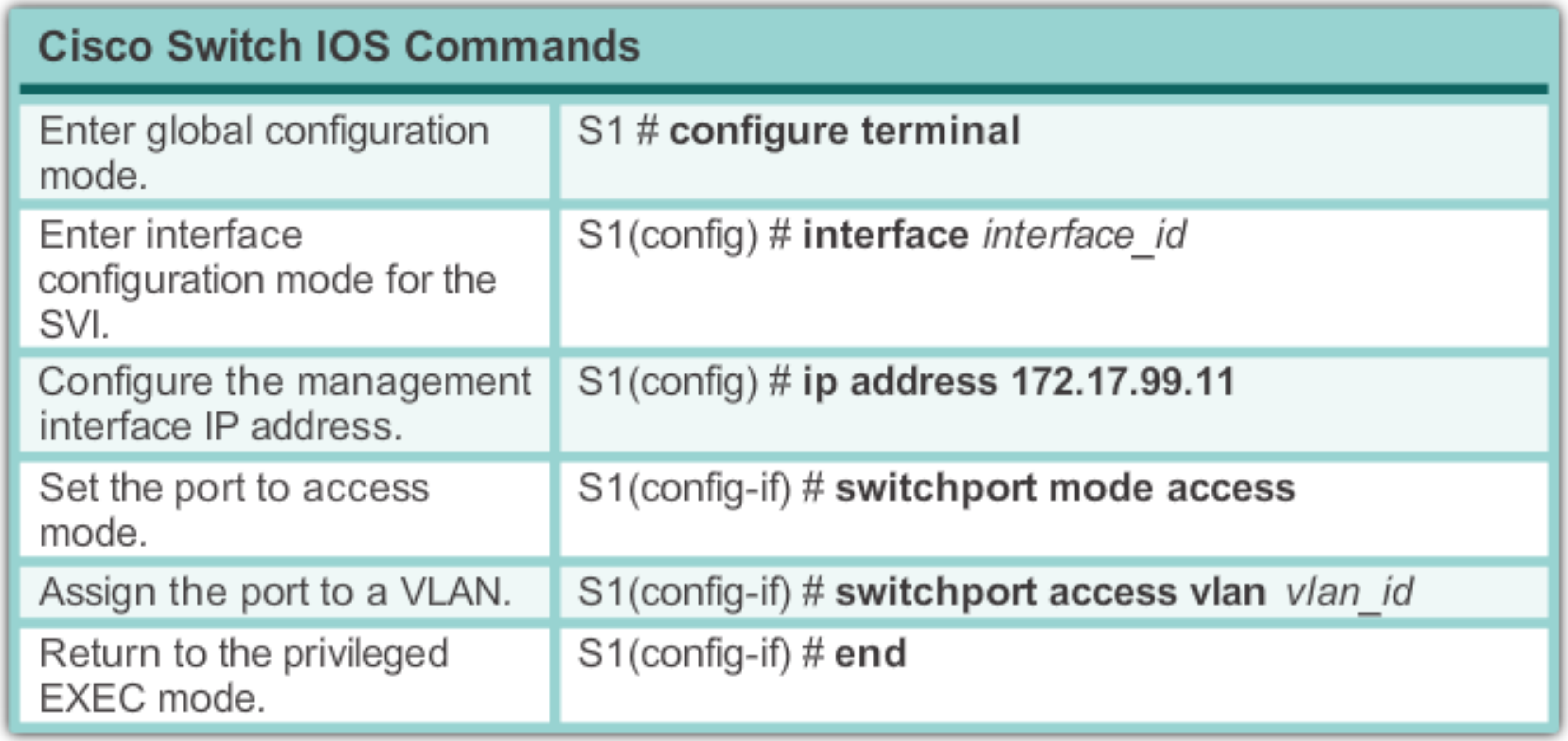


Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Create a VLAN with a valid id number.	`S1(config)# vlan vlan_id`
Specify a unique name to identify the VLAN.	`S1(config)# name vlan_name`
Return to the privileged EXEC mode.	`S1(config)# end`



VLAN Assignment

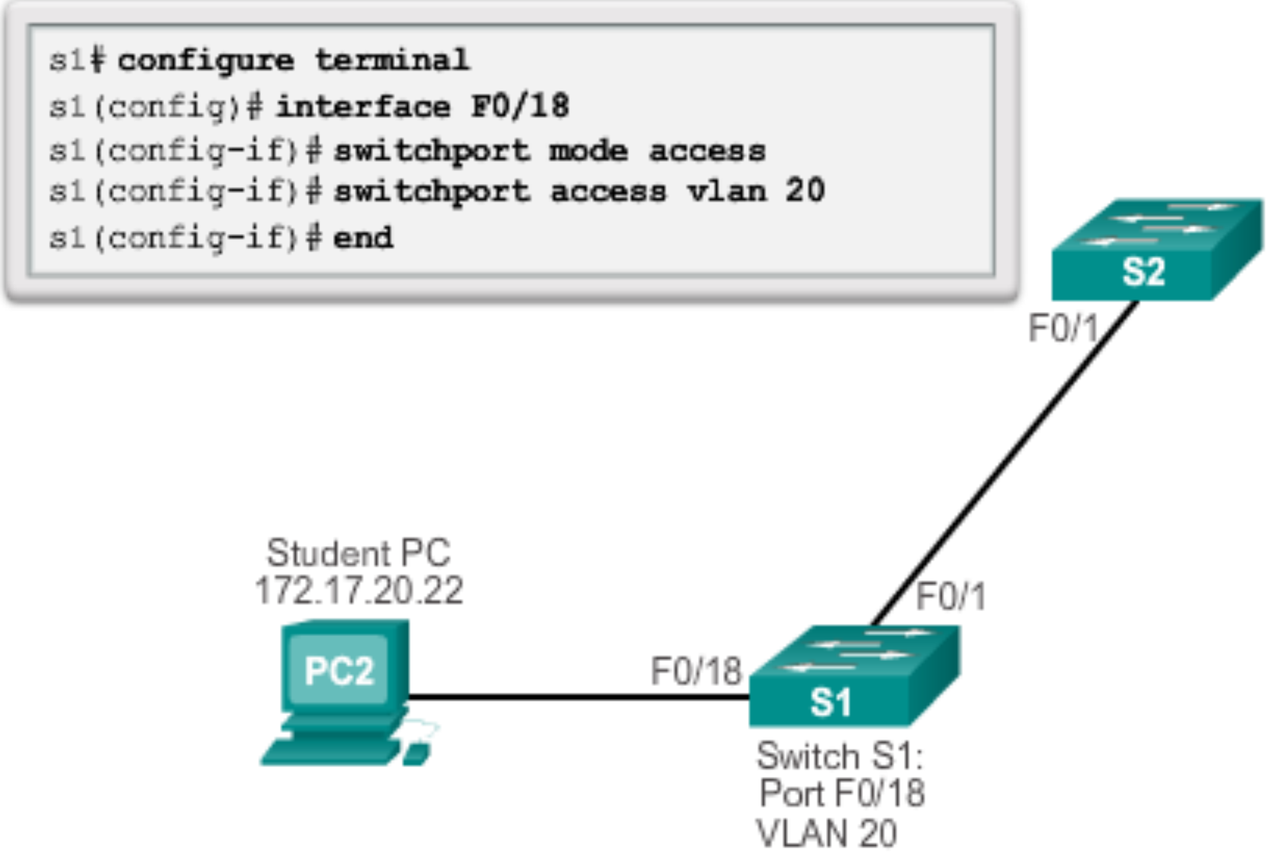
Assigning Ports to VLANs



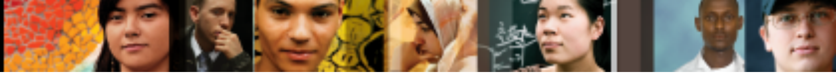
Cisco Switch IOS Commands	
Enter global configuration mode.	S1 # **configure terminal**
Enter interface configuration mode for the SVI.	S1(config) # **interface** *interface_id*
Configure the management interface IP address.	S1(config) # **ip address 172.17.99.11**
Set the port to access mode.	S1(config-if) # **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**

VLAN Assignment

Assigning Ports to VLANs (cont.)

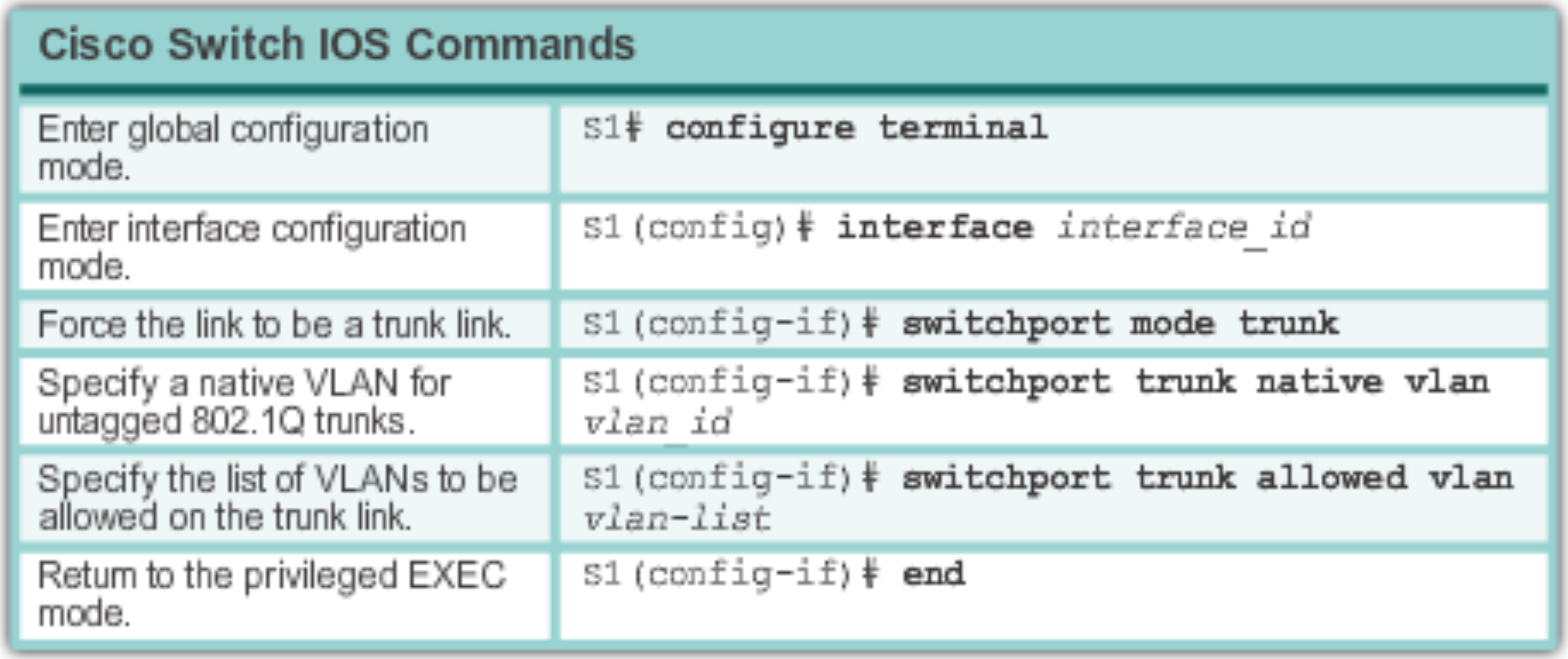


```
s1# configure terminal
s1(config)# interface F0/18
s1(config-if)# switchport mode access
s1(config-if)# switchport access vlan 20
s1(config-if)# end
```

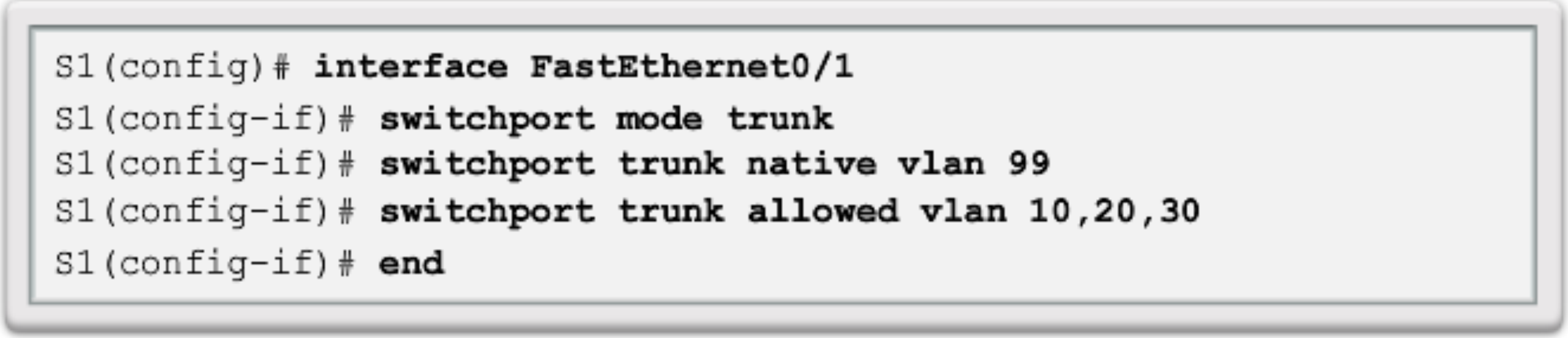


VLAN Assignment

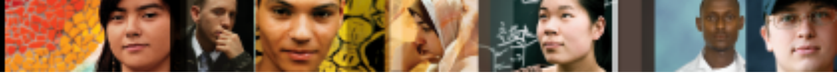
Configuring IEEE 802.1q Trunk Links



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 802.1Q trunks.	`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
S1(config-if)# end
```



Design Best Practices for VLANs

VLAN Design Guidelines

- Move all ports from VLAN 1 and assign them to a not-in-use VLAN
- Shut down all unused switch ports.
- Separate management and user data traffic.
- Change the management VLAN to a VLAN other than VLAN 1. (The same goes to the native VLAN.)
- Ensure that only devices in the management VLAN can connect to the switches.
- The switch should only accept SSH connections.
- Disable autonegotiation on trunk ports.
- Do not use the auto or desirable switch port modes.

Cisco | Networking Academy®

Mind Wide Open™