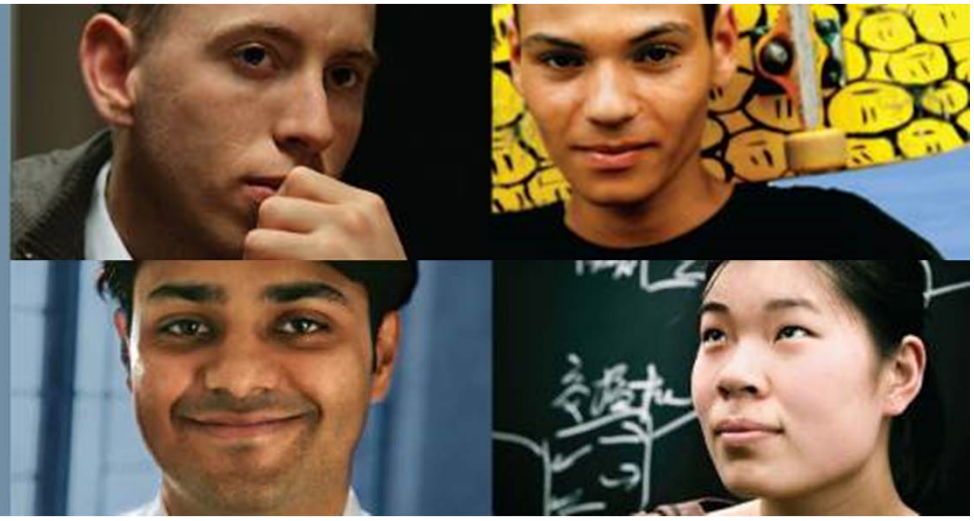
Chapter 3: VLANs



Routing & Switching

Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 3

3.1 VLAN Segmentation

3.2 VLAN Implementation

3.3 VLAN Security and Design

3.4 Summary

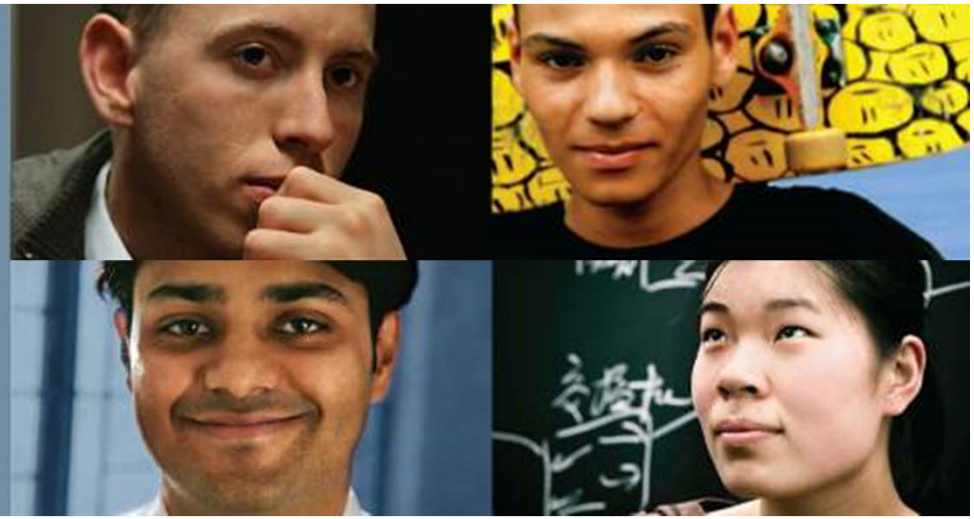
© 2008 Cisco Systems, Inc. All rights reserved.

Chapter 3: Objectives

- Explain the purpose of VLANs in a switched network.
- Analyze how a switch forwards frames based on VLAN configuration in a multi-switched environment.
- Configure a switch port to be assigned to a VLAN based on requirements.
- Configure a trunk port on a LAN switch.
- Configure Dynamic Trunk Protocol (DTP).
- Troubleshoot VLAN and trunk configurations in a switched network.
- Configure security features to mitigate attacks in a VLAN-segmented environment.
- Explain security best practices for a VLAN-segmented environment.

© 2008 Cisco Systems, Inc. All rights reserved.

3.1 VLAN Segmentation



Cisco | Networking Academy®
Mind Wide Open™

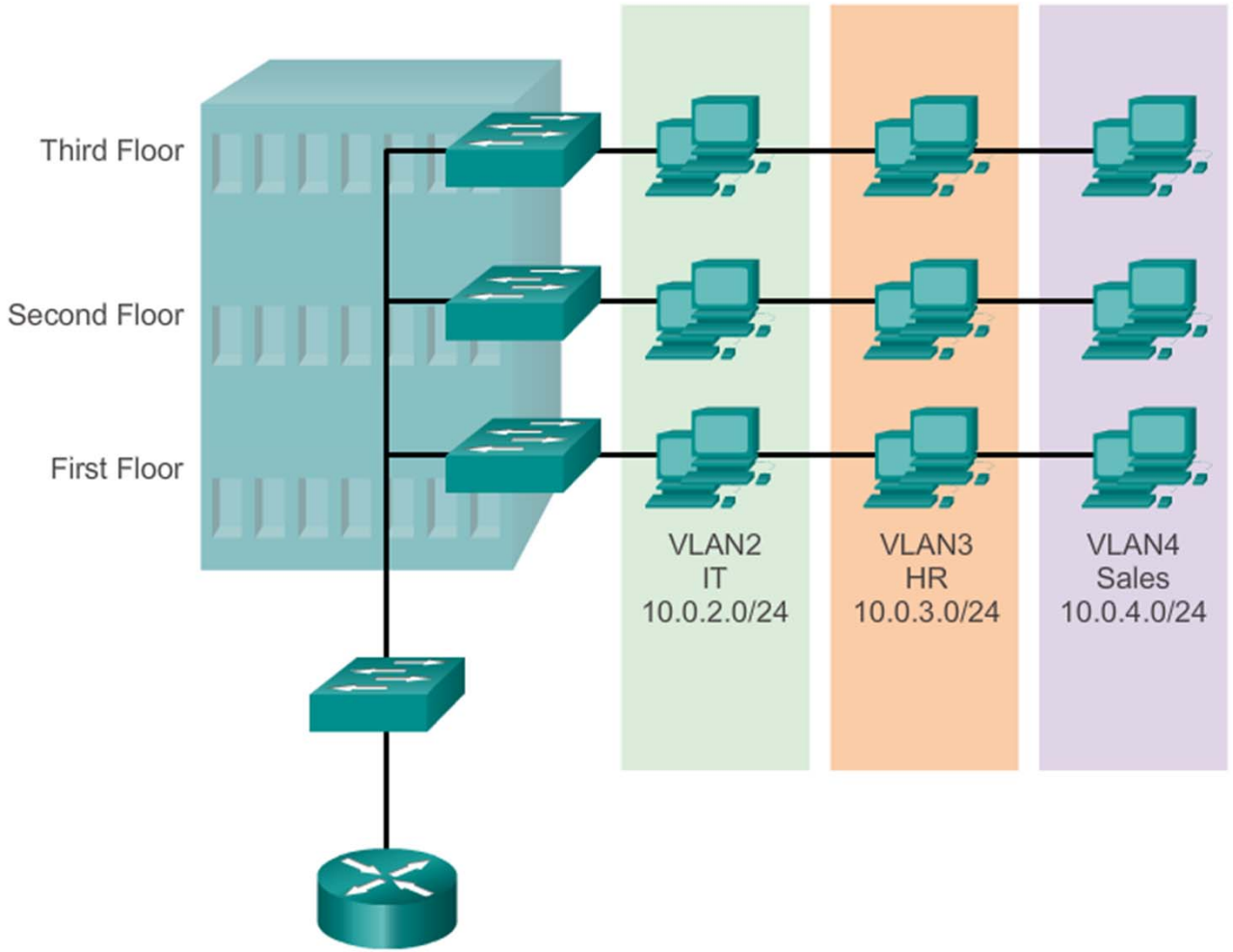
© 2008 Cisco Systems, Inc. All rights reserved.

VLAN Definitions

- 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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Definitions (cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

Benefits of VLANs

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

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Types of VLANs

- Data VLAN
- Default VLAN
- Native VLAN
- Management VLAN

© 2008 Cisco Systems, Inc. All rights reserved.

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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

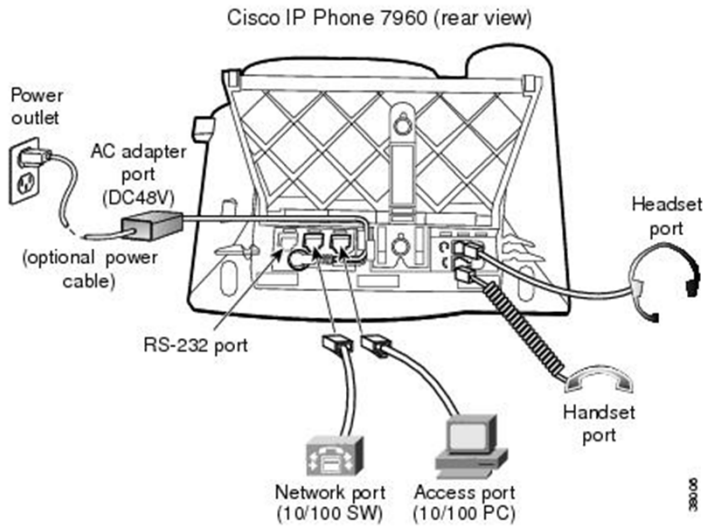
Voice VLANs

- 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.
- The switch can connect to a Cisco 7960 IP phone and carry IP voice traffic.
- The sound quality of an IP phone call can deteriorate if the data is unevenly sent; the switch supports quality of service (QoS).

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

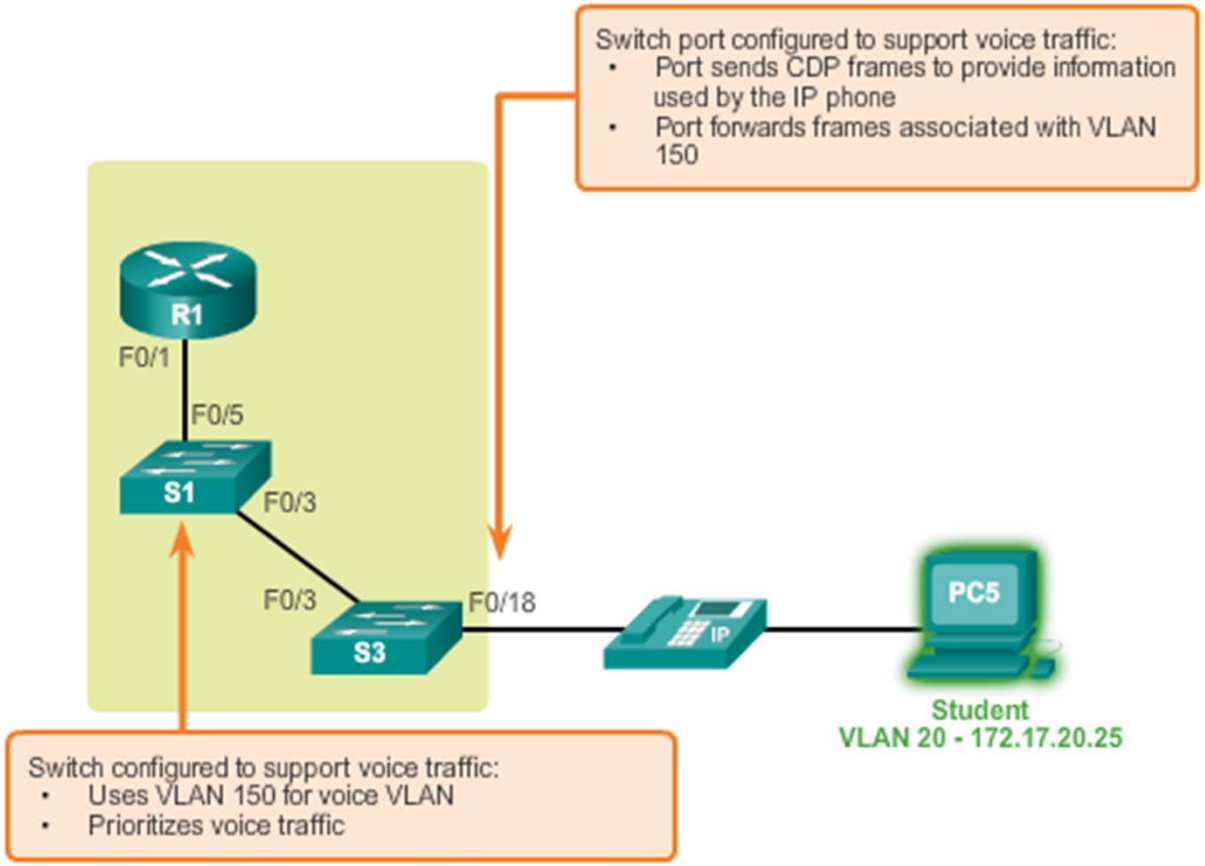
Voice VLANs (cont.)

- The Cisco 7960 IP phone has two RJ-45 ports that each support connections to external devices.
  - **Network Port (10/100 SW) -** Use this port to connect the phone to the network. The phone can also obtain inline power from the Cisco Catalyst switch over this connection.
  - **Access Port (10/100 PC) -** Use this port to connect a network device, such as a computer, to the phone.



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Voice VLANs (cont.)



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Trunks

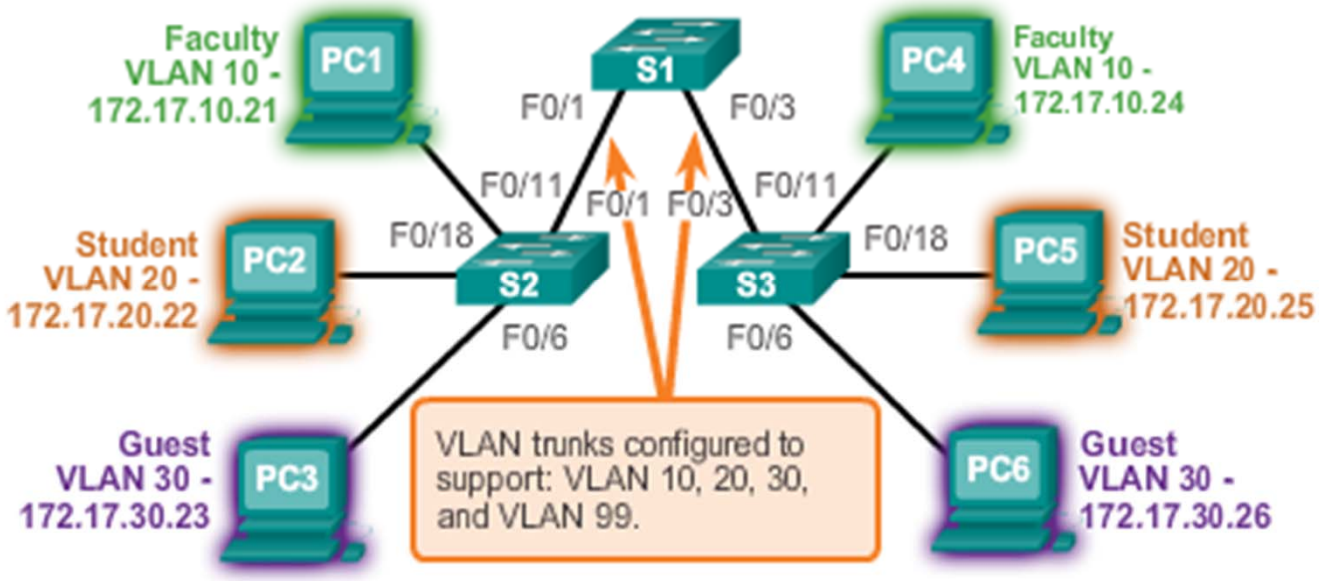
- A VLAN trunk carries more than one VLAN.
- A VLAN trunk is usually established between switches so same-VLAN devices can communicate, even if physically connected to different switches.
- A VLAN trunk is not associated to any VLANs; neither is the trunk ports used to establish the trunk link.
- Cisco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

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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.



© 2008 Cisco Systems, Inc. All rights reserved.

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.

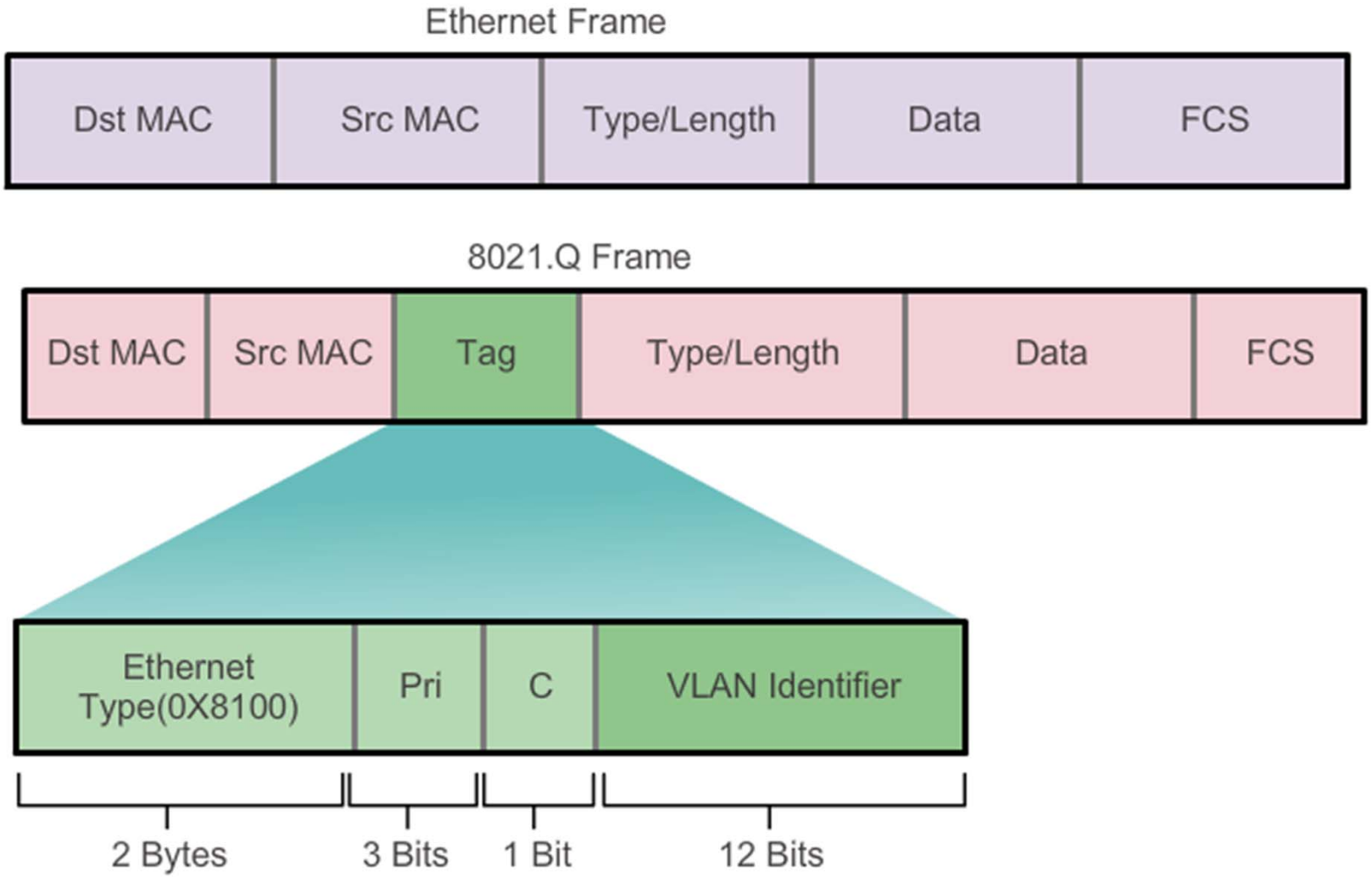
© 2008 Cisco Systems, Inc. All rights reserved.

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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Tagging Ethernet Frames for VLAN Identification



© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

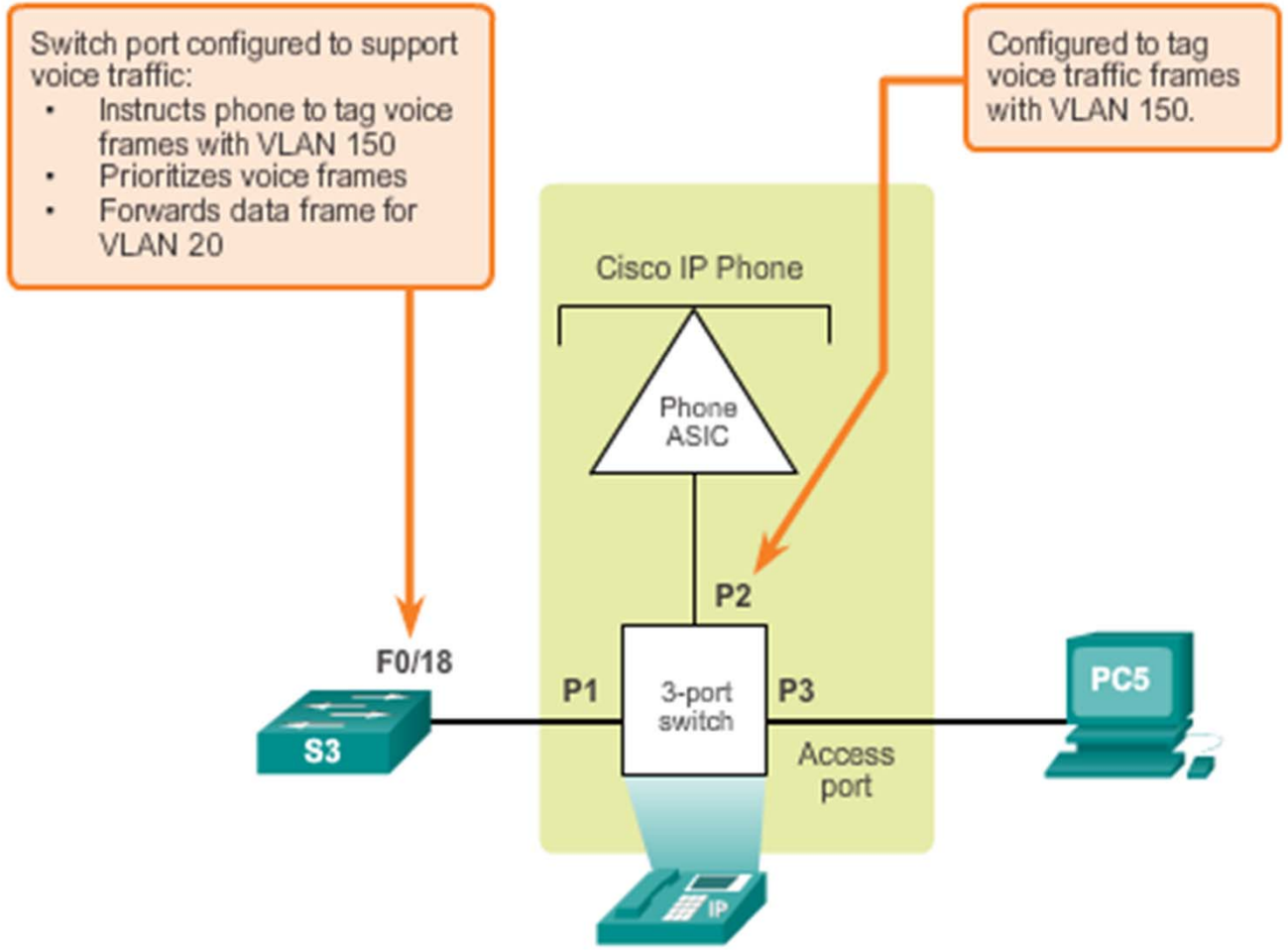
Native VLANs and 802.1Q Tagging

- 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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

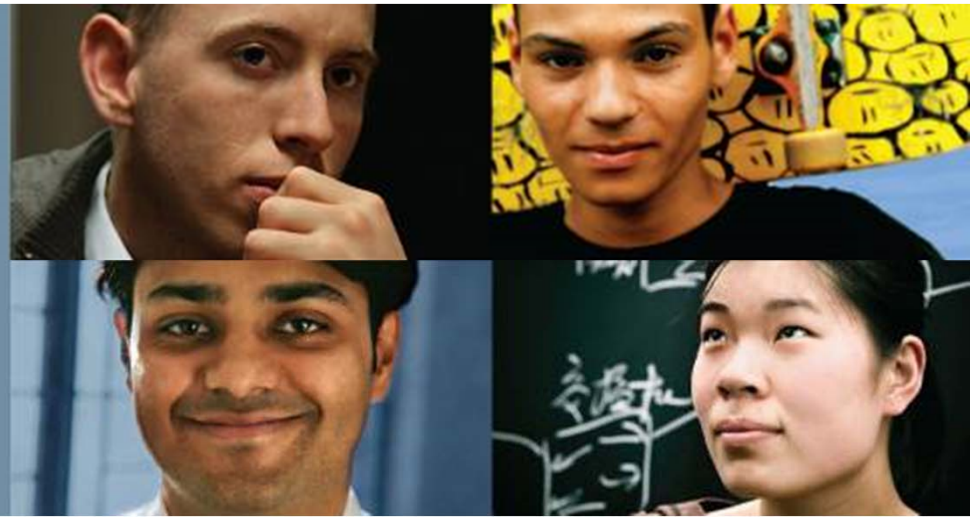
VLANs in a Multi-Switched Environment

Voice VLAN Tagging



© 2008 Cisco Systems, Inc. All rights reserved.

3.2 VLAN Implementations



Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

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

© 2008 Cisco Systems, Inc. All rights reserved.

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`

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Assignment

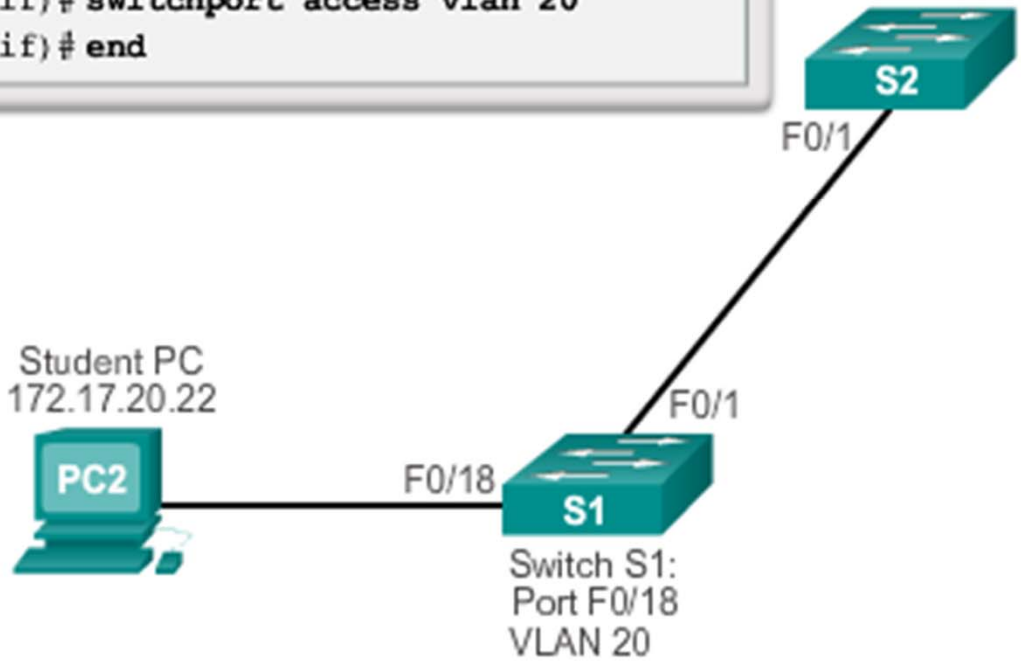
Assigning Ports to VLANs

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**

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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
```



© 2008 Cisco Systems, Inc. All rights reserved.

VLAN Assignment

Changing VLAN Port Membership

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

VLAN Name                Status    Ports
---- ----------------- ------- -------------------------------
1    default              active  Fa0/1, Fa0/2, Fa0/3, Fa0/4
                                  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#
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Changing VLAN Port Membership (cont.)

```
S1# config t
S1(config)# int fa0/11
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, Fa0/1
                                     Fa0/14, Fa0/15, Fa0/16, Fa0/
                                     Fa0/18, Fa0/19, Fa0/20, Fa0/
                                     Fa0/22, Fa0/23, Fa0/24, Gi0/
                                     Gi0/2
20   student              active     Fa0/11
1002 fddi-default         act/unsup
1003 token-ring-default   act/unsup
1004 fddinet-default      act/unsup
1005 trnet-default        act/unsup
S1#
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Assignment

Deleting VLANs

```
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#
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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#
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Assignment

Verifying VLAN Information (cont.)

```
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
```


© 2008 Cisco Systems, Inc. All rights reserved.

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
```


© 2008 Cisco Systems, Inc. All rights reserved.

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


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Resetting the Trunk To Default State (cont.)

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>
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

VLAN Assignment

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>
```


© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Introduction to DTP

- Switch ports can be manually configured to form trunks.
- Switch ports can also be configured to negotiate and establish a trunk link with a connected peer.
- The Dynamic Trunking Protocol (DTP) manages trunk negotiation.
- DTP is a Cisco proprietary protocol and is enabled, by default, in Cisco Catalyst 2960 and 3560 switches.
- If the port on the neighbor switch is configured in a trunk mode that supports DTP, it manages the negotiation.
- The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto.

© 2008 Cisco Systems, Inc. All rights reserved.

Negotiated Interface Modes

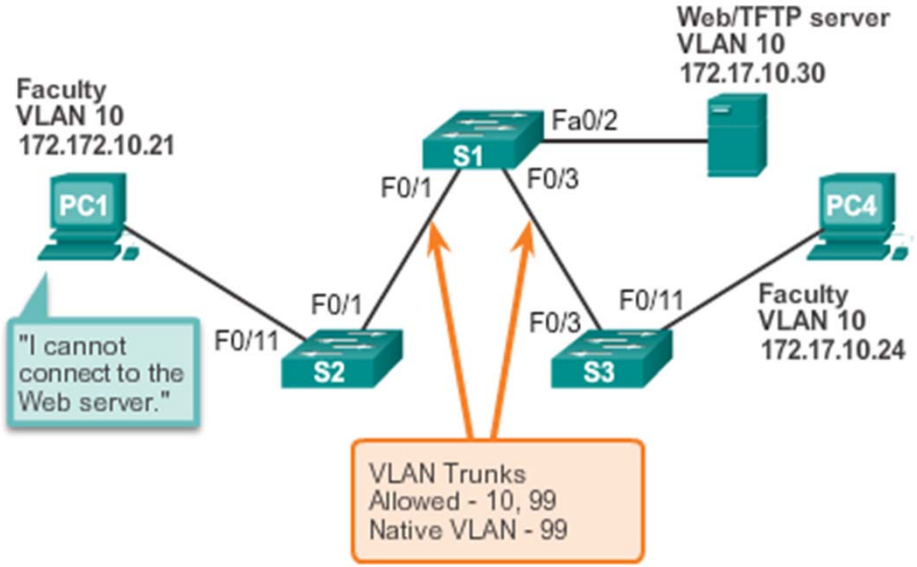
- Cisco Catalyst 2960 and 3560 support the following trunk modes:
  - Switchport mode dynamic auto
  - Switchport mode dynamic desirable
  - Switchport mode trunk
  - Switchport nonegotiate

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

© 2008 Cisco Systems, Inc. All rights reserved.

IP Addressing Issues with VLAN

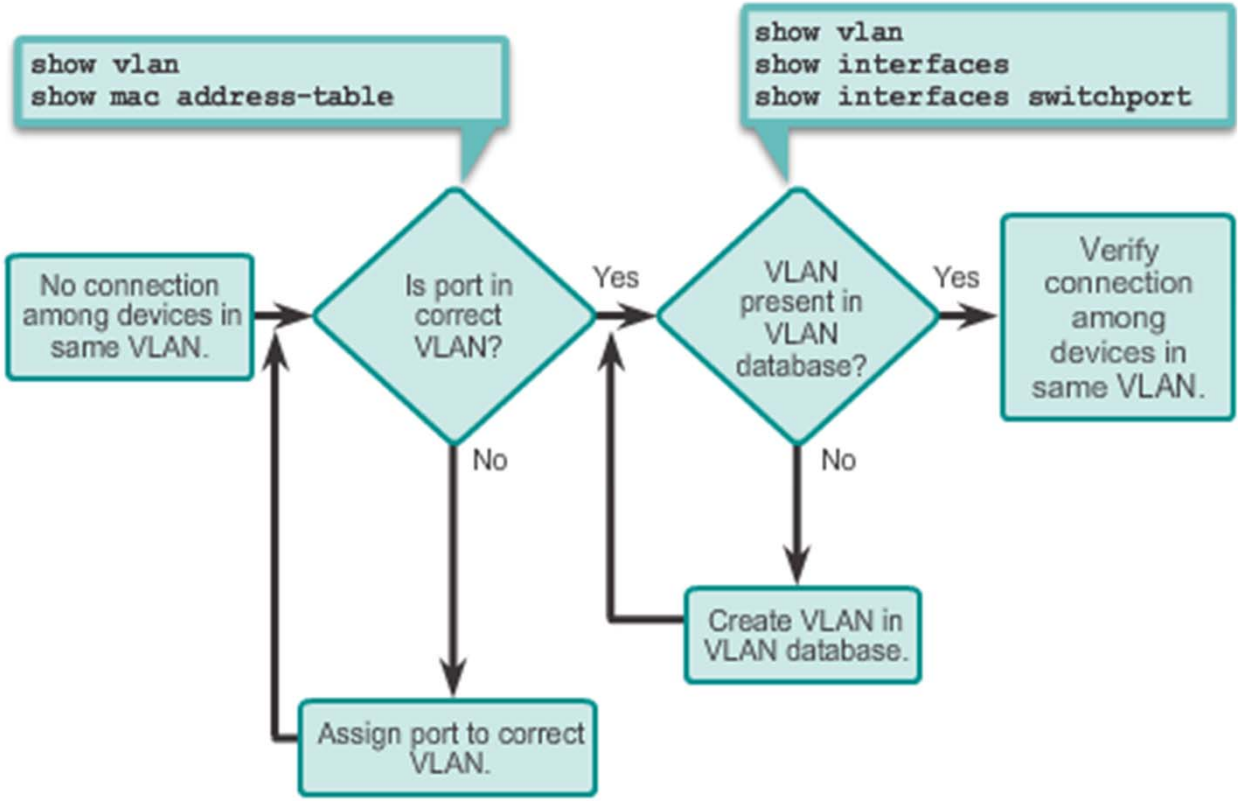
- It is a common practice to associate a VLAN with an IP network.
- Because different IP networks only communicate through a router, all devices within a VLAN must be part of the same IP network to communicate.
- The figure displays that PC1 cannot communicate to the server because it has a wrong IP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



© 2008 Cisco Systems, Inc. All rights reserved.

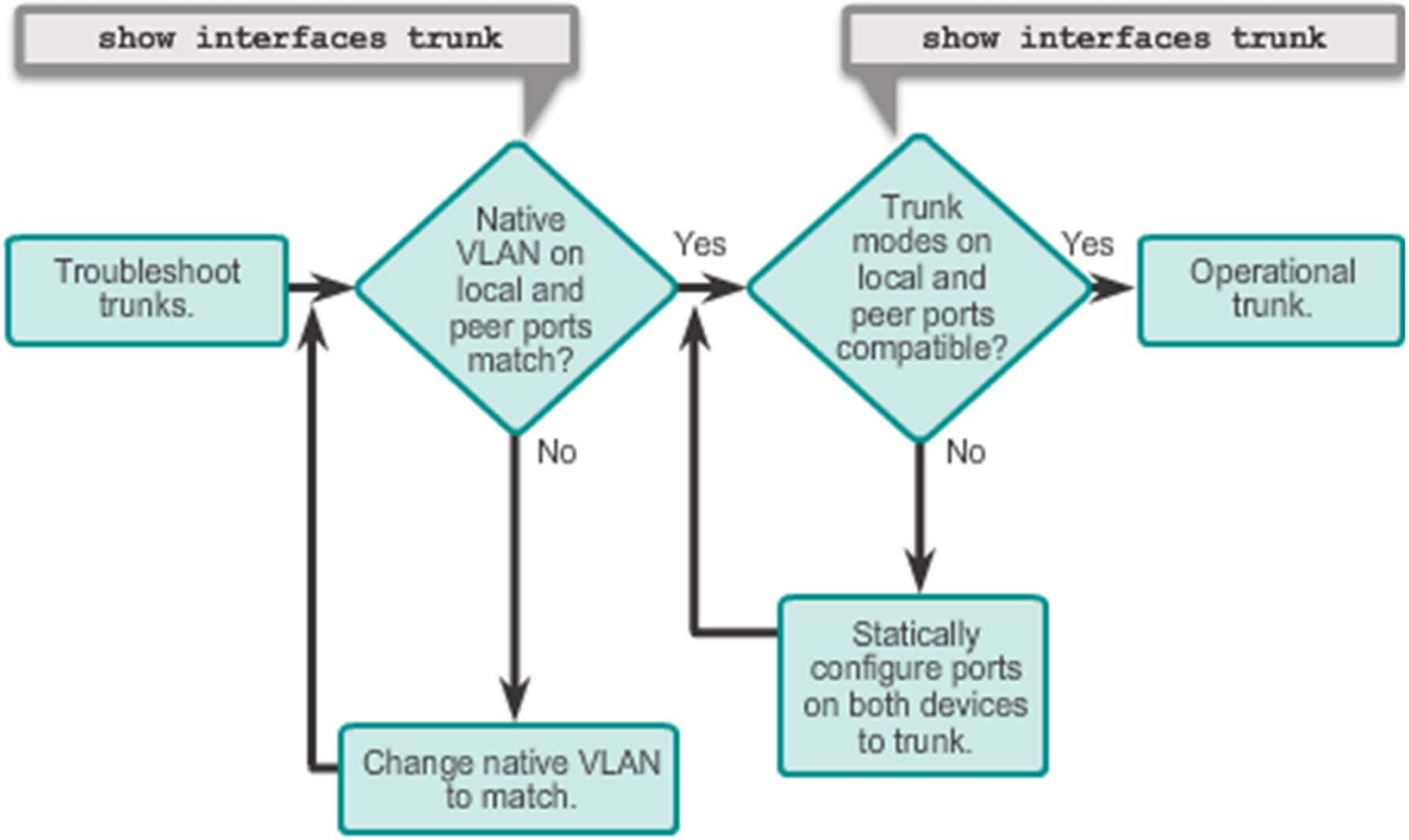
Missing VLANs

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



© 2008 Cisco Systems, Inc. All rights reserved.

Introduction to Troubleshooting Trunks



© 2008 Cisco Systems, Inc. All rights reserved.

Common Problems with Trunks

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

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Trunk Mode Mismatches

- If a port on a trunk link is configured with a trunk mode that is incompatible with the neighboring trunk port, a trunk link fails to form between the two switches.
- Use the **show interfaces trunk** command to check the status of the trunk ports on the switches.
- To fix the problem, configure the interfaces with proper trunk modes.

	Dynamic Auto	Dynamic Desirable	Trunk	Access
Dynamic auto	Access	Trunk	Trunk	Access
Dynamic desirable	Trunk	Trunk	Trunk	Access
Trunk	Trunk	Trunk	**Trunk**	Limited connectivity
Access	Access	Access	Limited connectivity	**Access**

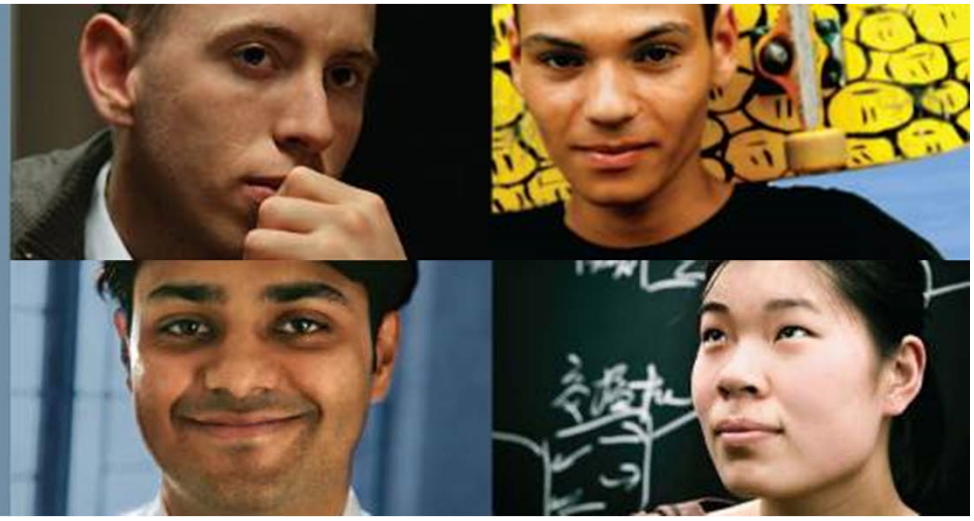
© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

3.3 VLAN Security and Design



Cisco | Networking Academy®
Mind Wide Open™

© 2008 Cisco Systems, Inc. All rights reserved.

Switch Spoofing Attack

- There are a number of different types of VLAN attacks in modern switched networks; VLAN hopping is one example.
- The default configuration of the switch port is dynamic auto.
- By configuring a host to act as a switch and form a trunk, an attacker could gain access to any VLAN in the network.
- Because the attacker is now able to access other VLANs, this is called a VLAN hopping attack.
- To prevent a basic switch spoofing attack, turn off trunking on all ports, except the ones that specifically require trunking.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

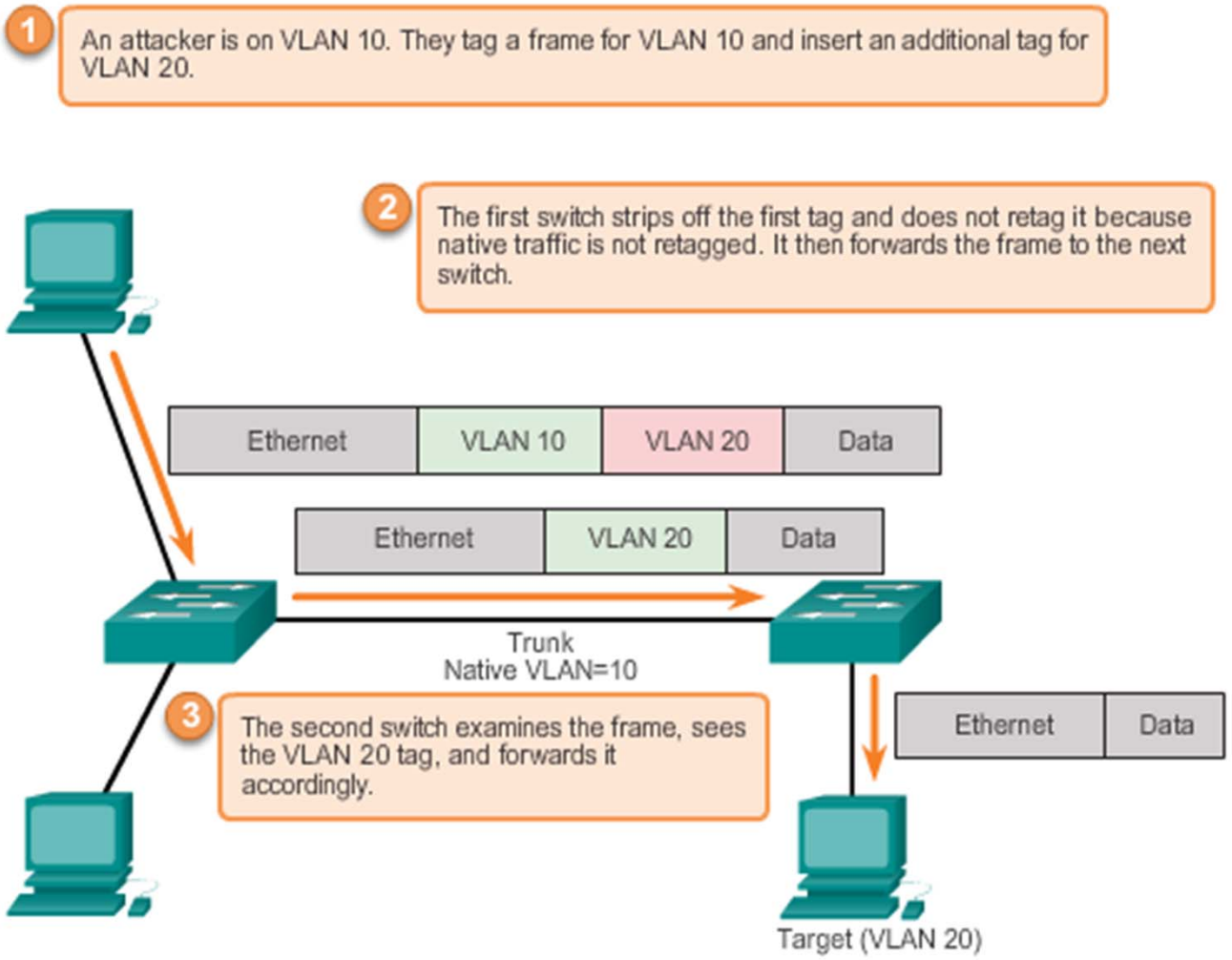
Double-Tagging Attack

- Double-tagging attack takes advantage of the way that hardware on most switches de-encapsulate 802.1Q tags.
- Most switches perform only one level of 802.1Q de-encapsulation, allowing an attacker to embed a second, unauthorized attack header in the frame.
- After removing the first and legit 802.1Q header, the switch forwards the frame to the VLAN specified in the unauthorized 802.1Q header.
- The best approach to mitigating double-tagging attacks is to ensure that the native VLAN of the trunk ports is different from the VLAN of any user ports.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Attacks on VLANs

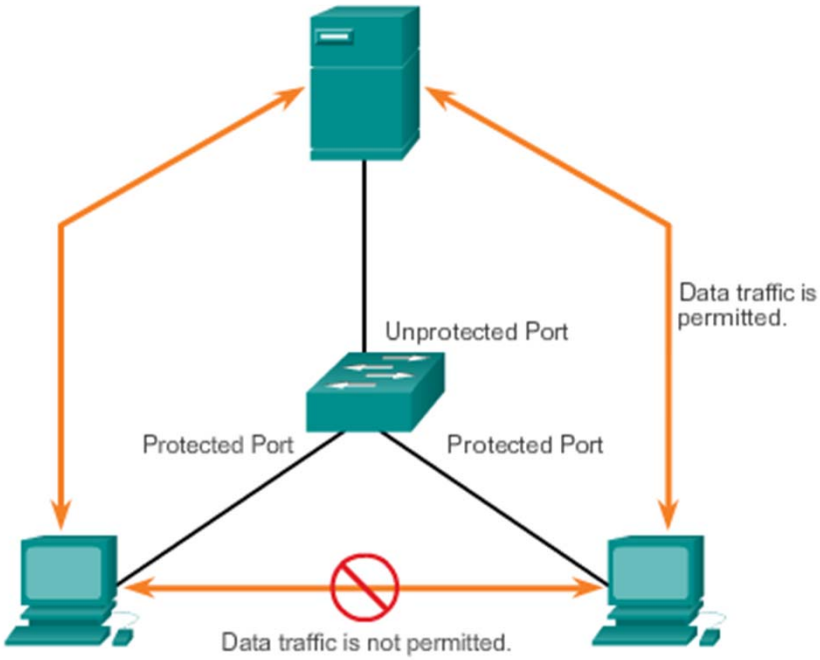
Double-Tagging Attack (cont.)



© 2008 Cisco Systems, Inc. All rights reserved.

PVLAN Edge

- The Private VLAN (PVLAN) Edge feature, also known as protected ports, ensures that there is no exchange of unicast, broadcast, or multicast traffic between protected ports on the switch.
- Local relevancy only.
- A protected port only exchanges traffic with unprotected ports.
- A protected port does not exchange traffic with another protected port.



© 2008 Cisco Systems, Inc. All rights reserved.
Cisco Confidential

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.

© 2008 Cisco Systems, Inc. All rights reserved. Cisco Confidential

Chapter 3: Summary

This chapter:

- Introduced VLANs and their types
- Described the connection between VLANs and broadcast domains
- Discussed IEEE 802.1Q frame tagging and how it enables differentiation between Ethernet frames associated with distinct VLANs as they traverse common trunk links.
- Examined the configuration, verification, and troubleshooting of VLANs and trunks using the Cisco IOS CLI and explored basic security and design considerations.

© 2008 Cisco Systems, Inc. All rights reserved.

© 2008 Cisco Systems, Inc. All rights reserved.