TNE10006/TNE60006: Networks and Switching

VLANs

Cisco | Networking Academy®
Mind Wide Open™

Outline

- VLANs

- Intra and Inter VLAN Communications

- Creating VLANs

- VLAN Access Ports

- VLAN Trunking Ports

- DTP – Dynamic Trunking Protocol

- VLAN Types

VLAN Definitions

- A VLAN is a logical partition of a Layer 2 network

- Multiple partitions (VLANs) can be created

- Each VLAN is a broadcast dom~~ai~~

- VLANs ar~~e~~

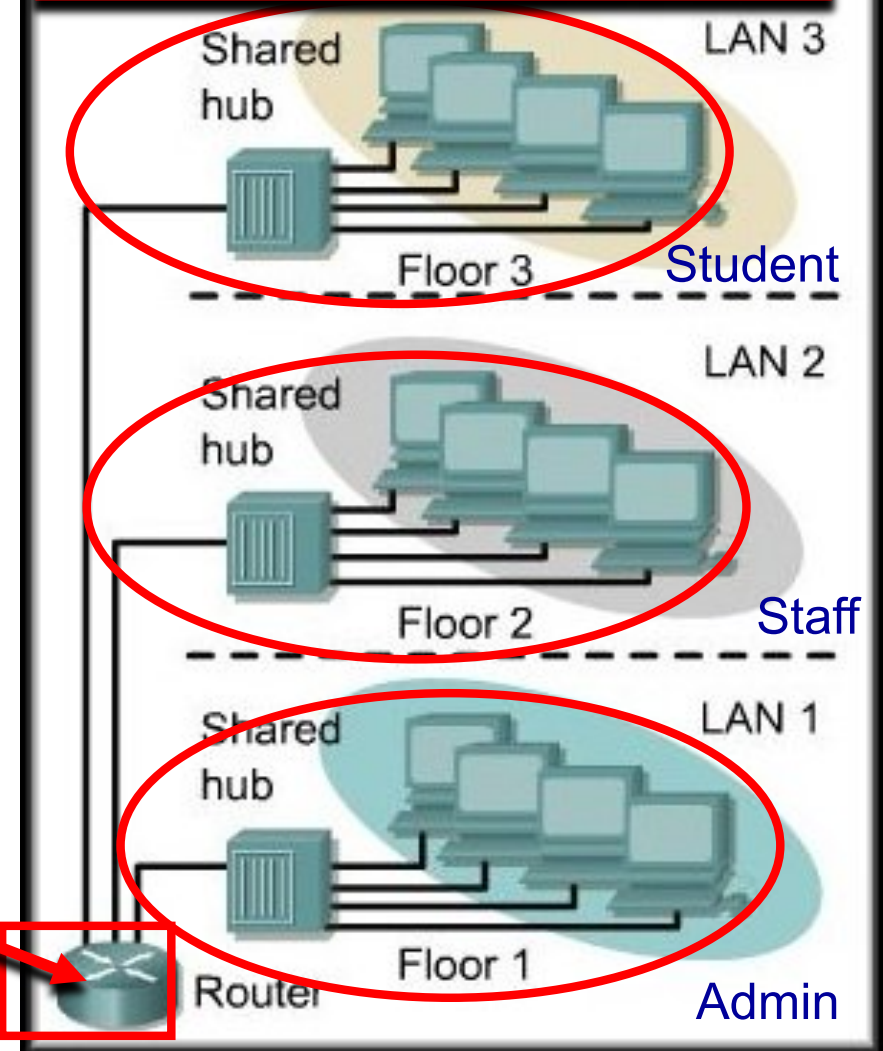VLANs effectively allow you to divide your physical switch into a number of virtual switches
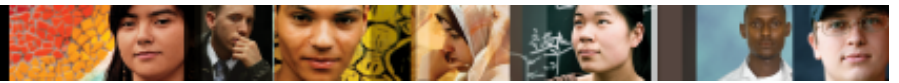
~~~~ are of the

VLAN Overview

Traditional switched LANs:

- Physical topology is closely related to logical topology

- Workstations must be grouped by their physical proximity to a switch

- To communicate among LANs, each segment must have a separate interface (fa0/0,fa0/1) on the backbone device (router)
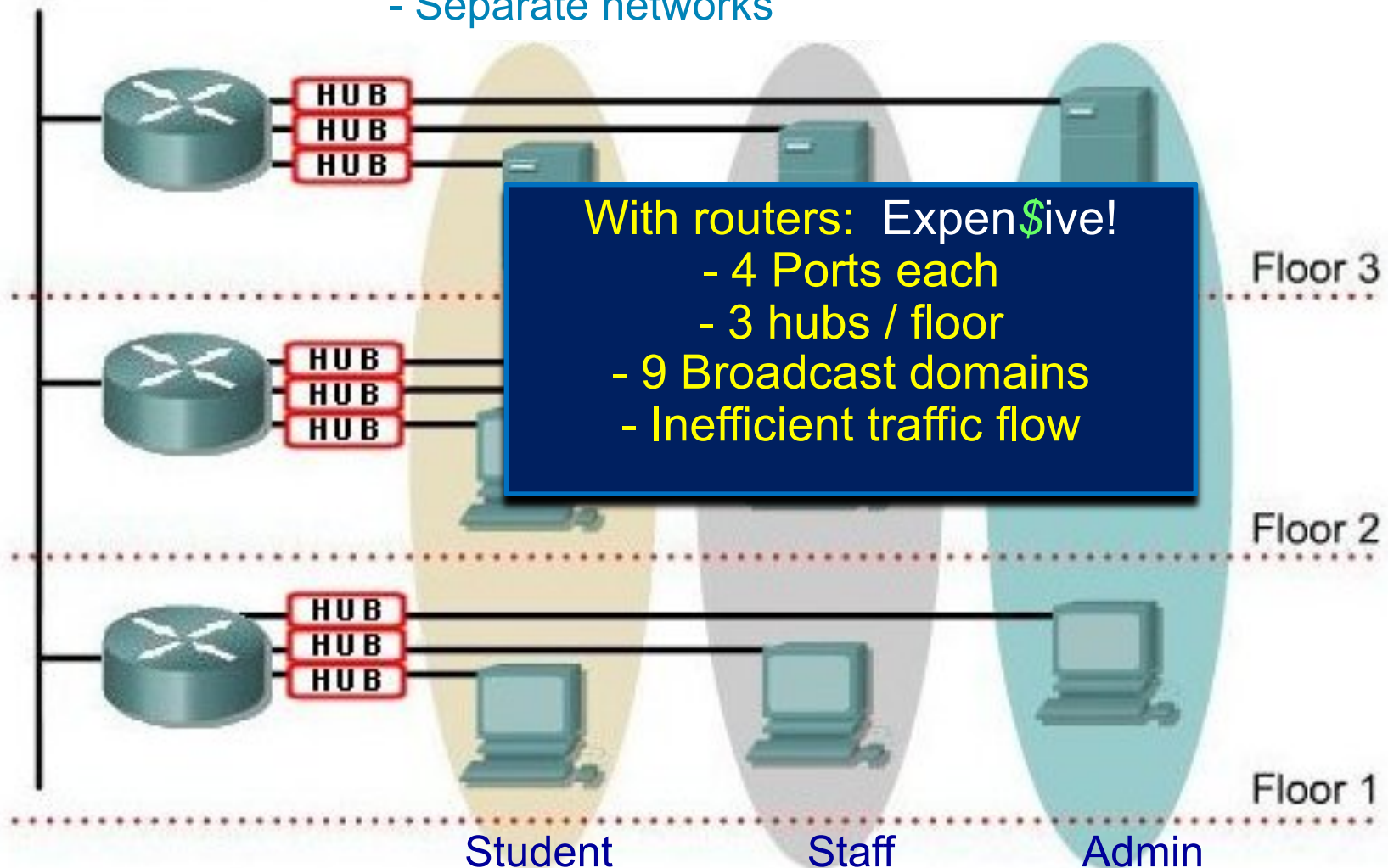
Separate Broadcast Domains

Without VLAN

Requirements:
- Students, Admins and Staffs on each floor.
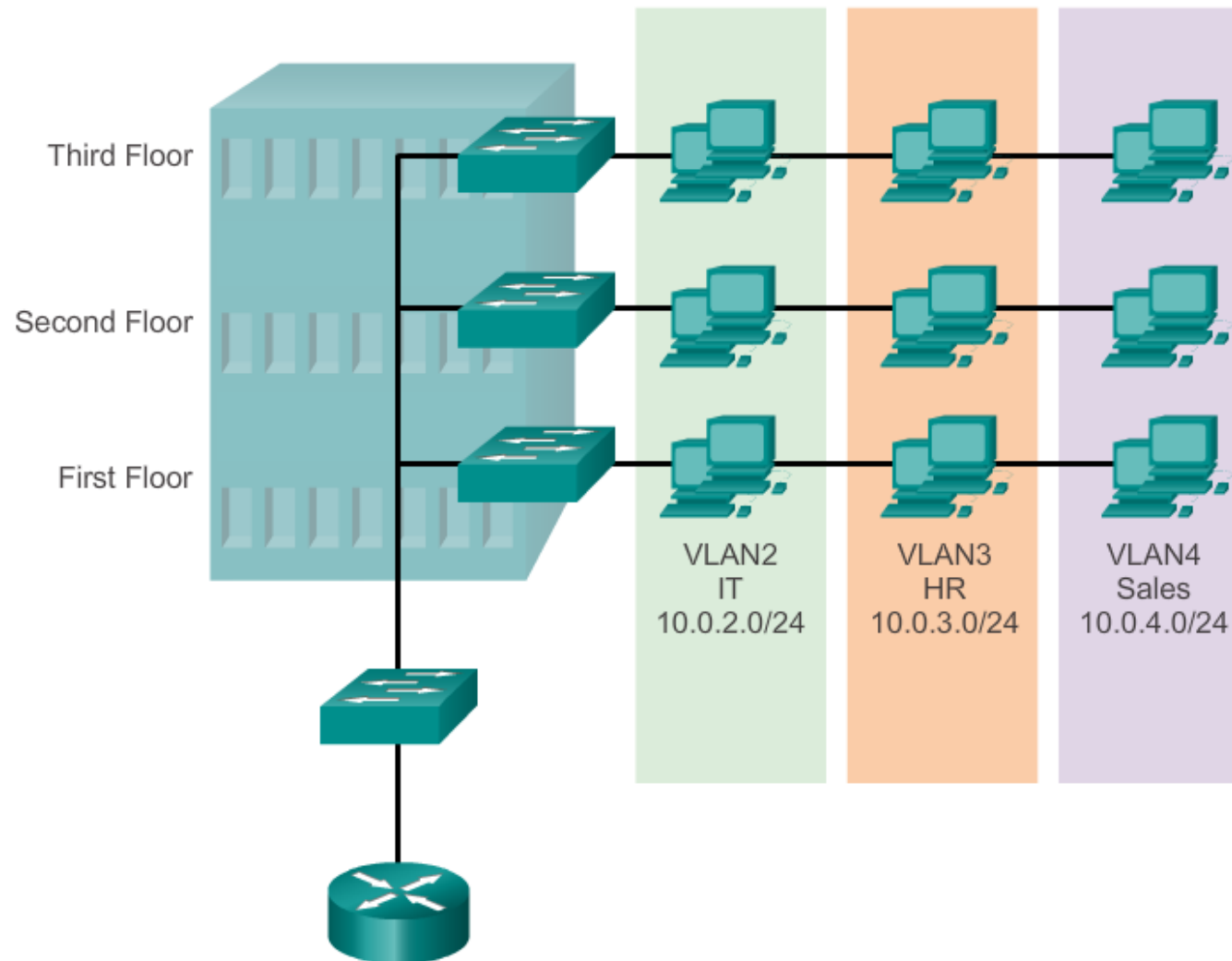- Three different LANs per floor.
- Separate networks

FastEthernet

With routers: Expen$ive!
- 4 Ports each
- 3 hubs / floor
- 9 Broadcast domains
- Inefficient traffic flow

HUB
HUB
HUB

HUB
HUB
HUB

HUB
HUB
HUB

Floor 3

Floor 2

Floor 1

Student   Staff   Admin

VLAN Definitions

Third Floor

Second Floor

First Floor

VLAN2
IT
10.0.2.0/24
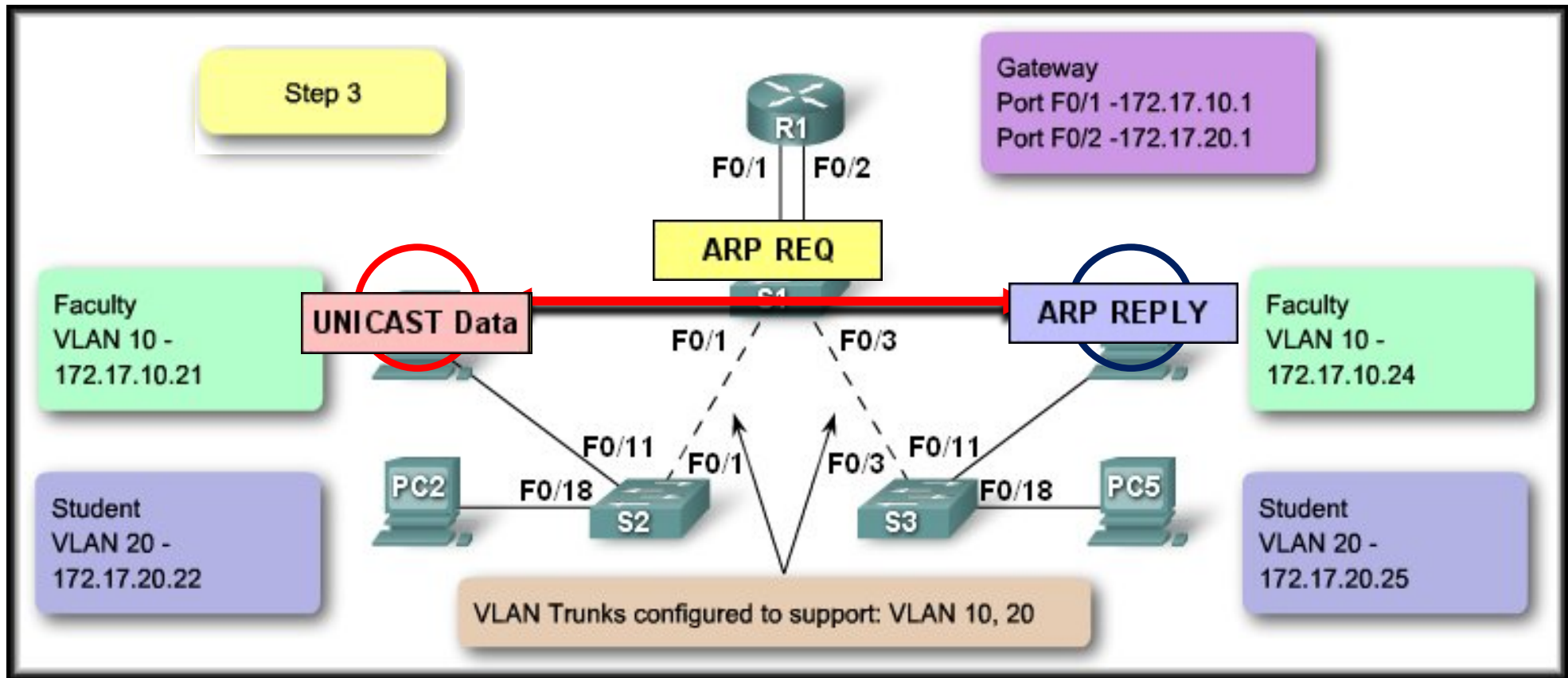
VLAN3
HR
10.0.3.0/24

VLAN4
Sales
10.0.4.0/24

Benefits of VLANs

- Security

- Cost reduction

- Better performance

- Shrink broadcast domains

Intra VLAN Communications

- PC1 pings PC4
- PC1 ARP table does not contain MAC address of PC4
- An ARP Request is a Broadcast

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)

    - Extended Range VLANs

        - VLAN numbers from 1,006 to 4,095

        - Configurations stored in the running configuration (NVRAM)

- Some limitations to Extended VLANs – should limit use to normal VLANs
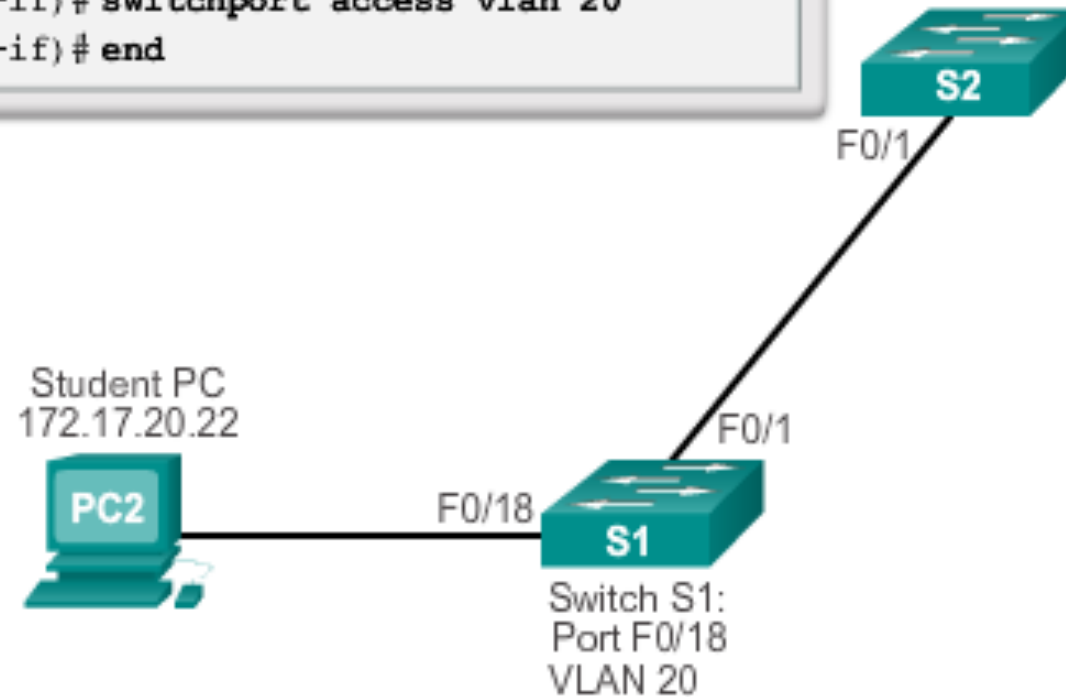
VLAN Assignment
VLAN Switch Ports

- **Step 1**: Create the VLAN on switch

  - All core/distribution layer switches need to know all VLANs for traffic they will see

  - All access layer switches need to know all VLANs for devices connected to them

- **Step 2**: assign switchports to particular VLAN

  - Default switchport mode is automatic – instead force mode

  - Non-used ports should be shutdown and not assigned to used VLAN

- **Step 3**: for Management VLANs, create the virtual interface and assign the IP address

  - Remember gateway to allow inter-VLAN access

VLAN Switch Ports


```
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
```

Student PC
172.17.20.22

F0/1

F0/1

S2

PC2

F0/18

S1

Switch S1:
Port F0/18
VLAN 20

Confirming VLAN Port Membership

```
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#
```
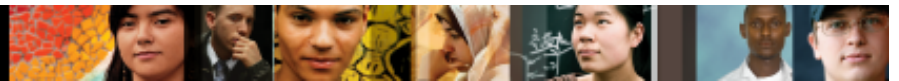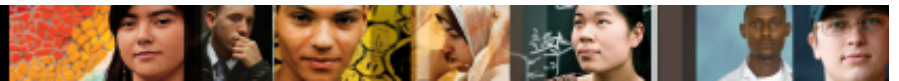
VLAN Access Ports

- Port can only belong to one VLAN

- Traffic is normal – *untagged* – Ethernet frames

- Network devices are unaware of VLAN

- Network devices see normal Ethernet network

- Traffic is restricted based on

    - Only traffic for that VLAN

    - Contents of switch CAM Table

VLAN Membership

Static VLAN

- Ports manually assigned to a VLAN

- Configured with:

  `switchport access vlan XX`

- Requires reconfiguration if circumstances change

Dynamic VLAN

- Membership is configured using a VMPS – VLAN Membership Policy Server

- Based on source Mac address of device

VLAN Trunks

- Inefficient to connect switches using Access Ports – need one connection for each VLAN

- Trunks allow a single connection to carry traffic of multiple VLANs

- Traffic is still segmented

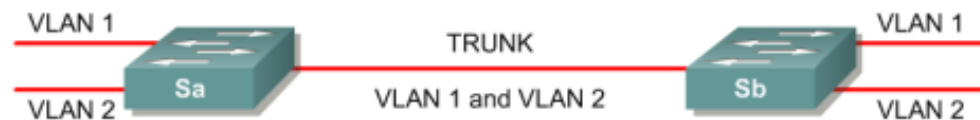- Frames are tagged to allow receiving switch to *know* which VLAN traffic *belongs* to

VLAN Trunking
VLAN Tagging

No VLAN Tagging

VLAN Tagging

VLAN Tagging is used when a link needs to carry traffic for more than one VLAN.

- There are two major methods of frame tagging, Cisco proprietary **Inter-Switch Link (ISL)** and **IEEE 802.1Q**.
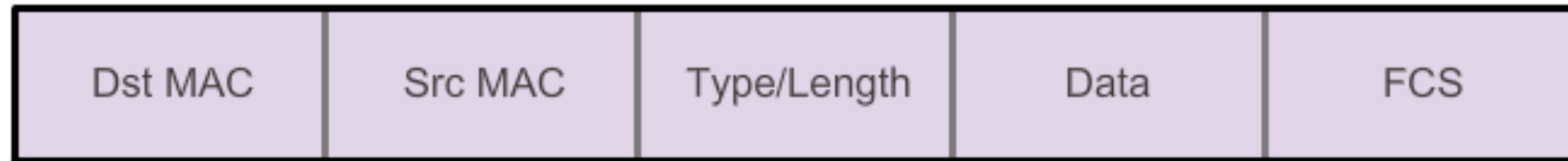
- Cisco recommends using 802.1Q.

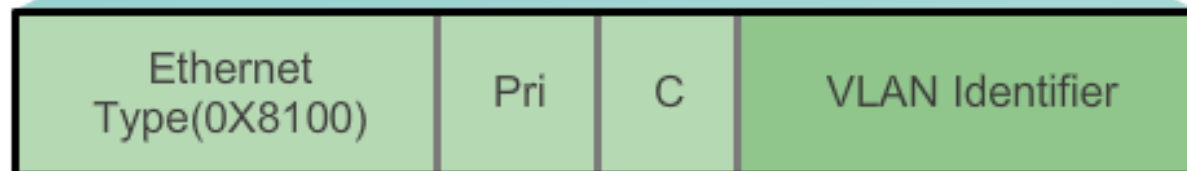| Tagging	Method	Media	Description
Inter-Switch Link (ISL)	Fast Ethernet	ISL header encapsulates the LAN frame and there is a VLAN ID field in the ISL header	Frame is lengthened
802.IQ	Fast Ethernet	IEEE defined Ethernet VLAN protocol	Header is modified
LAN Emulation (LANE)	ATM	No tagging	Virtual connection implies a VLAN ID

SWiN BUR *NE*

CENTRE FOR
ADVANCED
INTERNET
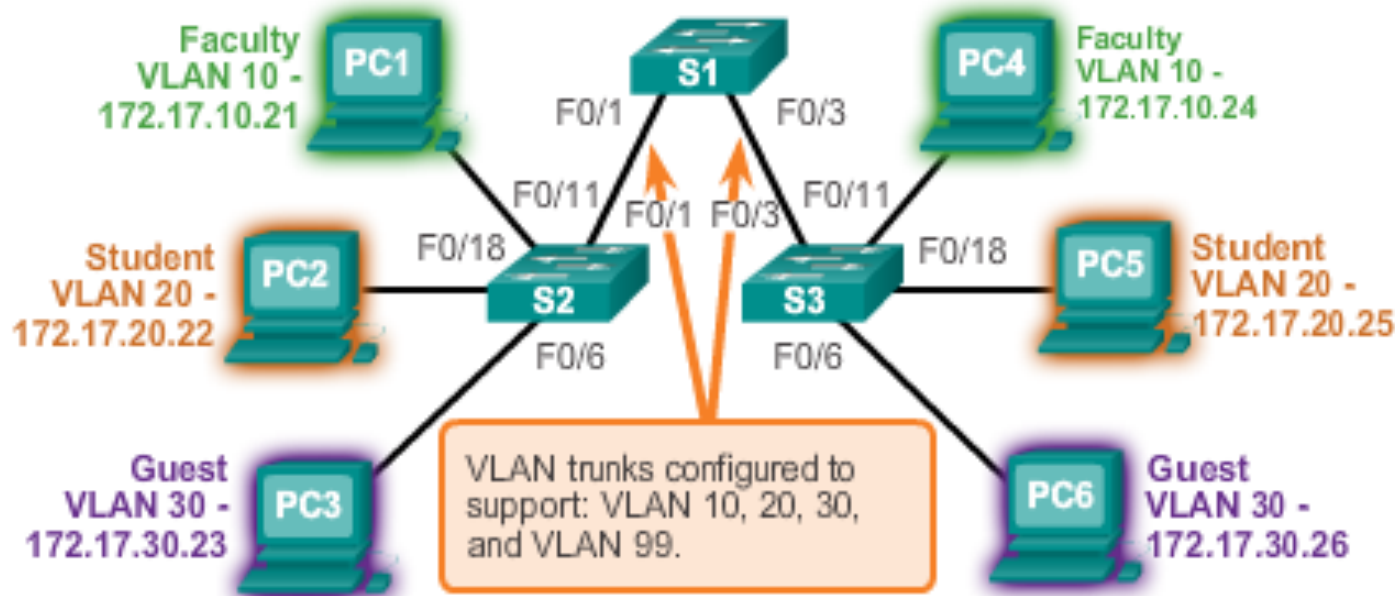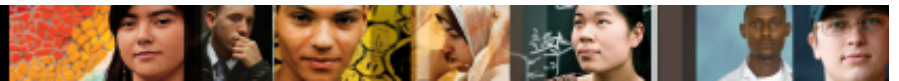ARCHITECTURES

Tagging Ethernet Frames for VLAN Identification

Trunk Operation

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.

Faculty
VLAN 10 -
172.17.10.21
PC1

S1
F0/1   F0/3

Faculty
VLAN 10 -
172.17.10.24
PC4

F0/11   F0/1 F0/3   F0/11

Student
VLAN 20 -
172.17.20.22
PC2

F0/18

S2

F0/1 F0/3

S3

F0/18

PC5
Student
VLAN 20 -
172.17.20.25

F0/6   F0/6

Guest
VLAN 30 -
172.17.30.23
PC3

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

PC6
Guest
VLAN 30 -
172.17.30.26

SWIN
BUR
* NE *

ARCHITECTURES

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

SWIN BUR NE

CENTRE FOR
ADVANCED
INTERNET
ARCHITECTURES

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
```

Introduction to DTP

- Cisco solution to automatically configure switch port state

- Dynamic Trunking Protocol (DTP) manages trunk negotiation

- Cisco proprietary protocol

- Default, enabled in Cisco Catalyst 2960 and 3560 switches

- The default DTP configuration for Cisco Catalyst 2960 and 3560 switches is dynamic auto
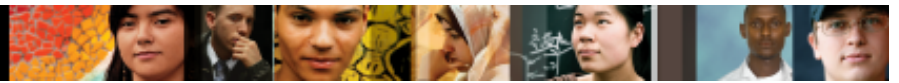
Negotiated Interface Modes

- 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**

VLAN Types
Available VLAN Types

- Data VLAN

- Default VLAN

- Native VLAN
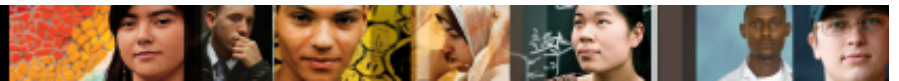
- Management VLAN

- Voice VLAN

Data and Default VLANs

Data VLAN

- Configured to Carry data traffic

- User VLANs for networked devices and computers

Default VLAN

- Default setting on unconfigured switch

- Cisco – VLAN 1

- Same features as other VLANs except it cannot be deleted or renamed

- Default – Carries all Layer 2 control traffic

Native and Management VLANs

Native VLAN

- Backwards compatibility with other switches

- Non tagged frames on an Ethernet Trunk will be assumed to belong to this VLAN
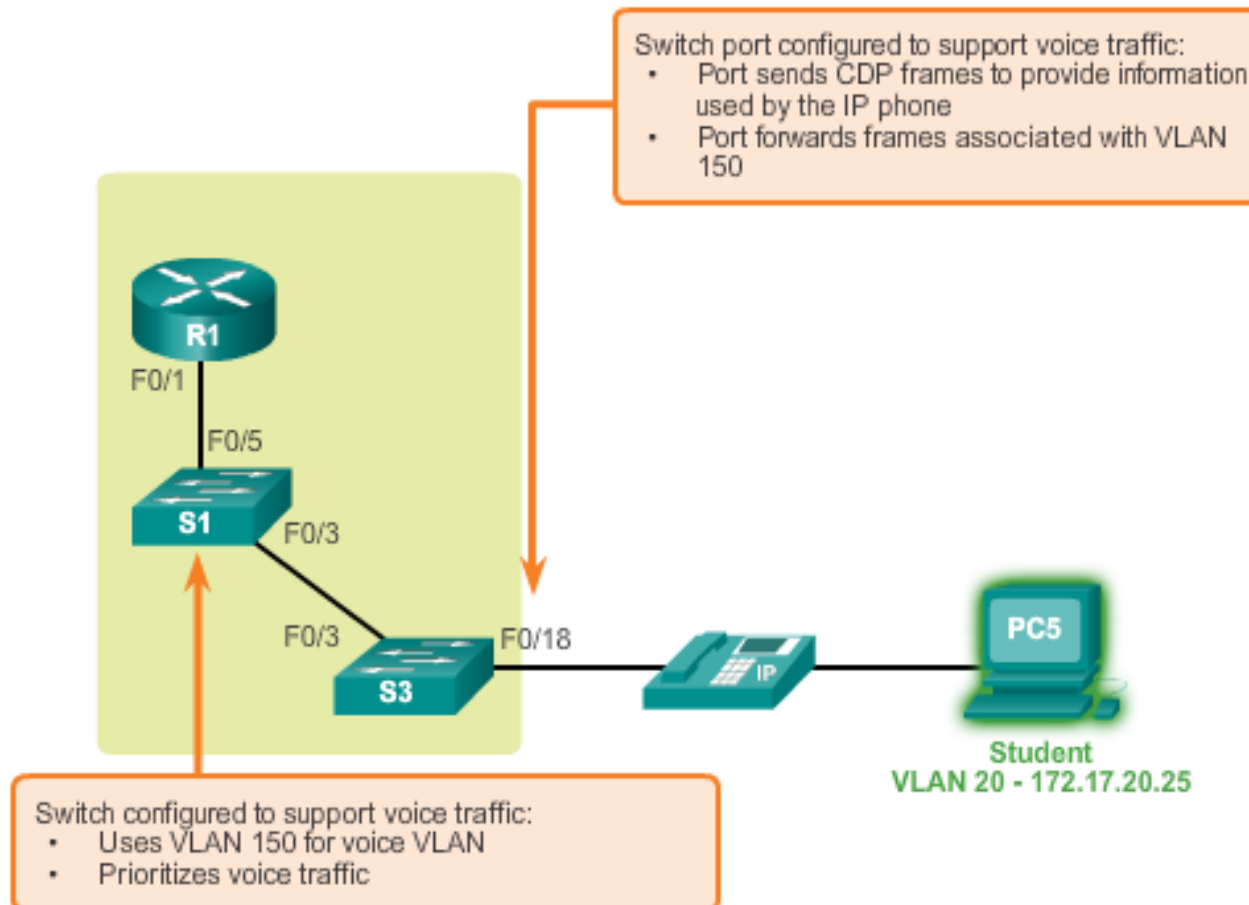
- Best practice – change from VLAN 1

Management VLAN

- Default – VLAN 1

- Assigned with IP address for network layer connectivity to switch

Voice VLANs

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

R1

F0/1

F0/5

S1   F0/3

F0/3   F0/18

S3

PC5

Student
VLAN 20 - 172.17.20.25

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

Summary

In this lecture, we covered:

- VLANs

- Intra and Inter VLAN Communications

- Creating VLANs

- VLAN Access Ports

- VLAN Trunking Ports

- DTP – Dynamic Trunking Protocol

- VLAN Types