



Chapter 3

Virtual Local Area Networks (VLANs)

Part I

CCNA3-1

Chapter 3-1

Note for Instructors

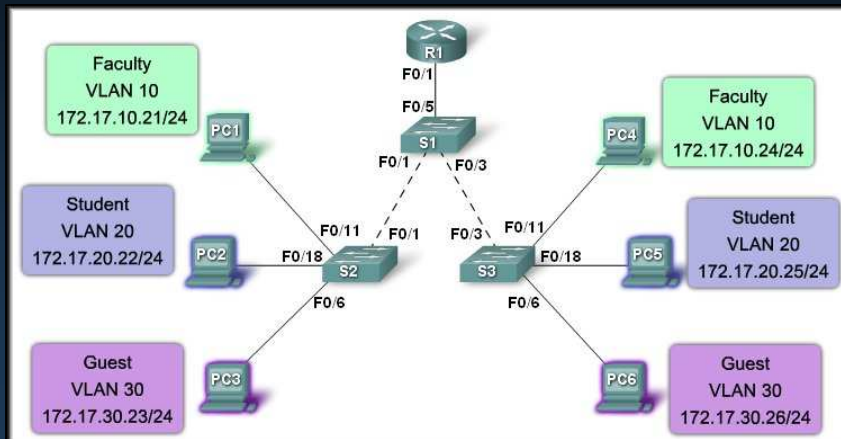
- These presentations are the result of a collaboration among the instructors at St. Clair College in Windsor, Ontario.
- Thanks must go out to Rick Graziani of Cabrillo College. His material and additional information was used as a reference in their creation.
- If anyone finds any errors or omissions, please let me know at:
 - tdame@stclaircollege.ca.

CCNA3-2

Chapter 3-1

Virtual Local Area Networks

Introducing VLANs



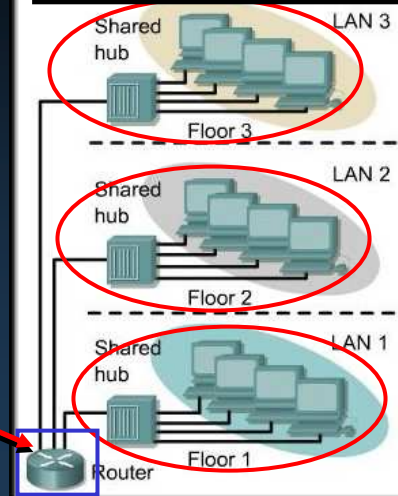
CCNA3-3

Chapter 3-1

Defining VLANs

- In **traditional** switched LANs, the physical topology is closely related to the logical topology.
- Generally, workstations must be **grouped by their physical proximity to a switch**.
- To communicate among LANs, each segment must have a **separate port** on the backbone device or a connection to a common backbone.

Separate Broadcast Domains



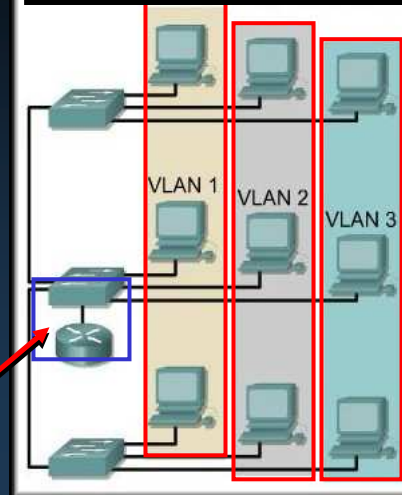
CCNA3-4

Chapter 3-1

Defining VLANs

- VLANs provide segmentation based on **broadcast domains**.
- *VLANs logically segment switched networks based on the functions, project teams, or applications of the organization regardless of the physical location or connections to the network.*
- Communication among VLANs still require a router. **BUT, only one physical connection** will handle all routing.

Separate Broadcast Domains



CCNA3-5

Chapter 3-1

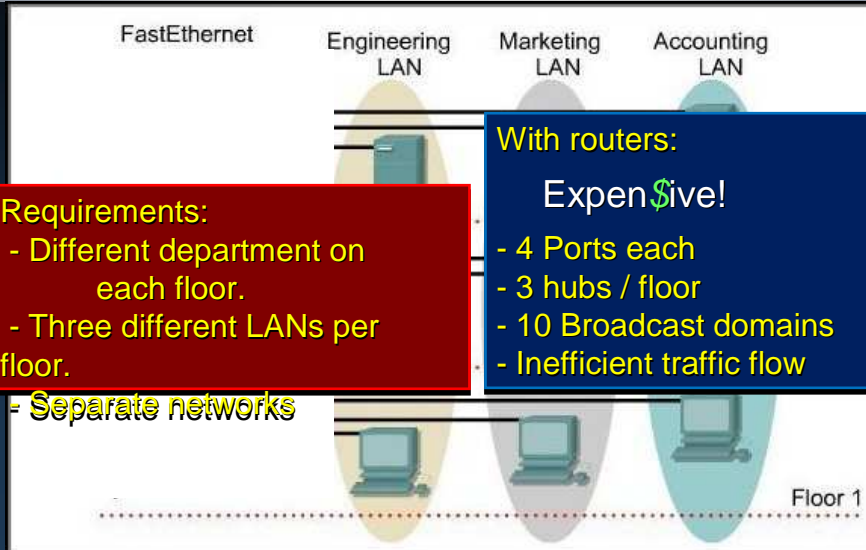
Defining VLANs

- VLANs are created to provide segmentation services traditionally provided by physical routers in LAN configurations.
 - They address:
 - Scalability
 - Security
 - Network Management
 - Broadcast Filtering
 - Traffic Flow Management
 - Switches **may not forward** any traffic between VLANs, as this would violate the integrity of the VLAN broadcast domain.
 - Traffic **must be routed** between VLANs.

CCNA3-6

Chapter 3-1

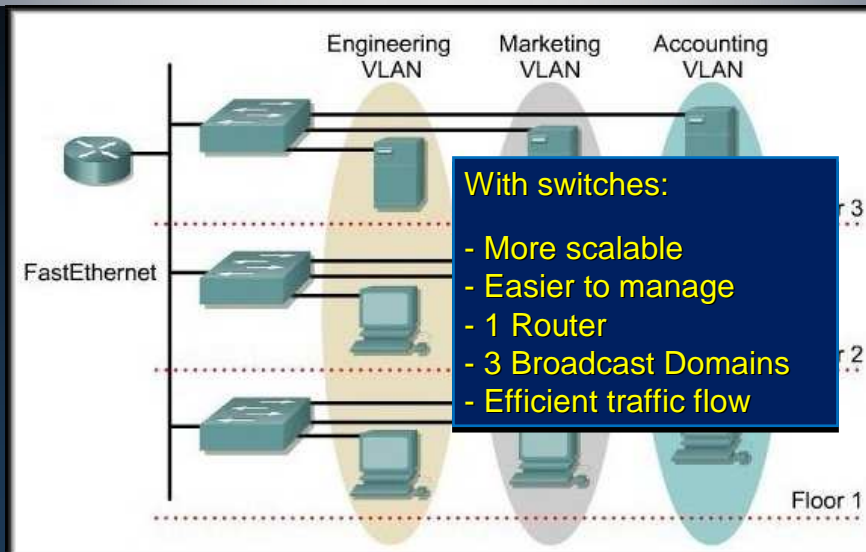
What Does This Mean?



CCNA3-7

Chapter 3-1

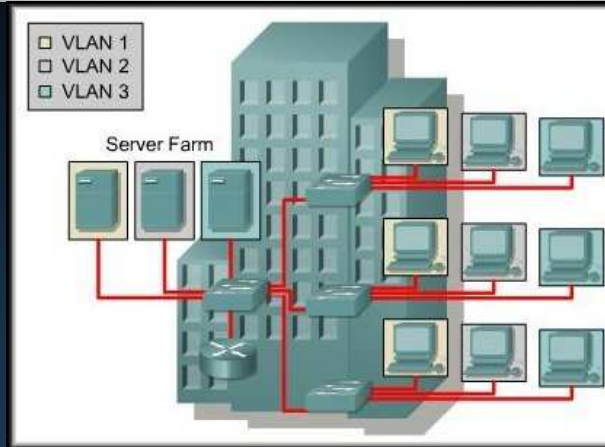
What Does This Mean?



CCNA3-8

Chapter 3-1

Defining VLANs

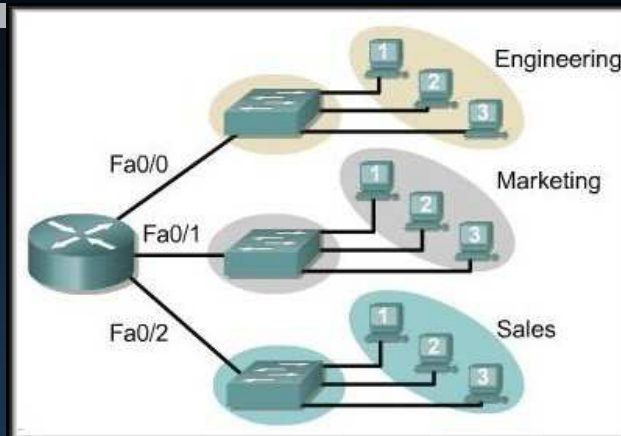


- A VLAN, then, is a broadcast domain (IP Subnet) created by one or more switches.

CCNA3-9

Chapter 3-1

Defining VLANs

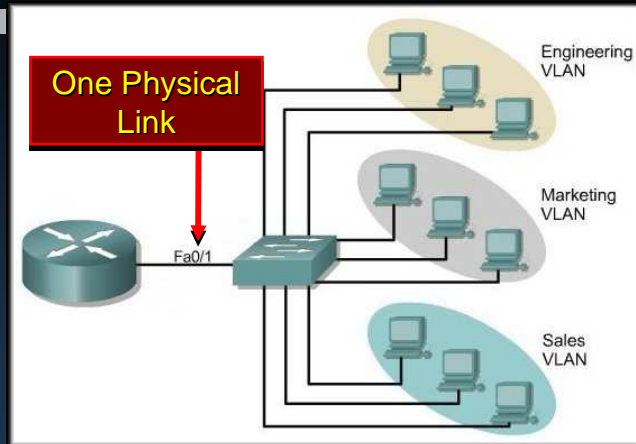


- The above design shows 3 separate broadcast domains created using one router with 3 ports and 3 switches.
- The router filters the broadcasts for each LAN.

CCNA3-10

Chapter 3-1

Defining VLANs



- A better design still creates the 3 separate broadcast domains but only requires 1 switch.
- The router provides broadcast filtering over a **single link**.

CCNA3-11

Chapter 3-1

Defining VLANs

- **A VLAN allows:**
 - Creation of groups of logically networked devices.
 - The devices to act as if they are on their own independent network.
 - The devices can share a common infrastructure.
- **Each VLAN is a separate broadcast domain.**
 - Broadcast traffic is controlled.
- **Each VLAN is a separate IP subnet.**
 - To communicate among VLANs, you must use a router (**MUCH** more later).

CCNA3-12

Chapter 3-1

Benefits of VLANs

- **Security:**
 - Groups with specific security needs are isolated from the rest of the network.
- **Cost Reduction:**
 - Need for expensive hardware upgrades is reduced.
 - Better use of existing bandwidth and links.
- **Higher Performance:**
 - Dividing large, flat Layer 2 networks into separate broadcast domains reduces unnecessary traffic on each new subnet.

Benefits of VLANs

- **Broadcast Storm Mitigation:**
 - Dividing a network into VLANs prevents a broadcast storm from propagating to the whole network.
- **Improved IT Staff Efficiency:**
 - Easier to manage the network because users with similar network requirements share the same VLAN.
- **Simpler Project or Application Management:**
 - Having separate functions makes working with a specialized application easier. For example, an e-learning development platform for faculty.

VLAN ID Ranges

- When configured, the number that is assigned to the VLAN becomes the VLAN ID.
- The numbers to be assigned are divided into two different ranges:
 - **Normal Range:** 1 – 1005
 - **Extended Range:** 1006 - 4096
- Each range has its own characteristics.

VLAN ID Ranges

- **Normal Range:** 1 – 1005
 - Used in small- and medium-sized business and enterprise networks.
 - IDs 1002 – 1005: Token Ring and FDDI VLANs.
 - **IDs 1 and 1002 to 1005 are automatically created and cannot be removed.**
 - Configurations are stored within a VLAN database file, called **vlan.dat**, located in the **flash** memory of the switch.
 - The VLAN Trunking Protocol (**VTP**), which helps manage VLAN configurations between switches, **can only learn normal range VLANs** and stores them in the VLAN database file. **(Chapter 4)**

VLAN ID Ranges

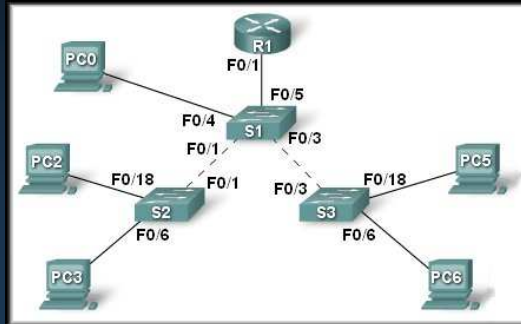
- **Extended Range:** 1006 – 4096
 - Enable service providers to extend their infrastructure to a greater number of customers.
 - Some global enterprises could be large enough to need extended range VLAN IDs.
 - Support fewer VLAN features than normal range VLANs.
 - Are saved in the running configuration file – not the vlan.dat file.
 - **VTP does not learn extended range VLANs.**

Types of VLANs

- **Traditionally, two methods of implementing VLANs:**
 - **Static or Port-Based:**
 - Ports on a switch are assigned to a specific VLAN.
 - **Dynamic:**
 - VLANs created by accessing a Network Management server. The MAC address/VLAN ID mapping is set up by the Network Administrator and the server assigns a VLAN ID when the device contacts it.
- *Today, there is essentially one method of implementing VLANs: **Port-Based.***

Types of Port-Based VLANs

- Defined by the type of traffic they support or by the functions they perform.
 - **Data** VLAN.
 - **Default** VLAN.
 - **Native** VLAN.
 - **Management** VLAN.
 - **Voice** VLAN.

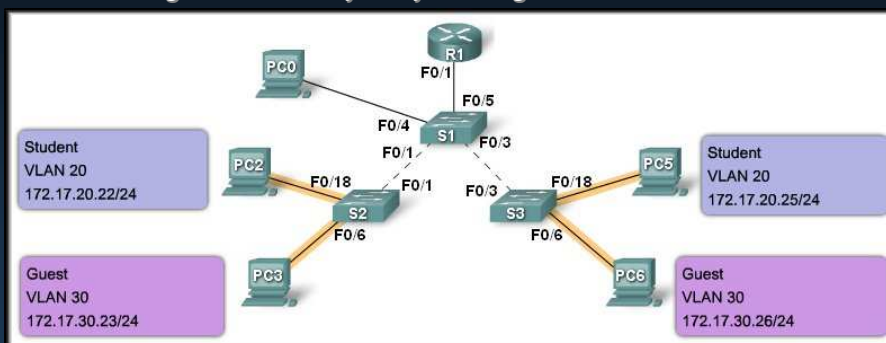


CCNA3-19

Chapter 3-1

Types of Port-Based VLANs

- **Data VLAN:**
 - Configured to carry only user-generated traffic.

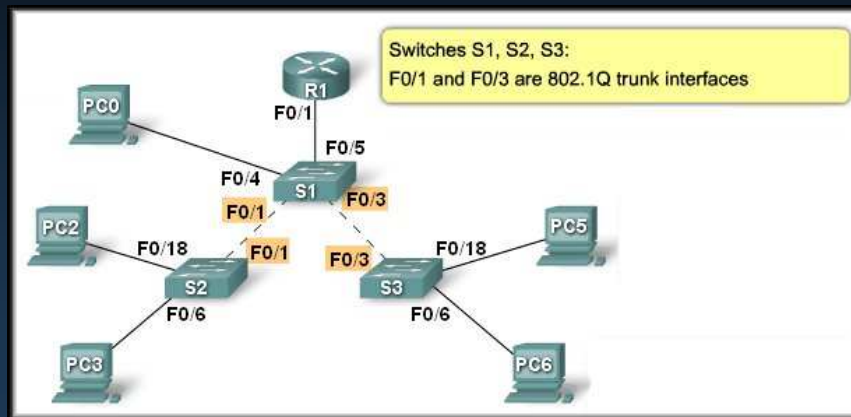


CCNA3-20

Chapter 3-1

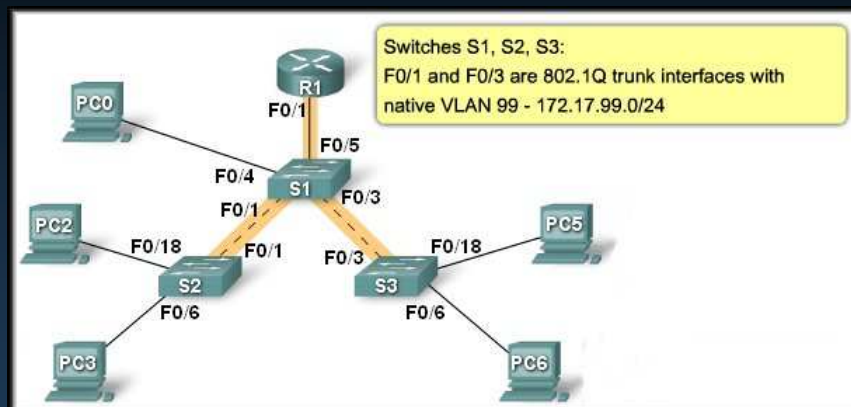
Types of Port-Based VLANs

- **Default VLAN:**
 - The default VLAN for Cisco switches is VLAN 1.



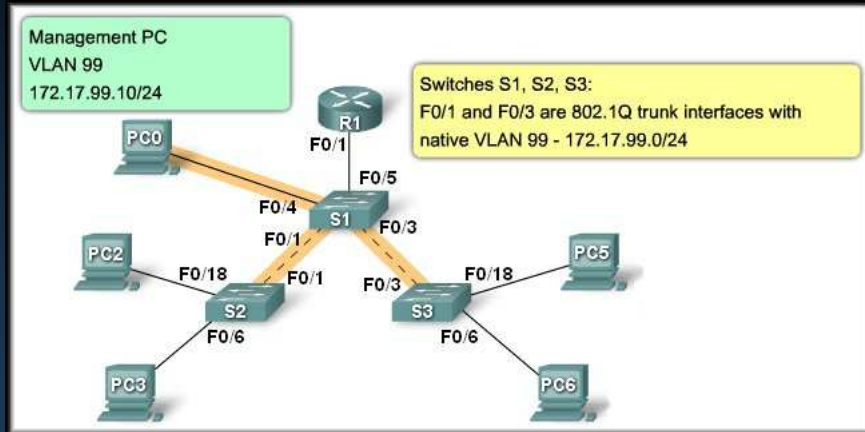
Types of Port-Based VLANs

- **Native VLAN:**



Types of Port-Based VLANs

- **Management VLAN:**



CCNA3-23

Chapter 3-1

Types of Port-Based VLANs

- **Voice VLANs:**

- Voice-over-IP (VoIP) traffic 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 milliseconds** (ms) across the network.
- The details of how to configure a network to support VoIP are beyond the scope of the course, but it is useful to summarize how a voice VLAN works between **a switch, a Cisco IP phone, and a computer.**

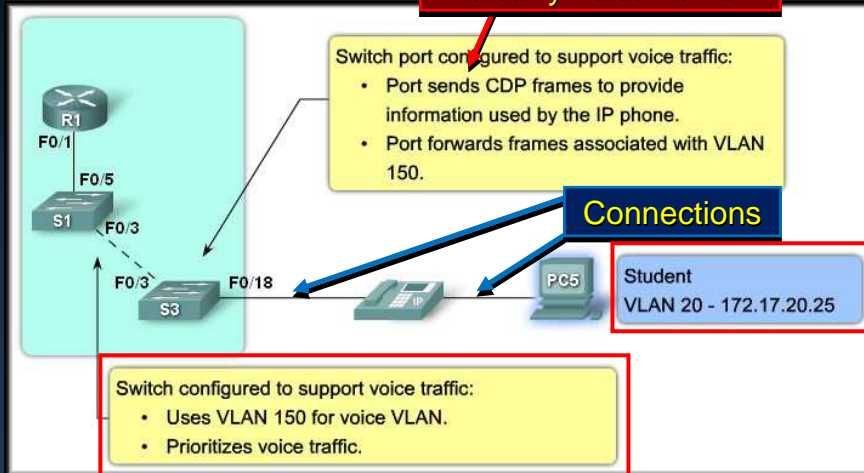
CCNA3-24

Chapter 3-1

Types of Port-Based VLANs

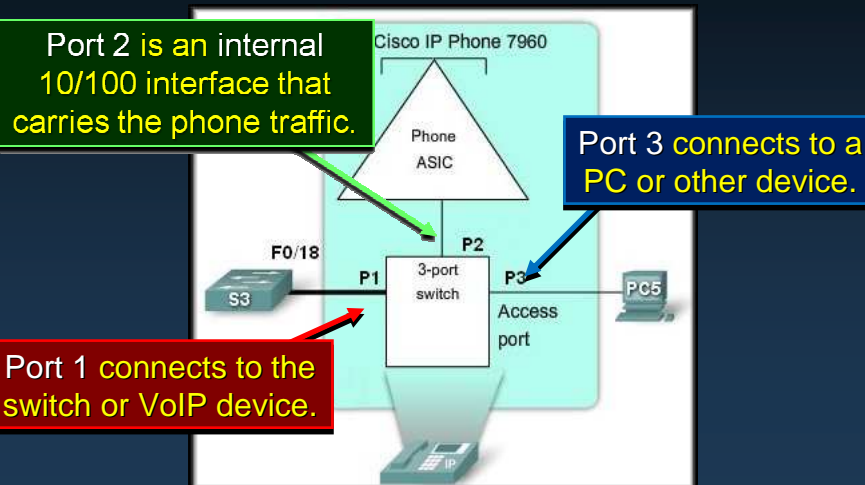
- **Voice VLANs:**

VLAN 150 is designed to carry voice traffic.



Types of Port-Based VLANs

- **Voice VLANs:** A Cisco IP Phone is a switch.



Types of Port-Based VLANs

- **Voice VLANs:** A Cisco IP Phone is a switch.

Switch S3 is configured to carry voice traffic on VLAN 150 and data traffic on VLAN 20.

Sending:

Phone tags voice traffic with VLAN 150 and sends data traffic untagged. The switch will tag the data traffic for VLAN 20.

MORE on the tagging process

later...

Receiving:

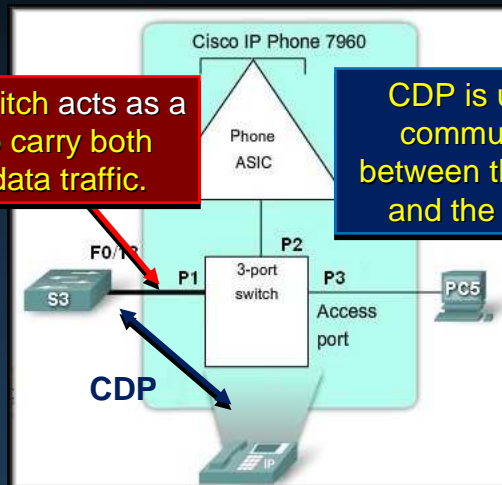
Phone acts on voice traffic and removes the tag for data traffic destined for the PC.

Types of Port-Based VLANs

- **Voice VLANs:** A Cisco IP Phone is a switch.

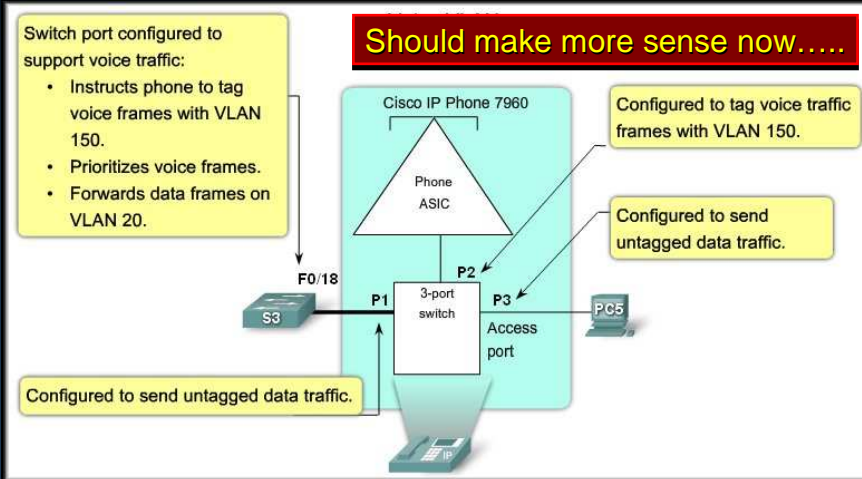
Link to the switch acts as a trunk link to carry both voice and data traffic.

CDP is used to communicate between the switch and the phone.



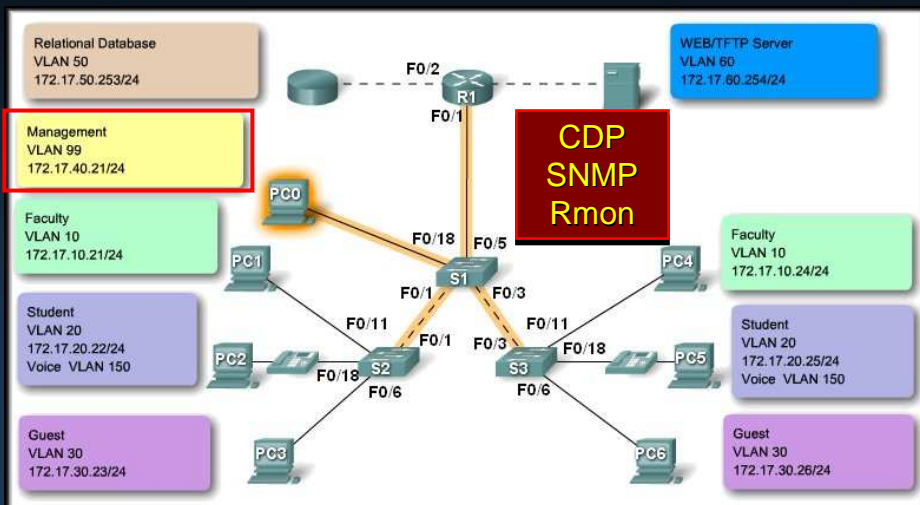
Types of Port-Based VLANs

- Voice VLANs:**



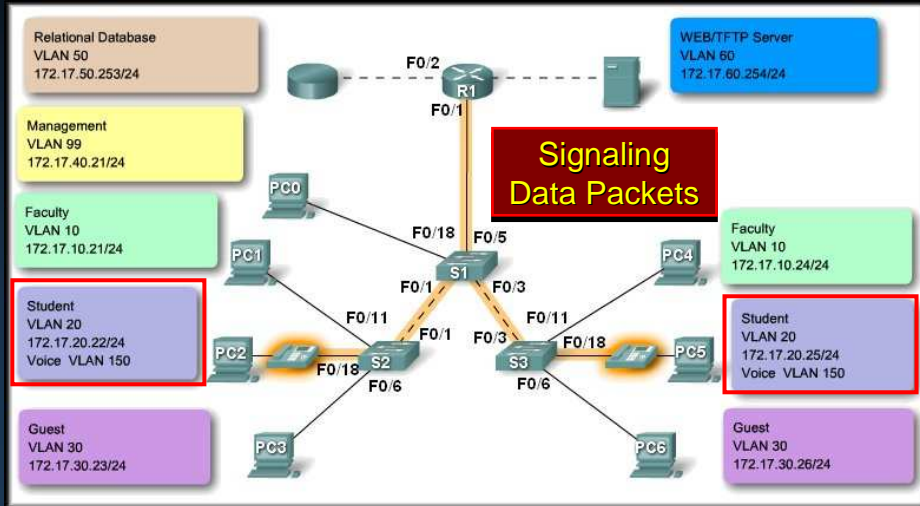
Network Traffic Types

Management Traffic



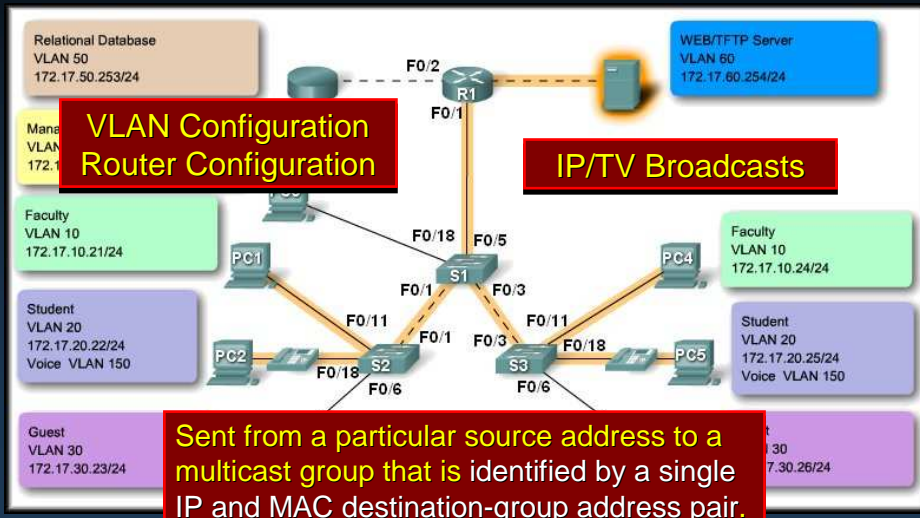
Network Traffic Types

IP Telephony Traffic



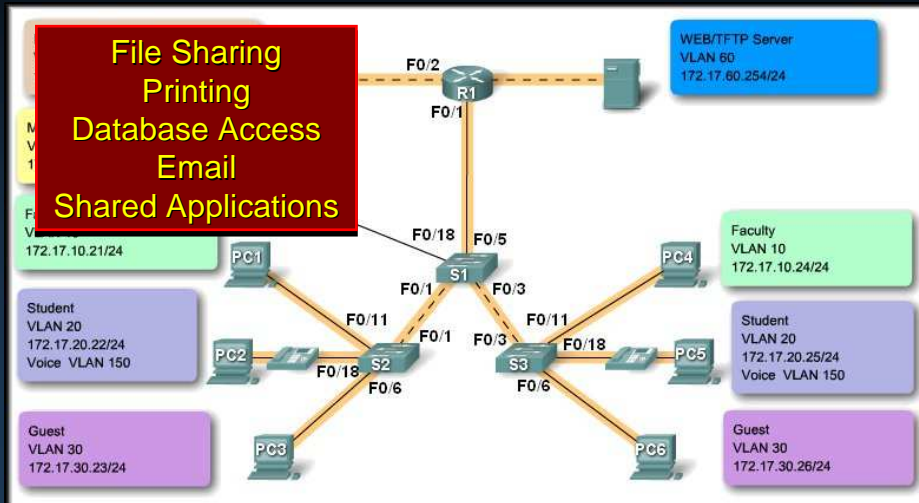
Network Traffic Types

IP Multicast Traffic



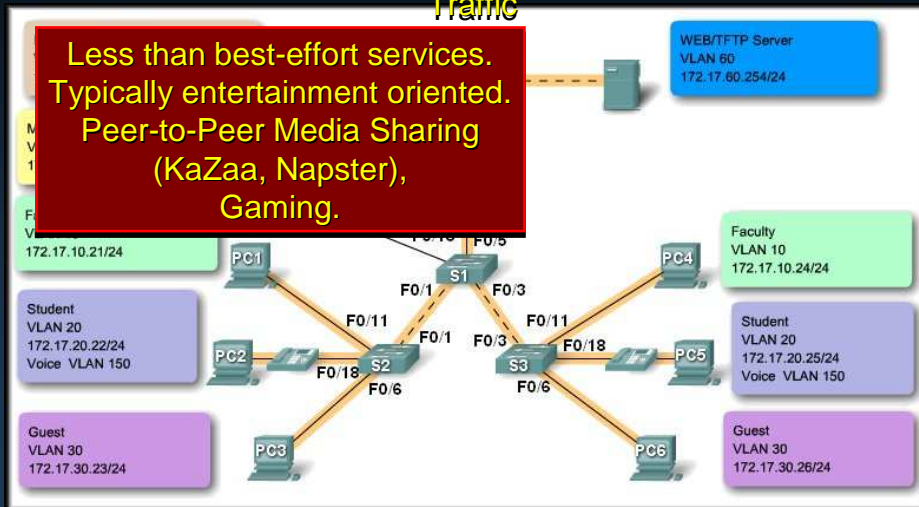
Network Traffic Types

Normal Data Traffic



Network Traffic Types

Scavenger Class Traffic



Switch Port Membership Modes

- **Switch Ports:**
 - **Layer 2-only interfaces** associated with a physical port.
 - Used for managing the physical interface and associated Layer 2 protocols.
 - **Do not handle routing or bridging.**
 - Can belong to **one or more** VLANs.
- **Configuring VLANs:**
 - Must assign a VLAN number.
 - Can configure a port specifying:
 - The type of traffic.
 - The VLANs to which it belongs.

Switch Port Membership Modes

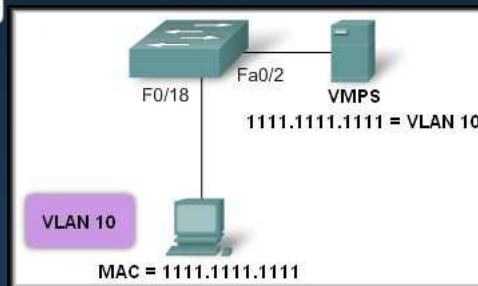
- **Static VLAN:**
 - Ports on a switch are manually assigned to a VLAN.
 - Static VLANs are configured using the Cisco CLI or a GUI Management application (e.g. Cisco Network Assistant).



Switch Port Membership Modes

- **Dynamic VLAN:**

- Configured using a special server called a VLAN Membership Policy Server (**VMPS**).
- Assign switch ports to VLANs based on the source MAC address of the device connected to the port.
- Benefit is that moving a user to a different port on a switch or to a new switch, the user is assigned to the proper VLAN dynamically.
- **Not widely used.**



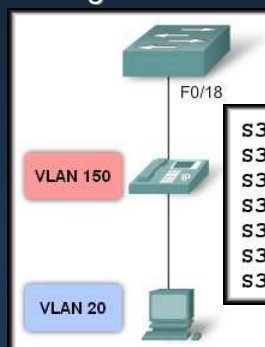
CCNA3-37

Chapter 3-1

Switch Port Membership Modes

- **Voice VLAN:**

- A port is configured to be in voice mode so that it can support an IP phone.
- Before you configure a voice VLAN on the port, you first configure a VLAN for voice and a VLAN for data.



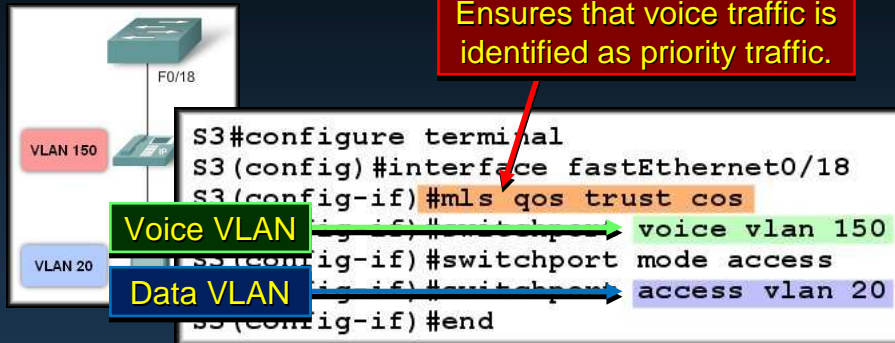
```
S3#configure terminal
S3(config)#interface fastEthernet0/18
S3(config-if)#mls qos trust cos
S3(config-if)#switchport voice vlan 150
S3(config-if)#switchport mode access
S3(config-if)#switchport access vlan 20
S3(config-if)#end
```

CCNA3-38

Chapter 3-1

Switch Port Membership Modes

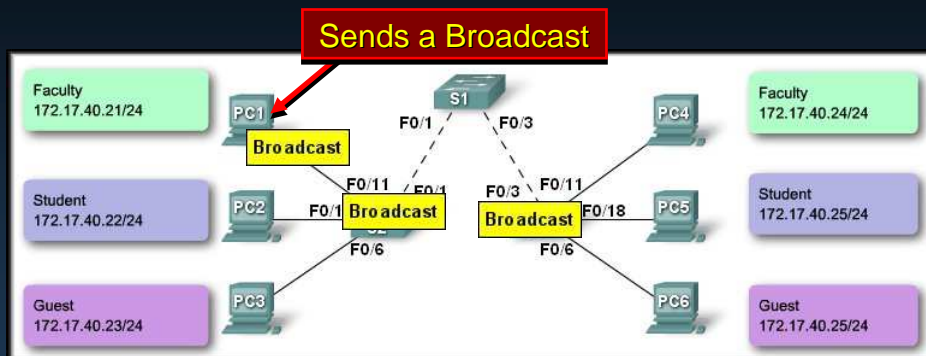
- Voice VLAN:



Remember that the entire network must be set up to prioritize voice traffic. You cannot just configure the switch port.

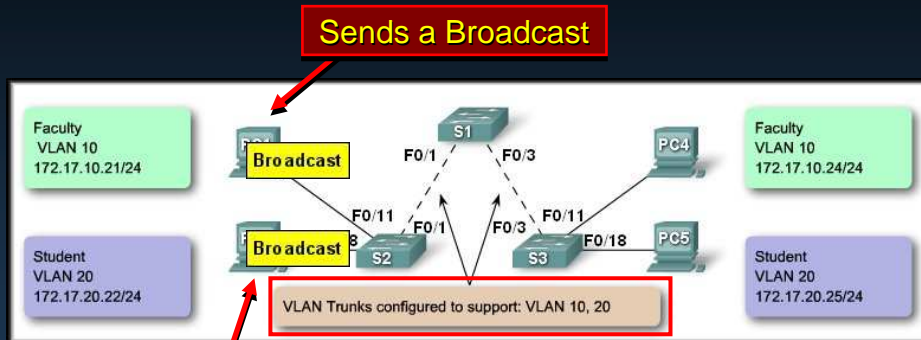
Controlling Broadcast Domains with VLANs

- Network without VLANs:



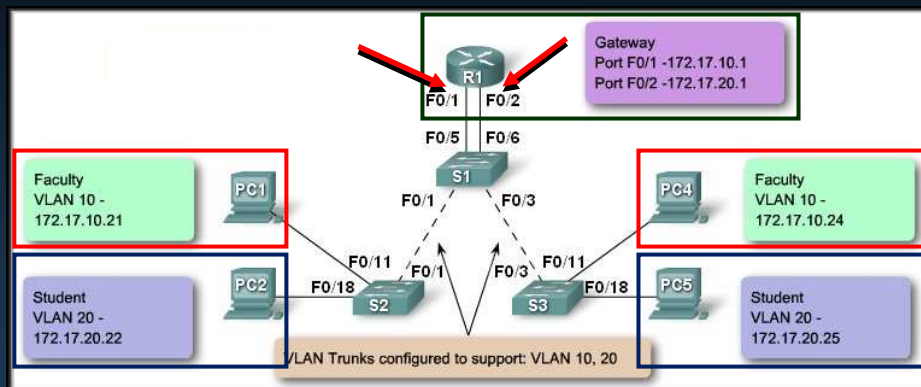
Controlling Broadcast Domains with VLANs

- Network with VLANs:



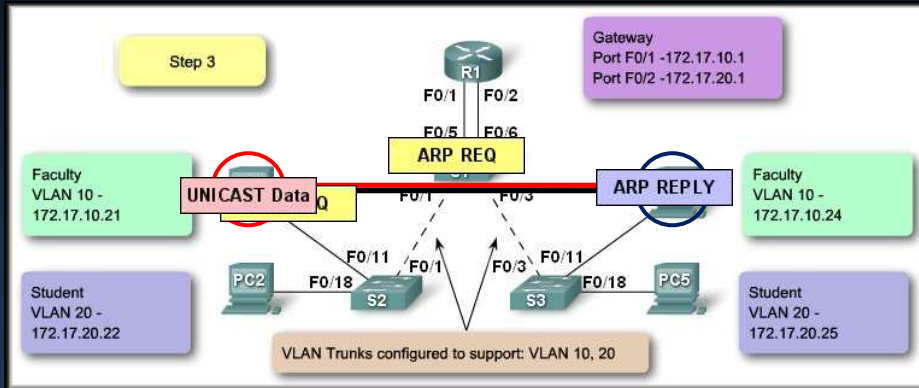
Controlling Broadcast Domains with VLANs

- Intra-VLAN Communications:



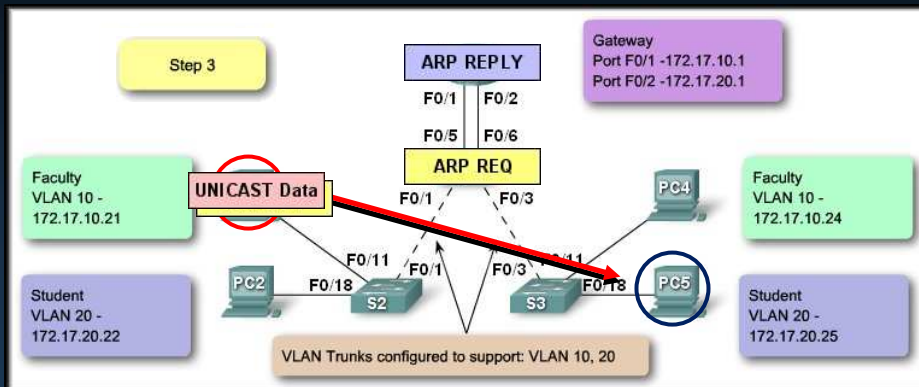
Controlling Broadcast Domains with VLANs

- Intra-VLAN Communications:



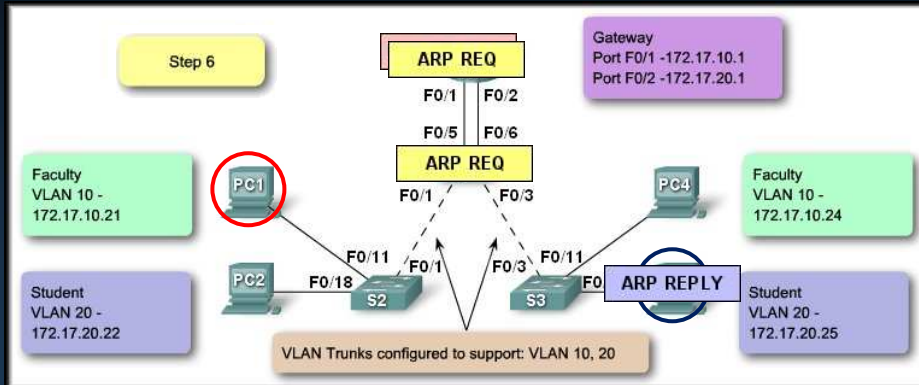
Controlling Broadcast Domains with VLANs

- Intra-VLAN Communications:



Controlling Broadcast Domains with VLANs

- **Intra-VLAN Communications:**



CCNA3-45

Chapter 3-1

Layer 3 Switch Forwarding

- **Layer 3 Switch:**
 - A Layer 3 switch has the ability to route transmissions between VLANs.
 - The procedure is the same as described for the inter-VLAN communication using a separate router.
- **Switch Virtual interface (SVI):**
 - A logical interface (SVI) is configured for each VLAN configured on the switch.



CCNA3-46

Chapter 3-1

Layer 3 Switch Forwarding

- **Layer 3 Switch:**

SVI 10 knows about SVI 20 (the location of VLAN 20).

Contains the SVI 20 information...NOT SVI 10

