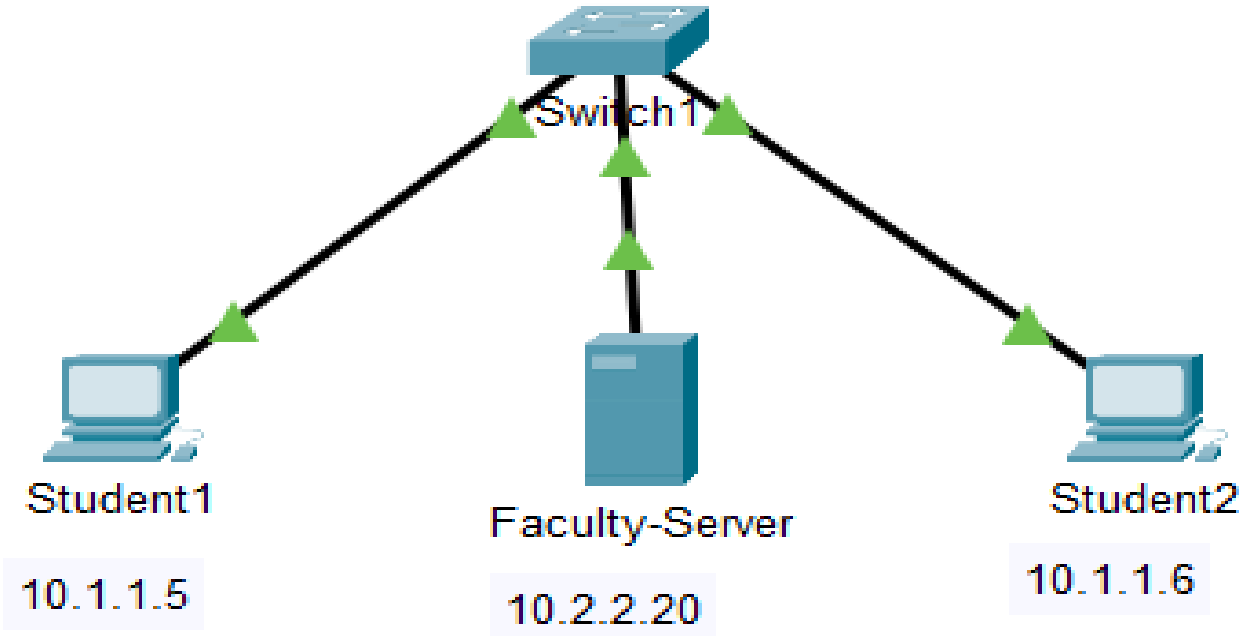
NET 363
Introduction to LANs

VLANs

Greg Brewster
DePaul University

Need for VLANs



Student1 and Student2 are on the Student Subnet 10.1.0.0/16. Faculty-Server is on Faculty Subnet 10.2.0.0/16.

BUT they all 3 connect to same switch!! How do we keep them separate (secure)? How do we support 2 IP subnets on 1 switch?

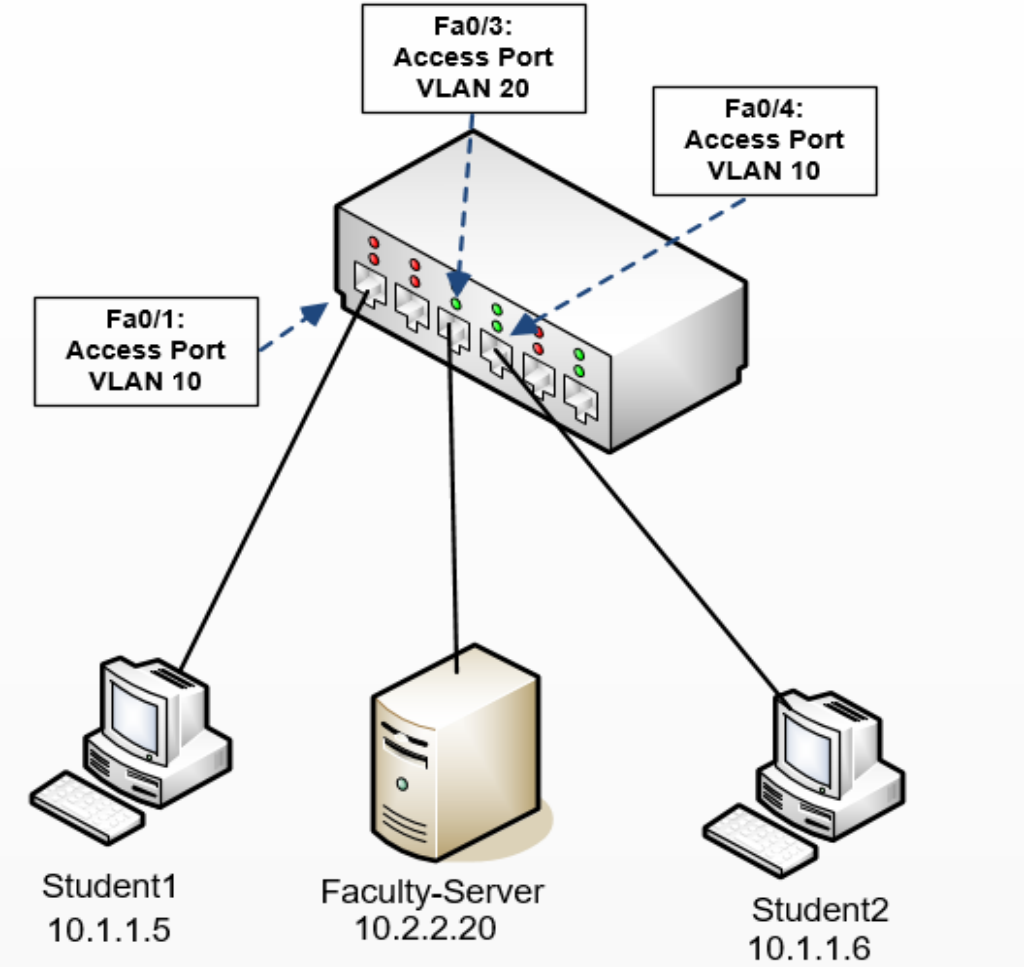
Need for VLANs

- For a basic Ethernet switch (without VLANs), all switch ports must be on the same IP subnet
  - Any Broadcast packet sent by 1 device is seen by all other devices connected to switch.
  - Every broadcast packet sent uses up bandwidth & CPU time on every connected device
  - Not much security
  - Every device can “find” any other device on the switch by sending an ARP broadcast.

VLAN Solution: Assign Switch Ports to different VLANs

- For switches that support **VLAN service**:
  - A VLAN Number is chosen for each IP subnet:
    - Student Subnet = VLAN #10
    - Faculty Subnet = VLAN #20
  - Each switch access port is configured with a single VLAN number.
  - Broadcast packets received on a VLAN port **are only sent out other ports on the same VLAN**.

VLAN Solution: Assign Switch Ports to different VLANs



Need for VLANs

- If we connect many switches together, we can get scalability problems.
- **Problem**: Broadcasts can start to consume a lot of bandwidth since each broadcast frame gets copied to every device on every switch.
- **Problem**: We may not want broadcasts sent everywhere due to security concerns
- **Solution**: Network can be split by network manager into several **Virtual LANs (VLANs)**. Each VLAN is it's own broadcast domain.

VLAN Definition

- A **Virtual LAN** is a set of switch ports that have been assigned to the same VLAN number by an admin.
- A single physical switch operates as if it were split into multiple smaller switches (one for each VLAN).
- Broadcast frames sent by any device are only forwarded out other ports on the same VLAN.
- Each VLAN is a separate IP subnet with its own set of IP addresses.

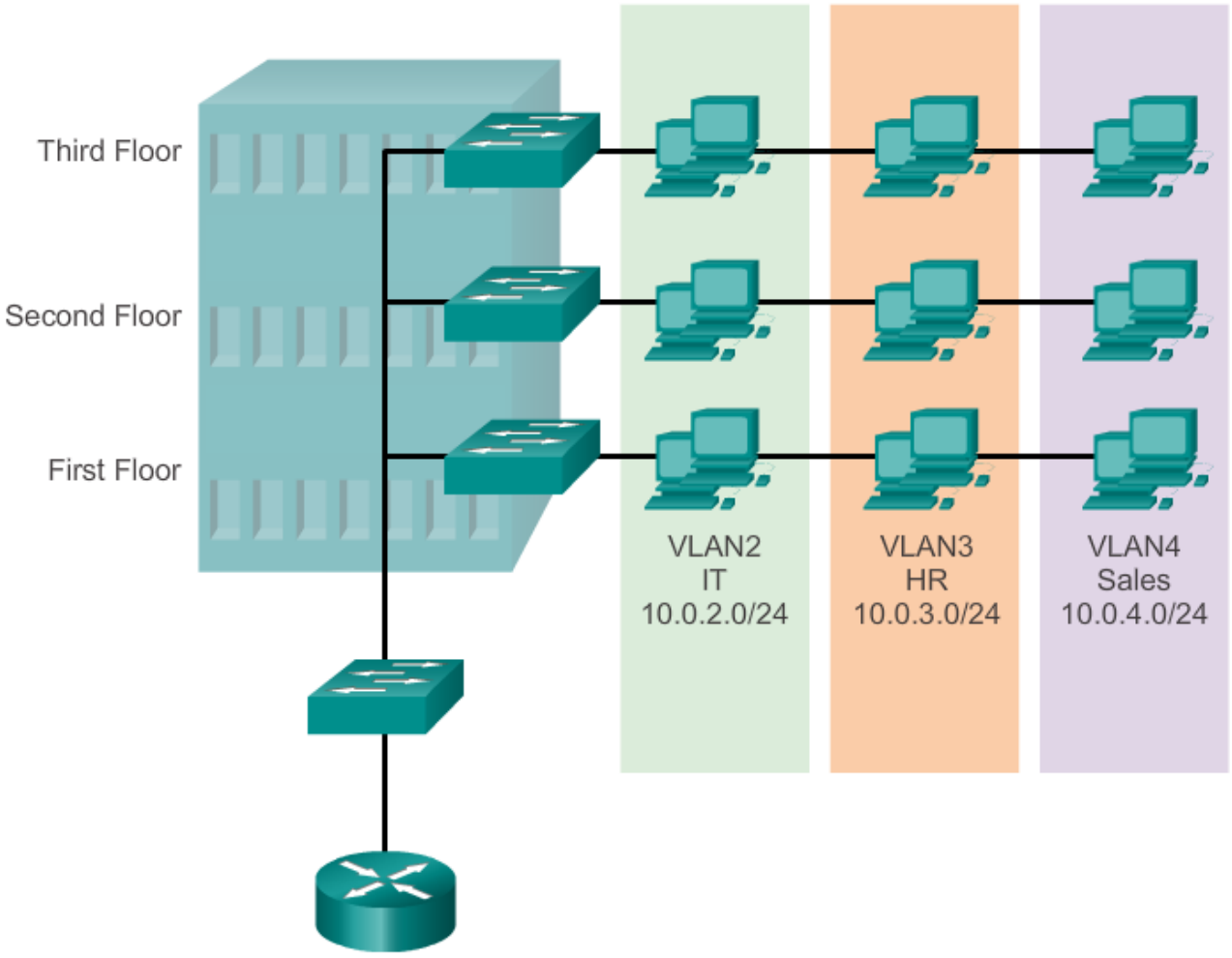
VLAN Advantages

- Better Security
  - Each device can only send packets directly to other devices on the same VLAN.
  - Packets must go through a router to get from source on one VLAN to destination on another VLAN.
  - Devices cannot use broadcasts to "find" devices on other VLANs.
- Better Performance
  - Less broadcast traffic = better performance
- Different priorities may be assigned to different VLAN IDs, giving multiple levels of service.

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.

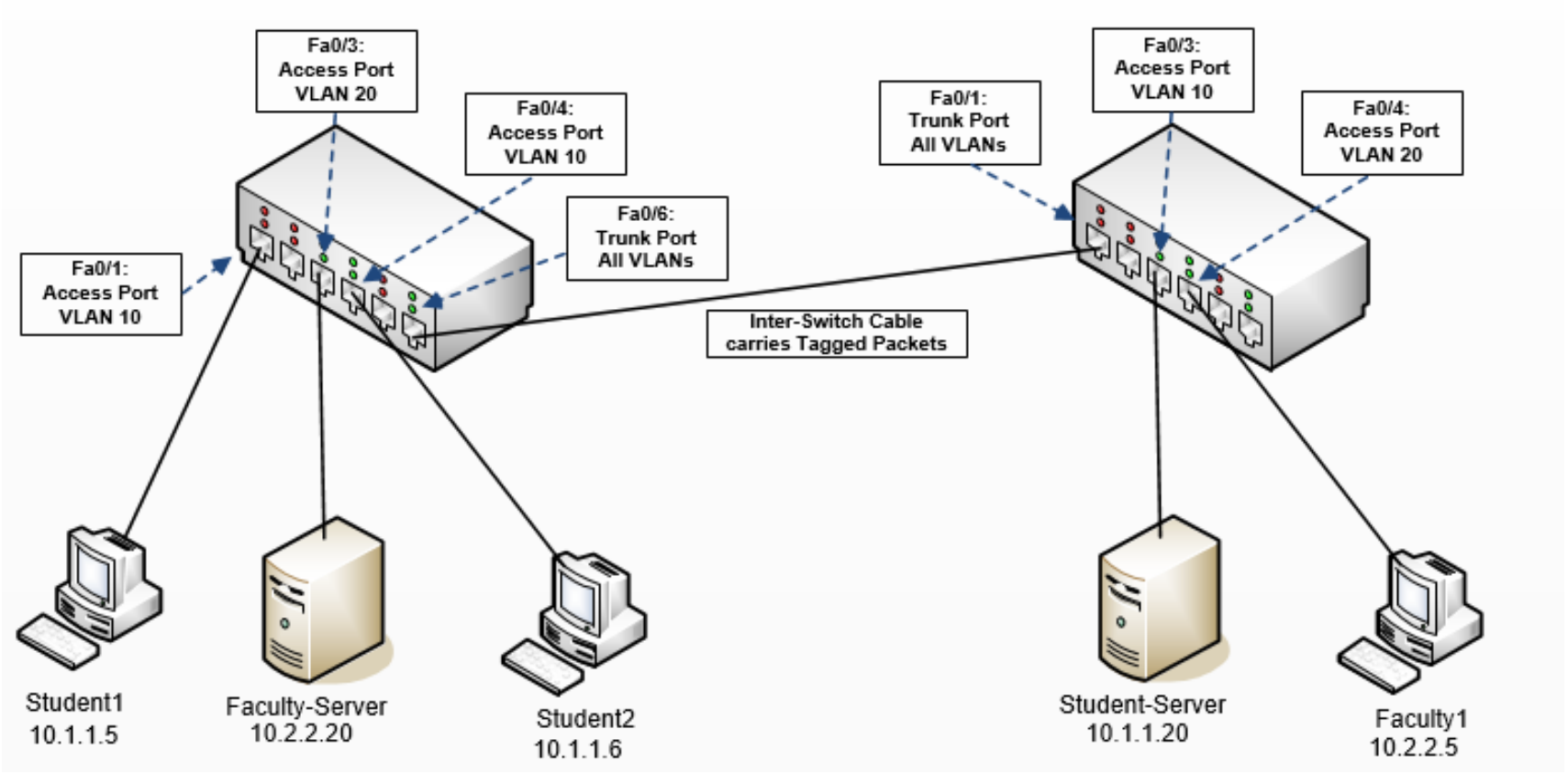
VLAN Definitions (cont.)



VLANs can span multiple switches

- What if some devices are on the same IP subnet (VLAN) but are connected to different switches?
- Answer: **Trunk Link with Tagged Packets**
  - Inter-switch data cable is called a **Trunk Link**
  - The switch ports connecting to the trunk link are **Trunk Ports**.
  - The data packets going over the trunk link are **Tagged** with their VLAN number**:**
    - When packet is sent out a Trunk Port, a 4-byte **VLAN Tag** (also called an **802.1Q subheader)** is added into the Ethernet header.
    - The VLAN number for the packet is sent in the VLAN Tag.
    - When tagged packet arrives on a Trunk Port, the VLAN Tag is removed and then the packet is only sent out ports matching its VLAN number.

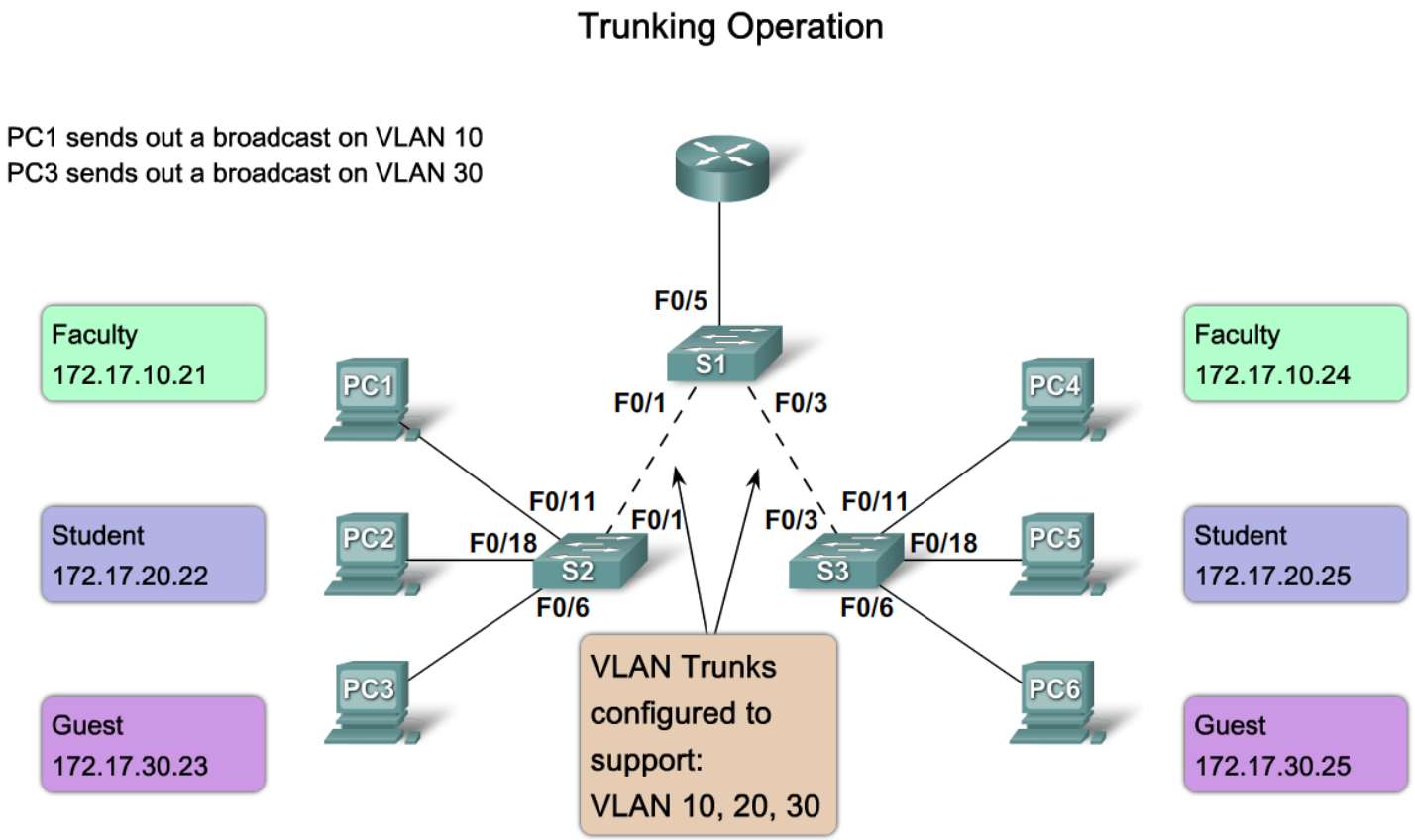
2 VLANs Spanning 2 Switches



Switchport Modes for Switch Interfaces

- Access Mode Interface
  - Connects this switch to host
  - In/out packets are not tagged
  - Interface is assigned to single VLAN (default: 1)
- Trunk Mode Interface
  - Connects this switch to another switch
  - In/out packets are tagged
  - By default: Interface allows all VLANs. But a list of Allowed VLANs can be configured.

VLAN Trunks



Each VLAN carries a separate IP subnet:

Faculty VLAN (VLAN 10): 172.17.10.0/24
Student VLAN (VLAN 20): 172.17.20.0/24
Guest VLAN (VLAN 30): 172.17.30.0/24

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`

Viewing Switch VLANs with “show vlan brief” command

VLAN 1

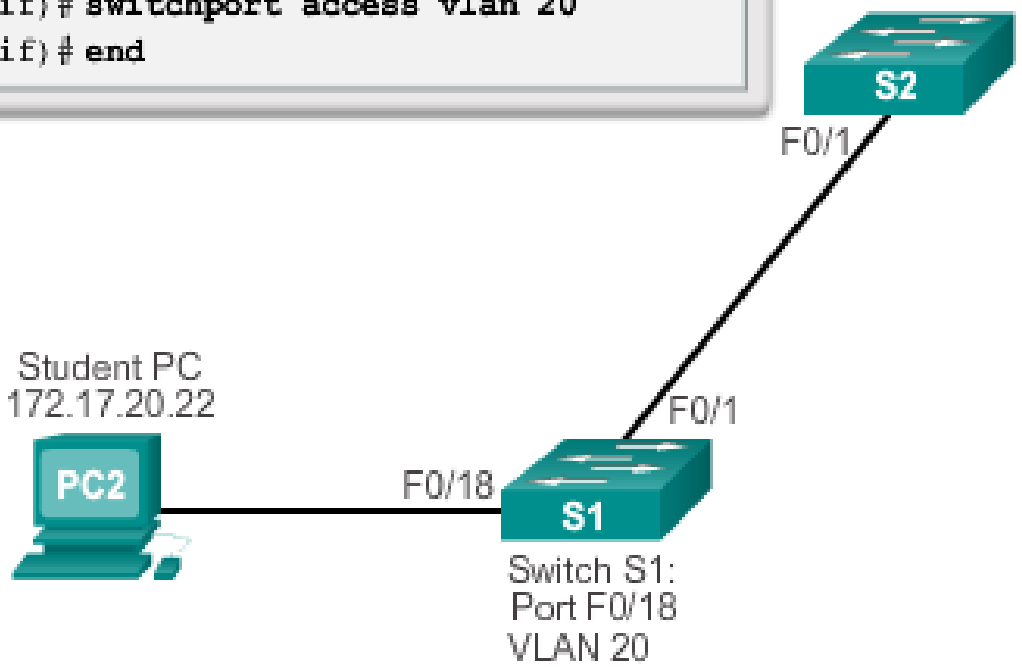
```
Switch# show vlan brief

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.

Assigning Switch Interface to a VLAN

```
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

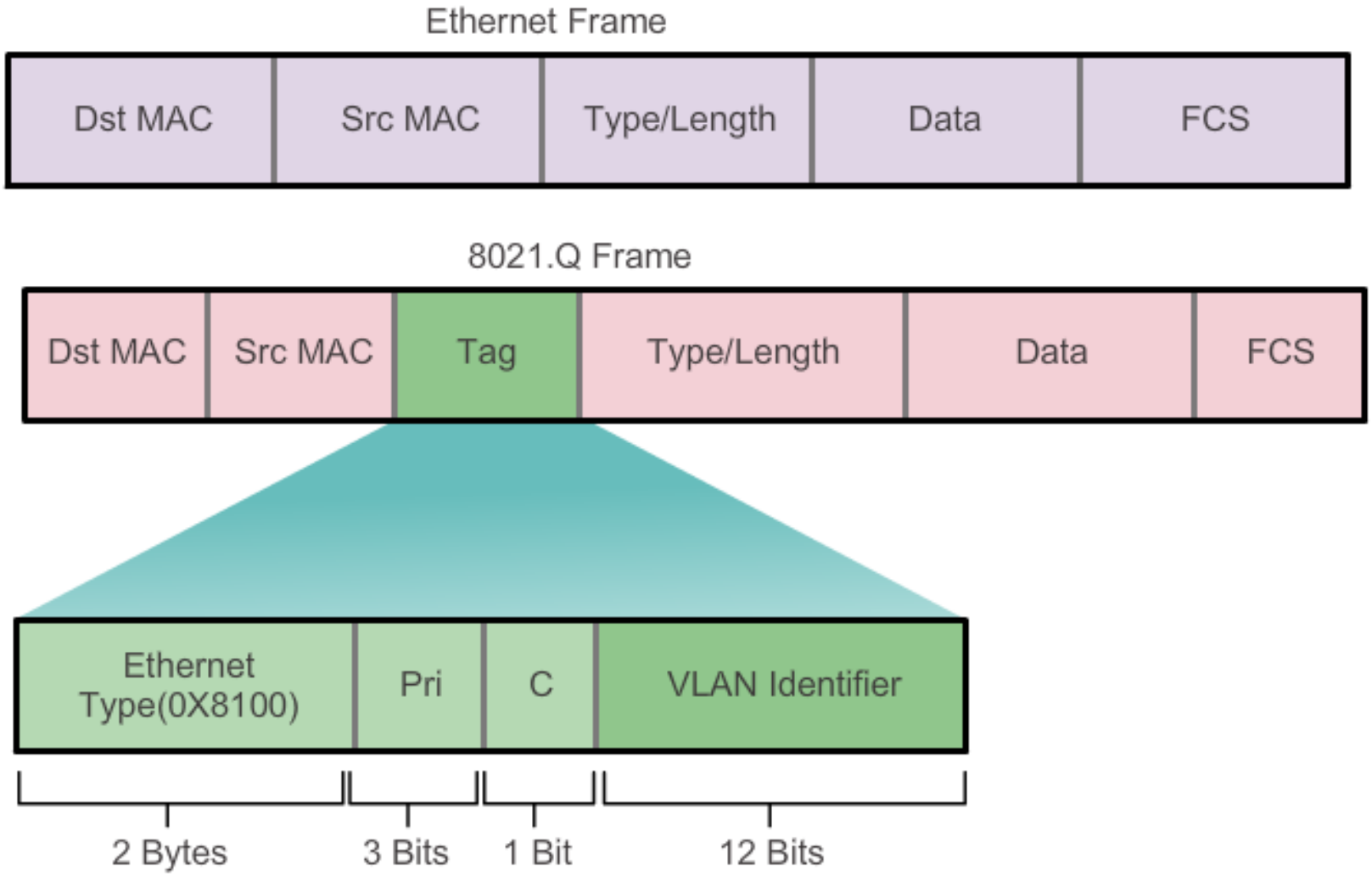
Cisco Switch IOS Commands	
Enter global configuration mode.	`S1# configure terminal`
Enter interface configuration mode.	`S1(config)# interface interface_id`
Force the link to be a trunk link.	`S1(config-if)# switchport mode trunk`
Specify a native VLAN for untagged 802.1Q trunks.	`S1(config-if)# switchport 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
```

The Native VLAN

- For each Trunk Port, a native VLAN number can be specified.
- If a packet arrives on a Trunk Port without any VLAN Tag then it is treated as a packet on the Native VLAN.
- By default, Native VLAN = 1.

Tagging Ethernet Frames for VLAN Identification



VLAN Tag Fields
IEEE 802.1q subheader

- The 802.1q subheader adds 4 bytes to Ethernet header:
  - Ethernet Type = hex 8100 (2 bytes)
    - Identifies that this is an 802.1q subheader
  - Priority (3 bits)
    - Can be used to set 8 priority levels for LAN frames
  - VLAN (12 bits)
    - This is the VLAN number for this frame

Switch Packet Priorities IEEE 802.1p

- IEEE 802.1p provides a standard way for LAN switches to use priority values carried in 802.1q subheaders.
- 8 priority classes:
  - **Priority 7:** Network-critical traffic, such as routing table update messages
  - **Priority 5,6:** Delay-sensitive traffic, such as interactive video or voice
  - **Priority 4:** Business-critical traffic, such as streaming data, SAP data, transaction processing
  - **Priority 2-3:** Less critical business data
  - **Priority 0-1:** Best-effort traffic, such as non-essential e-mails and file transfers

Dynamic Negotiated Trunk Modes

- Used when you want to allow the switch at the other end of the cable to determine whether this will be trunk interface or not.
- Dynamic Desirable Mode
  - This interface becomes a trunk if the interface at the other end of cable is set to trunk, desirable, or auto mode
- Dynamic Auto Mode
  - This interface becomes a trunk if the interface at the other end of cable is set to trunk, desirable, or auto mode.

Negotiated Interface Modes

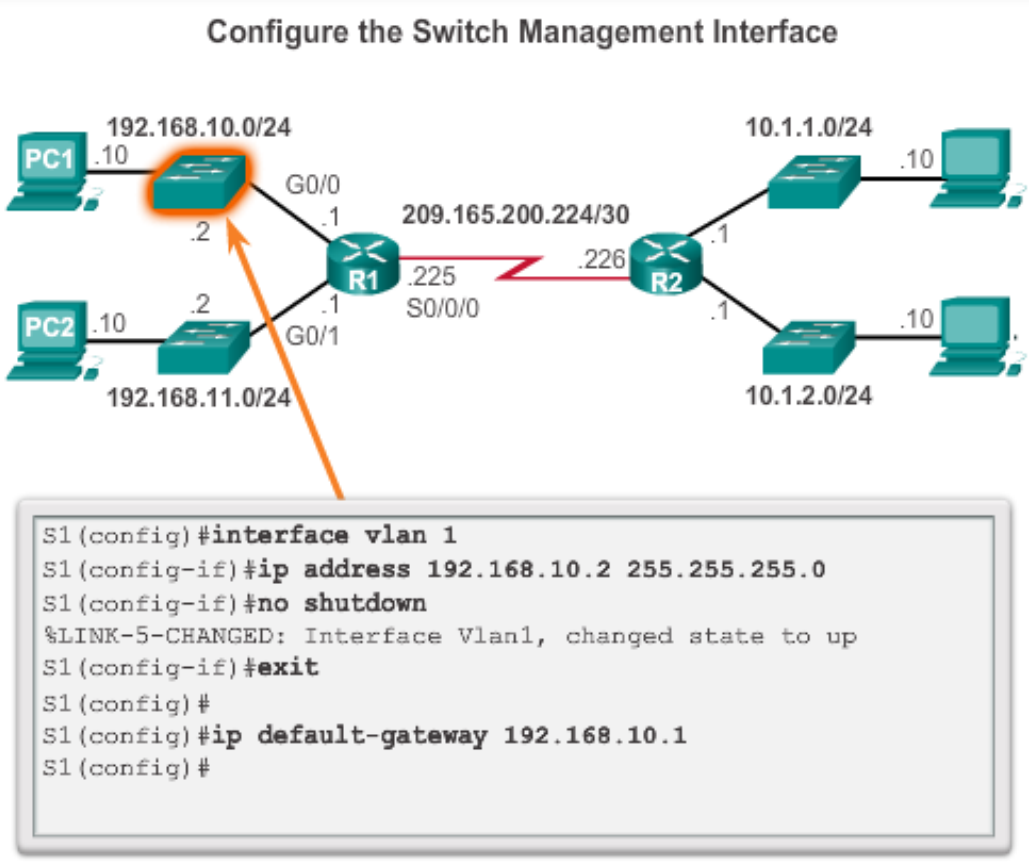
- Cisco Catalyst 2960 and 3560 support the following trunk modes:
  - Switchport mode dynamic auto
  - Switchport mode dynamic desirable
  - Switchport mode trunk
  - Switchport nonegotiate

Resulting Mode, given dynamic mode setting at each end of trunk.

	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**

Enable IP on a Switch using SVI

- Switches do not require IP addresses to forward packets.
- However, switches DO require IP addresses to enable remote management or ping/traceroute.
- The switch management IP address is assigned on a **switch virtual interface** (SVI) named VLAN1.
- The SVI IP is accessible through any switch interface.



Switch can have one SVI IP Address per VLAN.

- Each active VLAN on a switch has its own corresponding Switch Virtual Interface (SVI) which can be assigned an IP address from the IP subnet for that VLAN.
- Example: If VLAN 22 is active, then there is an SVI named "vlan22". To assign IP:
  - **S1(config)# interface vlan22**
  - **S1(config-if)# ip address 10.1.0.1 255.255.0.0**

VLAN Trunking Protocol (VTP)

- VTP is a Cisco proprietary protocol that allows switches to automatically synchronize their VLAN databases.
- All switches within VTP Domain use VTP messages to keep VLAN databases up to date.
- Used to reduce:
  - configuration errors
  - duplicate vlan names
  - security violations
- Details are not required for NET 363.