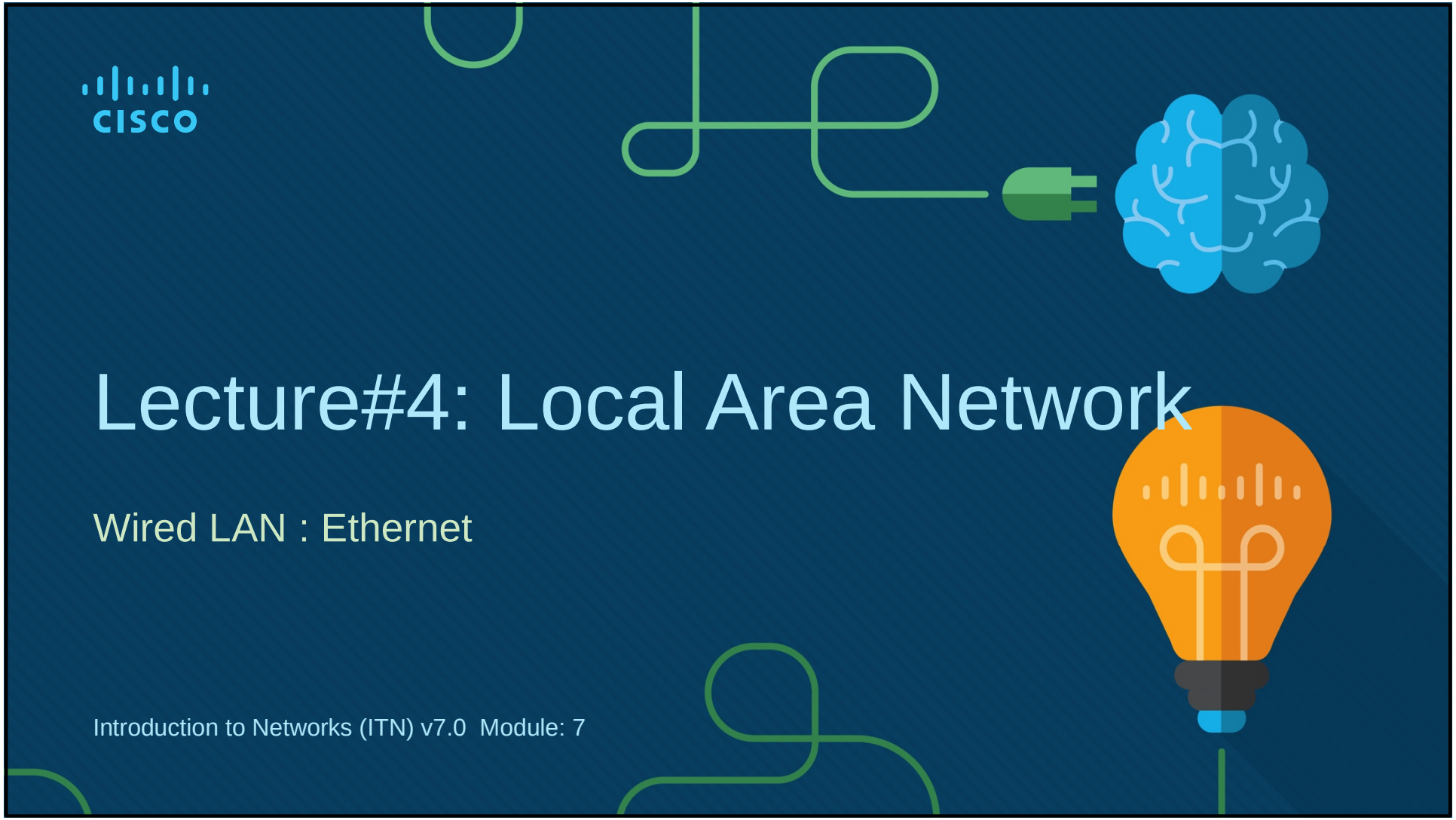
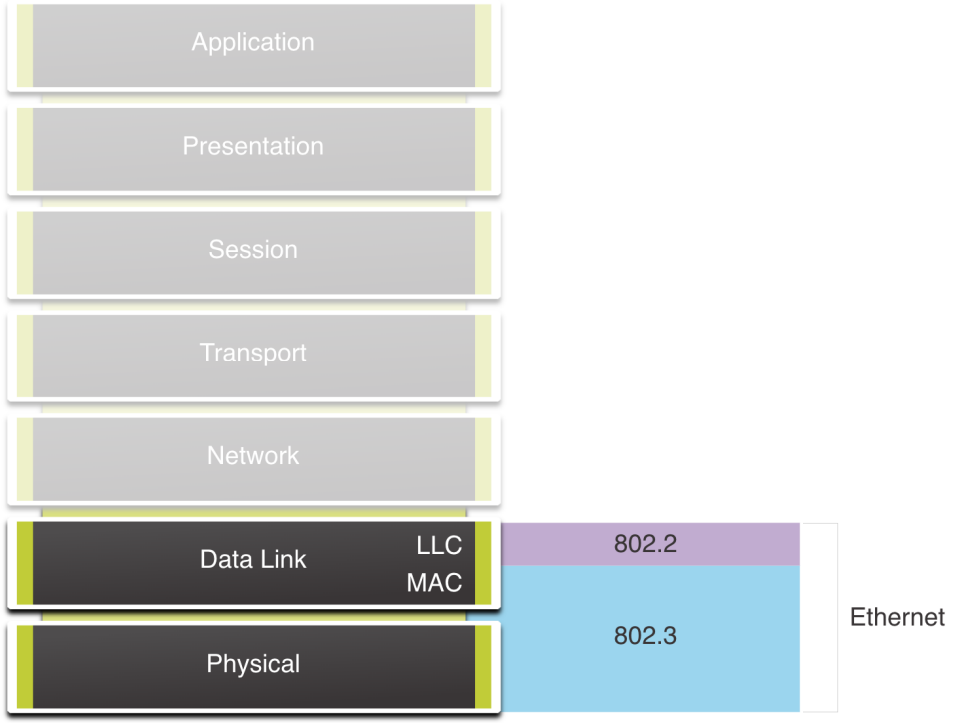

cisco
Lecture#4: Local Area Network
Wired LAN : Ethernet
Introduction to Networks (ITN) v7.0 Module: 7

4.1 Ethernet Frames

Ethernet Frames

Ethernet Encapsulation

- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.

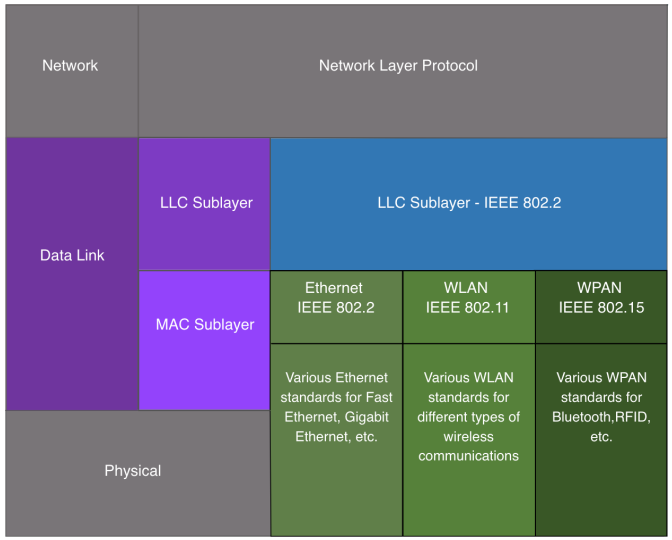


Ethernet Frames

Data Link Sublayers

The 802 LAN/MAN standards, including Ethernet, use two separate sublayers of the data link layer to operate:

- **LLC Sublayer**: (IEEE 802.2) Places information in the frame to identify which network layer protocol is used for the frame.
- **MAC Sublayer**: (IEEE 802.3, 802.11, or 802.15) Responsible for data encapsulation and media access control, and provides data link layer addressing.



Ethernet Frames

MAC Sublayer

The MAC sublayer is responsible for data encapsulation and accessing the media.

Data Encapsulation : IEEE 802.3 data encapsulation includes the following:

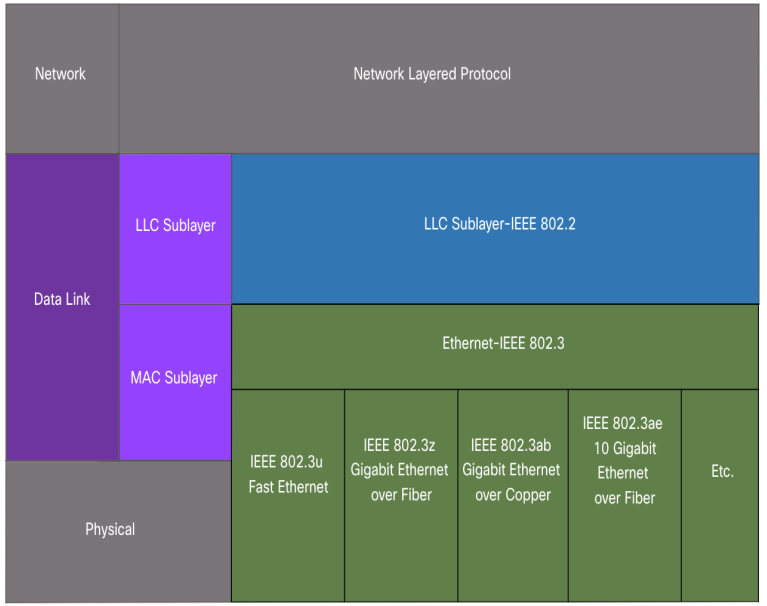
1) **Ethernet frame** - This is the internal structure of the Ethernet frame.
2) **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3) **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Ethernet Frames

MAC Sublayer

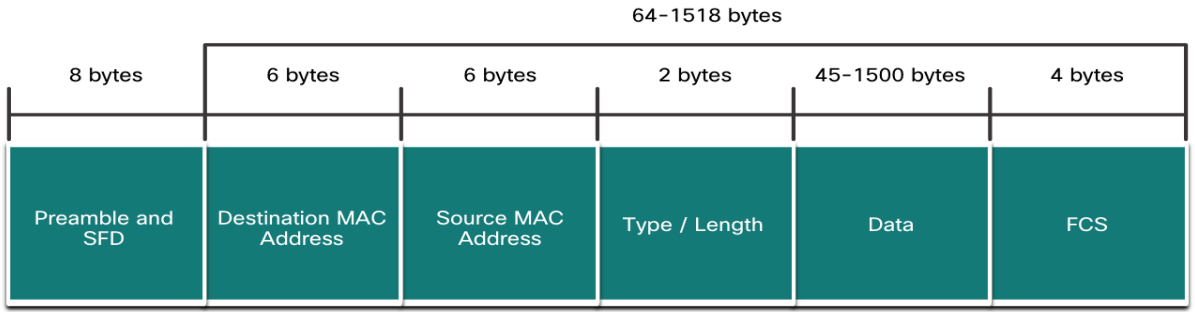
Media Access

- The IEEE 802.3 MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.
- Legacy Ethernet using a bus topology or hubs, is a shared, half-duplex medium. Ethernet over a half-duplex medium uses a contention-based access method, carrier sense multiple access/collision detection (CSMA/CD).
- Ethernet LANs of today use switches that operate in full-duplex. Full-duplex communications with Ethernet switches do not require access control through CSMA/CD.



Ethernet Frame Fields

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes.
  - The preamble field is not included when describing the size of the frame.
  - Any frame less than 64 bytes in length is considered a “collision fragment” or “runt frame” and is automatically discarded. Frames with more than 1500 bytes of data are considered “jumbo” or “baby giant frames”.
  - If the size of a transmitted frame is < minimum, or > maximum, the receiving device drops the frame. Dropped frames are likely to be the result of collisions or other unwanted signals. They are considered invalid. Jumbo frames are usually supported by most Fast Ethernet and Gigabit Ethernet switches and NICs.



Lab Activity

Wireshark - Use Wireshark to Examine Ethernet Frames

Task#1 : Examine the Header Fields in an Ethernet II Frame.

Task#2 : Use Wireshark to Capture and Analyze Ethernet Frames.

Ethernet MAC Address

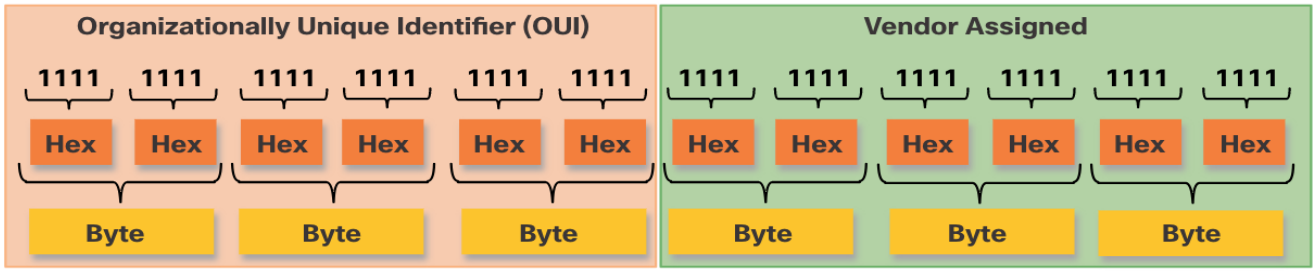
Ethernet MAC Addresses

MAC Address and Hexadecimal

- An Ethernet MAC address consists of a 48-bit binary value, expressed using 12 hexadecimal values.
- Given that 8 bits (one byte) is a common binary grouping, binary 00000000 to 11111111 can be represented in hexadecimal as the range 00 to FF,
- When using hexadecimal, leading zeroes are always displayed to complete the 8-bit representation. For example the binary value 0000 1010 is represented in hexadecimal as 0A.
- Hexadecimal numbers are often represented by the value preceded by **0x** (e.g., 0x73) to distinguish between decimal and hexadecimal values in documentation.
- Hexadecimal may also be represented by a subscript 16, or the hex number followed by an H (e.g., 73H).

Ethernet MAC Address

- In an Ethernet LAN, every network device is connected to the same, shared media. MAC addressing provides a method for device identification at the data link layer of the OSI model.
- An Ethernet MAC address is a 48-bit address expressed using 12 hexadecimal digits. Because a byte equals 8 bits, we can also say that a MAC address is 6 bytes in length.
- All MAC addresses must be unique to the Ethernet device or Ethernet interface. To ensure this, all vendors that sell Ethernet devices must register with the IEEE to obtain a unique 6 hexadecimal (i.e., 24-bit or 3-byte) code called the organizationally unique identifier (OUI).
- An Ethernet MAC address consists of a 6 hexadecimal vendor OUI code followed by a 6 hexadecimal vendor-assigned value.

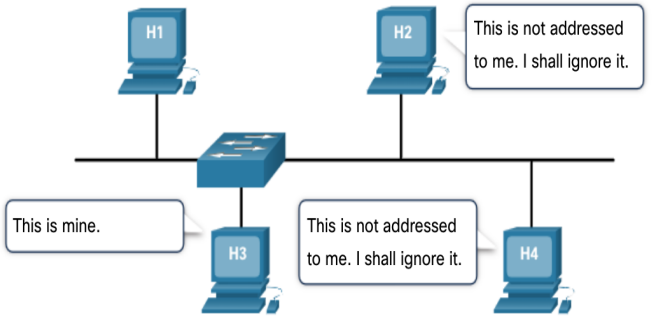


Ethernet MAC Addresses

Frame Processing

- When a device is forwarding a message to an Ethernet network, the Ethernet header include a Source MAC address and a Destination MAC address.
  - When a NIC receives an Ethernet frame, it examines the destination MAC address to see if it matches the physical MAC address that is stored in RAM. If there is no match, the device discards the frame. If there is a match, it passes the frame up the OSI layers, where the de-encapsulation process takes place.

Note: *Ethernet NICs will also accept frames if the destination MAC address is a broadcast or a multicast group of which the host is a member.*

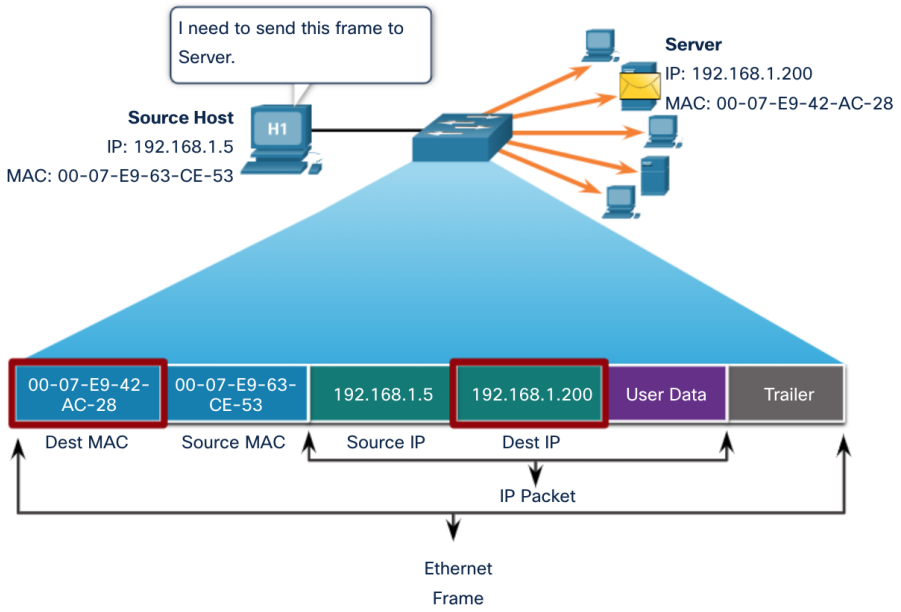


Ethernet MAC Addresses

Unicast MAC Address

In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

- A unicast MAC address is the unique address that is used when a frame is sent from a single transmitting device to a single destination device.
- The process that a source host uses to determine the destination MAC address associated with an IPv4 address is known as Address Resolution Protocol (ARP). The process that a source host uses to determine the destination MAC address associated with an IPv6 address is known as Neighbor Discovery (ND).



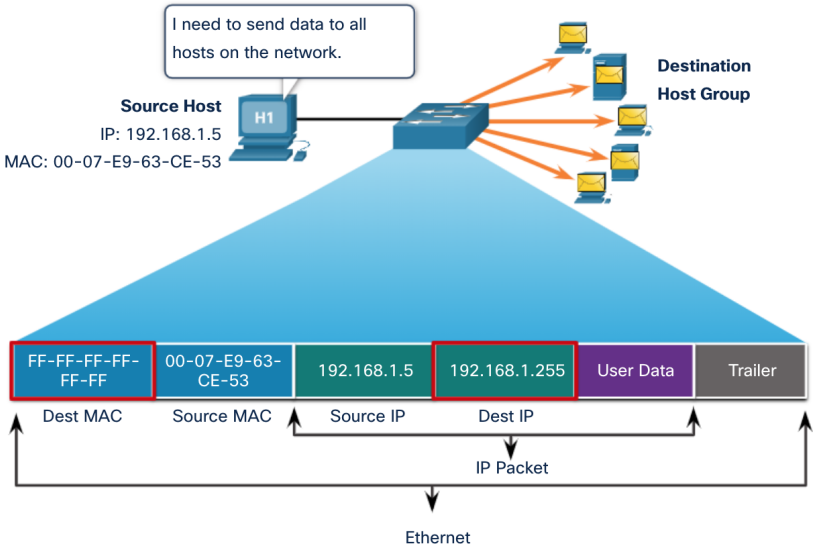
Note: *The source MAC address must always be a unicast.*

Ethernet MAC Addresses

Broadcast MAC Address

An Ethernet broadcast frame is received and processed by every device on the Ethernet LAN. The features of an Ethernet broadcast are as follows:

- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 address that has all ones (1s) in the host portion. This numbering in the address means that all hosts on that local network (broadcast domain) will receive and process the packet.

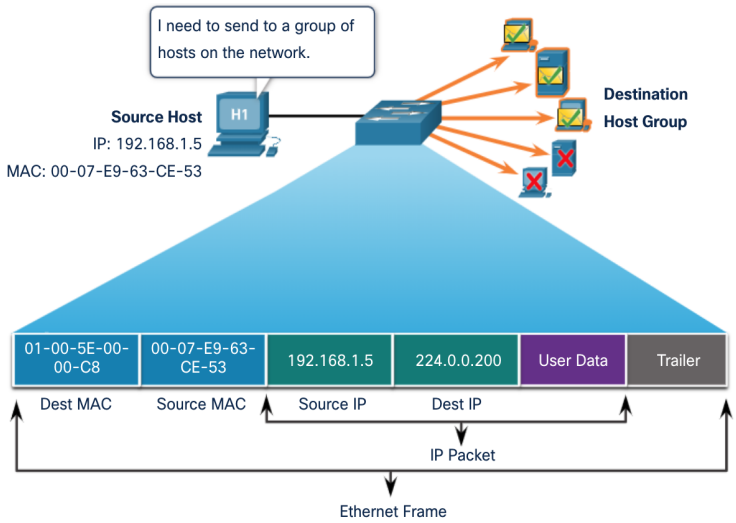


Ethernet MAC Addresses

Multicast MAC Address

An Ethernet multicast frame is received and processed by a group of devices that belong to the same multicast group.

- There is a destination MAC address of 01-00-5E when the encapsulated data is an IPv4 multicast packet and a destination MAC address of 33-33 when the encapsulated data is an IPv6 multicast packet.
- There are other reserved multicast destination MAC addresses for when the encapsulated data is not IP, such as Spanning Tree Protocol (STP).
- It is flooded out all Ethernet switch ports except the incoming port, unless the switch is configured for multicast snooping. It is not forwarded by a router, unless the router is configured to route multicast packets.
- Because multicast addresses represent a group of addresses (sometimes called a host group), they can only be used as the destination of a packet. The source will always be a unicast address.
- As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address.



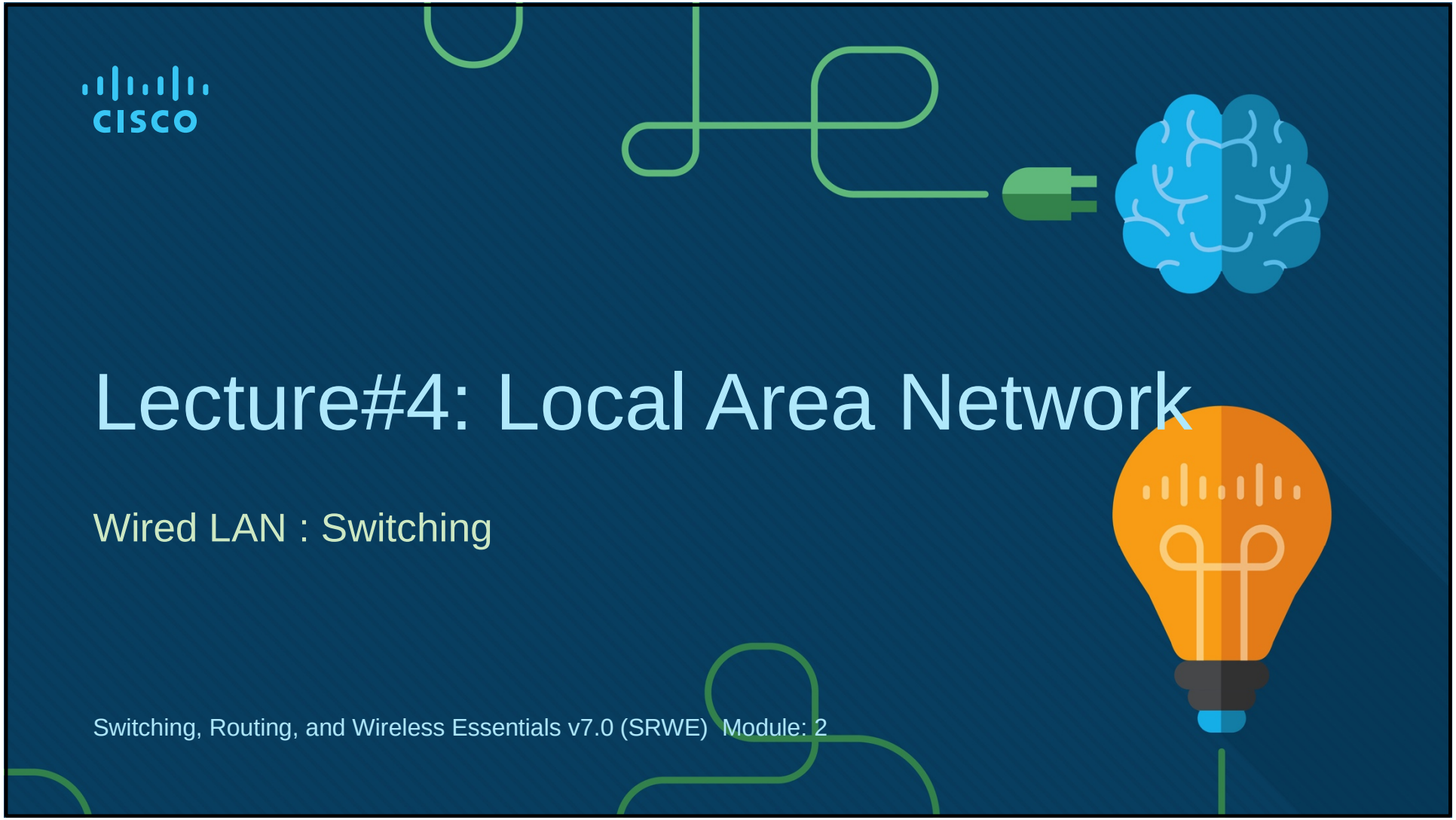
Lab Activity

Packet Tracer - View Network Device MAC Addresses

Task#1 : Set Up the Topology and Initialize Devices.

Task#2 : Configure Devices and Verify Connectivity.

Task#3 : Display, Describe, and Analyze Ethernet MAC Addresses


cisco
Lecture#4: Local Area Network
Wired LAN : Switching
Switching, Routing, and Wireless Essentials v7.0 (SRWE) Module: 2

4.2 Switching Concept

Frame Forwarding

Frame Forwarding

Switching in Networking

Two terms are associated with frames entering or leaving an interface:

- **Ingress** – entering the interface
- **Egress** – exiting the interface

A switch forwards based on the ingress interface and the destination MAC address.

A switch uses its MAC address table to make forwarding decisions.

***Note**: A switch will never allow traffic to be forwarded out the interface it received the traffic.*

Port Table

Destination Addresses	Port
EE	1
AA	2
BA	3
EA	4
AC	5
AB	6

Frame Forwarding

The Switch MAC Address Table

A switch will use the destination MAC address to determine the egress interface.

Before a switch can make this decision it must learn what interface the destination is located.

A switch builds a MAC address table, also known as a Content Addressable Memory (CAM) table, by recording the source MAC address into the table along with the port it was received.

Frame Forwarding

The Switch Learn and Forward Method

The switch uses a two step process:

Step 1. Learn – Examines Source Address

- Adds the source MAC if not in table
- Resets the time out setting back to 5 minutes if source is in the table

Step 2. Forward – Examines Destination Address

- If the destination MAC is in the MAC address table it is forwarded out the specified port.
- If a destination MAC is not in the table, it is flooded out all interfaces except the one it was received.

Frame Forwarding

Switch Forwarding Methods

Switches use software on application-specific-integrated circuits (ASICs) to make very quick decisions.

A switch will use one of two methods to make forwarding decisions after it receives a frame:

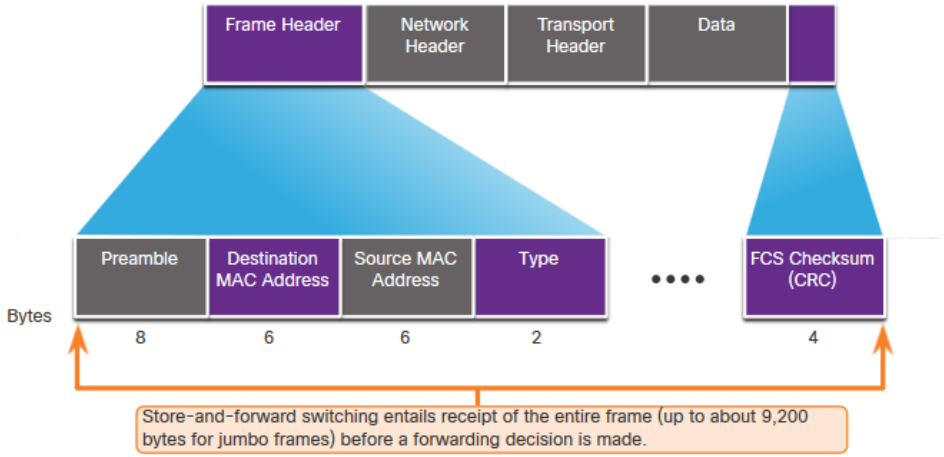
- **Store-and-forward switching** - Receives the entire frame and ensures the frame is valid. Store-and-forward switching is Cisco's preferred switching method.
- **Cut-through switching** – Forwards the frame immediately after determining the destination MAC address of an incoming frame and the egress port.

Frame Forwarding

Store-and-Forward Switching

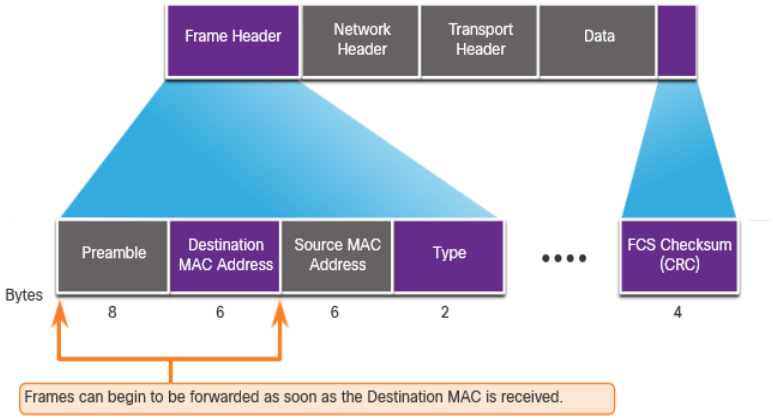
Store-and-forward has two primary characteristics:

- **Error Checking** – The switch will check the Frame Check Sequence (FCS) for CRC errors. Bad frames will be discarded.
- **Buffering** – The ingress interface will buffer the frame while it checks the FCS. This also allows the switch to adjust to a potential difference in speeds between the ingress and egress ports.



Cut-Through Switching

- **Cut-through** forwards the frame immediately after determining the destination MAC.
- **Fragment Free** method will check the destination and ensure that the frame is at least 64 Bytes. This will eliminate runts.



Concepts of **Cut-Through** switching:

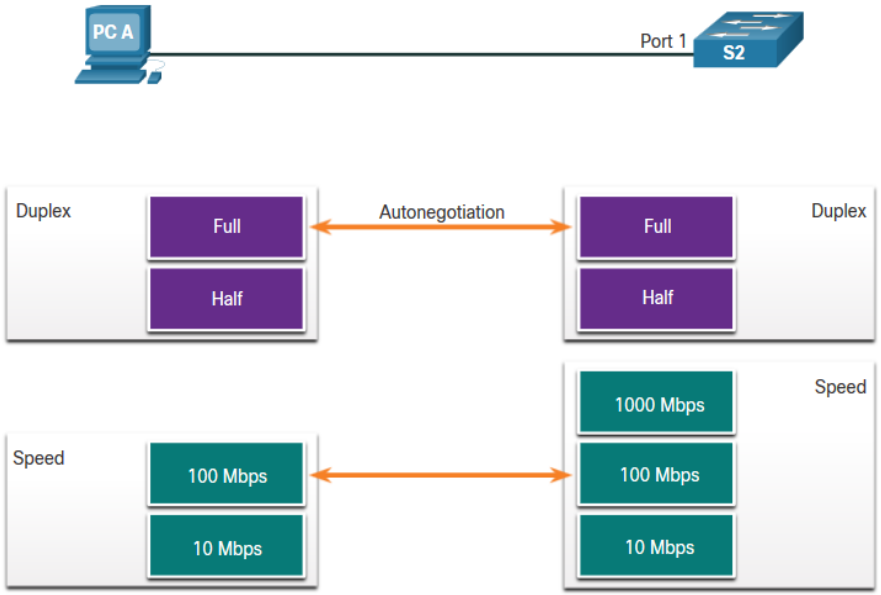
- Is appropriate for switches needing latency to be under 10 microseconds
- Does not check the FCS, so it can propagate errors
- May lead to bandwidth issues if the switch propagates too many errors
- Cannot support ports with differing speeds going from ingress to egress.

Switching Domains

Collision Domains

Switches eliminate collision domains and reduce congestion.

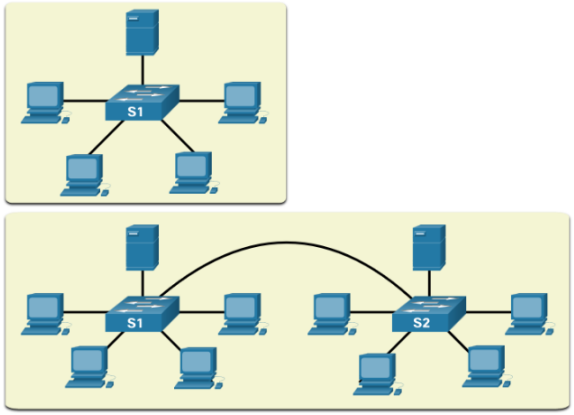
- When there is full duplex on the link the collision domains are eliminated.
- When there is one or more devices in half-duplex there will now be a collision domain.
  - § There will now be contention for the bandwidth.
  - § Collisions are now possible.
- Most devices, including Cisco and Microsoft use auto-negotiation as the default setting for duplex and speed.



Switching Domains

Broadcast Domains

- A broadcast domain extends across all Layer 1 or Layer 2 devices on a LAN.
  - Only a layer 3 device (router) will break the broadcast domain, also called a MAC broadcast domain.
  - The broadcast domain consists of all devices on the LAN that receive the broadcast traffic.



- When the layer 2 switch receives the broadcast it will flood it out all interfaces except for the ingress interface.
- Too many broadcasts may cause congestion and poor network performance.
- Increasing devices at Layer 1 or layer 2 will cause the broadcast domain to expand.

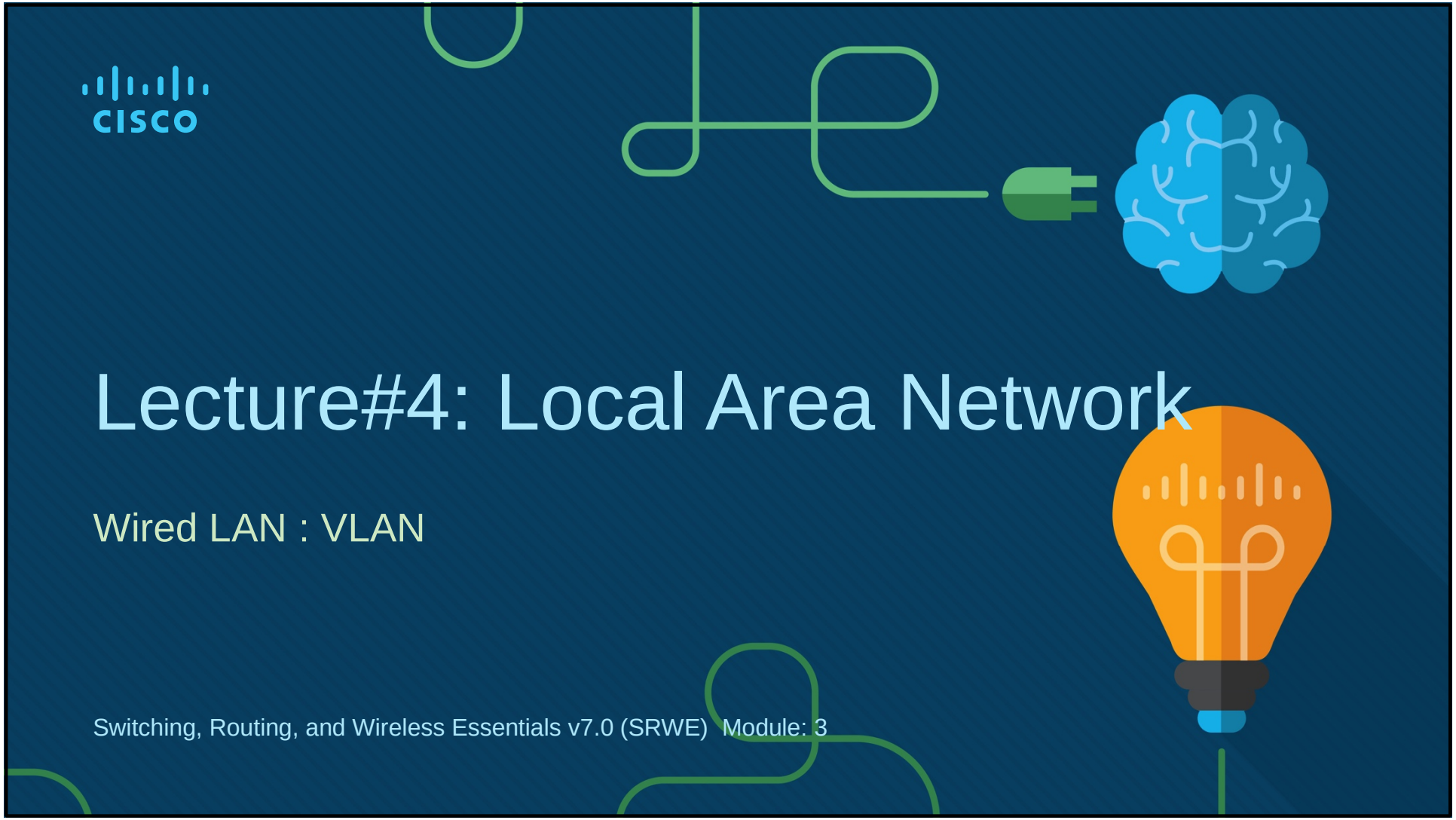
Switching Domains

Alleviated Network Congestion

Switches use the MAC address table and full-duplex to eliminate collisions and avoid congestion.

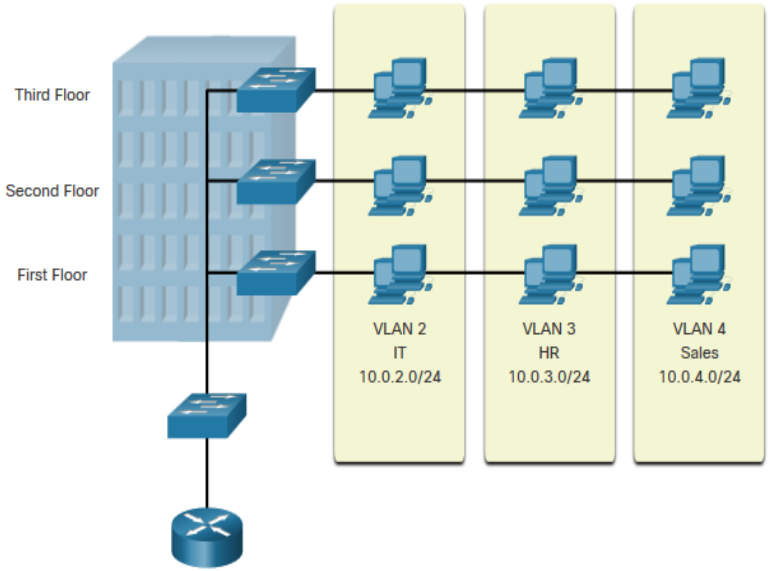
Features of the switch that alleviate congestion are as follows:

Protocol	Function
Fast Port Speeds	Depending on the model, switches may have up to 100Gbps port speeds.
Fast Internal Switching	This uses fast internal bus or shared memory to improve performance.
Large Frame Buffers	This allows for temporary storage while processing large quantities of frames.
High Port Density	This provides many ports for devices to be connected to LAN with less cost. This also provides for more local traffic with less congestion.


cisco
Lecture#4: Local Area Network
Wired LAN : VLAN
Switching, Routing, and Wireless Essentials v7.0 (SRWE) Module: 3

4.3 Overview of VLANs

VLAN Definitions



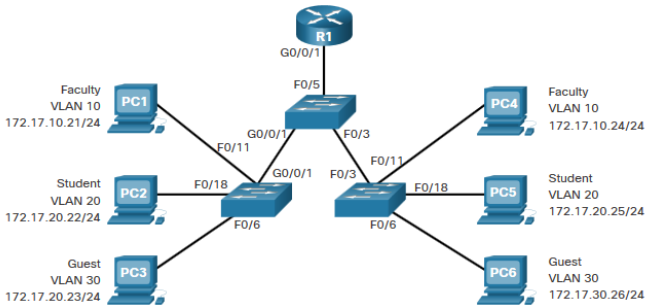
VLANs are logical connections with other similar devices.

Placing devices into various VLANs have the following characteristics:

- Provides segmentation of the various groups of devices on the same switches
- Provide organization that is more manageable
  - § Broadcasts, multicasts and unicasts are isolated in the individual VLAN
  - § Each VLAN will have its own unique range of IP addressing
  - § Smaller broadcast domains

Benefits of a VLAN Design

Benefits of using VLANs are as follows:



Benefits	Description
Smaller Broadcast Domains	Dividing the LAN reduces the number of broadcast domains
Improved Security	Only users in the same VLAN can communicate together
Improved IT Efficiency	VLANs can group devices with similar requirements, e.g. faculty vs. students
Reduced Cost	One switch can support multiple groups or VLANs
Better Performance	Small broadcast domains reduce traffic, improving bandwidth
Simpler Management	Similar groups will need similar applications and other network resources

Types of VLANs

VLAN 1 is the following:

- The default VLAN
- The default Native VLAN
- The default Management VLAN
- Cannot be deleted or renamed

```
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
```

***Note**: While we cannot delete VLAN1 Cisco will recommend that we assign these default features to other VLANs*

Types of VLANs (Cont.)

Data VLAN

- Dedicated to user-generated traffic (email and web traffic).
- VLAN 1 is the default data VLAN because all interfaces are assigned to this VLAN.

Native VLAN

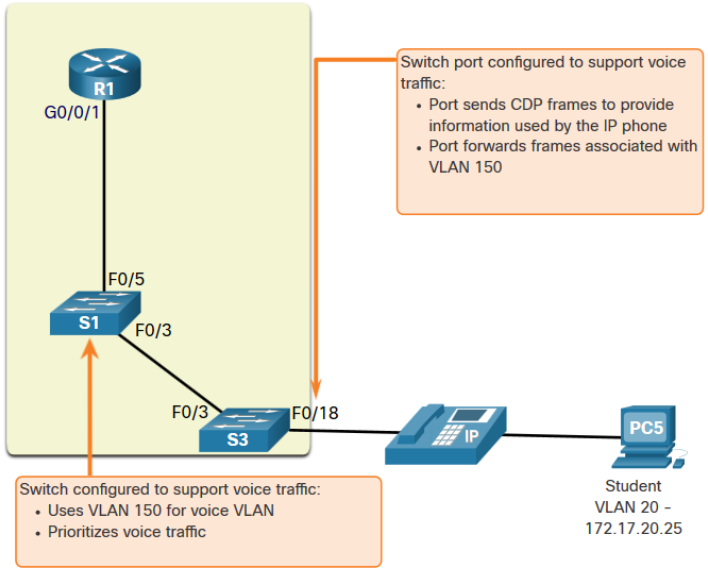
- This is used for trunk links only.
- All frames are tagged on an 802.1Q trunk link except for those on the native VLAN.

Management VLAN

- This is used for SSH/Telnet VTY traffic and should not be carried with end user traffic.
- Typically, the VLAN that is the SVI for the Layer 2 switch.

Types of VLANs (Cont.)

- A separate VLAN (**Voice VLAN**) is required because Voice traffic requires:
  - § Assured bandwidth
  - § High QoS priority
  - § Ability to avoid congestion
  - § Delay less that 150 ms from source to destination
- The entire network must be designed to support voice.



Lab Activity

Packet Tracer – Who Hears the Broadcast?

Task#1 : Observe Broadcast Traffic in a VLAN Implementation.

Task#2 : Complete Review Questions.


CISCO
COVID-19
STAY HOME
STAY SAFE