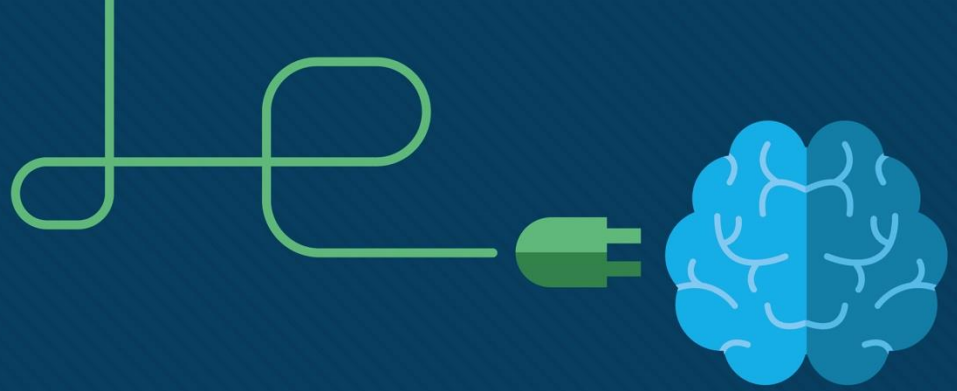
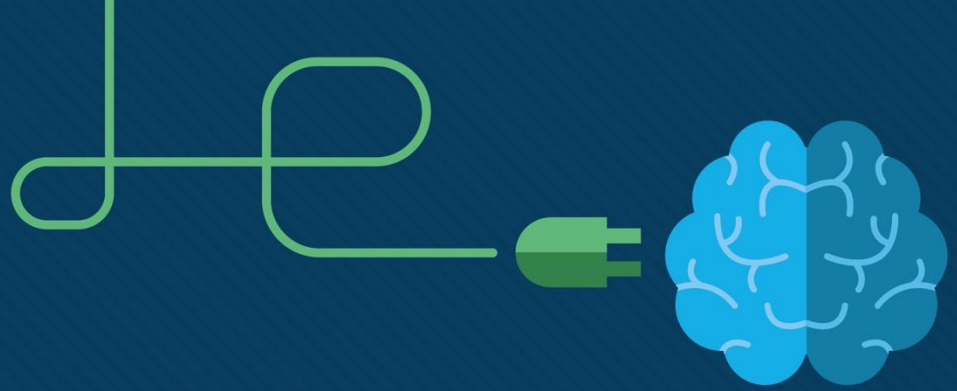


# Module 7: Ethernet Switching

Thomas Wyseur

Introduction to Networks v7.0
(ITN)



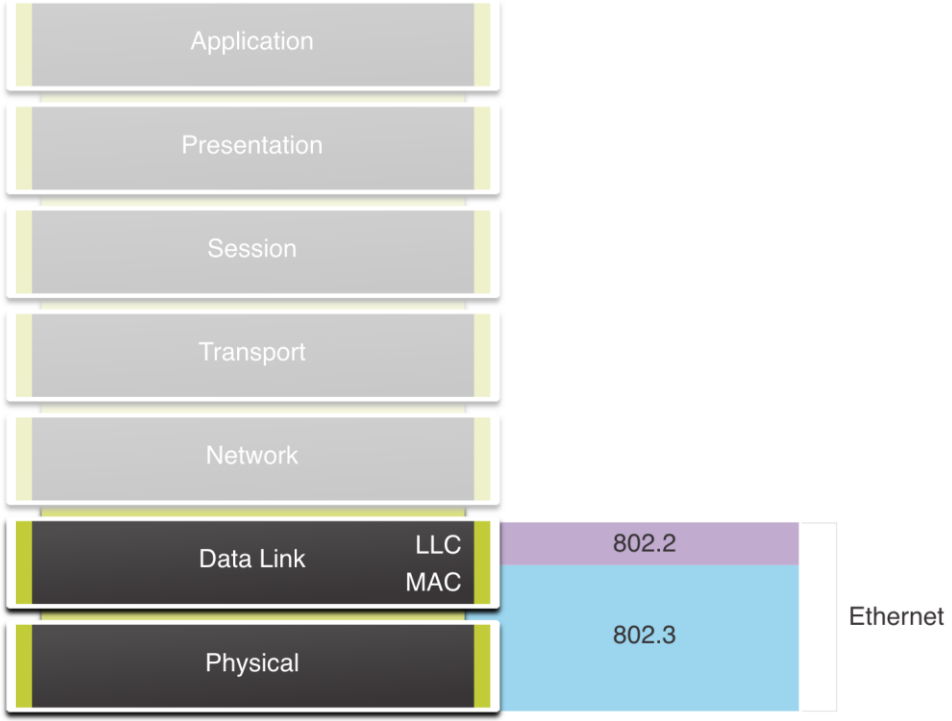
# Module 7: Ethernet Switching

Introduction to Networks v7.0
(ITN)

# 7.1 Ethernet Frames

# Ethernet Encapsulation

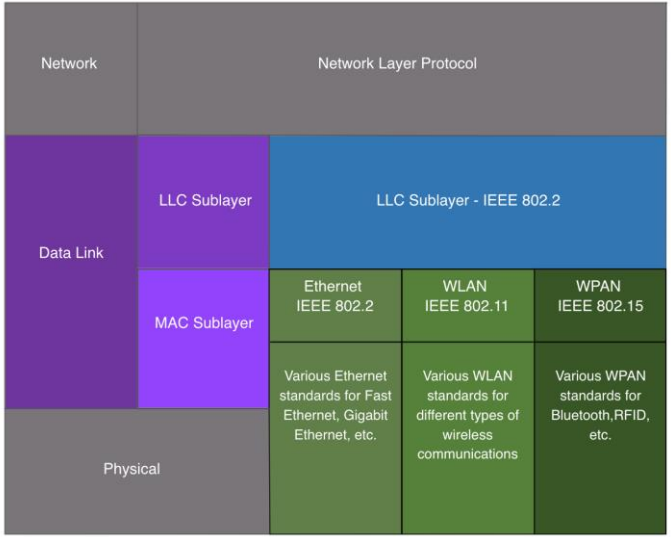
- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.



# 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.



# MAC Sublayer

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

## Data Encapsulation

IEEE 802.3 data encapsulation includes the following:

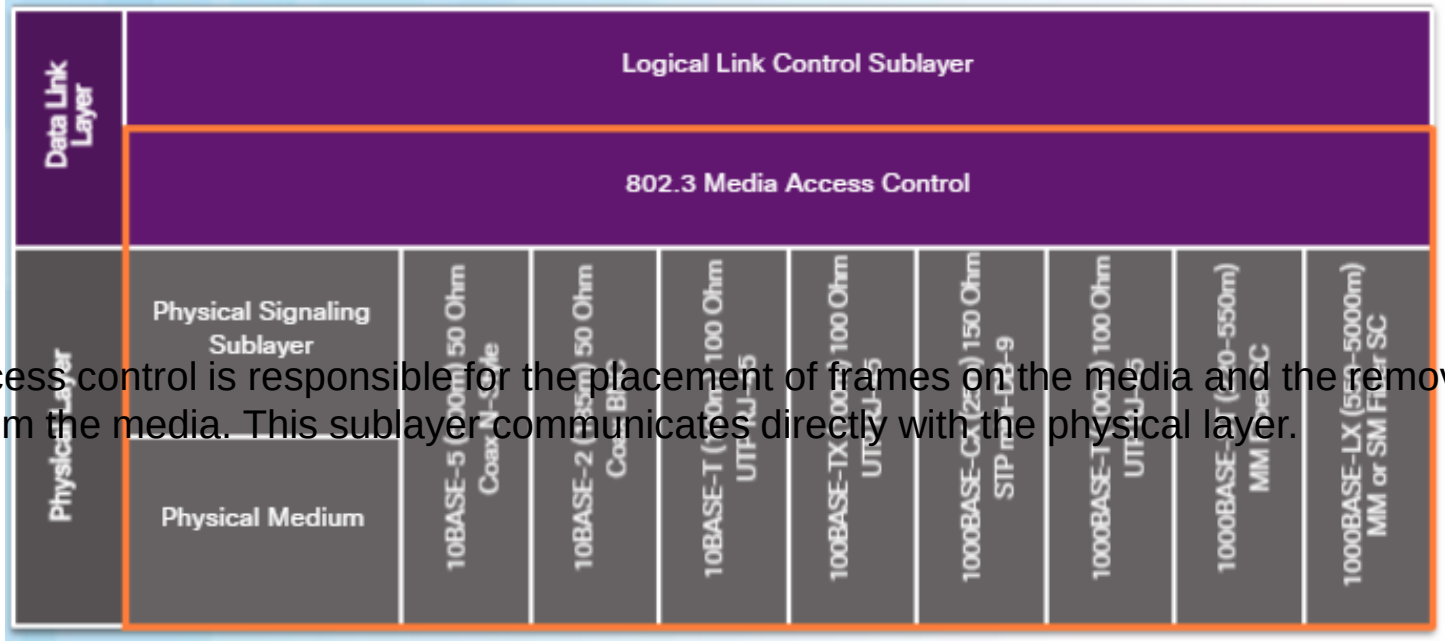
1. **Ethernet frame** - This is the internal structure of the Ethernet frame.
2. **Ethernet Addressing** - The Ethernet frame includes both a source and destination MAC address to deliver the Ethernet frame from Ethernet NIC to Ethernet NIC on the same LAN.
3. **Ethernet Error detection** - The Ethernet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

Data Encapsulation

- Frame delimiting
- Addressing
- Error detection

Media Access Control

- Control of frame placement on and off the media
- Media recovery

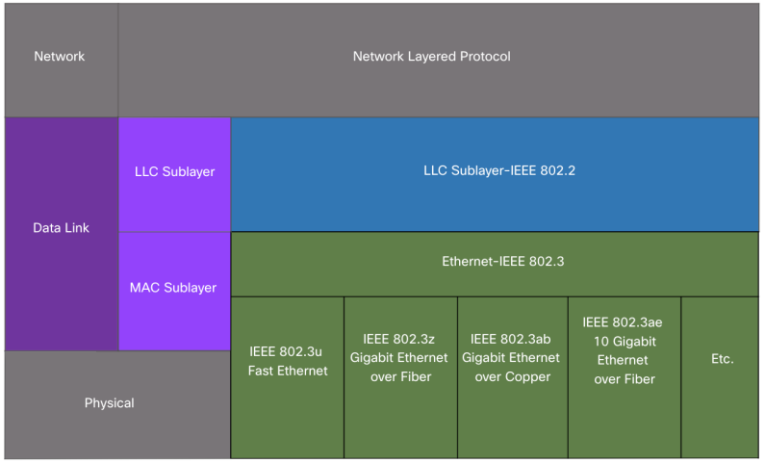



- Media access control is responsible for the placement of frames on the media and the removal of frames from the media. This sublayer communicates directly with the physical layer.

# MAC Sublayer

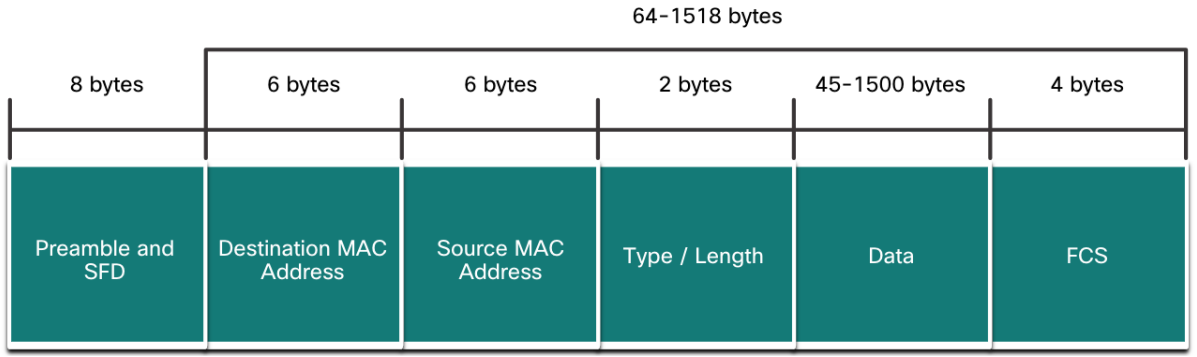
**Media Access**

- 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 less than the minimum, or greater than the 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.



# 7.2 Ethernet MAC Address

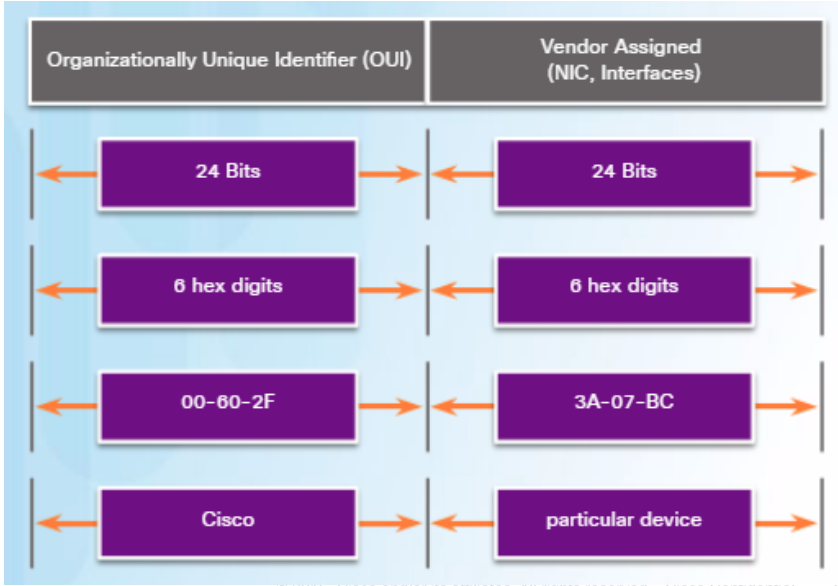
# MAC Address and Hexadecimal

- 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).

# MAC Addresses: Ethernet Identity

- MAC addresses were created to identify the actual source and destination.
  - The MAC address rules are established by IEEE.
  - The IEEE assigns the vendor a 3-byte (24-bit) code, called the Organizationally Unique Identifier (OUI).

- IEEE requires a vendor to follow two simple rules:
  - All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
  - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

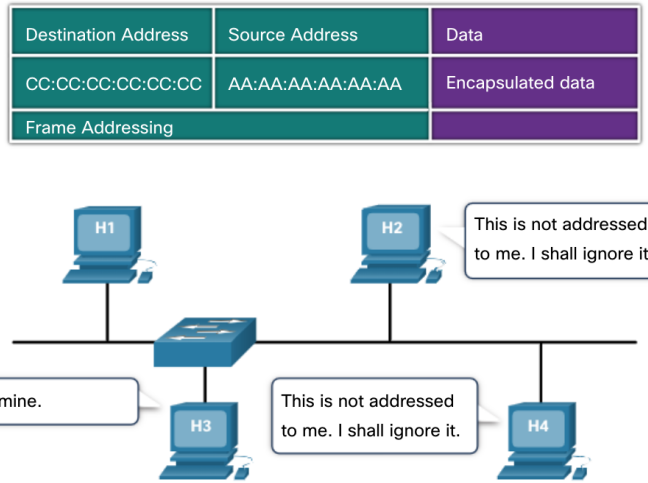


# Frame Processing

- 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.

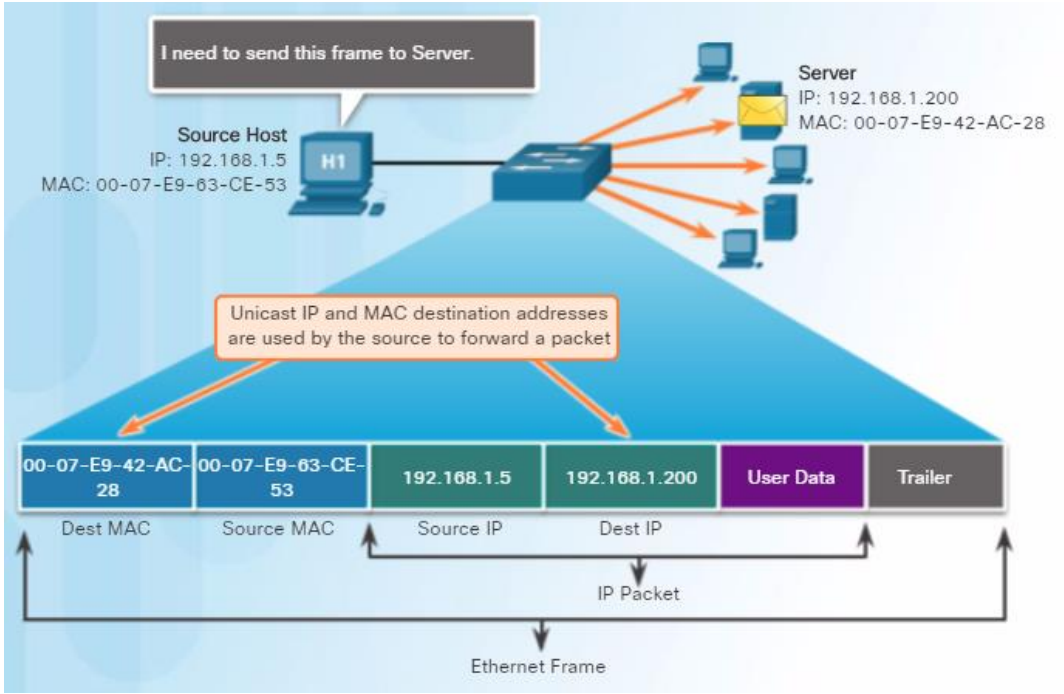
- Any device that is the source or destination of an Ethernet frame, will have an Ethernet NIC and therefore, a MAC address. This includes workstations, servers, printers, mobile devices, and routers.



# Unicast MAC Address

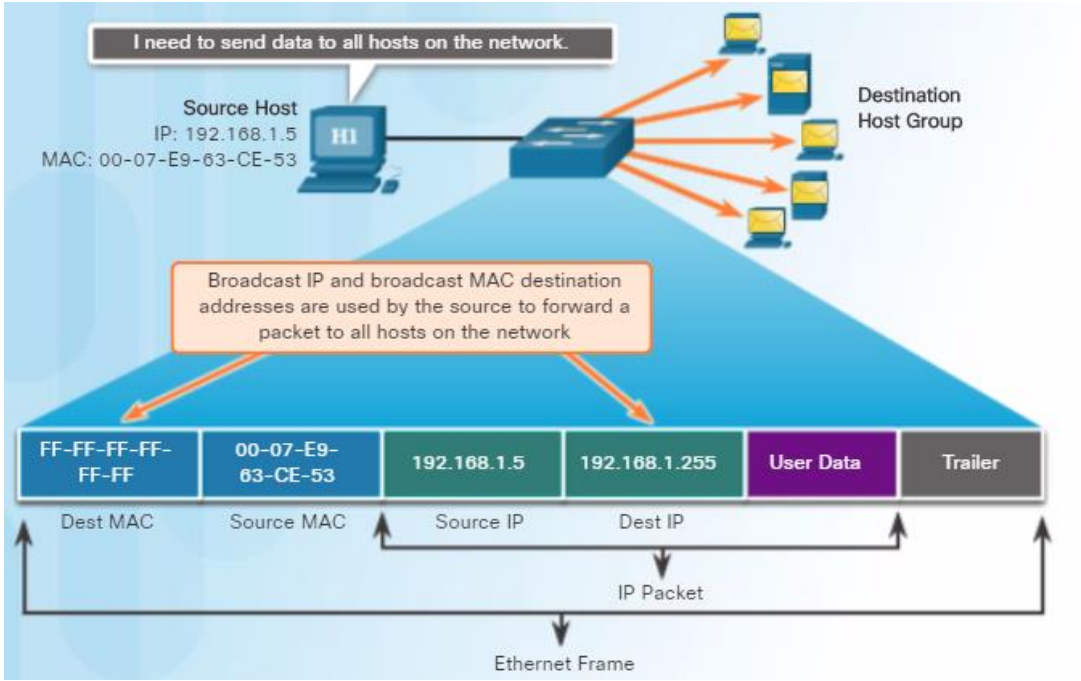
- A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.

- For a unicast packet to be sent and received, a destination IP address must be in the IP packet header and a corresponding destination MAC address must also be present in the Ethernet frame header.



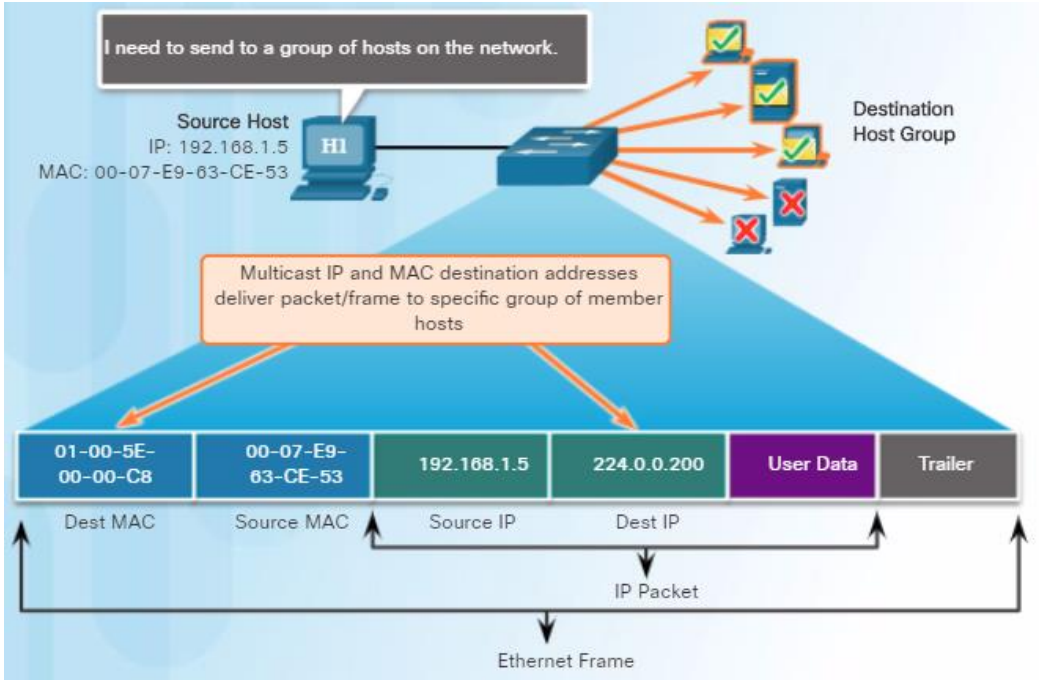
# Broadcast MAC Address

- Many network protocols, such as DHCP and ARP, use broadcasts.
- A broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion indicating that all hosts on that local network will receive and process the packet.
- When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).



# Multicast MAC Address

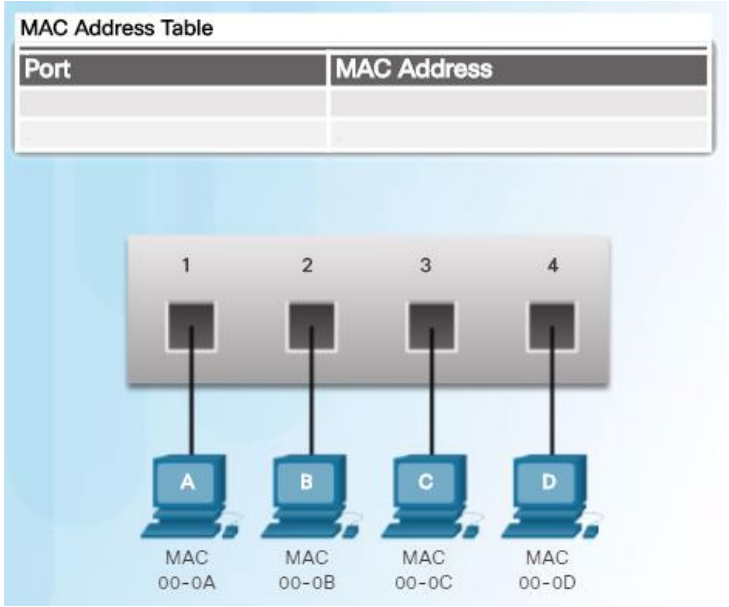
- Multicast addresses allow a source device to send a packet to a group of devices.
  - Devices in a multicast group are assigned a multicast group IP address in the range of 224.0.0.0 to 239.255.255.255 (IPv6 multicast addresses begin with FF00::/8).
  - The multicast IP address requires a corresponding multicast MAC address that begins with 01-00-5E in hexadecimal.



# 7.3 The MAC Address Table

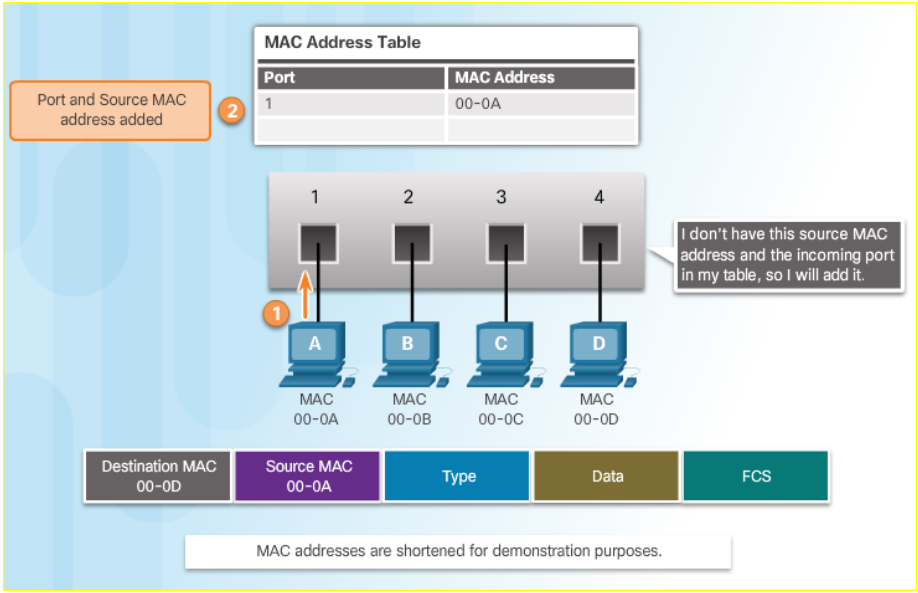
# Switch Fundamentals

- A Layer 2 Ethernet switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.
- A switch that is powered on, will have an empty MAC address table as it has not yet learned the MAC addresses for the four attached PCs.
- Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.



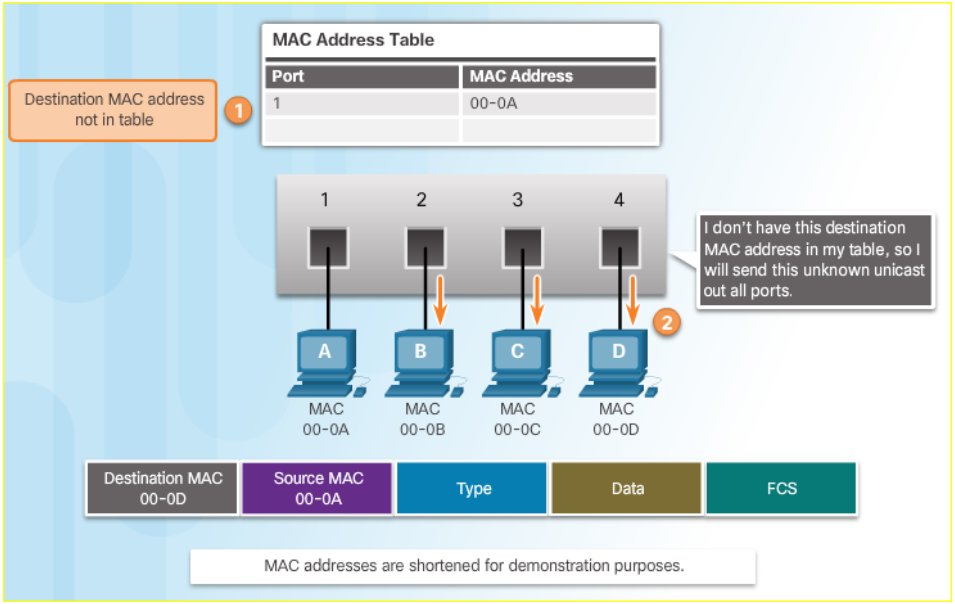
# Learning MAC Addresses

- The switch dynamically builds the MAC address table. The process to learn the Source MAC Address is:
  - Switches examine all incoming frames for new source MAC address information to learn.
  - If the source MAC address is unknown, it is added to the table along with the port number.
  - If the source MAC address does exist, the switch updates the refresh timer for that entry.
  - By default, most Ethernet switches keep an entry in the table for 5 minutes.



# Learning MAC Addresses (Cont.)

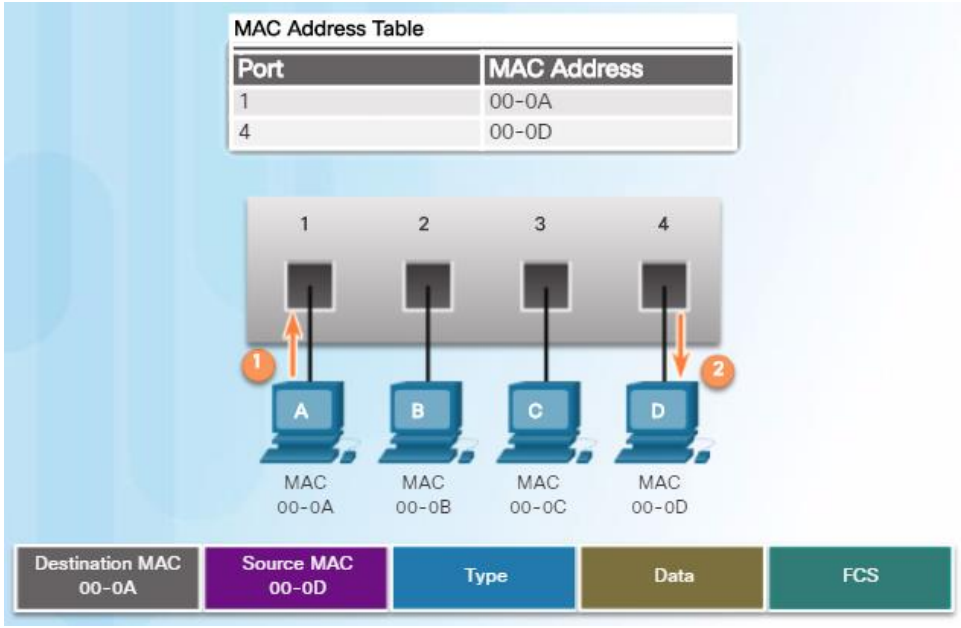
- The process to forward the Destination MAC Address is:
  - If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
  - If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
  - If the destination MAC address is in the table, it will forward the frame out the specified port.
  - If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.



# Filtering Frames

- As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame.

- When the switch's MAC address table contains the destination MAC address, it is able to filter the frame and forward out a single port.



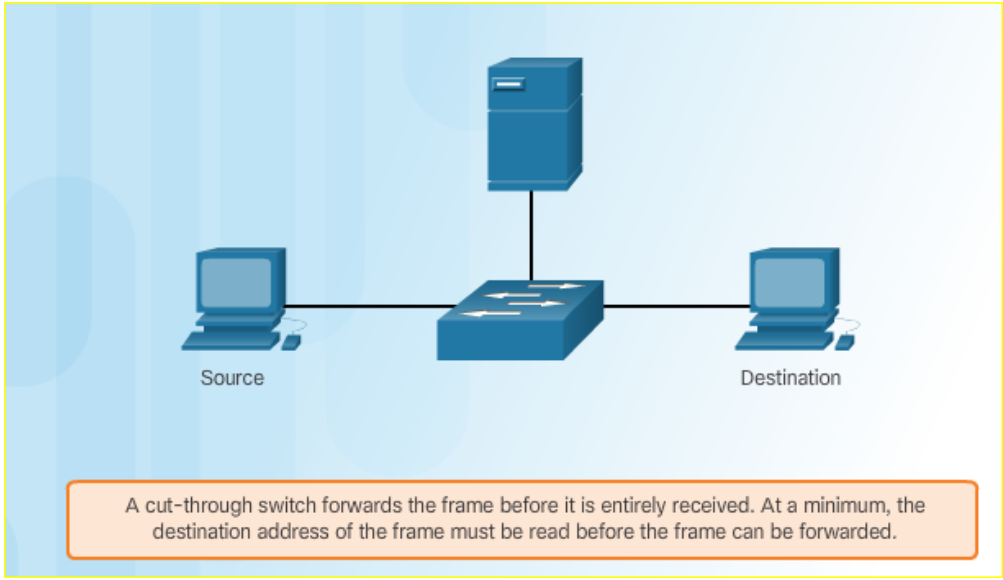
# 7.4 Switch Speeds and Forwarding Methods

# Frame Forwarding Methods on Cisco Switches

- Switches use one of the following forwarding methods for switching data between network ports:

# Cut-Through Switching

- In cut-through switching, the switch buffers just enough of the frame to read the destination MAC address so that it can determine to which port to forward the data. The switch does not perform any error checking on the frame.
- There are two variants of cut-through switching:
  - Fast-forward switching offers the lowest level of latency. The switch immediately forwards a packet after reading the destination address. This is the most typical form of cut-through switching.
  - Fragment-free switching, in which the switch stores the first 64 bytes of the frame before forwarding. It is a compromise between store-and-forward and fast-forward switching.



# Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them or when the destination port is busy because of congestion.

| Method | Description |
|---|---|
| **Port-based memory** | •Frames are stored in queues that are linked to specific incoming and outgoing ports.<br>•A frame is transmitted to the outgoing port only when all the frames ahead in the queue have been successfully transmitted.<br>•It is possible for a single frame to delay the transmission of all the frames in memory because of a busy destination port.<br>•This delay occurs even if the other frames could be transmitted to open destination ports. |
| **Shared memory** | •Deposits all frames into a common memory buffer shared by all switch ports and the amount of buffer memory required by a port is dynamically allocated.<br>•The frames in the buffer are dynamically linked to the destination port enabling a packet to be received on one port and then transmitted on another port, without moving it to a different queue. |

- Shared memory buffering also results in larger frames that can be transmitted with fewer dropped frames. This is important with asymmetric switching which allows for different data rates on different ports. Therefore, more bandwidth can be dedicated to certain ports (e.g., server port).

# Duplex and Speed Settings

Two of the most basic settings on a switch are the bandwidth (“speed”) and duplex settings for each individual switch port. It is critical that the duplex and bandwidth settings match between the switch port and the connected devices.

There are two types of duplex settings used for communications on an Ethernet network:

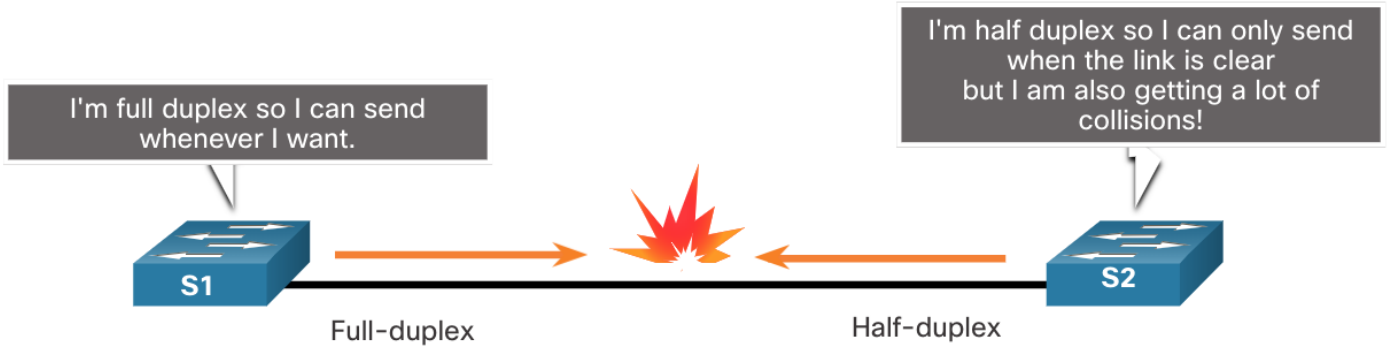
- **Full-duplex** - Both ends of the connection can send and receive simultaneously.
- **Half-duplex** - Only one end of the connection can send at a time.

Autonegotiation is an optional function found on most Ethernet switches and NICs. It enables two devices to automatically negotiate the best speed and duplex capabilities.

**Note**: Gigabit Ethernet ports only operate in full-duplex.

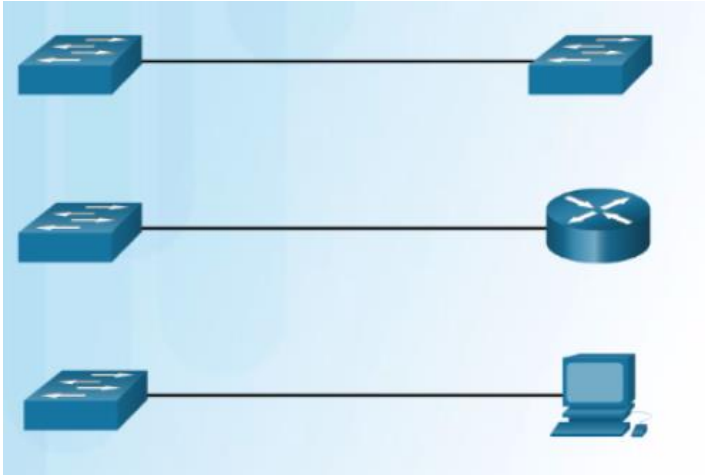
# Duplex and Speed Settings

- Duplex mismatch is one of the most common causes of performance issues on 10/100 Mbps Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.
- This can occur when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration.
- It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off. Best practice is to configure both Ethernet switch ports as full-duplex.



# Auto-MDIX

- Connections between specific devices such as switch-to-switch, switch-to-router, switch-to-host, and router-to-host devices, once required the use of specific cable types (crossover or straight-through).



- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. This is enabled by default on switches since IOS 12.2(18)SE.

- When enabled using the **mdix auto** interface configuration command, the switch detects the type of cable attached to the port, and configures the interfaces accordingly.


CISCO