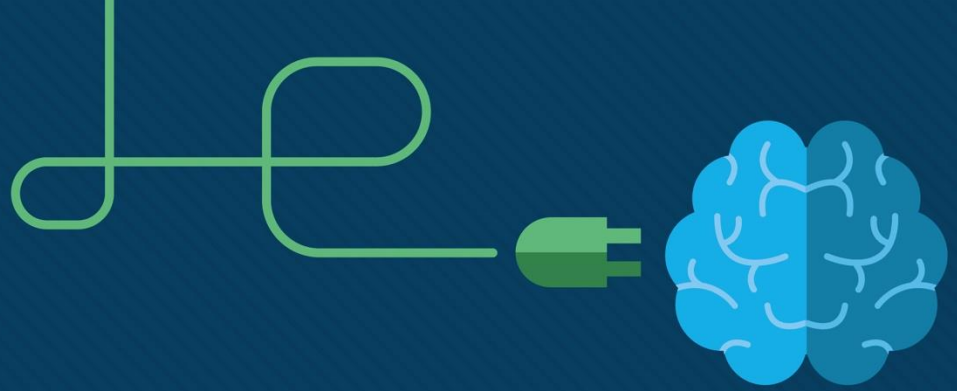


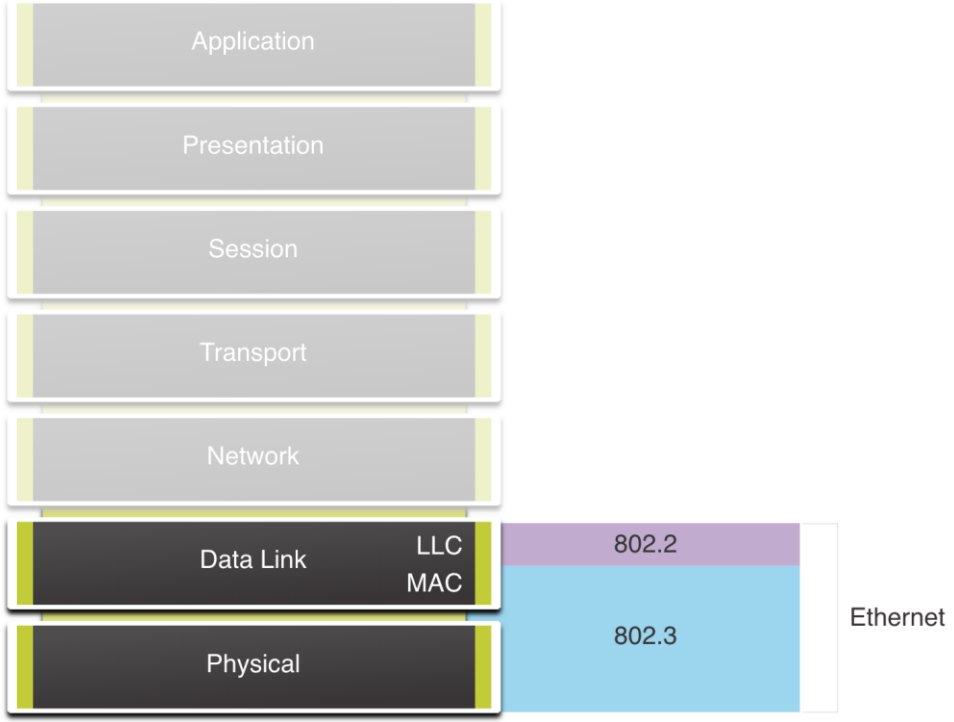
Module 7: Ethernet Switching

Introduction to Networks v7.0 (ITN)

7.1 Ethernet Frames

Ethernet Encapsulation

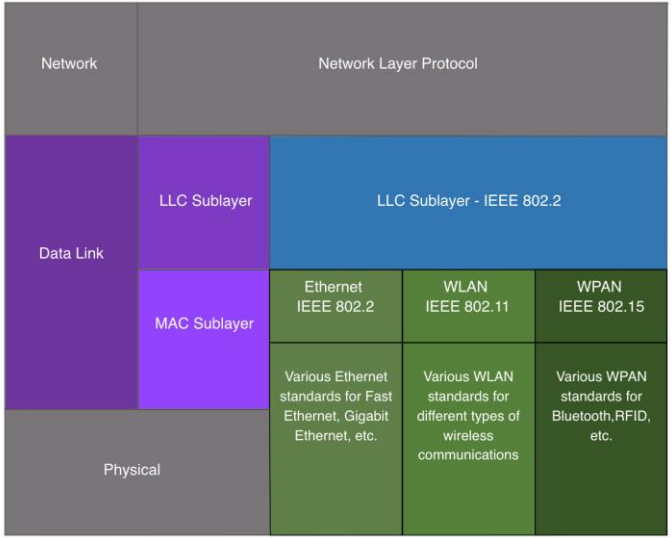
- Ethernet operates in the data link layer and the physical layer.
- It is a family of networking technologies defined in the IEEE 802.2 and 802.3 standards.



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

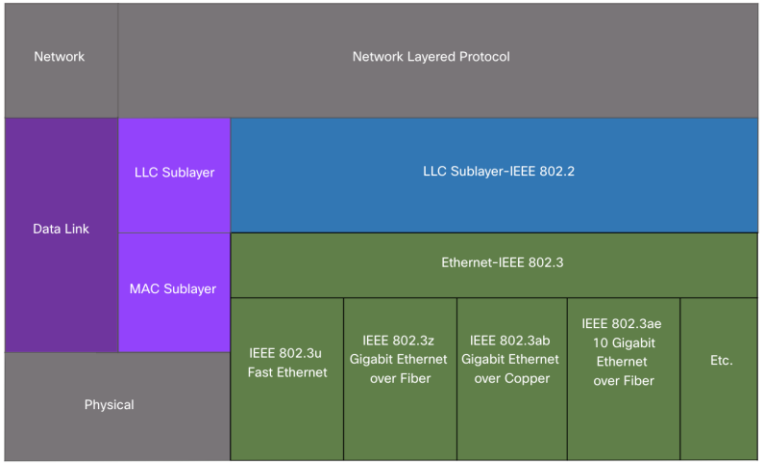
IEEE 802.3 data encapsulation includes the following:

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.

MAC Sublayer

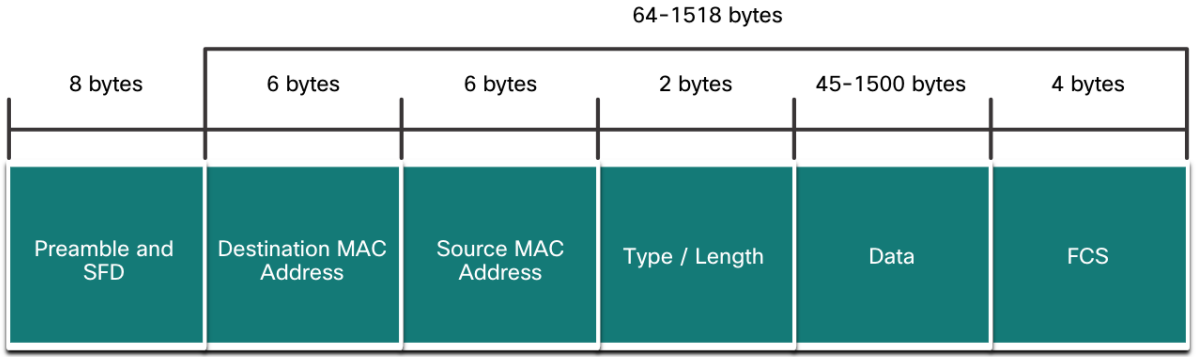
Media Access

- 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.



Lab – Use Wireshark to Examine Ethernet Frames

In this lab, you will complete the following objectives:

- Part 1: Examine the Header Fields in an Ethernet II Frame
- Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

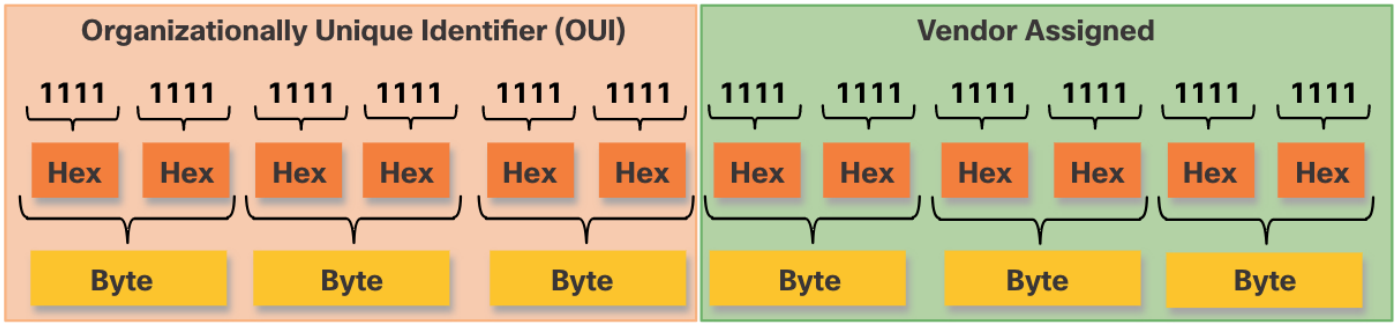
7.2 Ethernet MAC Address

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).

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.

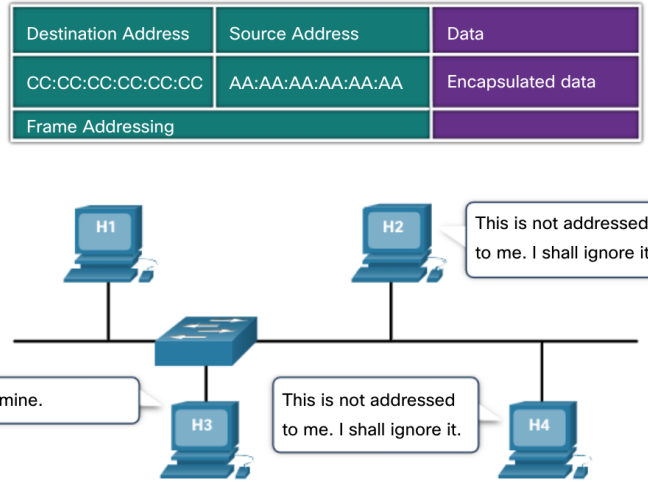


Frame Processing

- 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.

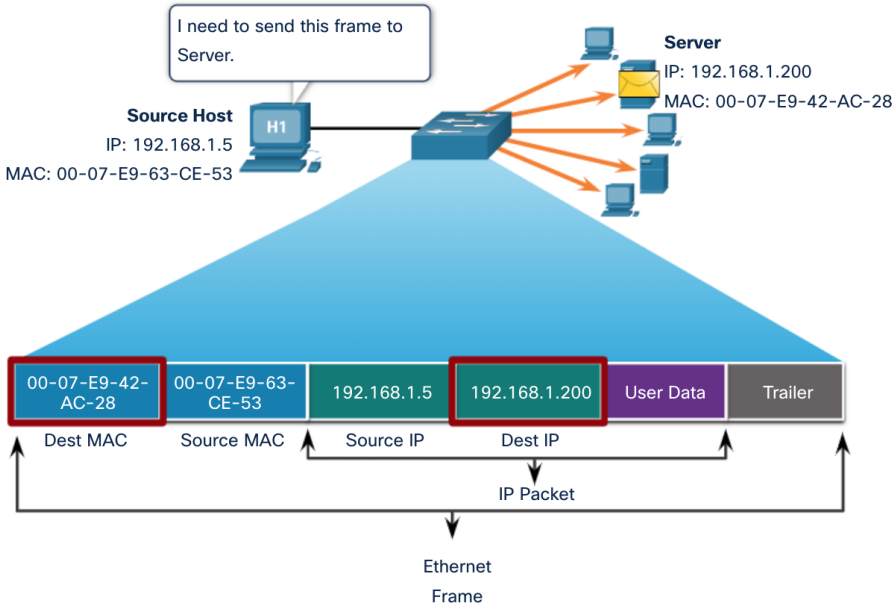


Unicast MAC Address

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).

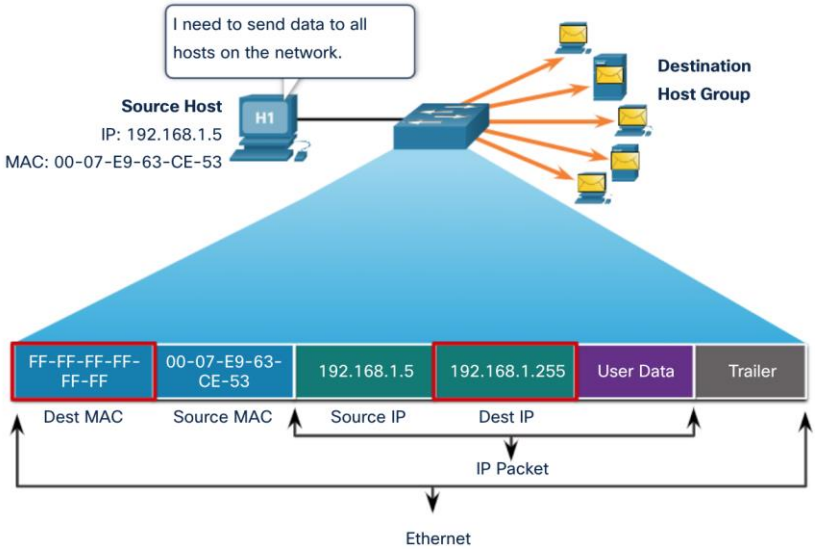
Note: The source MAC address must always be a unicast.



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:

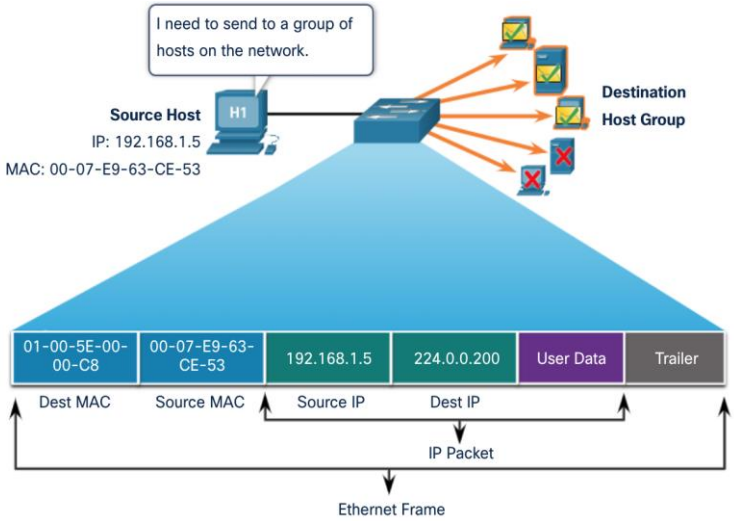
- It has a destination MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).
- It is flooded out all Ethernet switch ports except the incoming port. It is not forwarded by a router.
- If the encapsulated data is an IPv4 broadcast packet, this means the packet contains a destination IPv4 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.



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 – View Network Device MAC Addresses

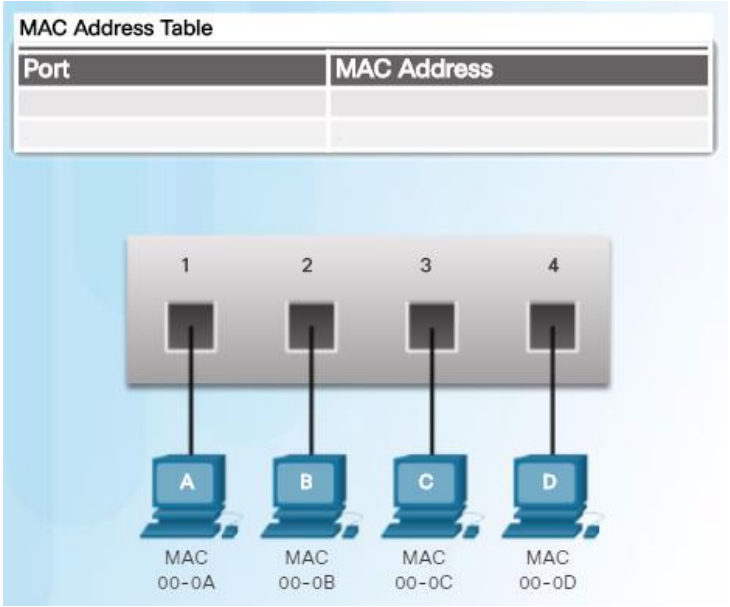
In this lab, you will complete the following objectives:

- Part 1: Set Up the Topology and Initialize Devices
- Part 2: Configure Devices and Verify Connectivity
- Part 3: Display, Describe, and Analyze Ethernet MAC Addresses

7.3 The MAC Address Table

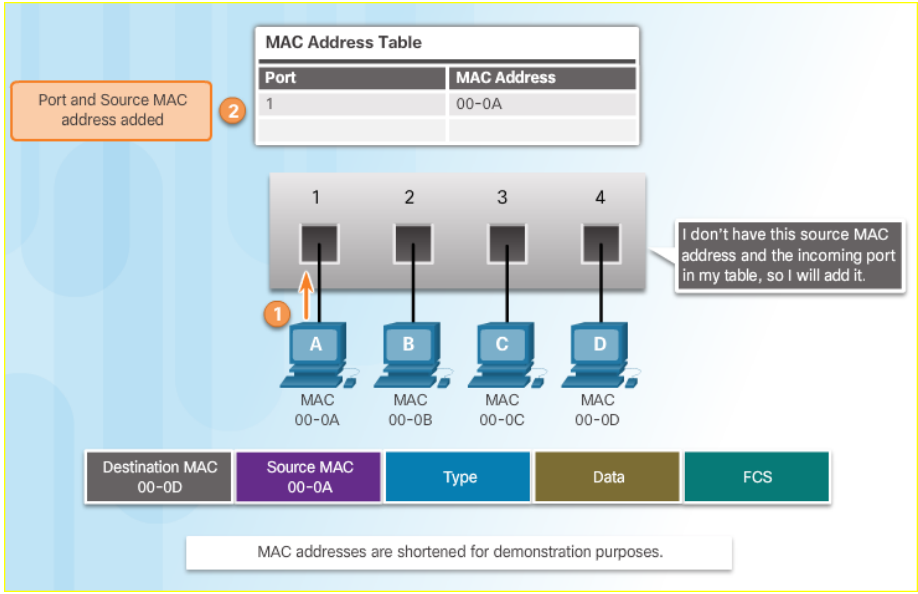
Switch Fundamentals

- 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.



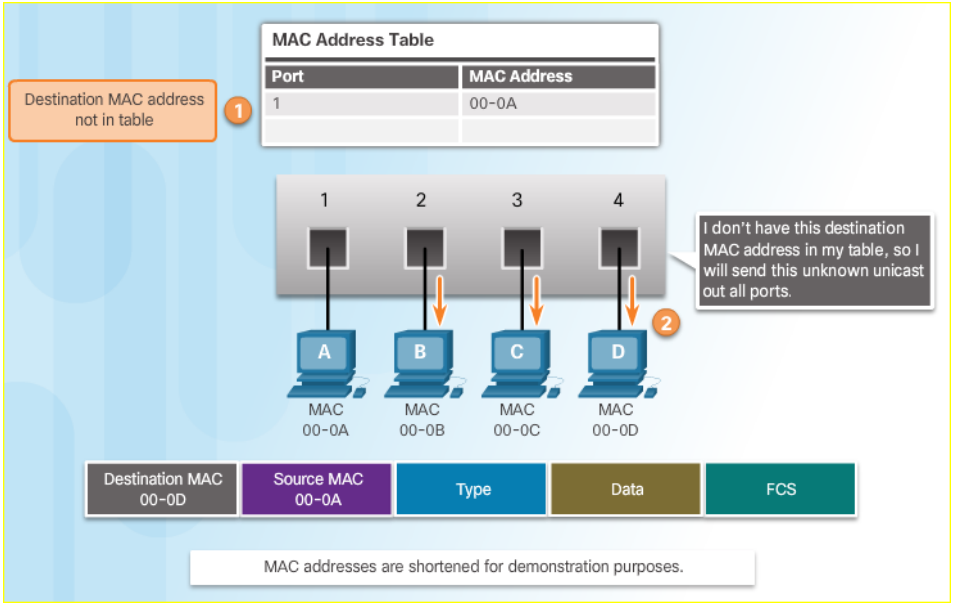
Learning MAC Addresses

- 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.)

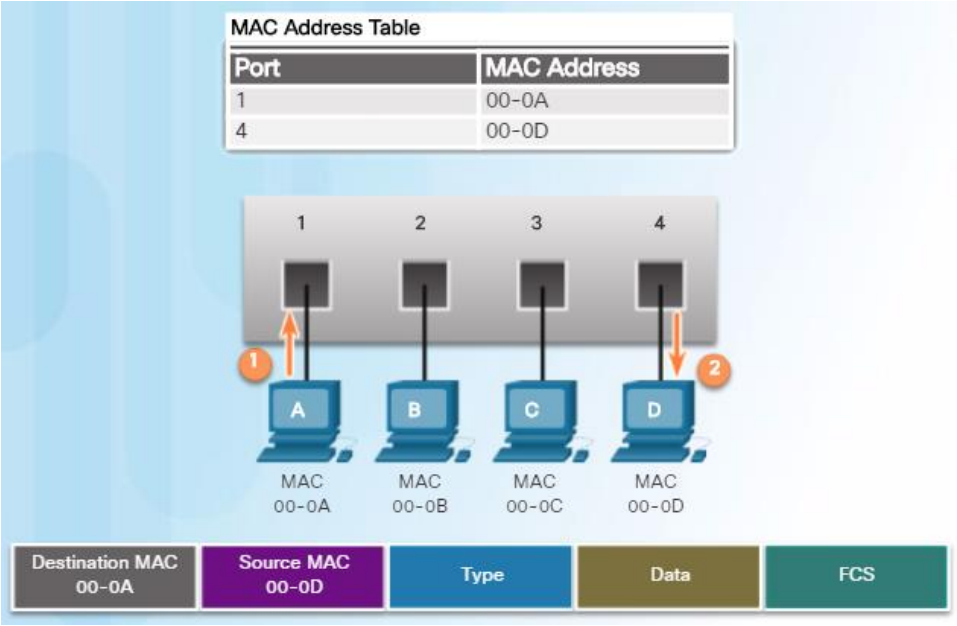
- The process to forward the Destination MAC Address is:
  - If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
  - If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
  - 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.



Switch Fundamentals

Switching Process	Description
Learn Examining the Source MAC Address	• 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.

Forward
Examining the Destination MAC Address
	• 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.

Lab – View the Switch MAC Address Table

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Examine the Switch MAC Address Table

7.5 Module Practice and Quiz

What did I learn in this module?

- Ethernet operates in the data link layer and the physical layer. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- Ethernet uses the LLC and MAC sublayers of the data link layer to operate.
- The Ethernet frame fields are: preamble and start frame delimiter, destination MAC address, source MAC address, EtherType, data, and FCS.
- 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, or 6 bytes.
- When a device is forwarding a message to an Ethernet network, the Ethernet header includes the source and destination MAC addresses. In Ethernet, different MAC addresses are used for Layer 2 unicast, broadcast, and multicast communications.

What did I learn in this module? (Contd.)

- A Layer 2 Ethernet switch makes its forwarding decisions based solely on the Layer 2 Ethernet MAC addresses.
- The switch dynamically builds the MAC address table by examining the source MAC address of the frames received on a port.
- The switch forwards frames by searching for a match between the destination MAC address in the frame and an entry in the MAC address table.


CISCO