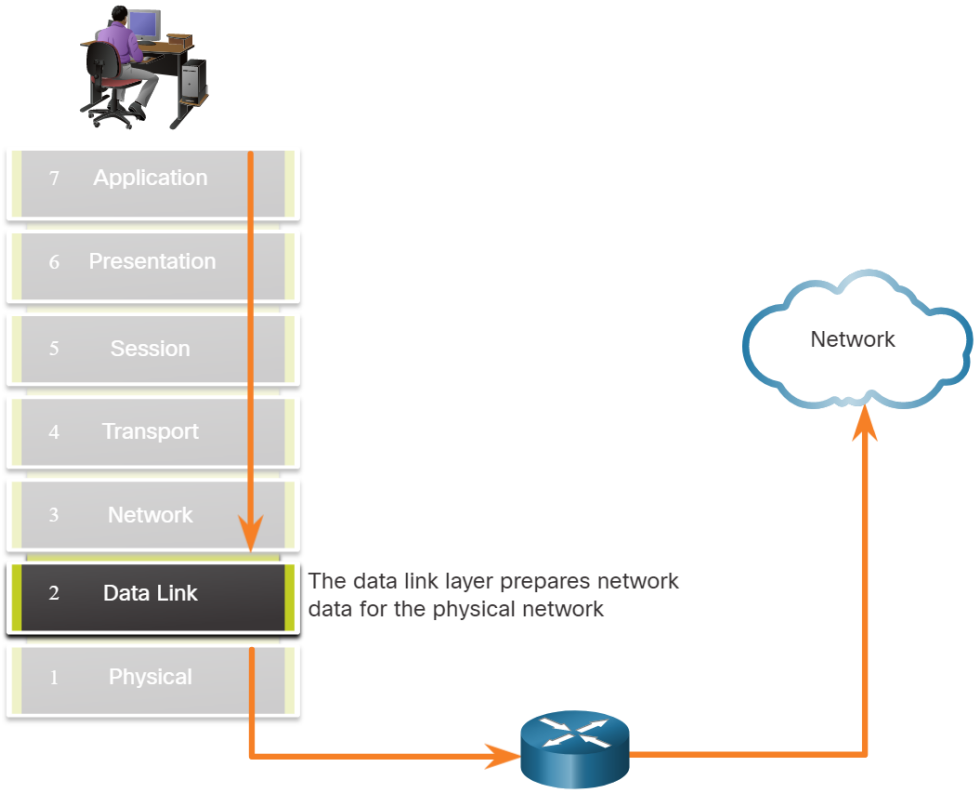
Chapter 6 & 7: Data link Layer and Ethernet Switching (CCNA v7.0)

Introduction to Networks

Cisco | Networking Academy®
Mind Wide Open™

Purpose of the Data Link Layer

- The data link layer of the OSI model (Layer 2), prepares network data for the physical network.
- The data link layer is responsible for network interface card (NIC) to network interface card communications.

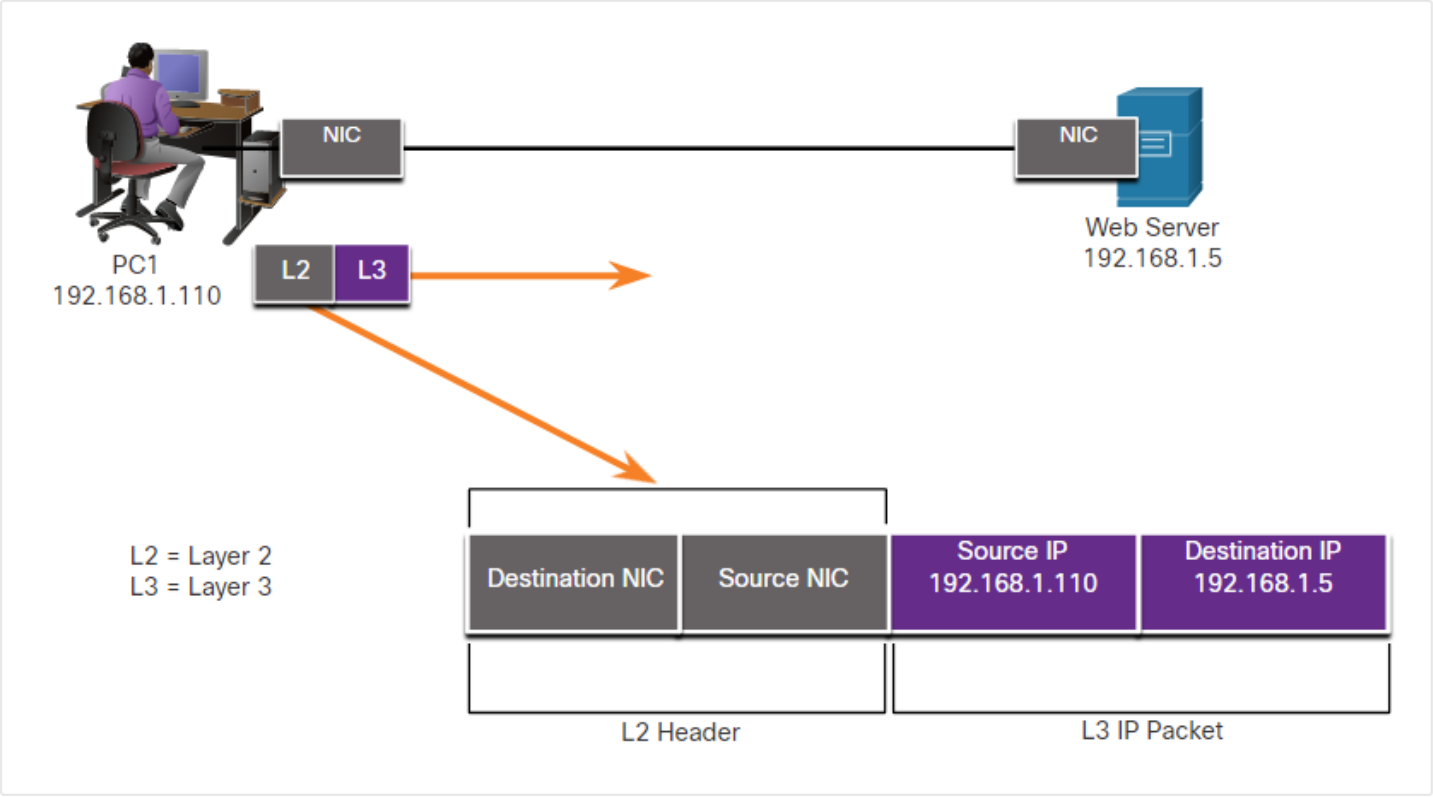


Purpose of the Data Link Layer

- The data link layer does the following:
  - Enables upper layers to access the media. The upper layer protocol is completely unaware of the type of media that is used to forward the data.
  - Accepts data, usually Layer 3 packets (i.e., IPv4 or IPv6), and encapsulates them into Layer 2 frames.
  - Controls how data is placed and received on the media.
  - Exchanges frames between endpoints over the network media.
  - Performs error detection and rejects any corrupt frame.

Purpose of the Data Link Layer

- The figure displays an example of how the data link layer adds Layer 2 Ethernet destination and source NIC information to a Layer 3 packet. It would then convert this information to a format supported by the physical layer (i.e., Layer 1).



Ethernet

Ethernet

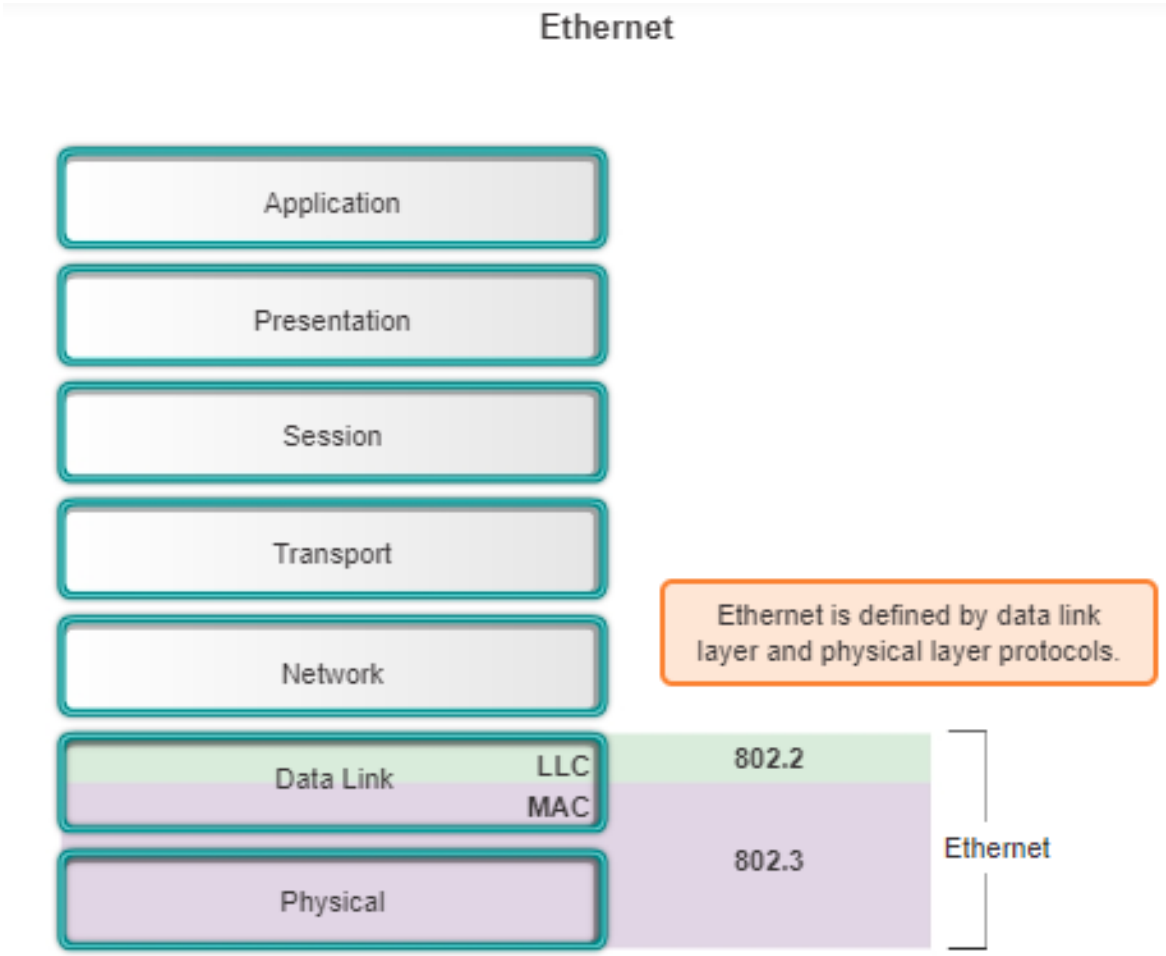
- One of the most widely used LAN technologies
- Operates in the data link layer and the physical layer
- Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports data bandwidths of 10 Mbps, 100 Mbps, 1000 Mbps (1Gbps), 10,000 Mbps (10 Gbps), 40,000 Mbps (40 Gbps), and 100,000 Mbps (100 Gbps)

Ethernet Standards

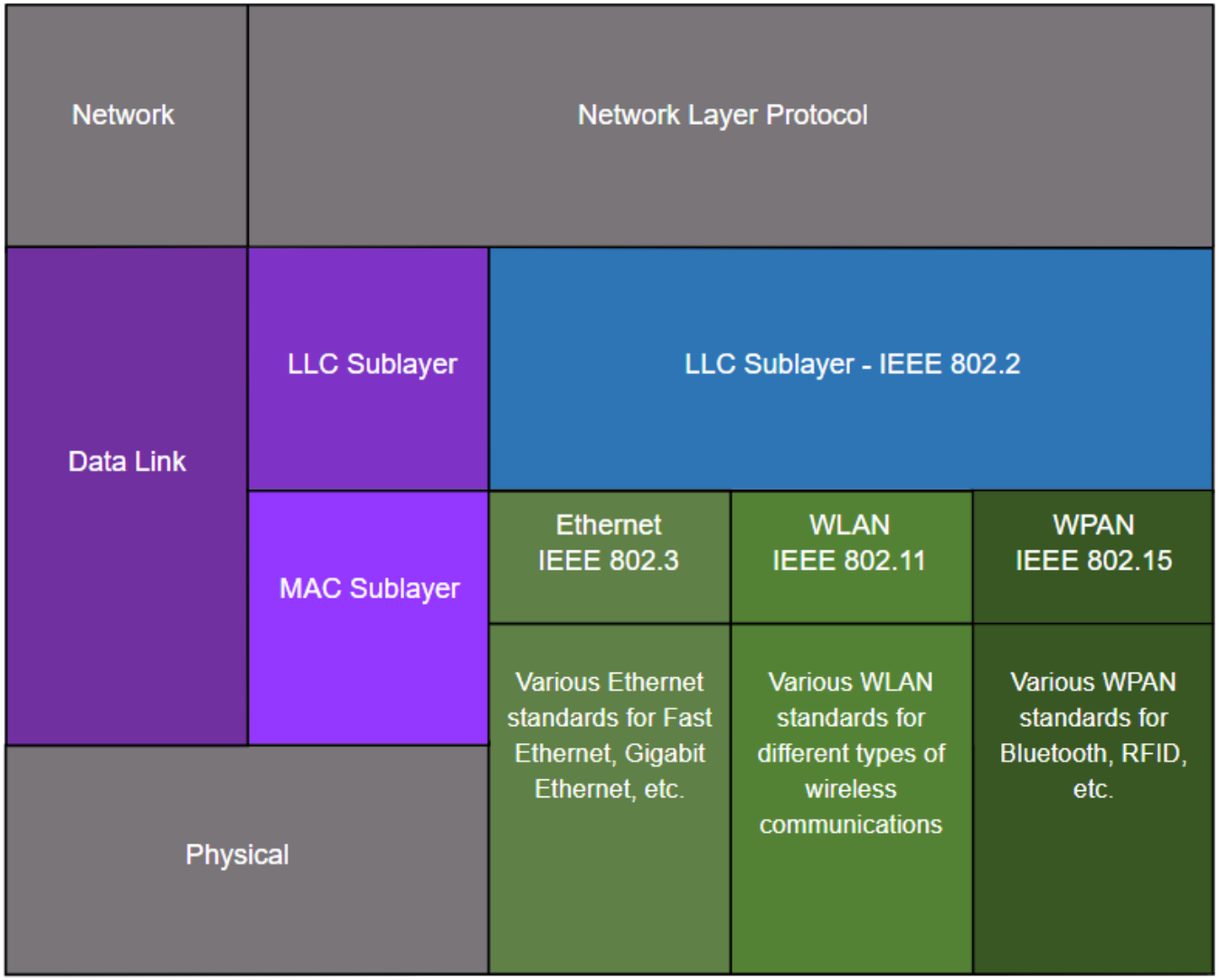
- Define Layer 2 protocols and Layer 1 technologies
- Two separate sub layers of the data link layer to operate – Logical link control (LLC) and the MAC sublayers

Ethernet Operation

LLC and MAC Sublayers



LLC and MAC Sublayers (cont.)



LLC Sublayer

Logical Link Control (LLC)

- This IEEE 802.2 sublayer communicates between the networking software at the upper layers and the device hardware at the lower layers.
- It places information in the frame that identifies which network layer protocol is being used for the frame.
- Implemented in software, and its implementation is independent of the hardware.
- In a computer, the LLC can be considered the driver software for the NIC.

MAC Sublayer

Media Access Control (MAC)

- This sublayer (IEEE 802.3, 802.11, or 802.15 for example) is implemented in hardware.
- It is responsible for data encapsulation and media access control.
- It provides data link layer addressing and it is integrated with various physical layer technologies.

MAC Sublayers (cont.)

Data Encapsulation - IEEE 802.3 data encapsulation includes the following:

- **Ethernet frame** - This is the internal structure of the Ethernet frame.
- **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.
- **Ethernet Error detection** - The Ethernet frame includes a frame check sequence (FCS) trailer used for error detection.

Accessing the Media

- MAC sublayer includes the specifications for different Ethernet communications standards over various types of media including copper and fiber.

Media Access Control

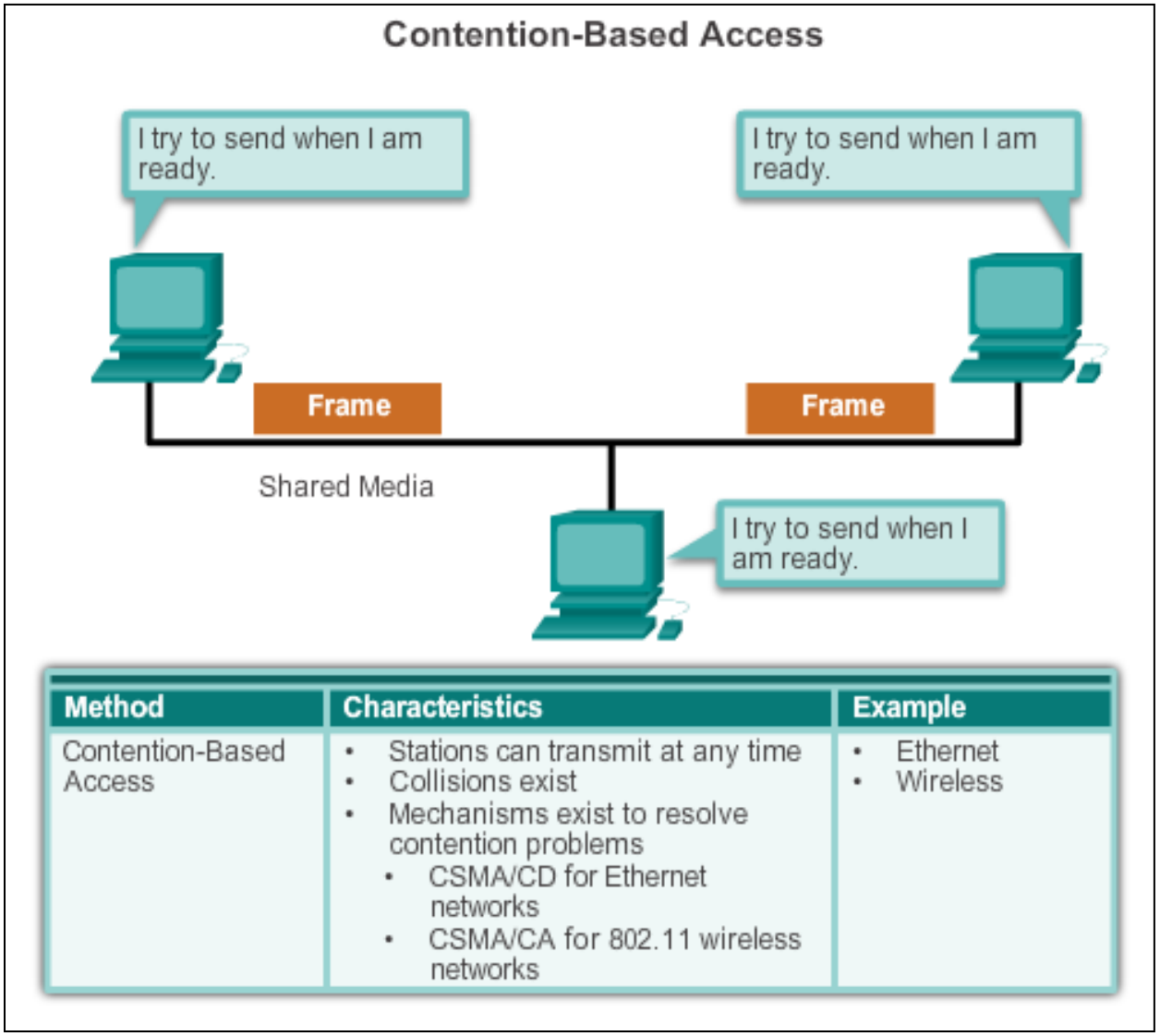
- Ethernet LANs and WLANs are examples of multiaccess networks.
- A multiaccess network is a network that can have two or more end devices attempting to access the network simultaneously.
- If multiple devices on a single medium attempt to forward data simultaneously, the data will collide resulting in corrupted, unusable data
- Ethernet provides a method for controlling how the nodes share access through the use of a Carrier Sense Multiple Access (CSMA) technology

Media Access Control (cont.)

Carrier Sense Multiple Access (CSMA) process

- Used to first detect if the media is carrying a signal
- If no carrier signal is detected, the device transmits its data
- If two devices transmit at the same time - data collision

Media Access Control (cont.)



Method	Characteristics	Example

Contention-Based Access	• Stations can transmit at any time
	• Collisions exist
	• Mechanisms exist to resolve contention problems
	  • CSMA/CD for Ethernet networks
	  • CSMA/CA for 802.11 wireless networks
		• Ethernet
		• Wireless

Carrier Sense Multiple Access/Collision Detection

CSMA/CD

- The device monitors the media for the presence of a data signal
- If a data signal is absent, indicating that the media is free, the device transmits the data
- If signals are then detected that show another device was transmitting at the same time, all devices stop sending & try again later
- Almost all wired connections between devices in a LAN today are full-duplex connections - a device is able to send and receive simultaneously. Therefore collisions do not occur and the processes utilized by CSMA/CD are really unnecessary
- Wireless connections in a LAN environment still have to take collisions into account

Carrier Sense Multiple Access/Collision Avoidance

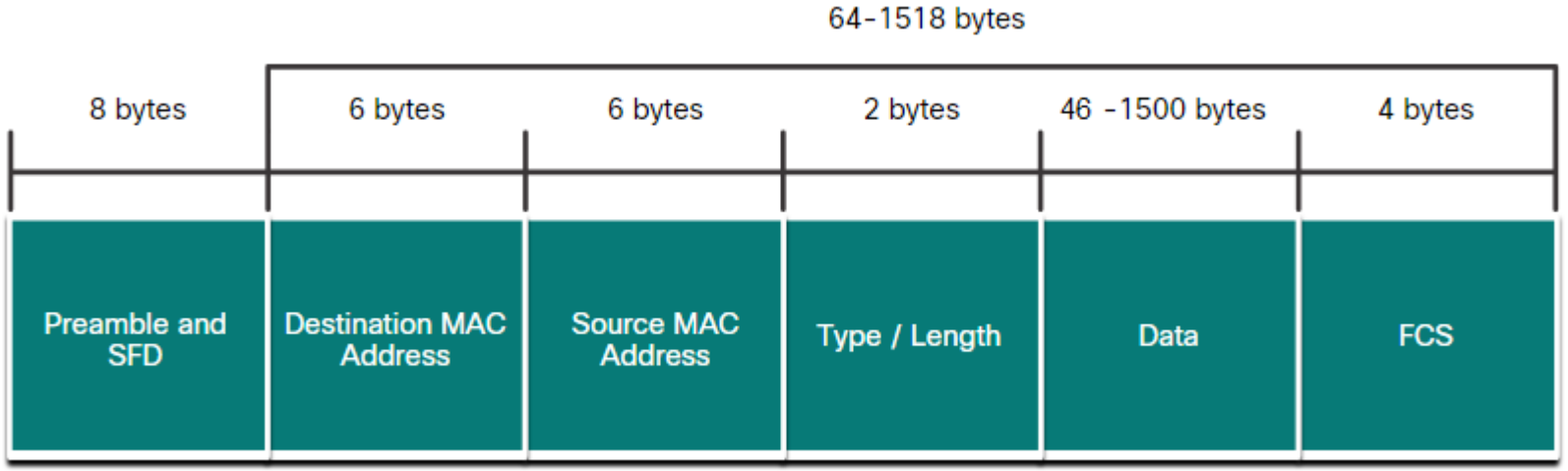
CSMA/CA

- Device examines the media for the presence of data signal - if the media is free, the device sends a notification across the media of its intent to use it
- The device then sends the data
- Used by 802.11 wireless networking technologies

Ethernet Frame Size

- The minimum Ethernet frame size is 64 bytes and the maximum is 1518 bytes.
- This includes all bytes from the destination MAC address field through the frame check sequence (FCS) field.
- 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 by receiving stations.
- 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.

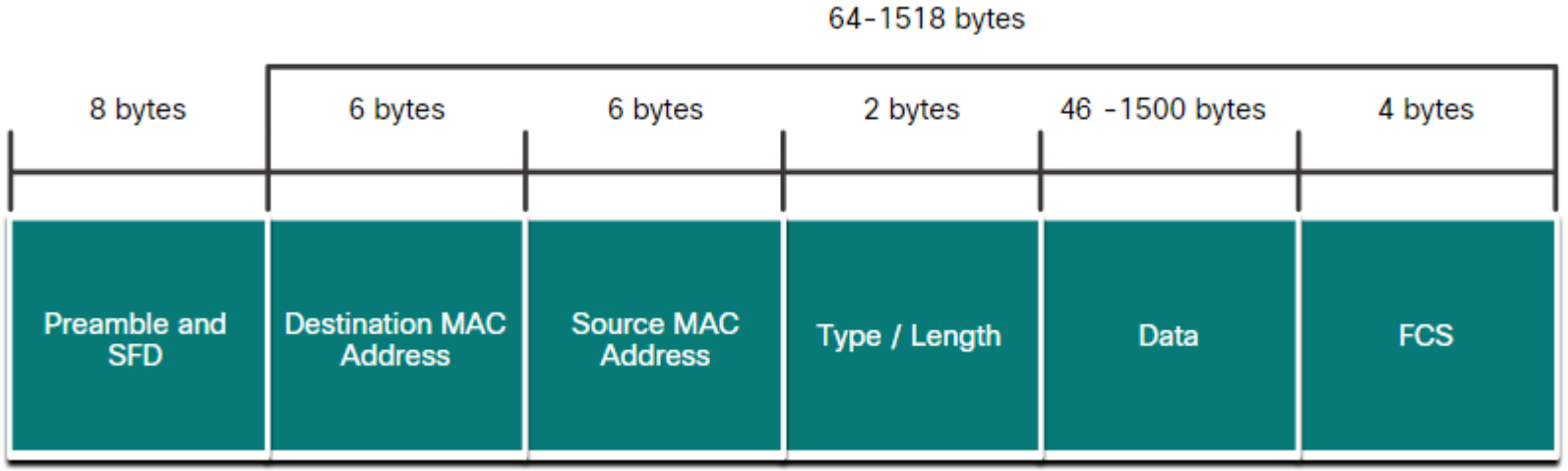
Ethernet Frame



Preamble and Start Frame Delimiter Fields

- Also called the Start of Frame.
- Used for synchronization between the sending and receiving devices.
- Essentially, the first few bytes tell the receivers to get ready to receive a new frame.

Ethernet Frame



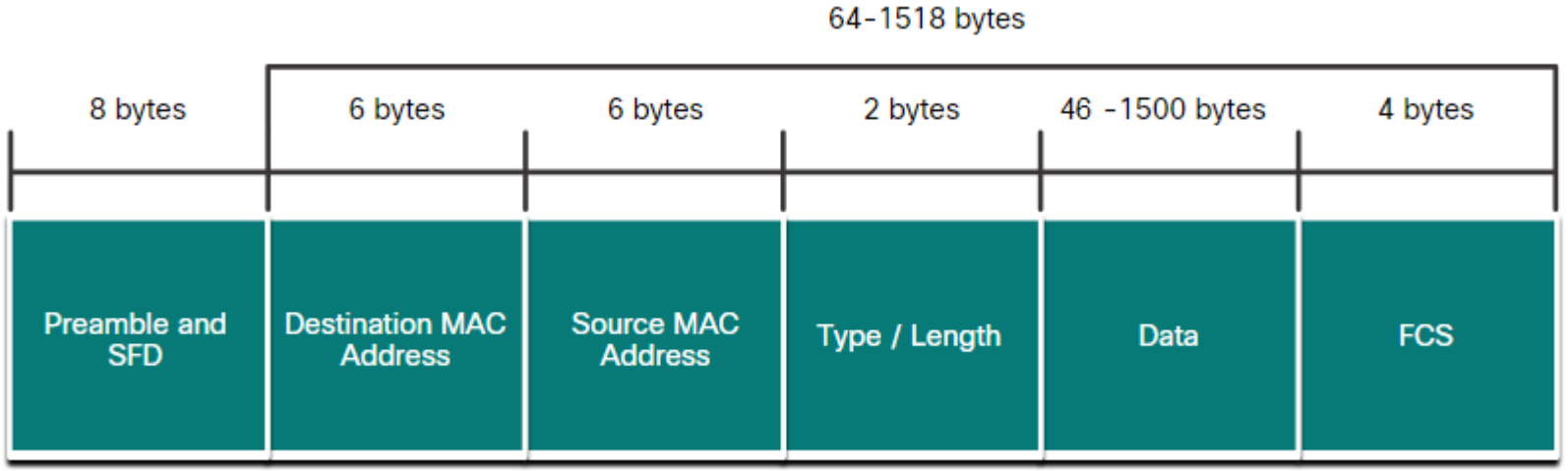
Length/Type Field –

- This 2-byte field identifies the upper layer protocol encapsulated in the Ethernet frame.
- Common values are, in hexadecimal, 0x800 for IPv4, 0x86DD for IPv6 and 0x806 for ARP.

Data Field –

- Contains the encapsulated data from a higher layer, an IPv4 packet.
- All frames must be at least 64 bytes long.
- If a small packet is encapsulated, additional bits called a pad are used to increase the size of the frame to this minimum size.

Ethernet Frame

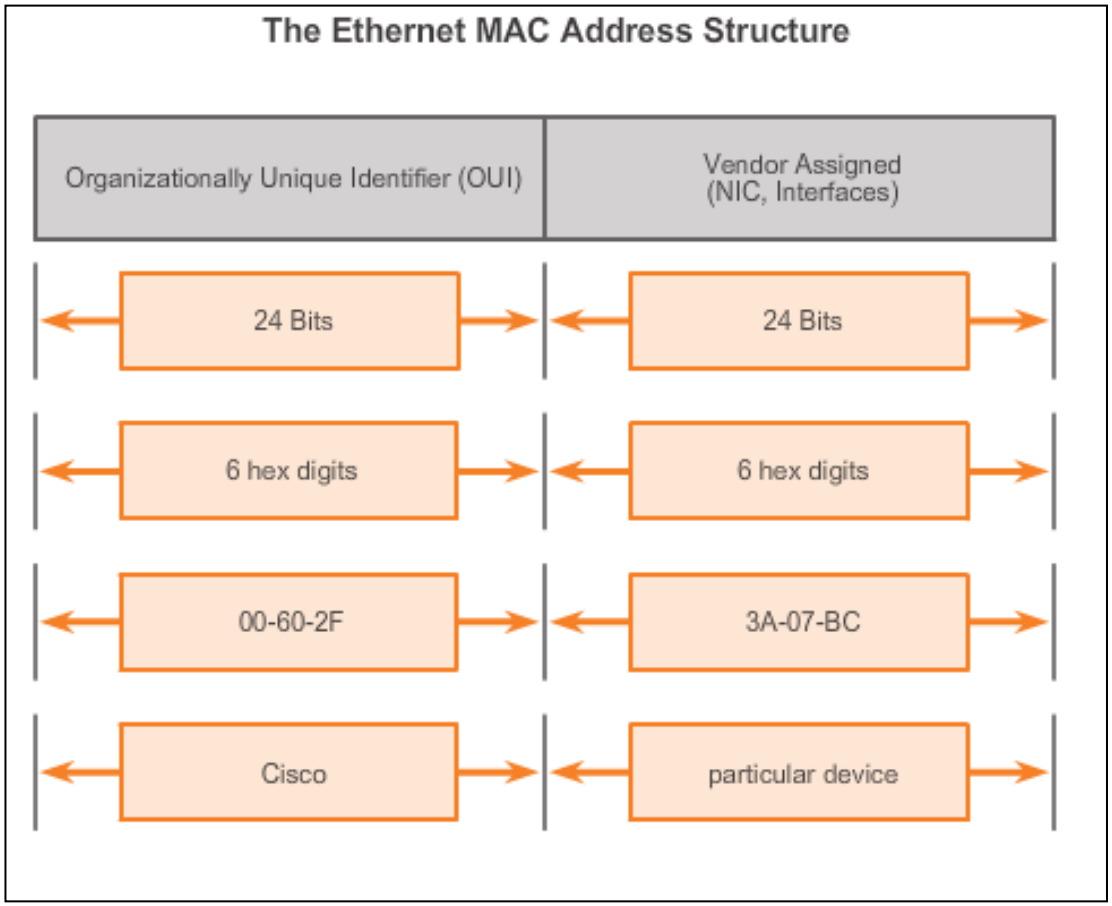


Frame Check Sequence Field

- Used to detect errors in a frame with cyclic redundancy check (4 bytes).
- If calculations match at source and receiver, no error occurred.
- If calculations do not match, the data has changed; therefore, the frame is dropped.

MAC Address: Ethernet Identity

- Layer 2 Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits.
- IEEE requires a vendor to follow these rules:
  - Must use that vendor's assigned OUI as the first 6 hexadecimal digits.
  - All MAC addresses with the same OUI must be assigned a unique value in the last 6 hexadecimal digits.



Frame Processing

- MAC addresses assigned to workstations, servers, printers, switches, and routers.
- Example MACs:
  - 00-05-9A-3C-78-00
  - 00:05:9A:3C:78:00
  - 0005.9A3C.7800.
- When a device is forwarding a message to an Ethernet network, attaches header information to the packet, contains the source and destination MAC address.
- Each NIC views information to see if the destination MAC address in the frame matches the device's physical MAC address stored in RAM.
- No match, the device discards the frame.
- Matches the destination MAC of the frame, the NIC passes the frame up the OSI layers, where the de-encapsulation process takes place.

MAC Address Representations

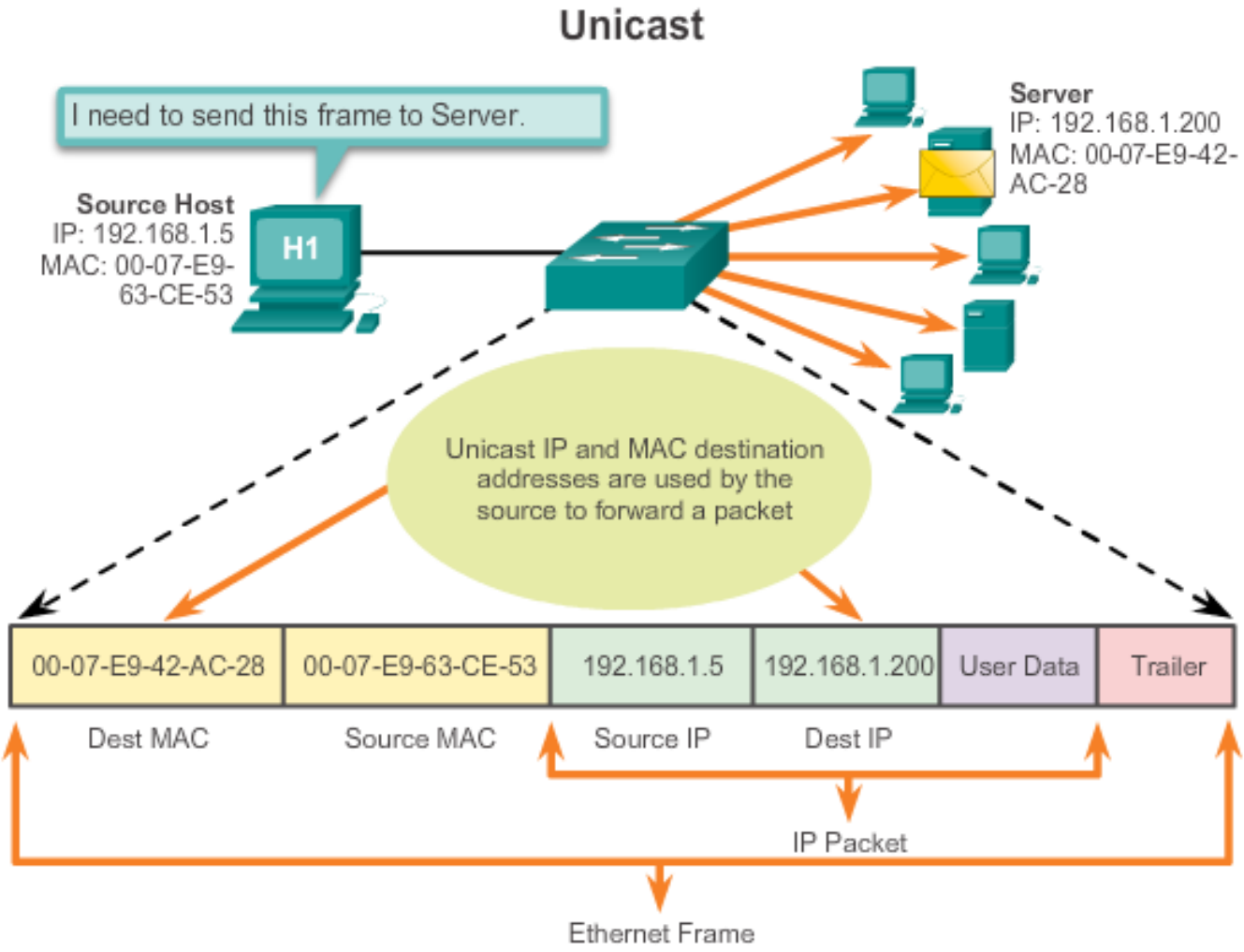
```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-18-DE-C7-F3-FB
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 192.168.1.67(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, November 26, 2012 12:14:48 PM
   Lease Expires . . . . . . . . . . : Saturday, December 01, 2012 12:15:02 AM
   Default Gateway . . . . . . . . . : 192.168.1.254
   DHCP Server . . . . . . . . . . . : 192.168.1.254
   DNS Servers . . . . . . . . . . . : 192.168.1.254
```

With Dashes 00-60-2F-3A-07-BC

With Colons 00:60:2F:3A:07:BC

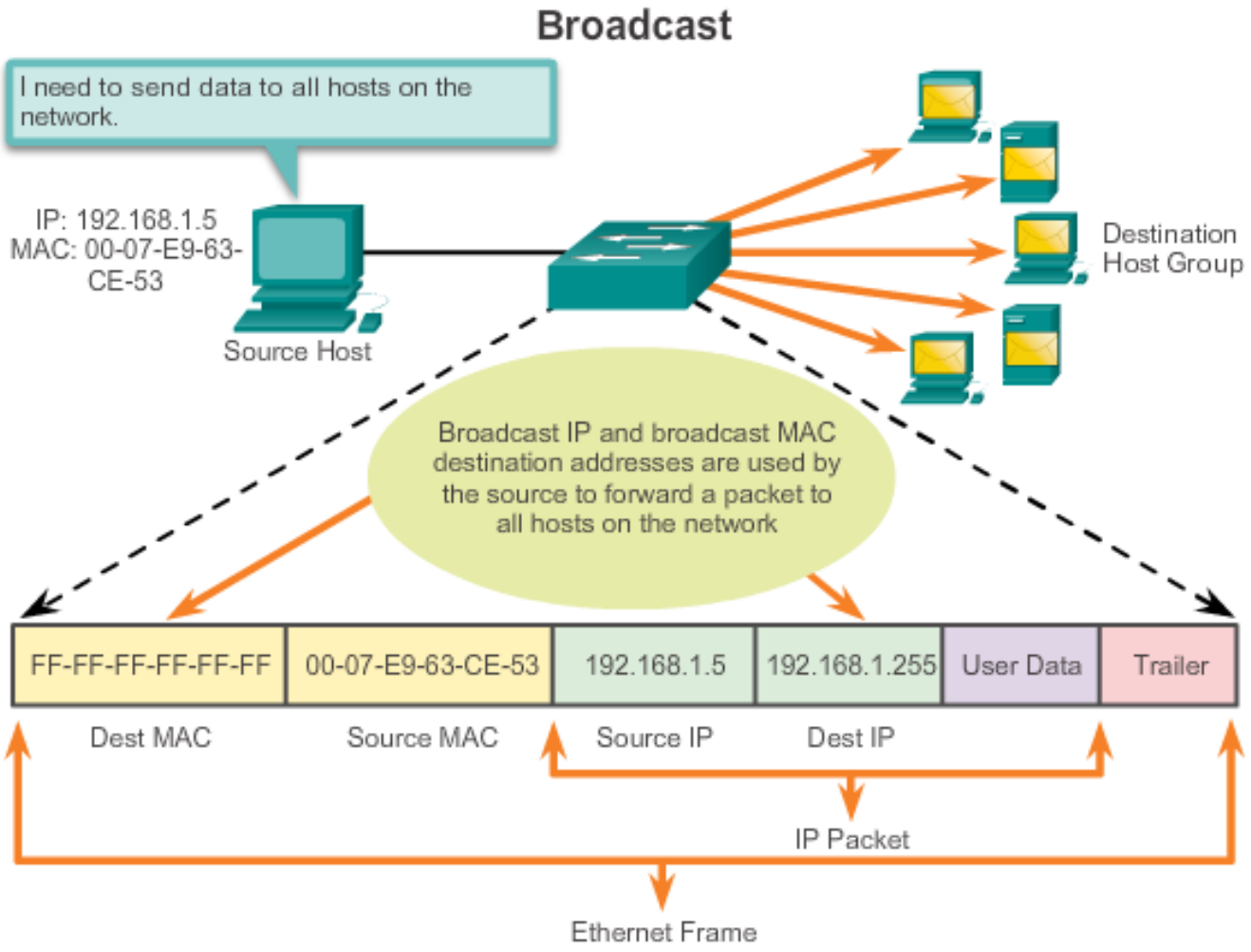
With Periods 0060.2F3A.07BC

Unicast MAC Address

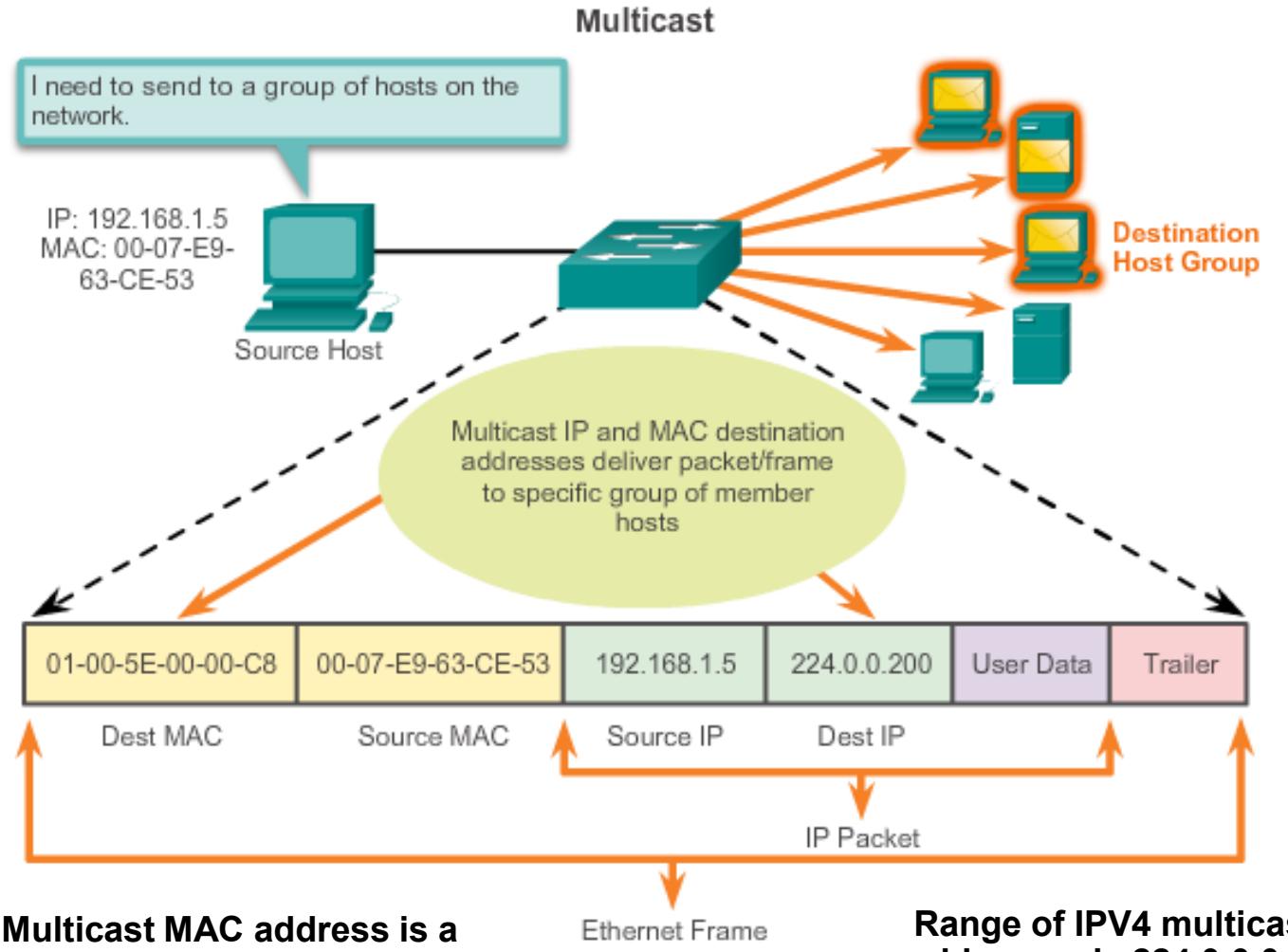


Ethernet MAC

Broadcast MAC Address



Multicast MAC Address



Multicast MAC address is a special value that begins with 01-00-5E in hexadecimal

Range of IPV4 multicast addresses is 224.0.0.0 to 239.255.255.255

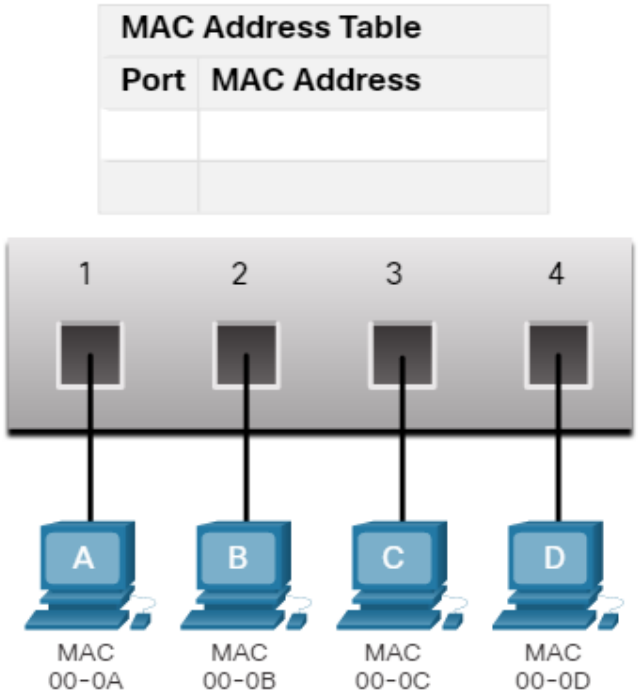
Switch Fundamentals

Layer 2 Ethernet Switch

- Connects end devices to a central intermediate device on most Ethernet networks
- Uses Layer 2 MAC addresses to make forwarding decisions. It is completely unaware of the data (protocol) being carried in the data portion of the frame, such as an IPv4 packet, an ARP message, or an IPv6 packet.
- Builds a MAC address table that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks

Switch Fundamentals

In the figure, the four-port switch was just powered on. The table shows the MAC Address Table which has not yet learned the MAC addresses for the four attached PCs.



The switch MAC address table is empty.

Switch Learning and forwarding

- 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.

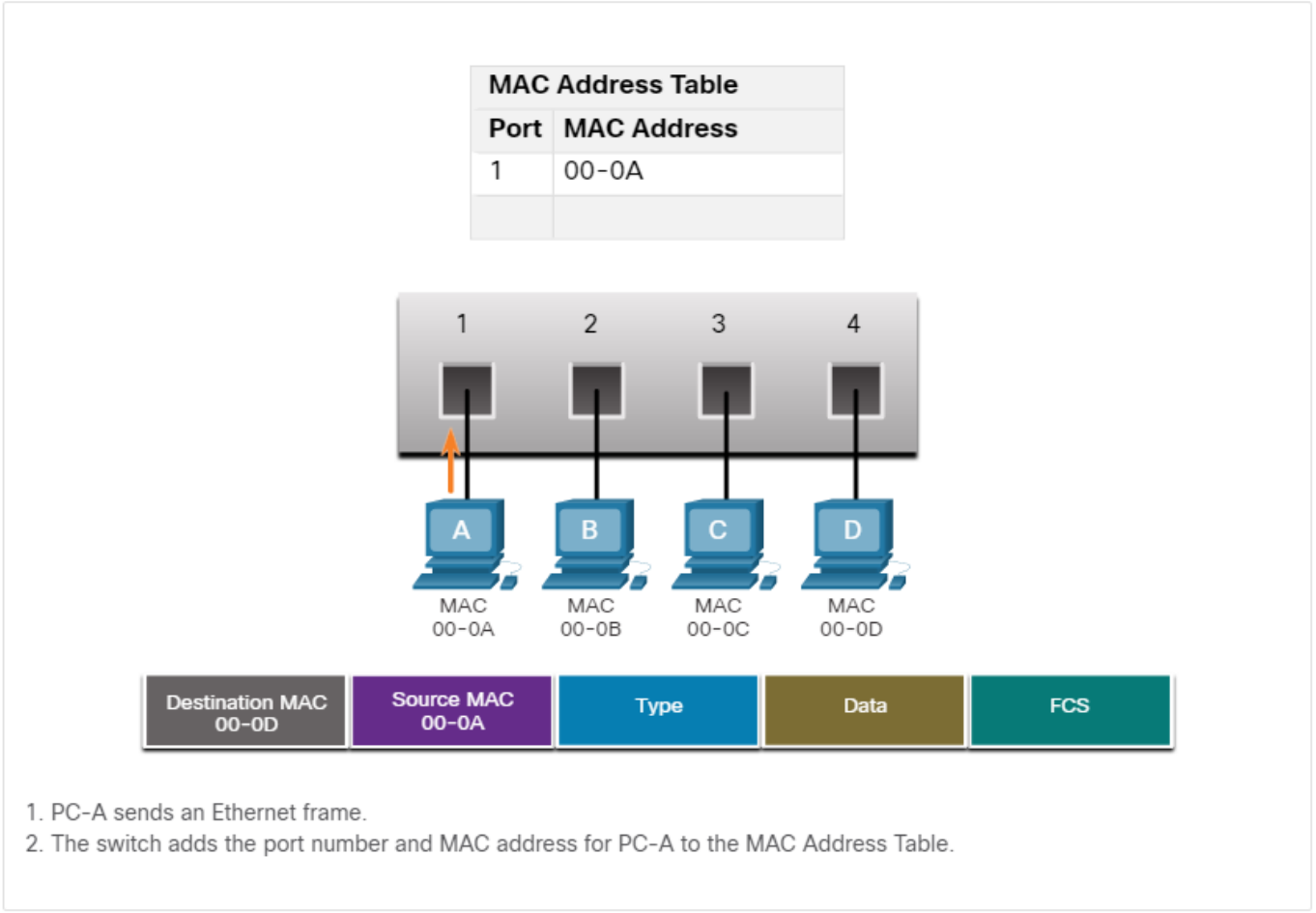
Switch Learning

Examine the Source MAC Address

- Every frame that enters a switch is checked for new information to learn.
- It does this by examining the source MAC address of the frame and the port number where the frame entered the switch.
- If the source MAC address does not exist, it is added to the table along with the incoming 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.

Switch Learning

In the figure for example, PC-A is sending an Ethernet frame to PC-D. The table shows the switch adds the MAC address for PC-A to the MAC Address Table.



Switch Forwarding

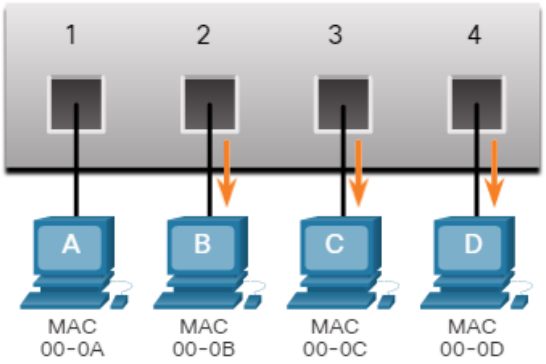
Find the Destination MAC Address

- If the destination MAC address is a unicast address, the switch will look for a match between the destination MAC address of the frame and an entry 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, the switch will forward the frame out all ports except the incoming port. This is called an unknown unicast.

Switch Forwarding

As shown in the figure, the switch does not have the destination MAC address in its table for PC-D, so it sends the frame out all ports except port 1.

MAC Address Table	
Port	MAC Address
1	00-0A



1. The destination MAC address is not in the table.
2. The switch forwards the frame out all other ports.

Do the activity!