Ch 5: Ethernet

Computer Networks Course

BY

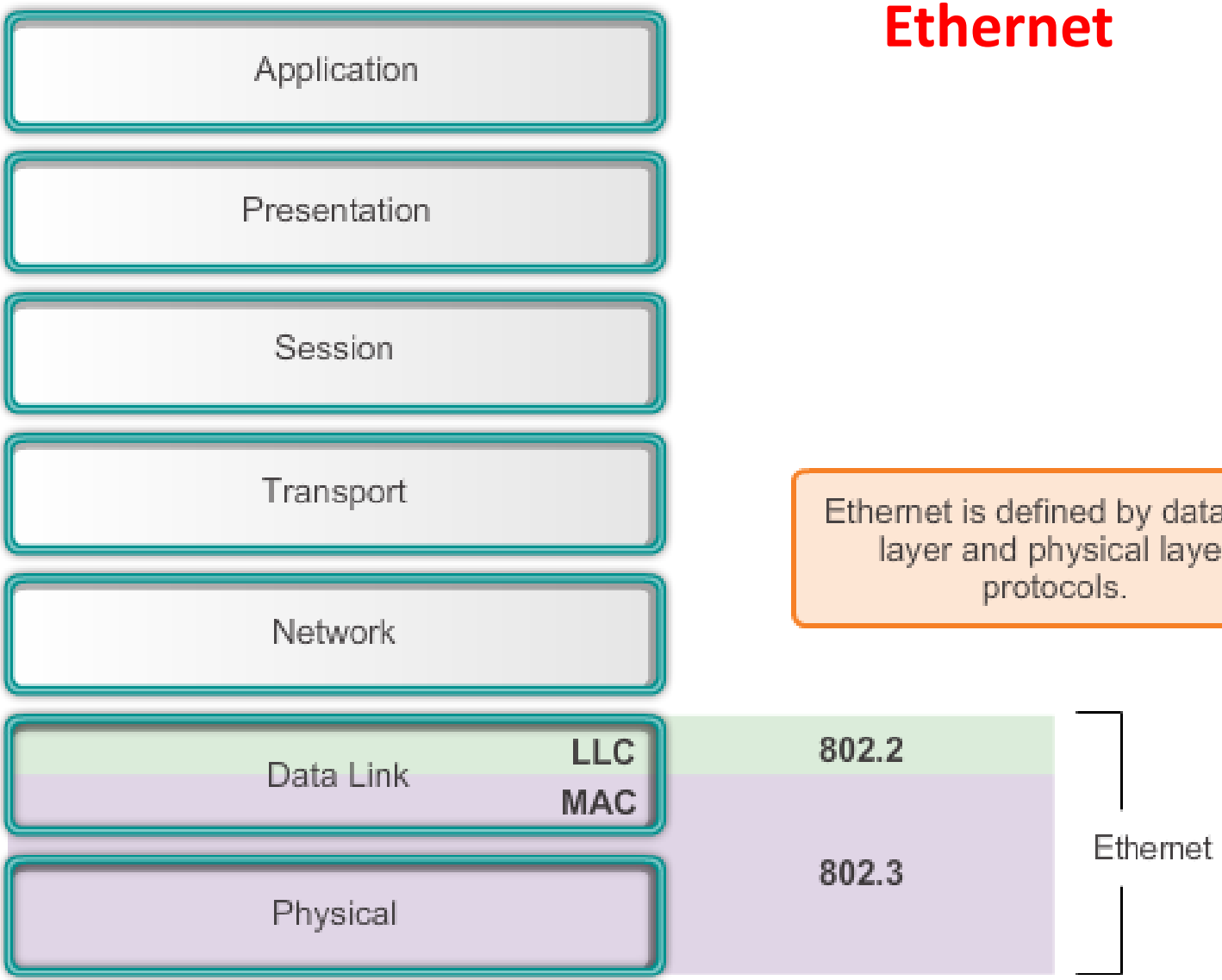
Dr. Essam Halim Houssein

Cisco | Networking Academy®
Mind Wide Open™

Version 5.0

The Ethernet protocol standards define many aspects of network communication including **frame format, frame size, timing, and encoding.** When messages are sent between hosts on an Ethernet network, the hosts format the messages into the frame layout that is specified by the standards. The OSI model separates the data link layer functionalities of addressing, framing, and accessing the media from the physical layer standards of the media. **Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.**

Ethernet



Ethernet is defined by data link layer and physical layer protocols.

LLC sublayer

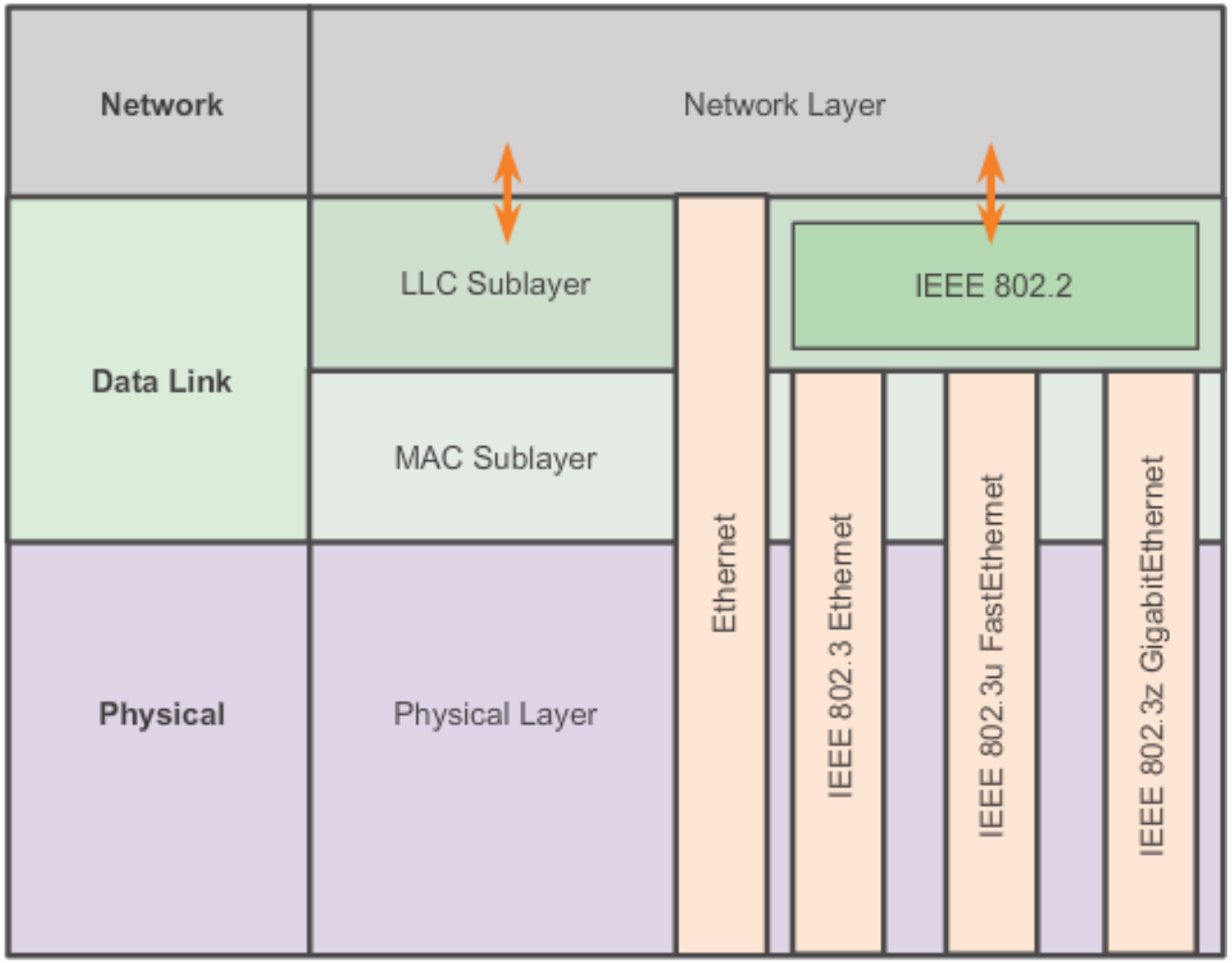
The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. **This is typically between the networking software and the device hardware.** The LLC is used to communicate with the upper layers of the application, and transition the packet to the lower layers for delivery.

LLC is 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

MAC constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, **typically in the computer NIC**. The specifics are listed in the IEEE 802.3 standards. Next figure lists common IEEE Ethernet standards.

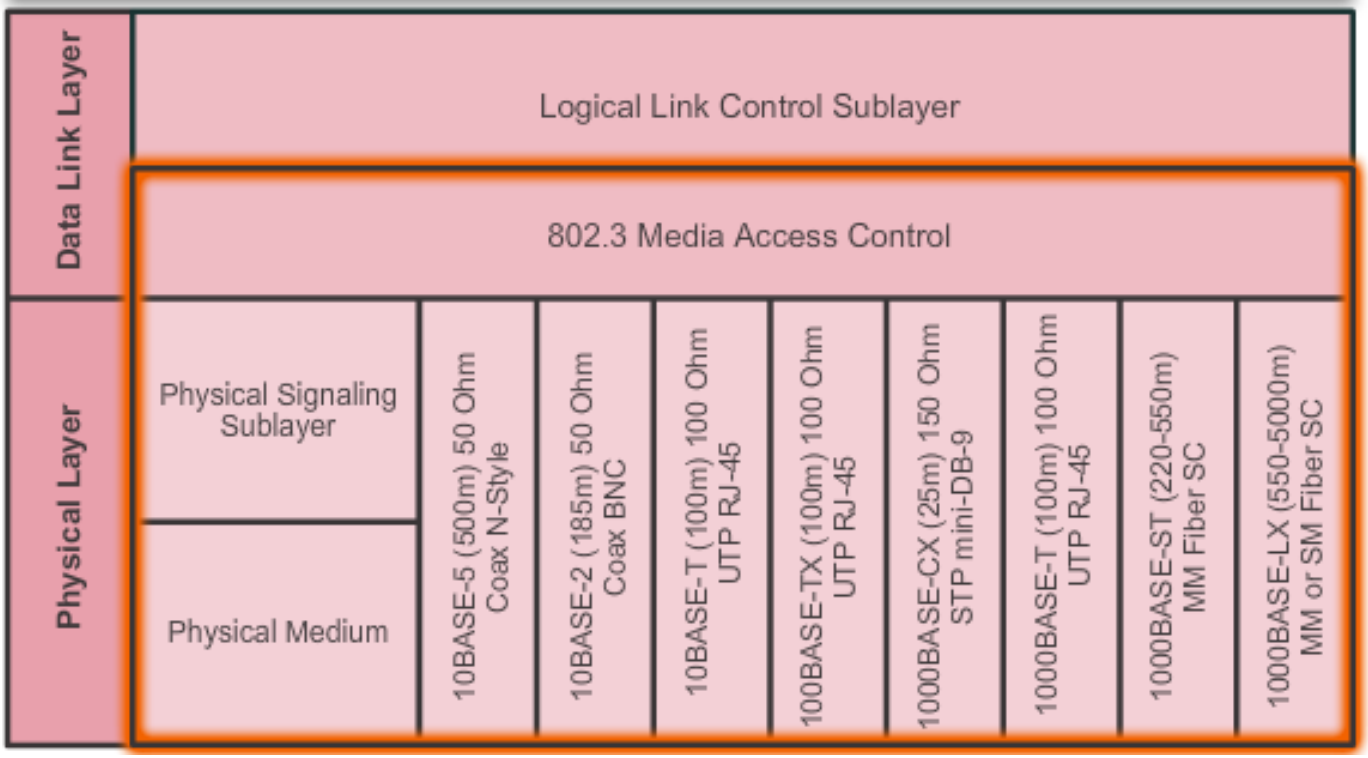
Common IEEE Ethernet standards



the Ethernet MAC sublayer has two primary responsibilities:

Data Encapsulation
- Frame delimiting
- Addressing
- Error detection

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



Data encapsulation

Data encapsulation provides three primary functions:

Frame delimiting - These delimiting bits provide synchronization between the transmitting and receiving nodes.

Addressing - The encapsulation process contains the Layer 3 PDU and also provides for data link layer addressing.

Error detection - Each frame contains a trailer used to detect any errors in transmissions.

The use of frames aids in the transmission of bits as they are placed on the media and in the grouping of bits at the receiving node.

Media Access Control

Media access control is responsible for the placement of frames on the media and the removal of frames from the media. **As its name implies, it controls access to the media. This sublayer communicates directly with the physical layer.**

Ethernet Frame Fields

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 a frame.

Frame less than 64 bytes in length is considered a "collision fragment" or "runt frame". Frames with more than 1500 bytes of data are considered "jumbo" or "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 II Frame Structure and Field Size

Ethernet II is the Ethernet frame format used in TCP/IP networks.

Ethernet II

8 Bytes	6 Bytes	6 Bytes	2 Bytes	46 to 1500 Bytes	4 Bytes
Preamble	Destination Address	Source Address	Type	Data	Frame Check Sequence

Activity (1)

	MAC	LLC
1. Controls the network interface card through software drivers.		
2. Works with the upper layers to add application information for delivery of data to higher level protocols.		
3. Works with hardware to support bandwidth requirements and checks errors in the bits sent and received.		
4. Controls access to the media through signaling and physical media standards requirements.		
5. Supports Ethernet technology by using CSMA/CD or CSMA/CA.		
6. Remains relatively independent of physical equipment.		

	MAC	LLC
1. Controls the network interface card through software drivers.		✓
2. Works with the upper layers to add application information for delivery of data to higher level protocols.		✓
3. Works with hardware to support bandwidth requirements and checks errors in the bits sent and received.	✓	
4. Controls access to the media through signaling and physical media standards requirements.	✓	
5. Supports Ethernet technology by using CSMA/CD or CSMA/CA.	✓	
6. Remains relatively independent of physical equipment.		✓

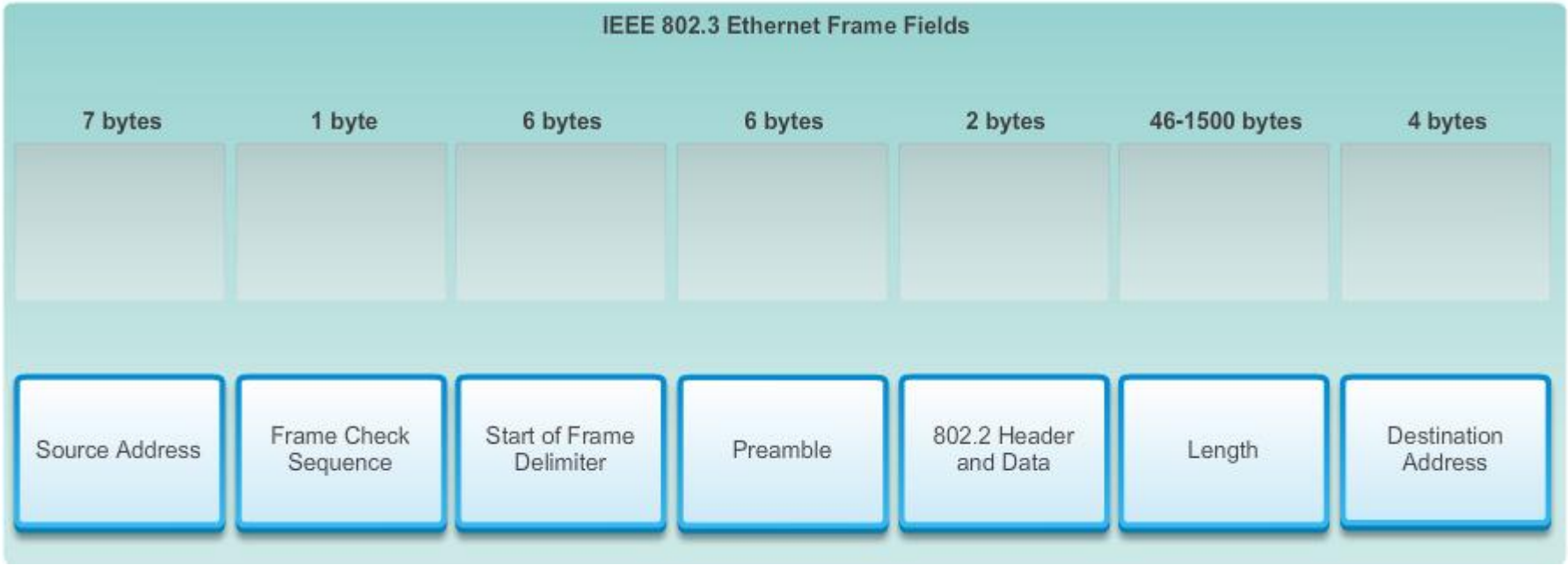
Activity (2)

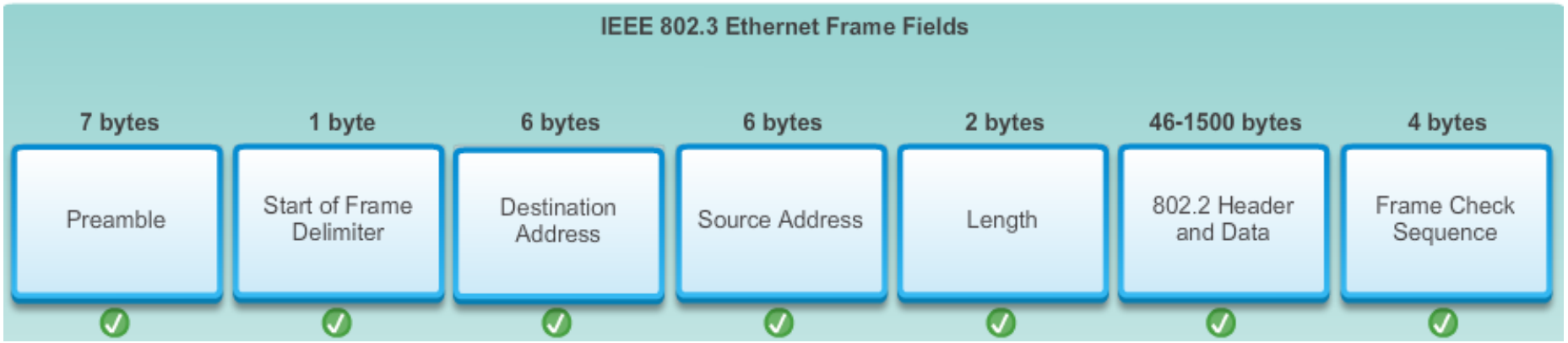
- 802.2 Header and Data
- Frame Check Sequence
- Type
- Start of Frame Delimiter
- Destination Address
- Preamble
- Source Address

Field Name	802.3 Ethernet Frame Field Descriptions
	Uses Pad to increase this frame field to at least 64 bytes
	Describes which higher-layer protocol has been used
	The frame's originating NIC or interface MAC address
	Assists a host in determining if the frame received is addressed to it
	Notifies destinations to get ready for a new frame
	Synchronizes sending and receiving devices for frame delivery
	Detects errors in an Ethernet frame

Field Name	802.3 Ethernet Frame Field Descriptions
802.2 Header and Data	Uses Pad to increase this frame field to at least 64 bytes
Type	Describes which higher-layer protocol has been used
Source Address	The frame's originating NIC or interface MAC address
Destination Address	Assists a host in determining if the frame received is addressed to it
Preamble	Notifies destinations to get ready for a new frame
Start of Frame Delimiter	Synchronizes sending and receiving devices for frame delivery
Frame Check Sequence	Detects errors in an Ethernet frame

Activity (3)





MAC Address and Hexadecimal

An Ethernet MAC address is a 48-bit binary value expressed as **12 hexadecimal** digits (4 bits per hexadecimal digit).

The base sixteen number system uses the numbers 0 to 9 and the letters A to F.

Representing Hexadecimal Values

The technical representation of hexadecimal is preceded with "0x" (zero X). Therefore, the examples above would be shown as 0x0A and 0x73 respectively.

Hexadecimal is used to represent Ethernet MAC addresses and IP Version 6 addresses.

Hexadecimal Conversions

it is usually easier to convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as appropriate.

Hexadecimal Numbering

Selected Decimal, Binary, and Hexadecimal equivalents

Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111 0000	F0
255	1111 1111	FF

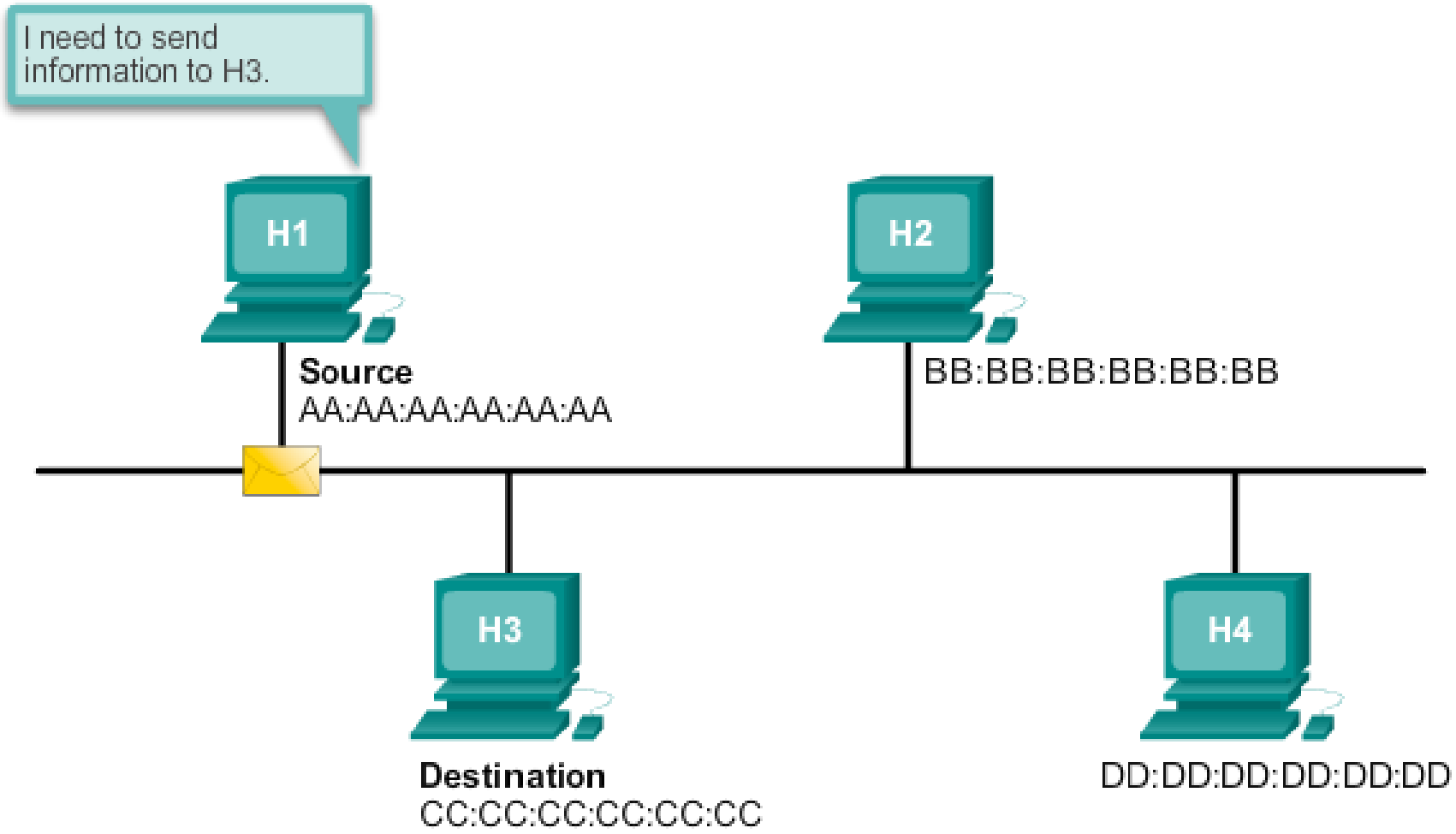
MAC Address Structure

The MAC address value is a direct result of IEEE-enforced rules for vendors to ensure globally unique addresses for each Ethernet device. The IEEE assigns the vendor a 3-byte (24-bit) code, called the **Organizationally Unique Identifier (OUI).**

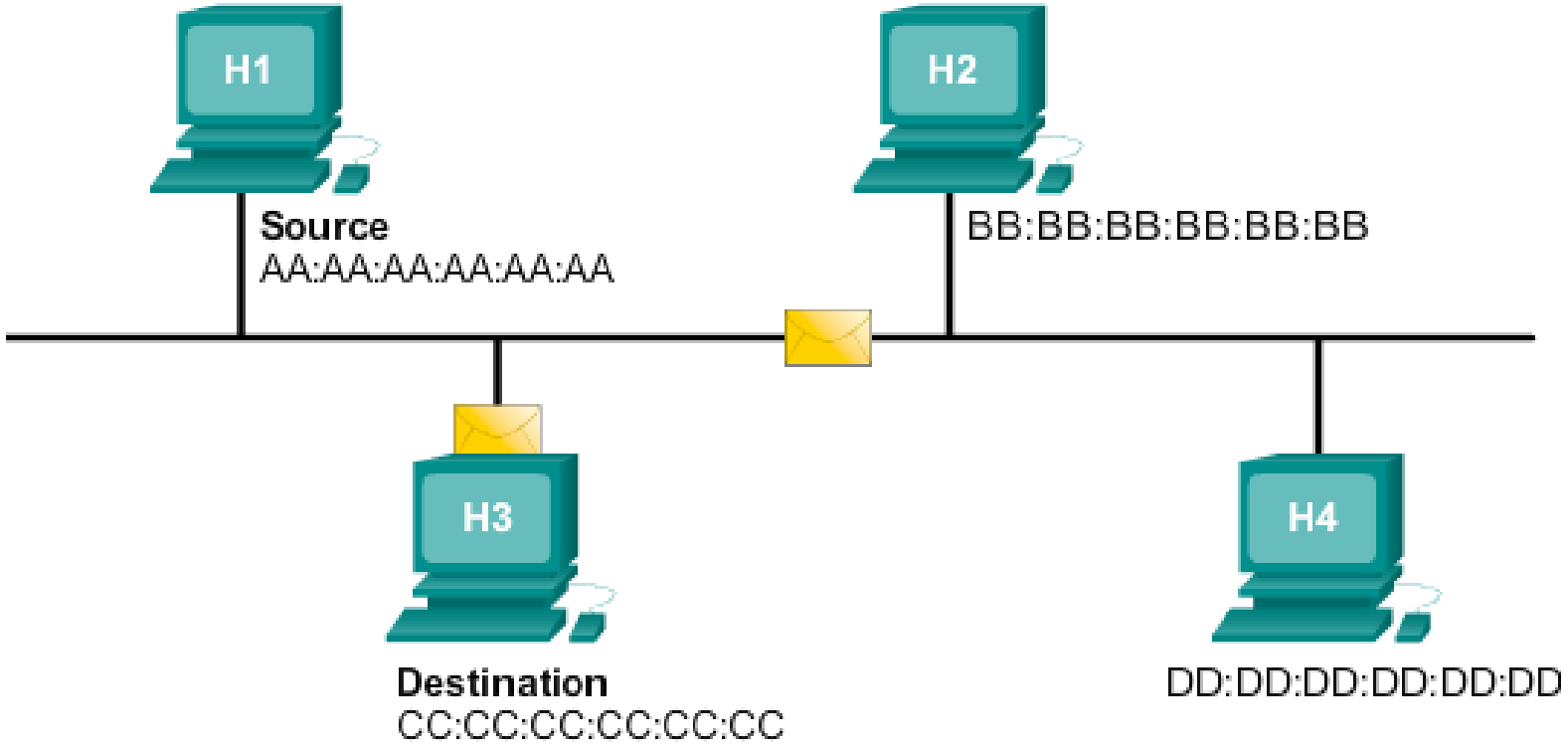
IEEE requires a vendor to follow two simple rules:

1. All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
2. All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

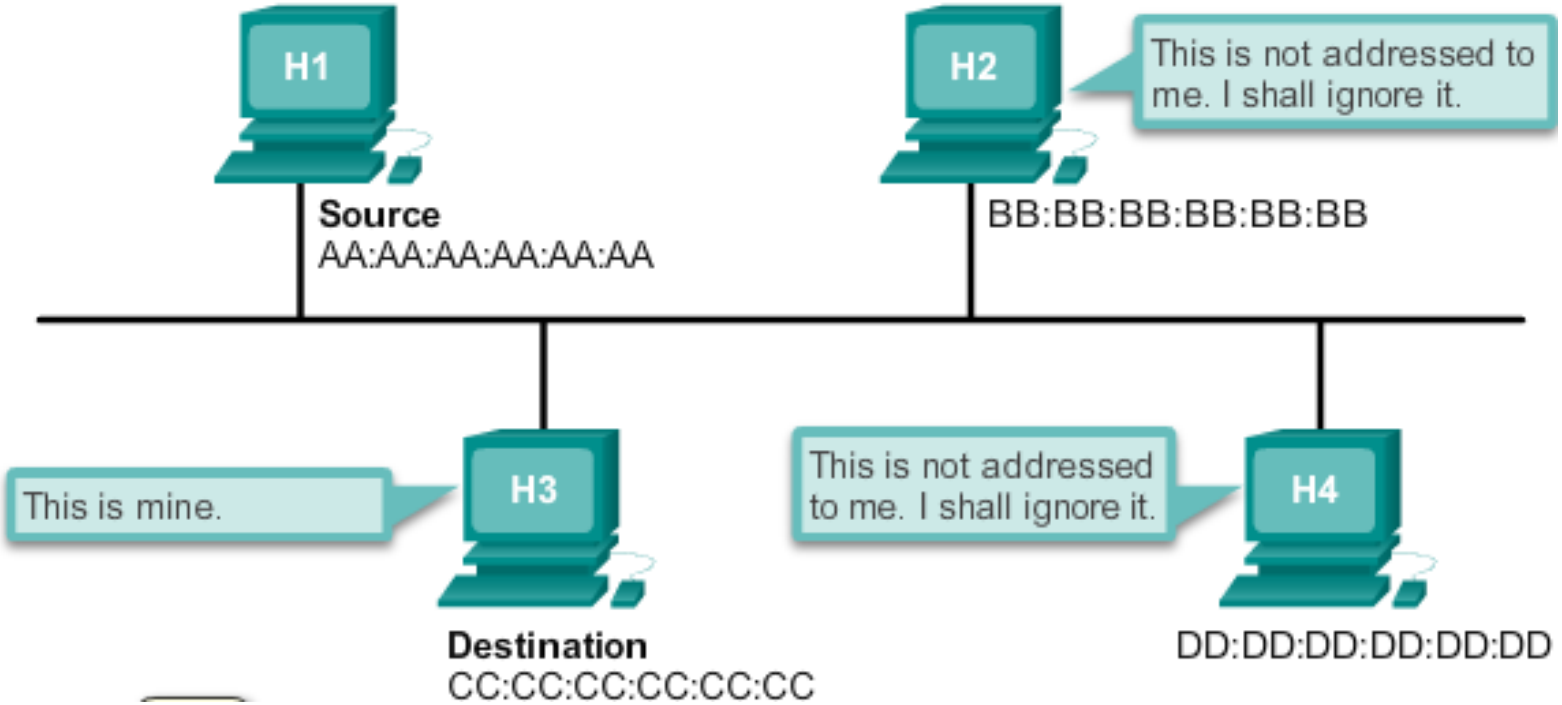
Frame Processing



Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		



Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		



MAC Address Representations

Different hardware and software manufacturers might represent the MAC address in different hexadecimal formats, as shown in the following:

00-05-9A-3C-78-00

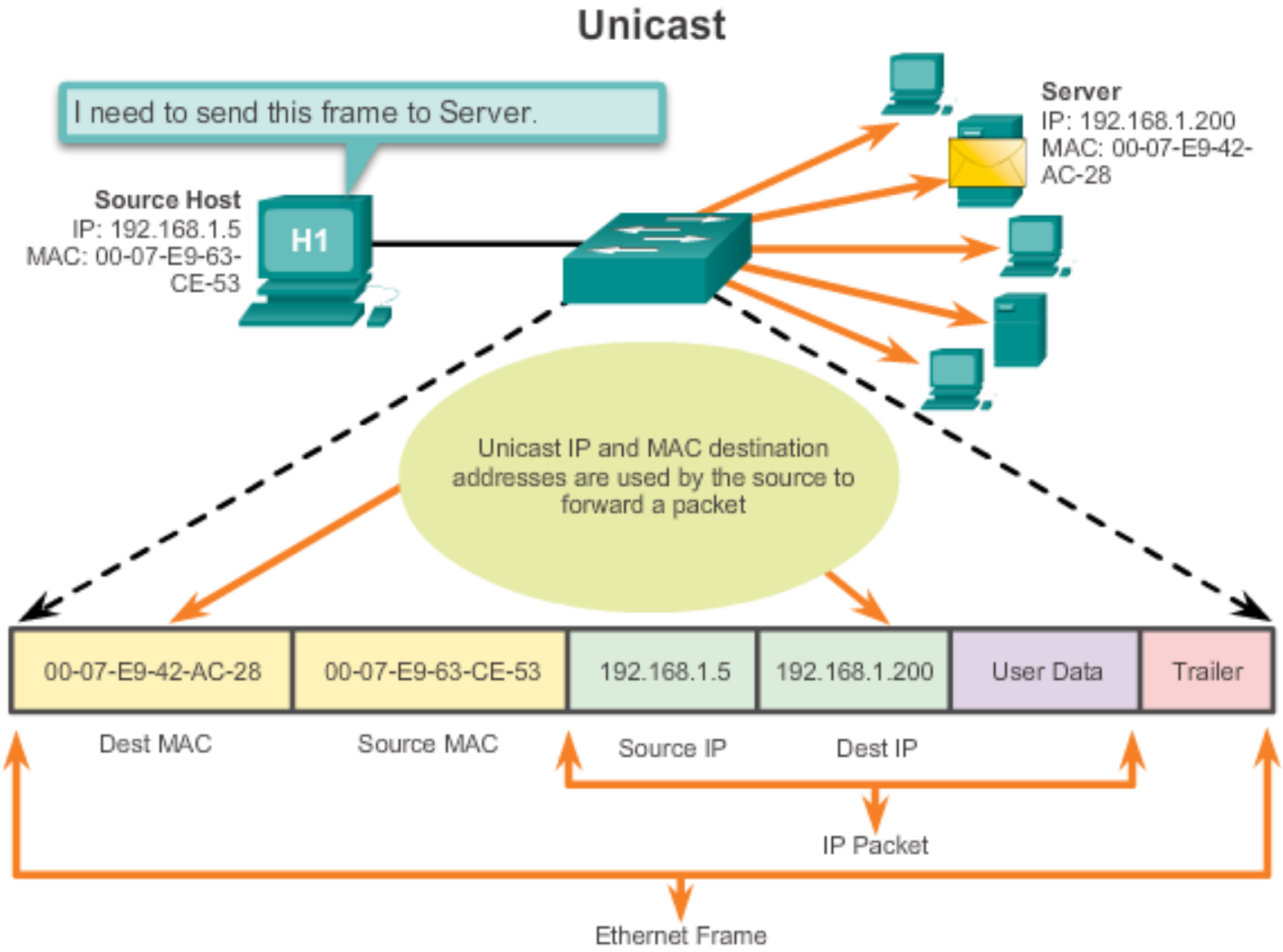
00:05:9A:3C:78:00

0005.9A3C.7800

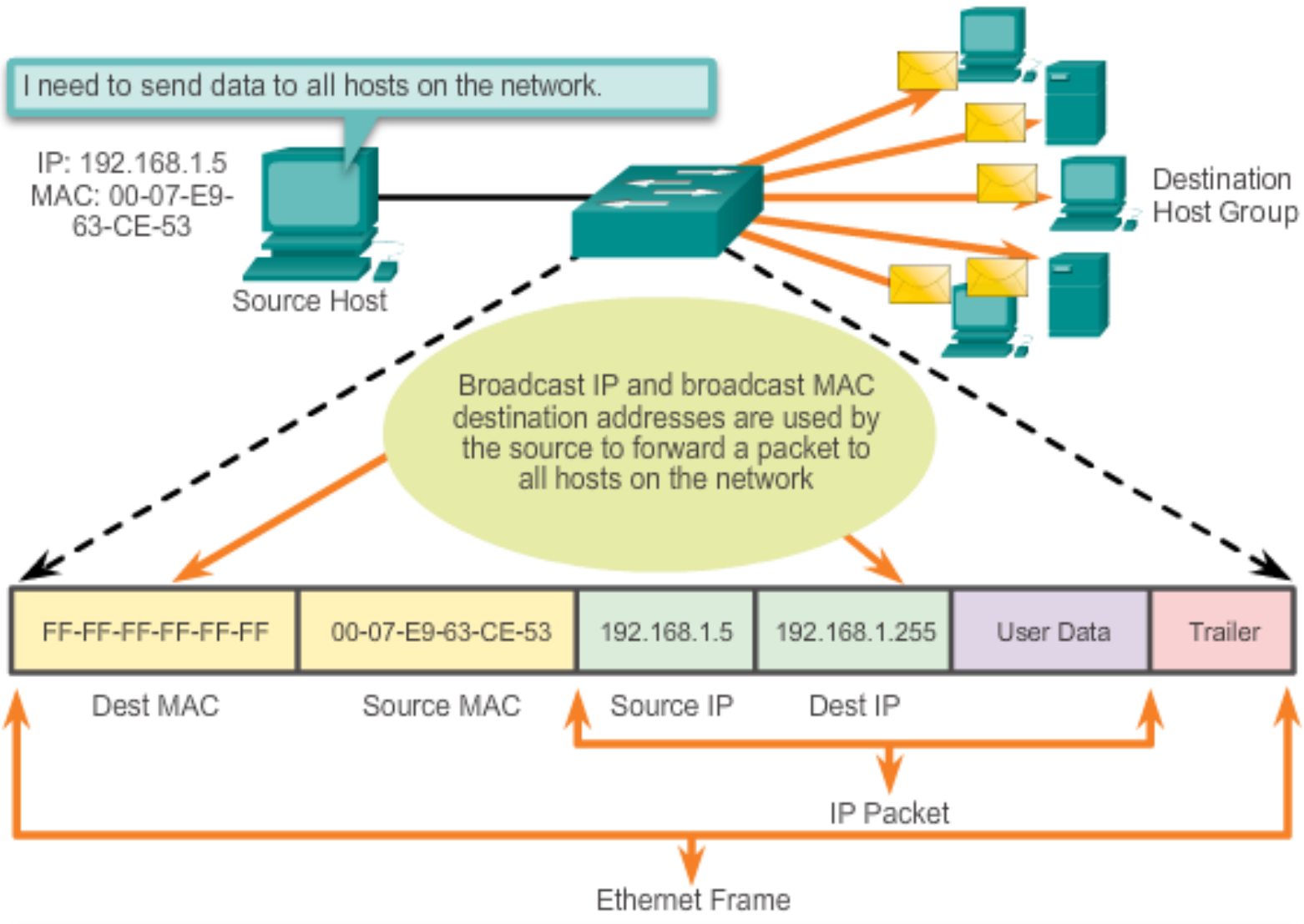
On a Windows host, the **ipconfig /all** command can be used to identify the MAC address of an Ethernet adapter. **On a MAC or Linux** host, the **ifconfig** command is used.

In Ethernet, different MAC addresses are used for L 2:

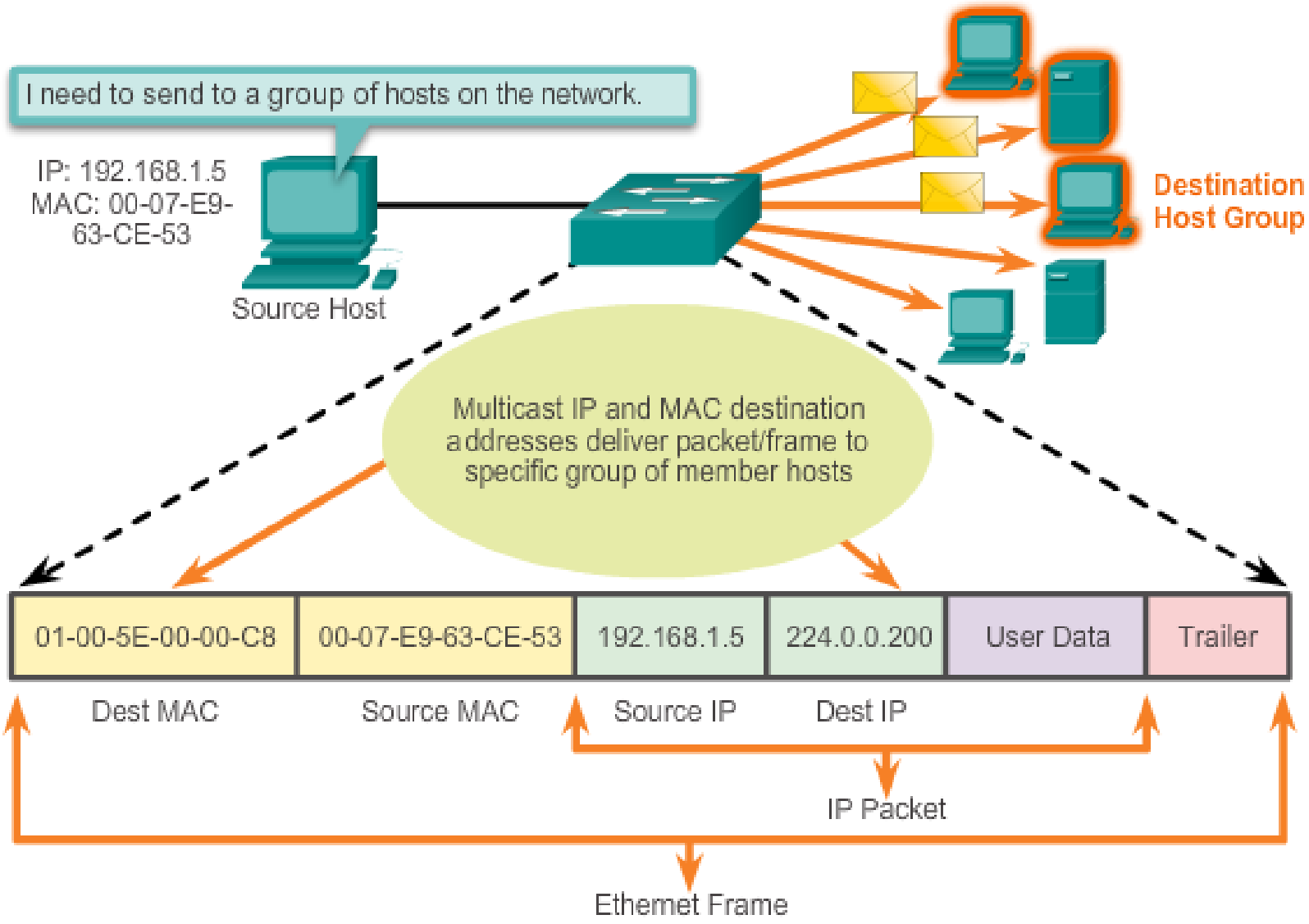
1. Unicast,
2. Broadcast, and
3. Multicast communications.



Broadcast



Multicast



The MAC Address Table

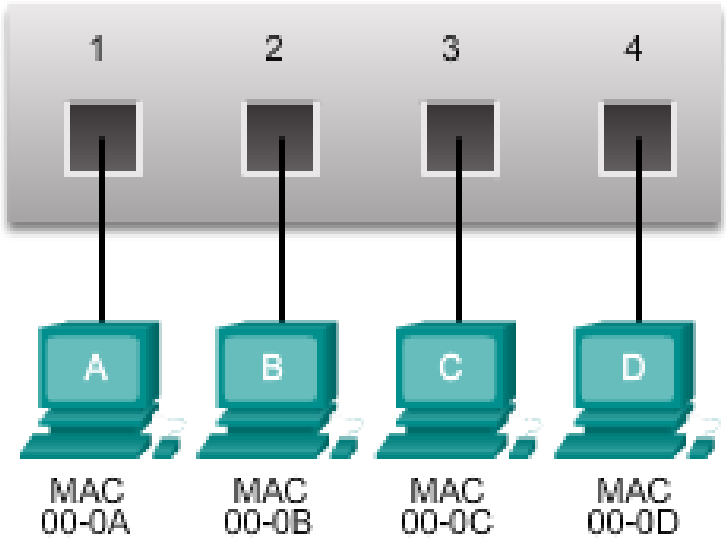
An **Ethernet switch** is a Layer 2 device, which means it uses MAC addresses to make forwarding decisions. It is completely unaware of the protocol being carried in the data portion of the frame, such as an IPv4 packet. The switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.

Unlike an **Ethernet hub** that repeats bits out all ports except the incoming port, **an Ethernet switch consults a MAC address table to make a forwarding decision for each frame.** In the figure, the four-port switch was just powered on. 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.

Learn: Examine Source MAC Address

MAC Address Table	
Port	**MAC Address**



Learning MAC Addresses

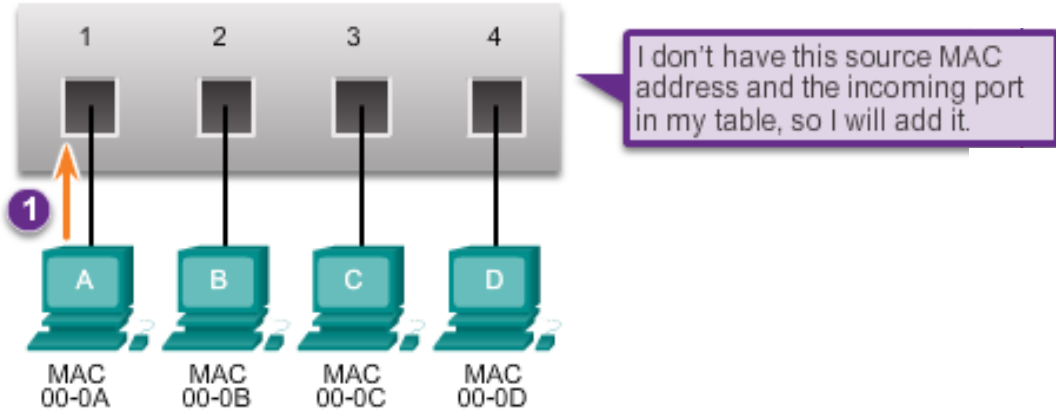
Learn: Examine Source MAC Address

Port and Source MAC address added

2

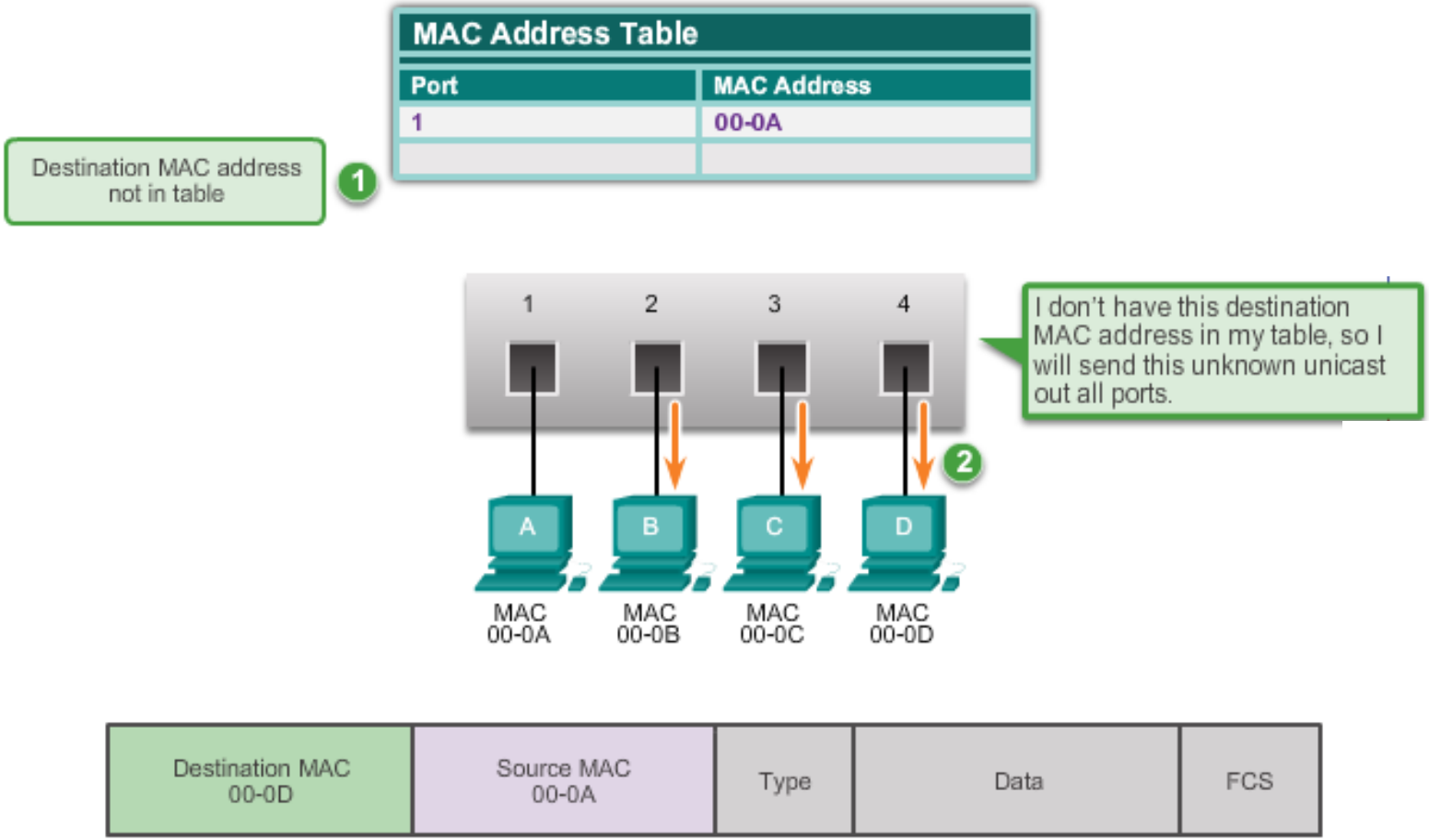
MAC Address Table

Port	MAC Address
1	00-0A



Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS

Forward: Examine Destination MAC Address



Video Demonstration - Sending a Frame to the Default Gateway

Frame Forwarding Methods on Cisco Switches

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

1. **Store-and-forward switching**
2. **Cut-through switching**

Switch Packet Forwarding Methods

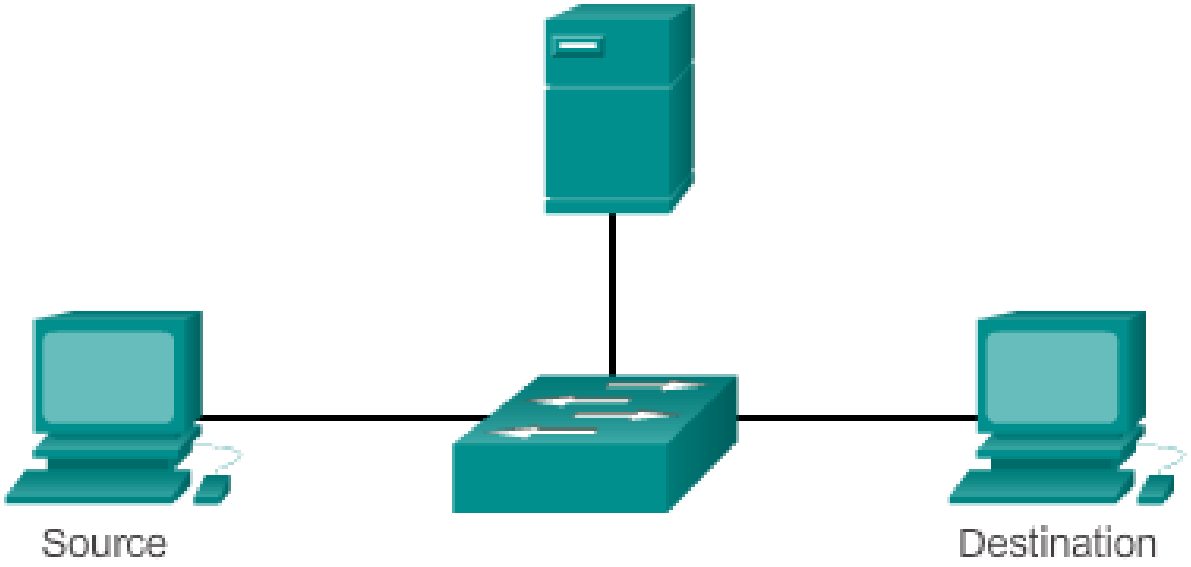
Store-and-forward

A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-through

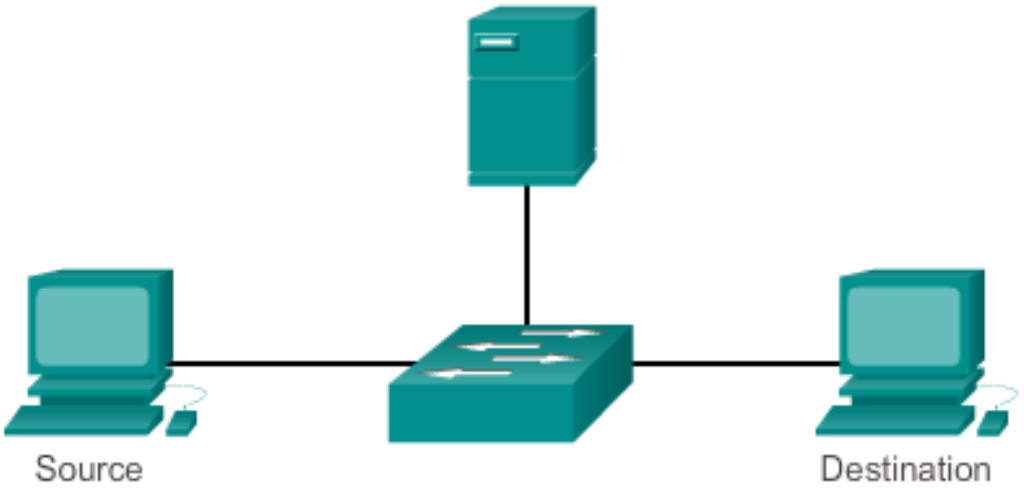
A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

Store-and-Forward Switching



A store-and-forward switch receives the entire frame, and computes the CRC. If the CRC is valid, the switch looks up the destination address, which determines the outgoing interface. The frame is then forwarded out the correct port.

Cut-Through Switching



A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

There are two variants of cut-through switching:

- **Fast-forward switching -**
- **Fragment-free switching**

Memory Buffering on Switches

There are two methods of memory buffering: port-based and shared memory.

Port-based Memory Buffering

Shared Memory Buffering

There are **two types of duplex settings** used for communications on an Ethernet network: half duplex and full duplex.

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.

Two primary addresses assigned to a device on an Ethernet LAN:

Physical address (the MAC address) – Used for Ethernet NIC to Ethernet NIC communications on the same network.

Logical address (the IP address) – Used to send the packet from the original source to the final destination.

The Layer 2 Ethernet frame contains:

Destination MAC address – This is the MAC address of the file server's Ethernet NIC.

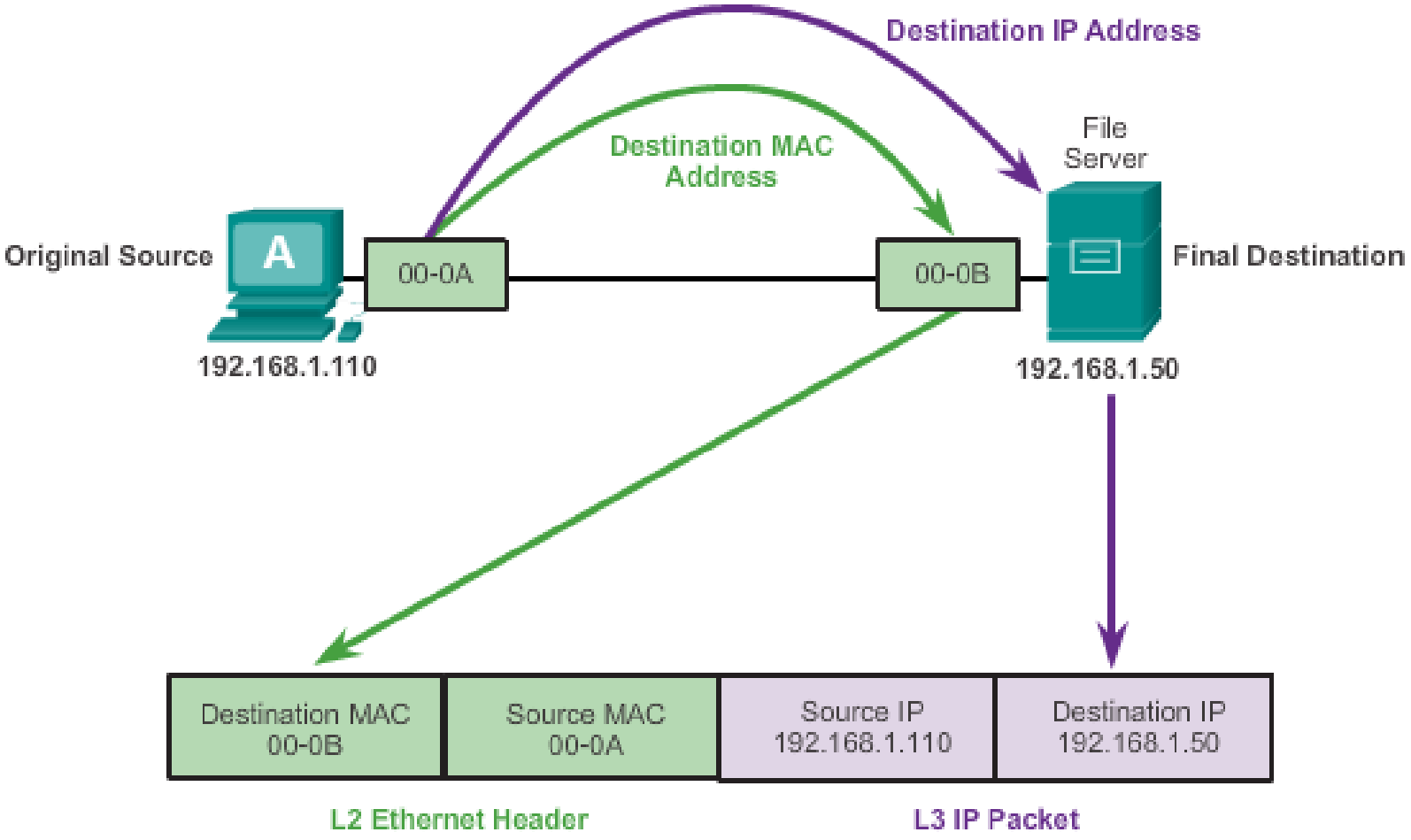
Source MAC address – This is the MAC address of PC-A's Ethernet NIC.

The Layer 3 IP packet contains:

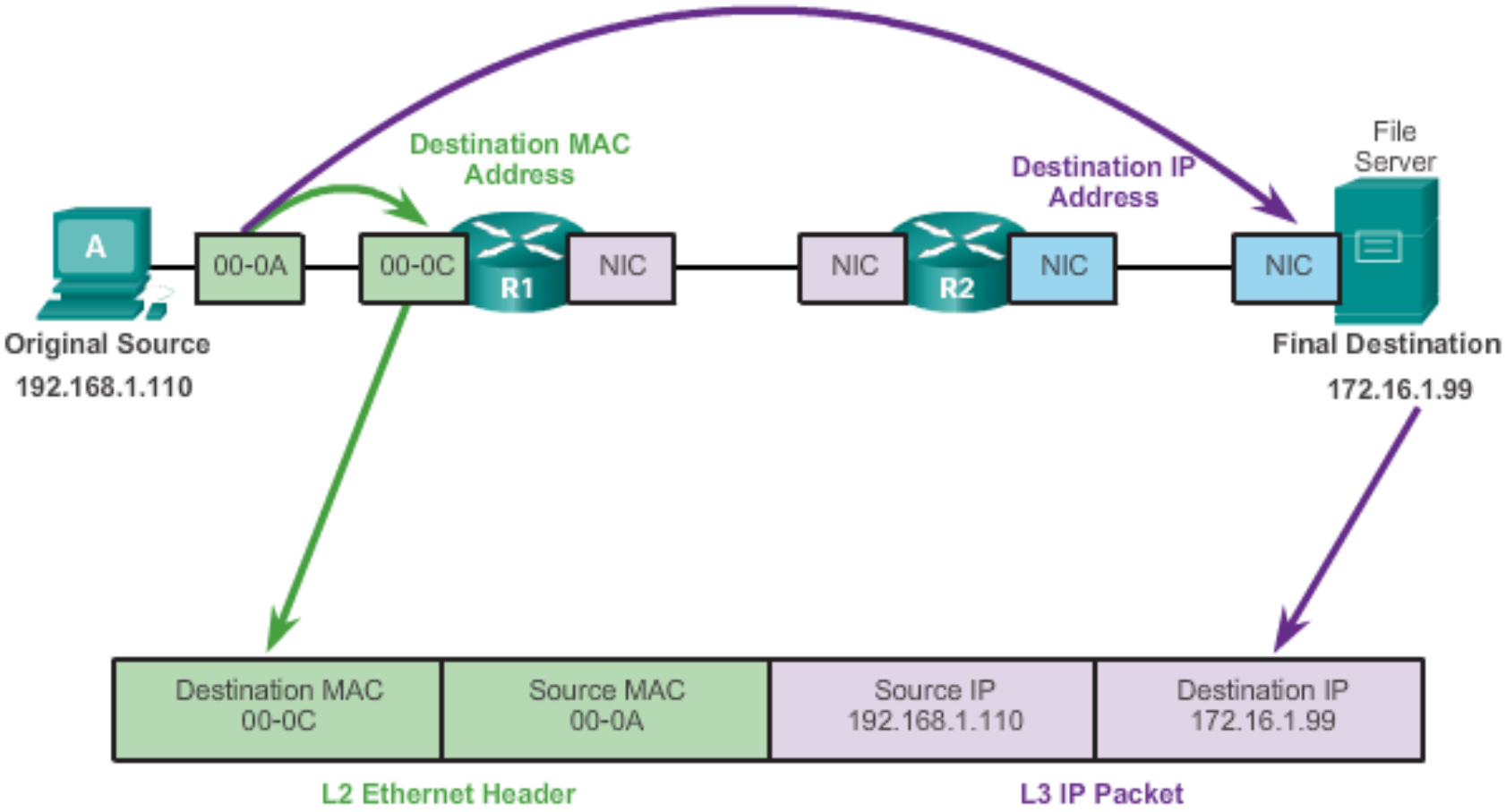
Source IP address – This is the IP address of the original source, PC-A.

Destination IP address – This is the IP address of the final destination, the file server.

Communicating on a Local Network



Communicating to a Remote Network



Introduction to ARP

Recall that every device with an IP address on an Ethernet network also has an Ethernet MAC address. When a device sends an Ethernet frame, it contains these two addresses:

Destination MAC address - The MAC address of the Ethernet NIC, which will be either the MAC address of the final destination device or the router.

Source MAC address - The MAC address of the sender's Ethernet NIC.

To determine the destination MAC address, the device uses ARP.

ARP provides two basic functions:

1. **Resolving IPv4 addresses to MAC addresses**
2. **Maintaining a table of mappings**

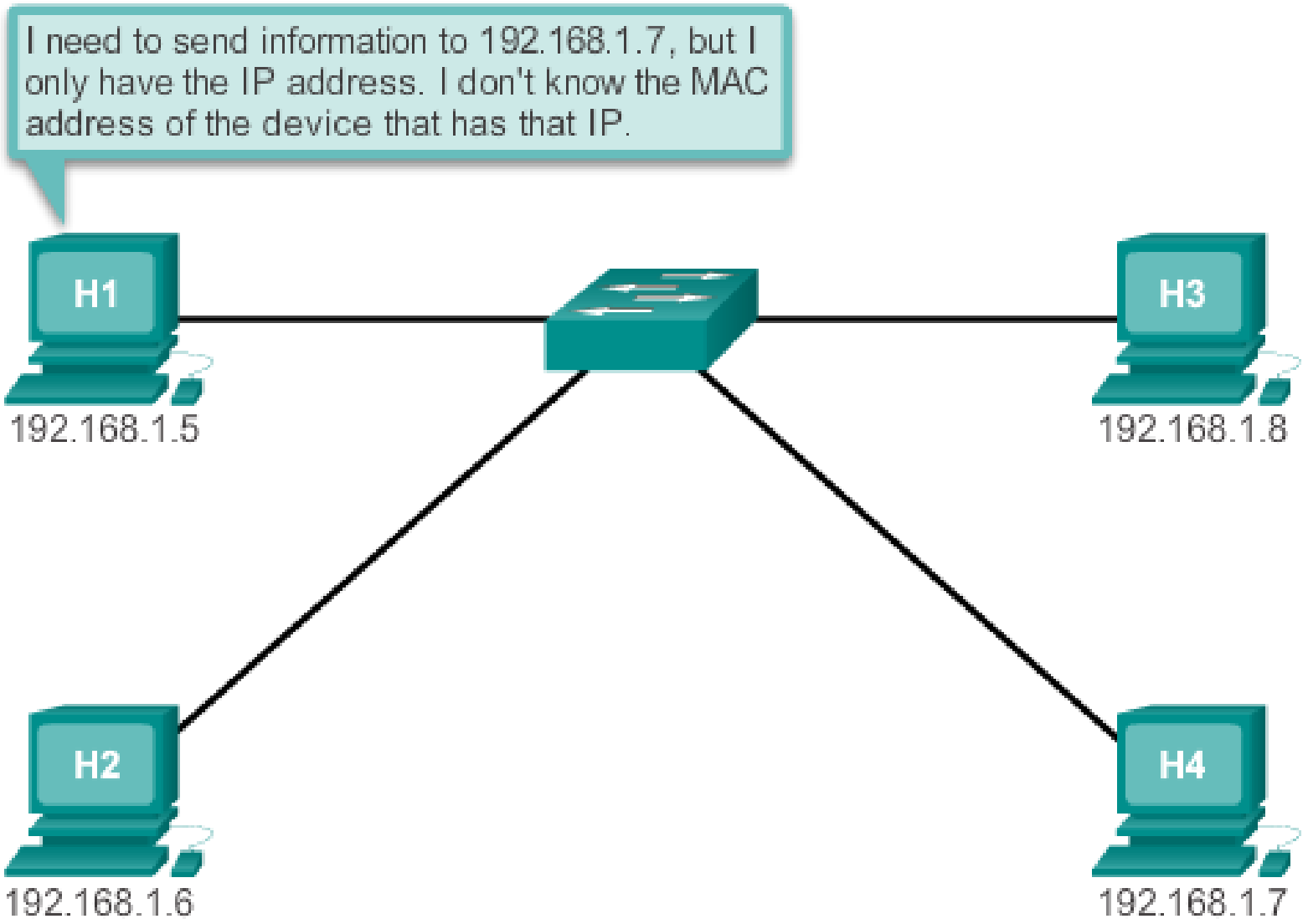
ARP Functions

Resolving IPv4 Addresses to MAC Addresses

When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table in its memory to find the MAC address that is mapped to the IPv4 address. **This table is called the ARP table or the ARP cache**. **The ARP table is stored in the RAM of the device.**

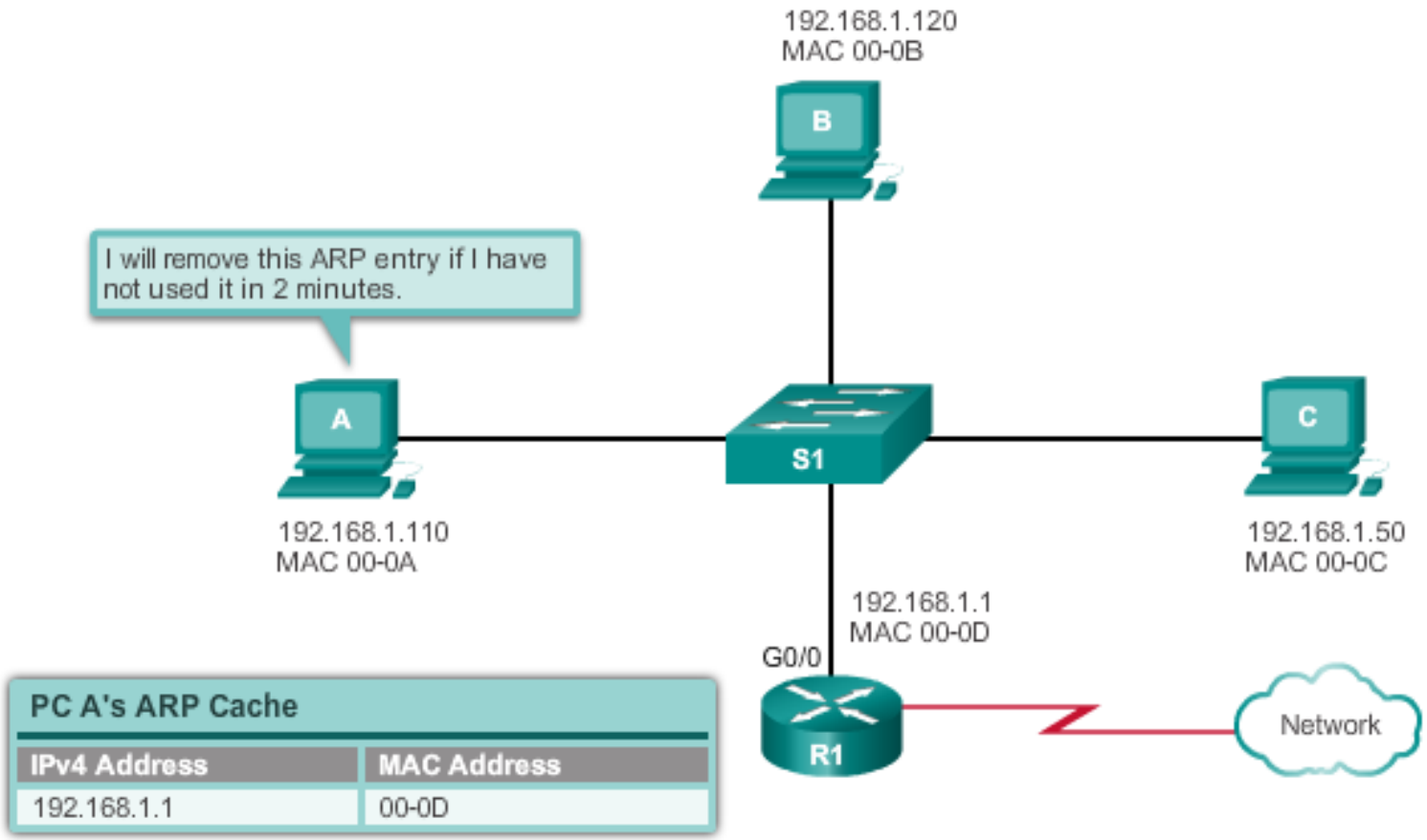
The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address.

1. If the packet's destination IPv4 address is on the same network as the source IPv4 address, **the device will search the ARP table for the destination IPv4 address.**
2. If the destination IPv4 address is on a different network than the source IPv4 address, **the device will search the ARP table for the IPv4 address of the default gateway.**



Removing Entries from an ARP Table

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time.



ARP Tables

On a Cisco router, the **show ip arp** command is used to display the ARP table.

On a Windows 7 PC, the **arp –a** command is used to display the ARP table.

- ✓ **ARP Broadcasts**
- ✓ **ARP spoofing or ARP poisoning**

Summary

Ethernet is the most widely used LAN technology today. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies. For the Layer 2 protocols, as with all 802 IEEE standards, Ethernet relies on the two separate sublayers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sublayers.

At the data link layer, the frame structure is nearly identical for all bandwidths of Ethernet. The Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.

There are two styles of Ethernet framing: IEEE 802.3 Ethernet standard and the DIX Ethernet standard which is now referred to Ethernet II. The most significant difference between the two standards is the addition of a Start Frame Delimiter (SFD) and the change of the Type field to a Length field in the 802.3. Ethernet II is the Ethernet frame format used in TCP/IP networks. As an implementation of the IEEE 802.2/3 standards, the Ethernet frame provides MAC addressing and error checking.

The Layer 2 addressing provided by Ethernet supports unicast, multicast, and broadcast communications. Ethernet uses the Address Resolution Protocol to determine the MAC addresses of destinations and map them against known IPv4 addresses.

Each node on an IPv4 network has both a MAC address and an IPv4 address. The IP addresses are used to identify the original source and final destination of the packet. The Ethernet MAC addresses are used to send the packet from one Ethernet NIC to another Ethernet NIC on the same IP network. ARP is used to map a known IPv4 address to a MAC address, so the packet can be encapsulated in an Ethernet frame with the correct Layer 2 address.

ARP relies on certain types of Ethernet broadcast messages and Ethernet unicast messages, called ARP requests and ARP replies. The ARP protocol resolves IPv4 addresses to MAC addresses and maintains a table of mappings.

On most Ethernet networks, end devices are typically connected on a point-to-point basis to a Layer 2, full-duplex switch. A Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address. A Layer 2 switch builds a MAC address table that it uses to make forwarding decisions. Layer 2 switches depend on routers to pass data between independent IP subnetworks.