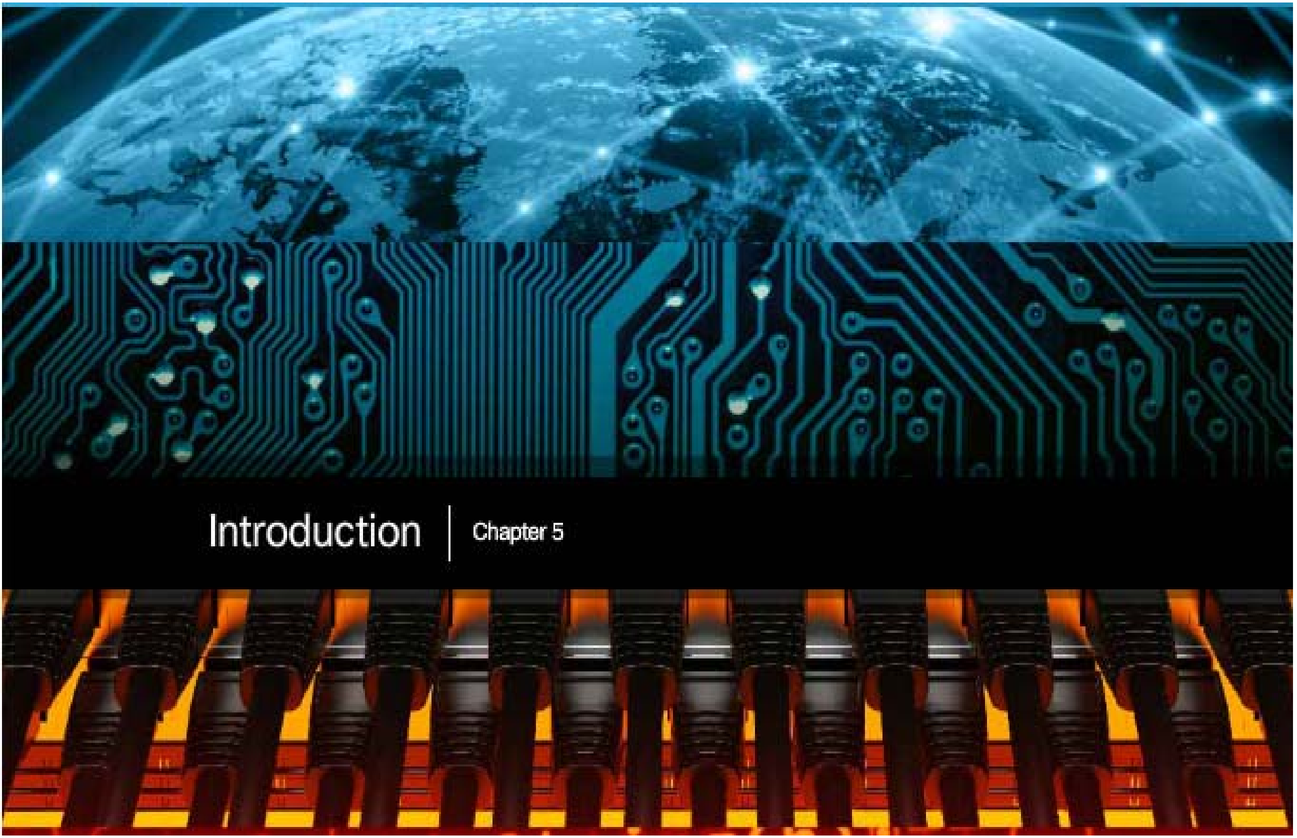
5.0.1.1 Chapter 5: Ethernet

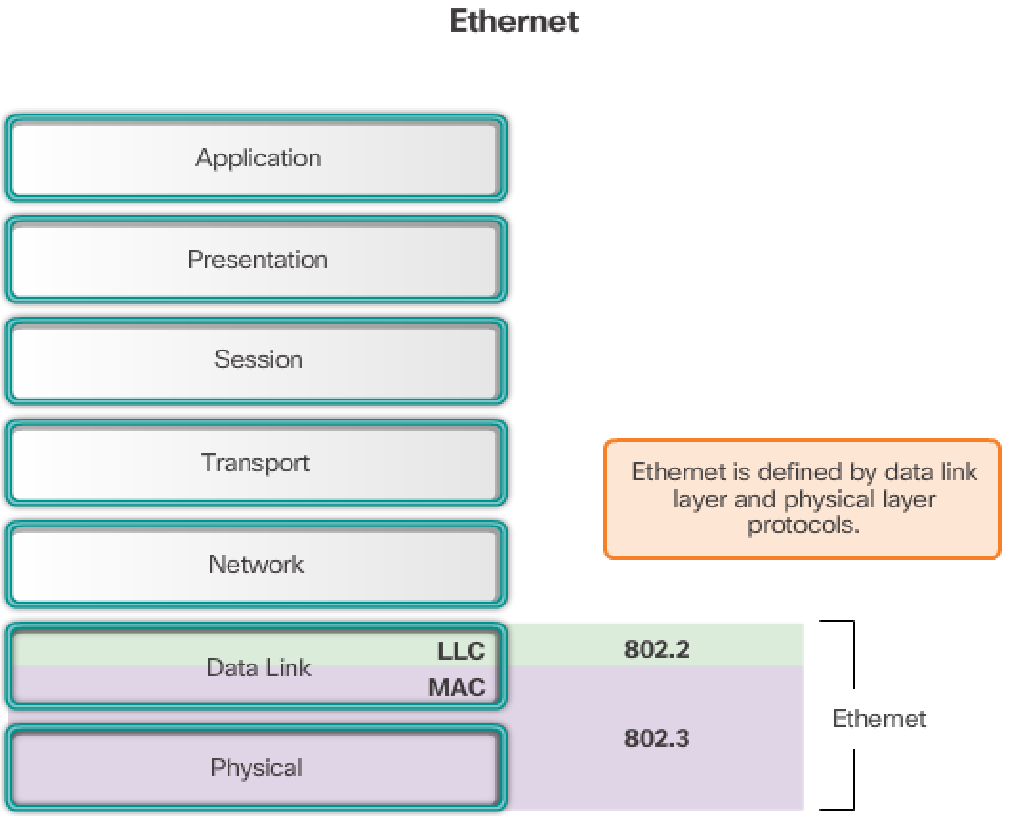


Ethernet is now the predominant LAN technology in the world. Ethernet operates in the data link layer and the physical layer. The Ethernet protocol standards define many aspects of network communication including frame format, frame size, timing, and encoding. When messages are sent between hosts on an Ethernet network, the hosts format the messages into the frame layout that is specified by the standards

5.0.1.2 Class Activity - Join My Social Circle!

How are communications groups identified?

5.1.1.1 Ethernet Encapsulation



Ethernet operates in the data link layer and the physical layer. It is a family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards. Ethernet supports data bandwidths of:

- 10 Mb/s
- 100 Mb/s
- 1000 Mb/s (1 Gb/s)
- 10,000 Mb/s (10 Gb/s)
- 40,000 Mb/s (40 Gb/s)
- 100,000 Mb/s (100 Gb/s)

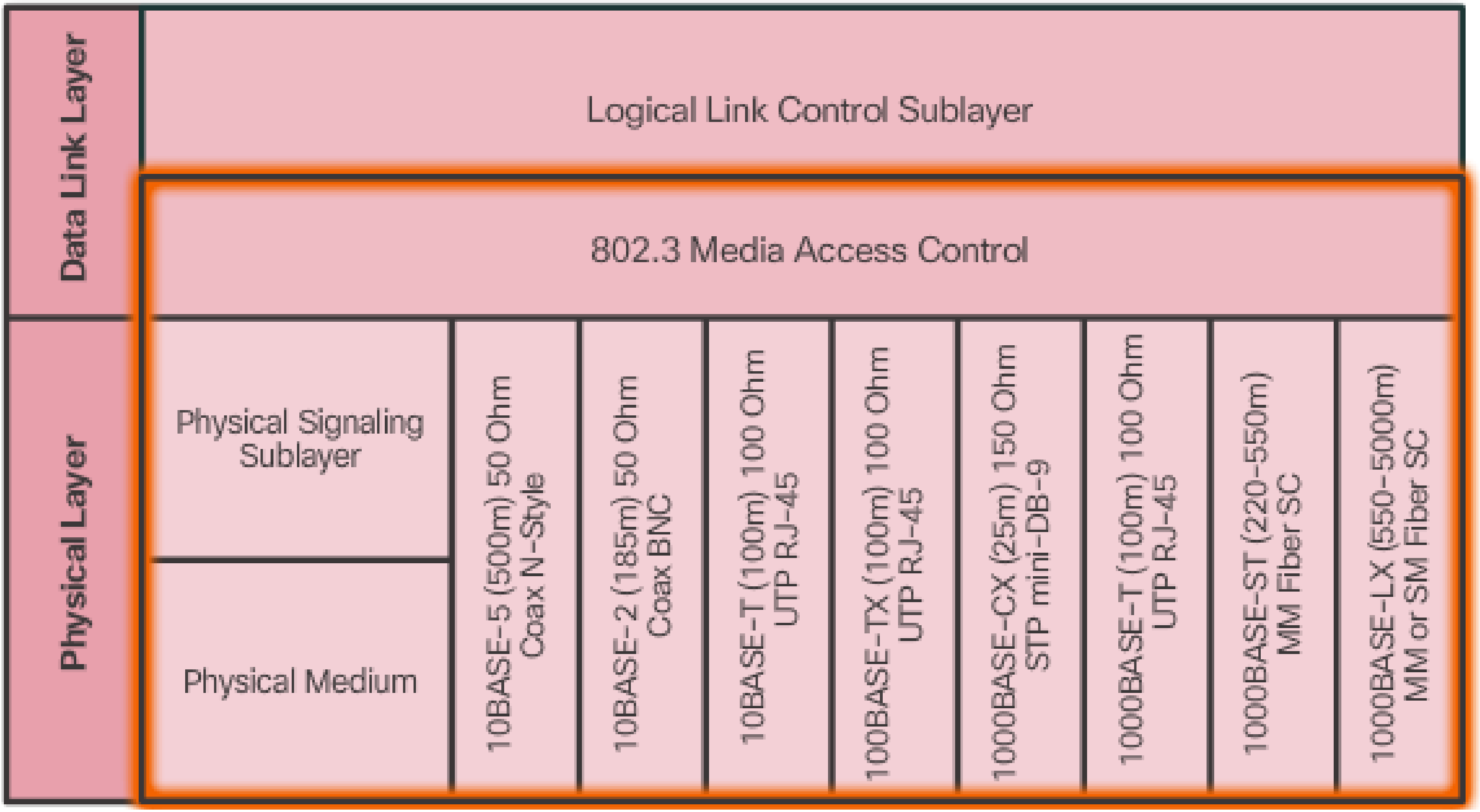
LLC sublayer

The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers

MAC sublayer

MAC constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC.

5.1.1.2 MAC Sublayer



MAC Sublayer

Two primary responsibilities:

- Data encapsulation
- Media access control

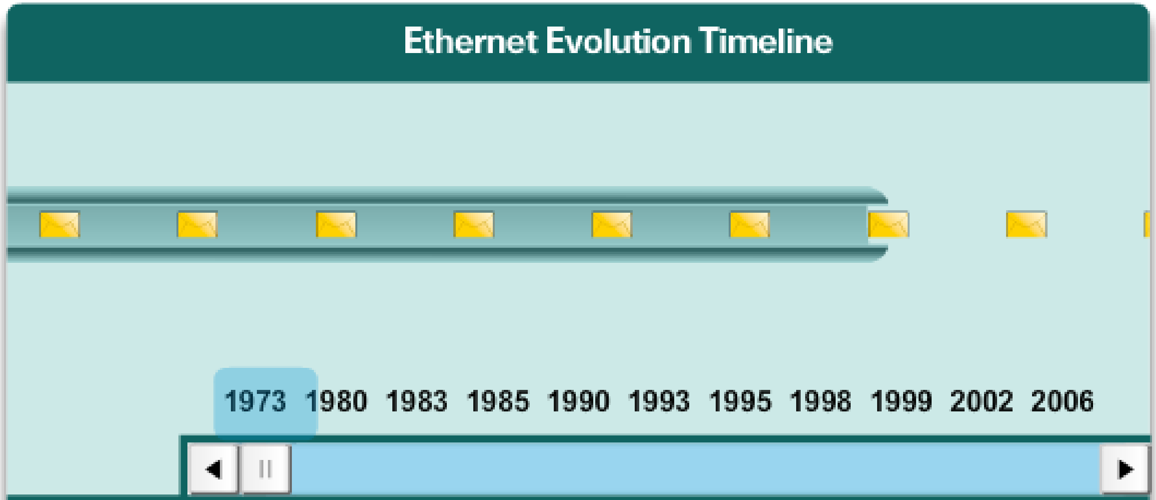
Encapsulation

- Frame delimiting
- Addressing
- Error detection

Media Access Control

Media access control is responsible for the placement of frames on the media and the removal of frames from the media

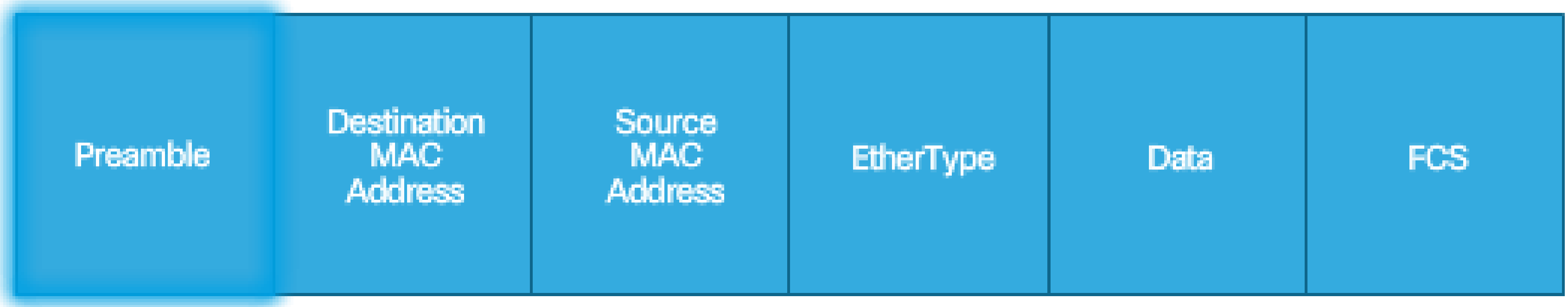
5.1.1.3 Ethernet Evolution



Year	1973	1980	1983
Standard	Ethernet	DIX standard Ethernet II	IEEE 8 10 BA
Description	Ethernet invented by Dr Robert Metcalf of Xerox corp.	Digital Equipment Corp, Intel and Xerox (DIX) release a standard for 10 Mb/s Ethernet over coaxial cable	10 MI coaxi

Drag the slider bar across the timeline to see how Ethernet standards have developed over time.

5.1.1.4 Ethernet Frame Fields



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.

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”.

5.1.1.5 Activity - MAC and LLC Sublayers

Activity - MAC and LLC Sublayers

Descriptions of the MAC and LLC sublayers are provided in the table. Click in the MAC or LLC fields to match the descriptions to the correct sublayer.

	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.		✓

5.1.18 Activity – Ethernet Frame Fields

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

5.1.1.7 Lab – using Wireshark to Examine Ethernet Frames

5.1.2.1 MAC Address and Hexadecimal

Hexadecimal Numbering

Decimal and Binary equivalents of 0 to F Hexadecimal

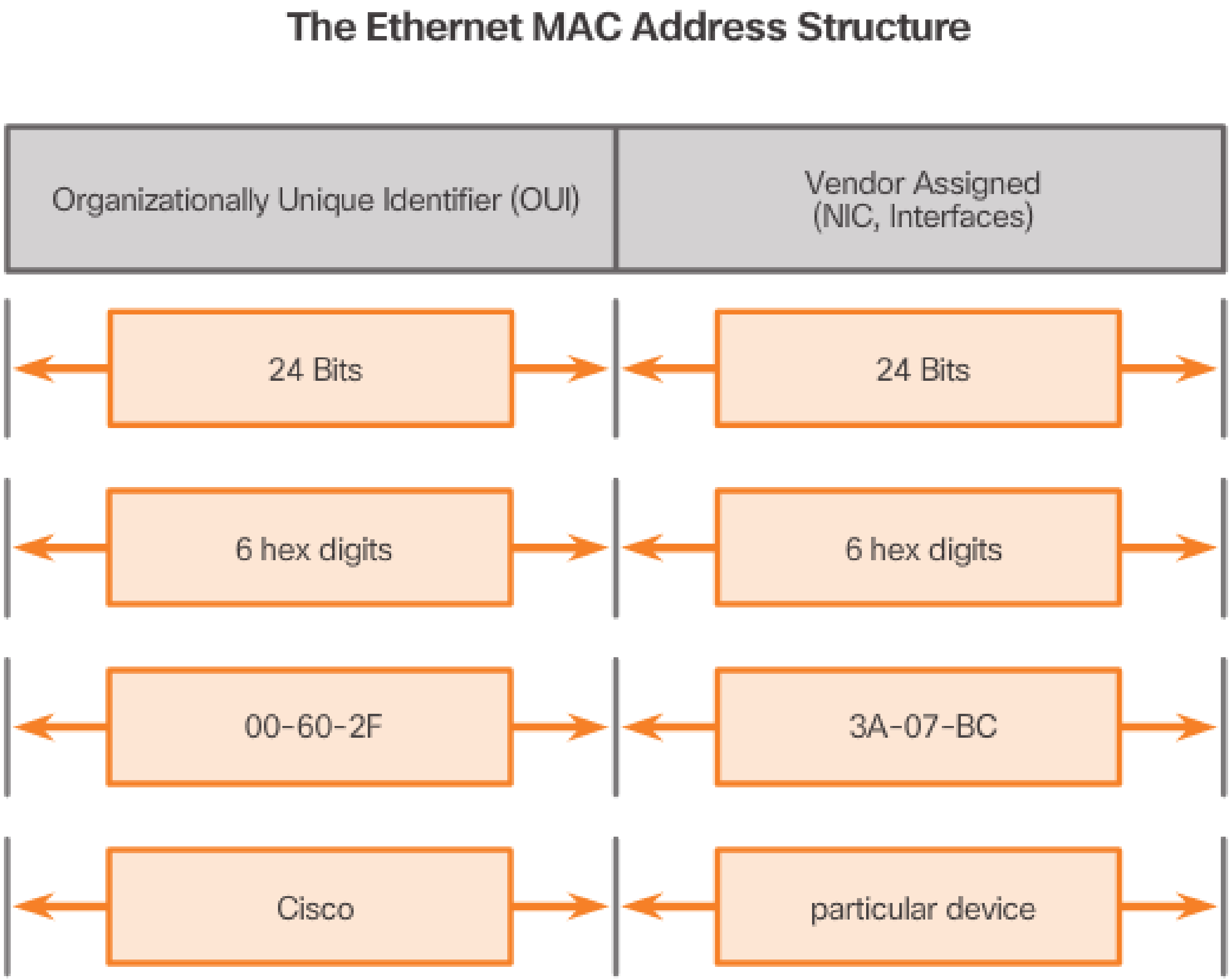
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

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

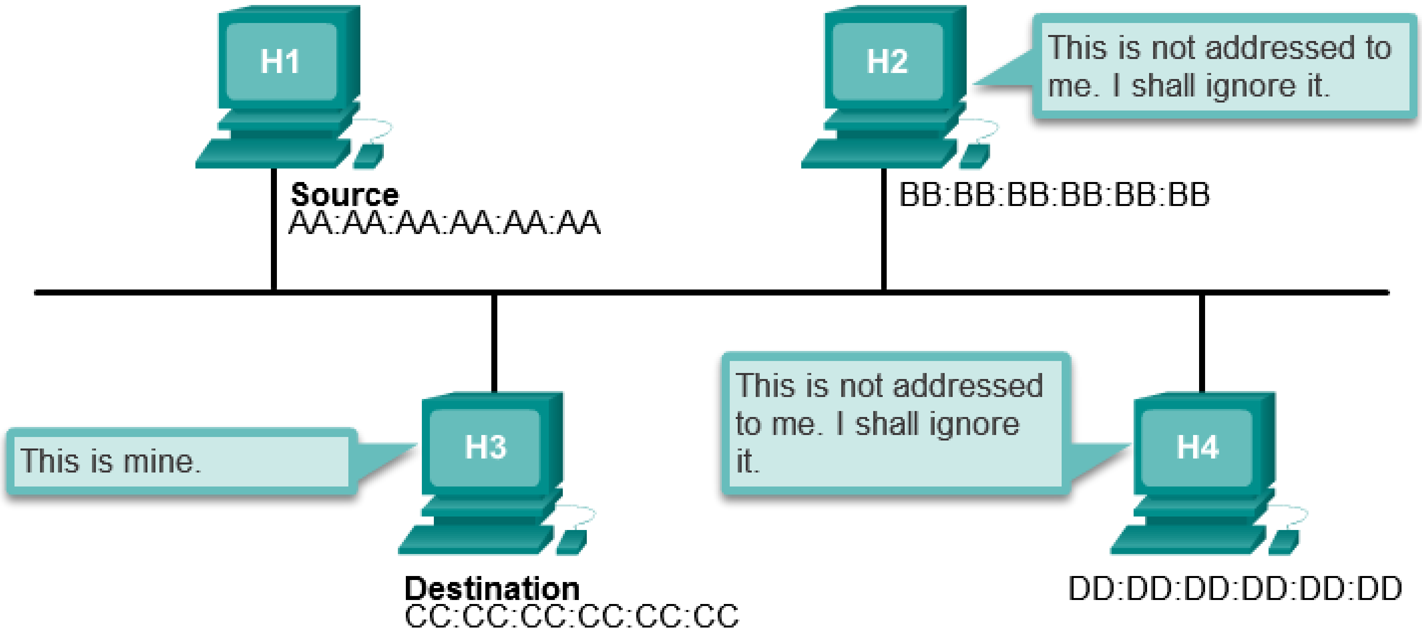
5.1.1.2 MAC Address Ethernet Identity



5.1.2.3 Frame Processing

Frame Forwarding

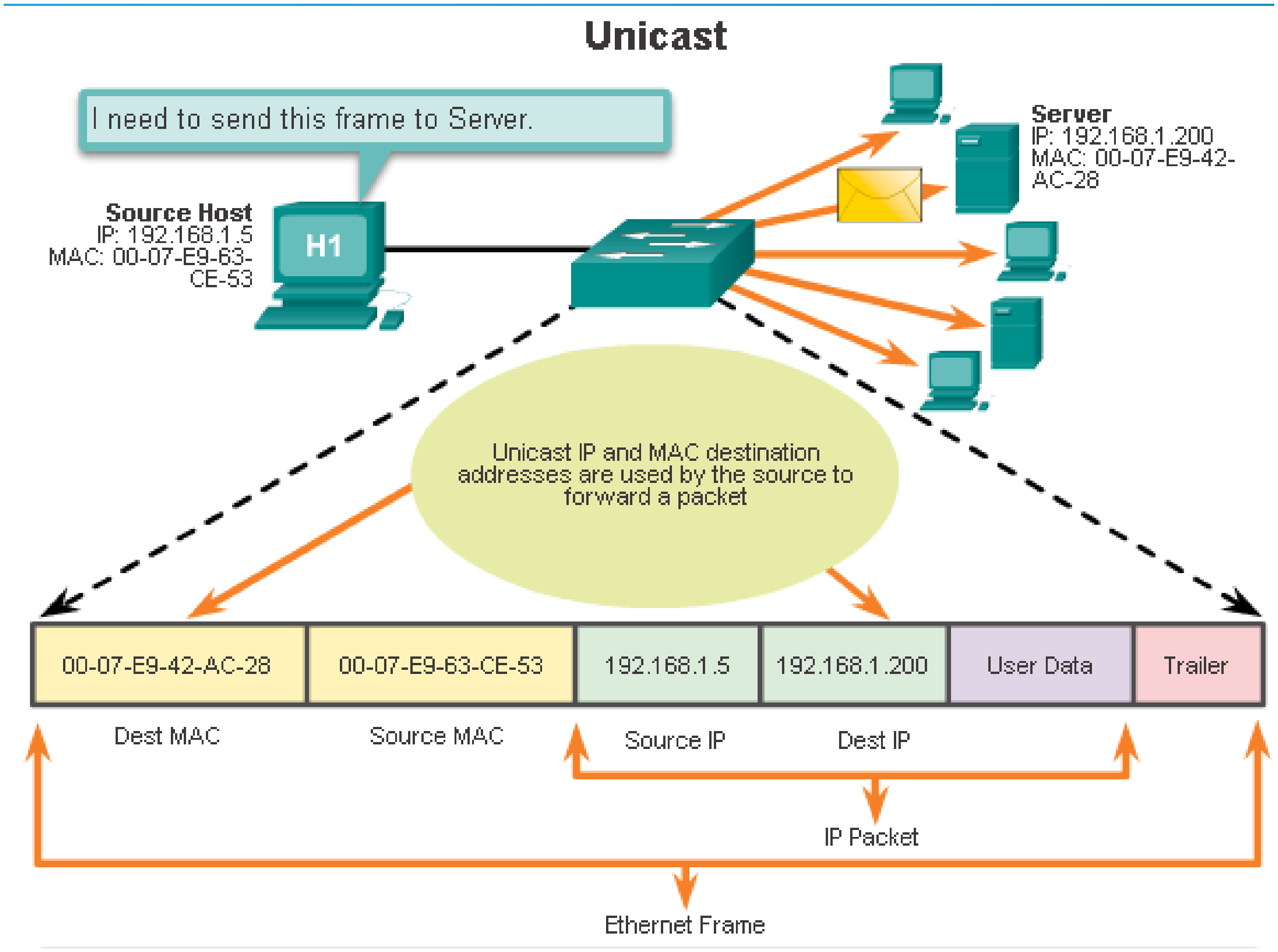
Destination Address	Source Address	Data
CC:CC:CC:CC:CC:CC	AA:AA:AA:AA:AA:AA	Encapsulated data
Frame Addressing		



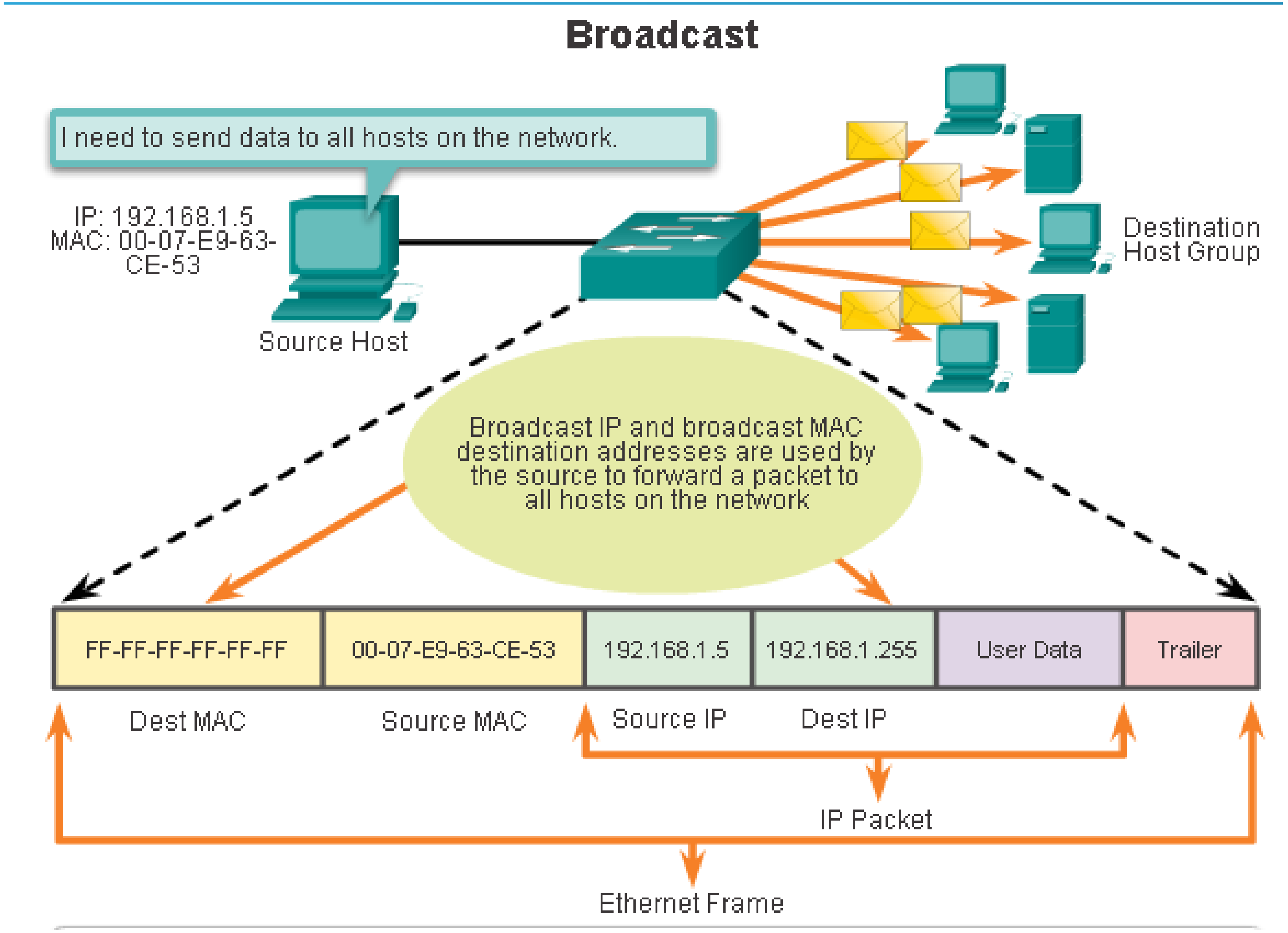
5.1.2.4 MAC Address Representations

```
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-DD-A7-B2
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::449f:c2:de06:ebad%10(Preferred)
   IPv4 Address. . . . . . . . . . . : 10.10.10.2(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Monday, June 01, 2015 11:19:48 AM
   Lease Expires . . . . . . . . . . : Thursday, June 04, 2015 11:19:49 PM
   Default Gateway . . . . . . . . . : 10.10.10.1
   DHCP Server . . . . . . . . . . . : 10.10.10.1
   DNS Servers . . . . . . . . . . . : 10.10.10.1
```

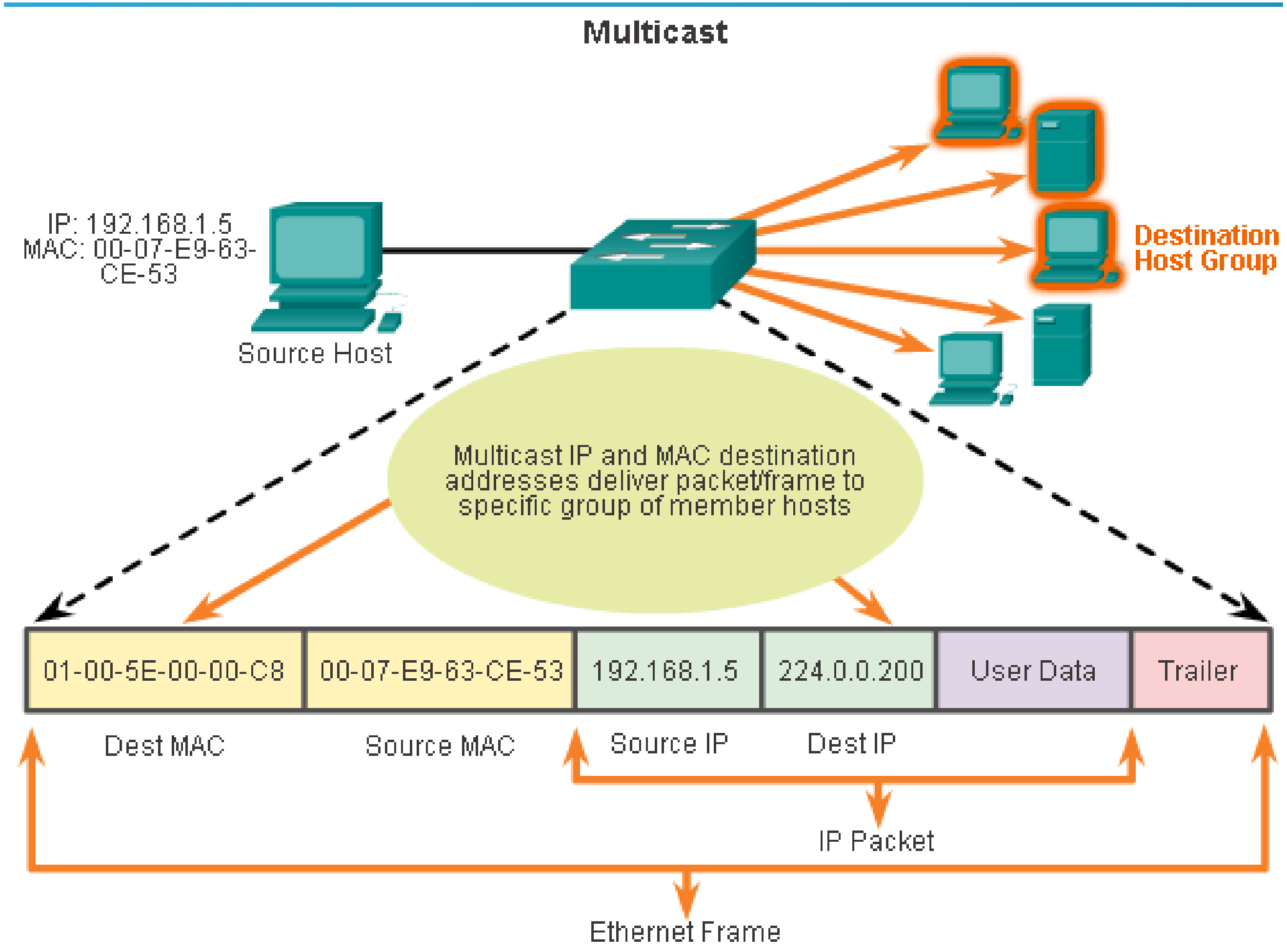
5.1.2.5 Unicast MAC Address



5.1.2.6 Broadcast MAC Address



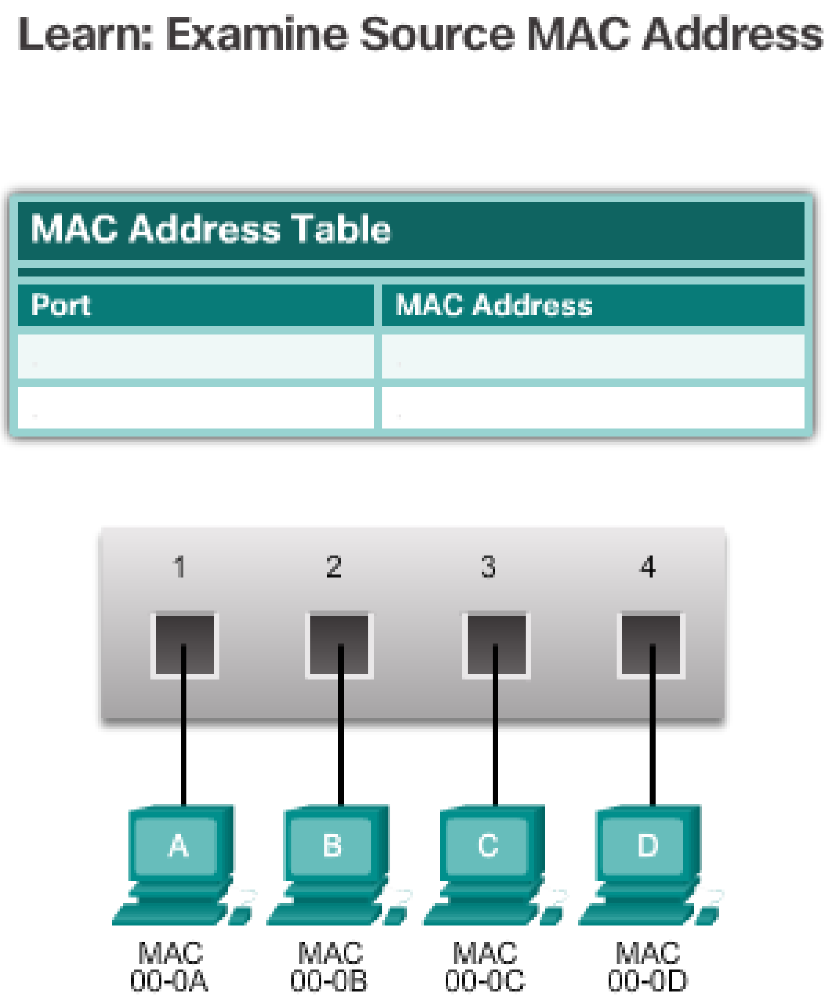
5.1.2.7 Multicast MAC Address



Multicast addresses allow a source device to send a packet to a group of devices. Devices that belong to a multicast group are assigned a multicast group IP address. The range of IPv4 multicast addresses is 224.0.0.0 to 239.255.255.255. 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.

5.1.2.8 Lab - Viewing Network Device MAC Addresses

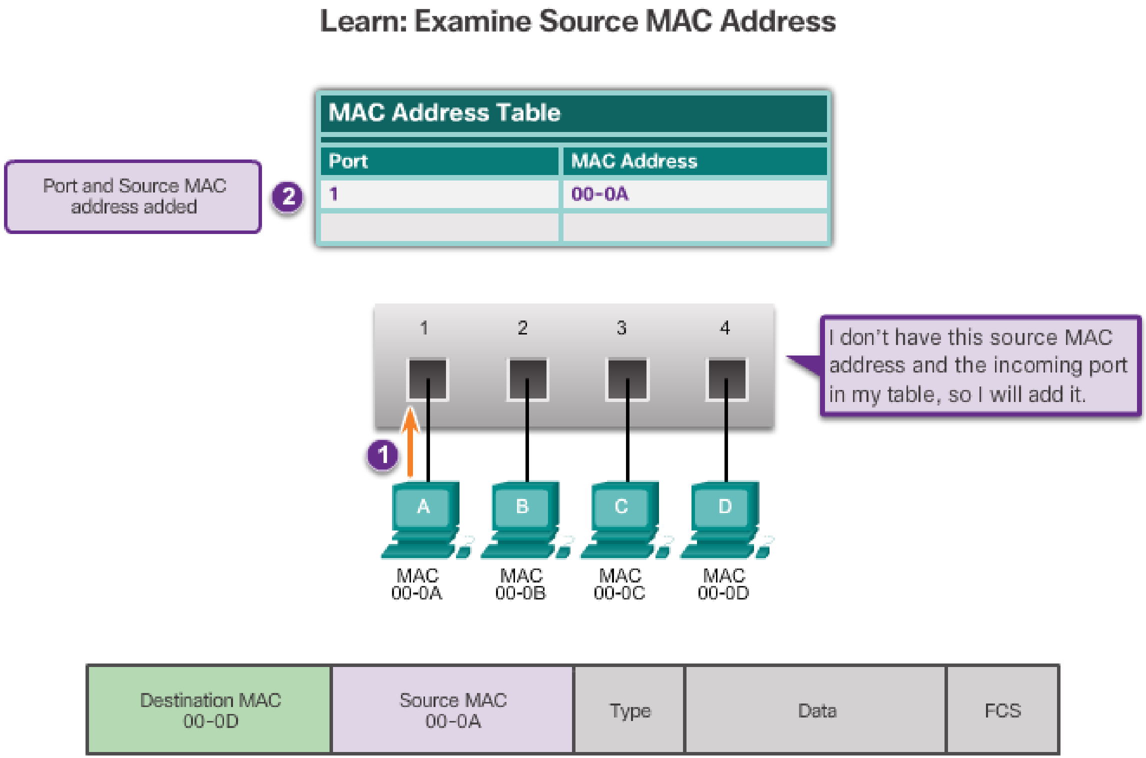
5.2.1.1 Switch Fundamentals



Switch Fundamentals
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.

5.2.1.2 Learning MAC Addresses

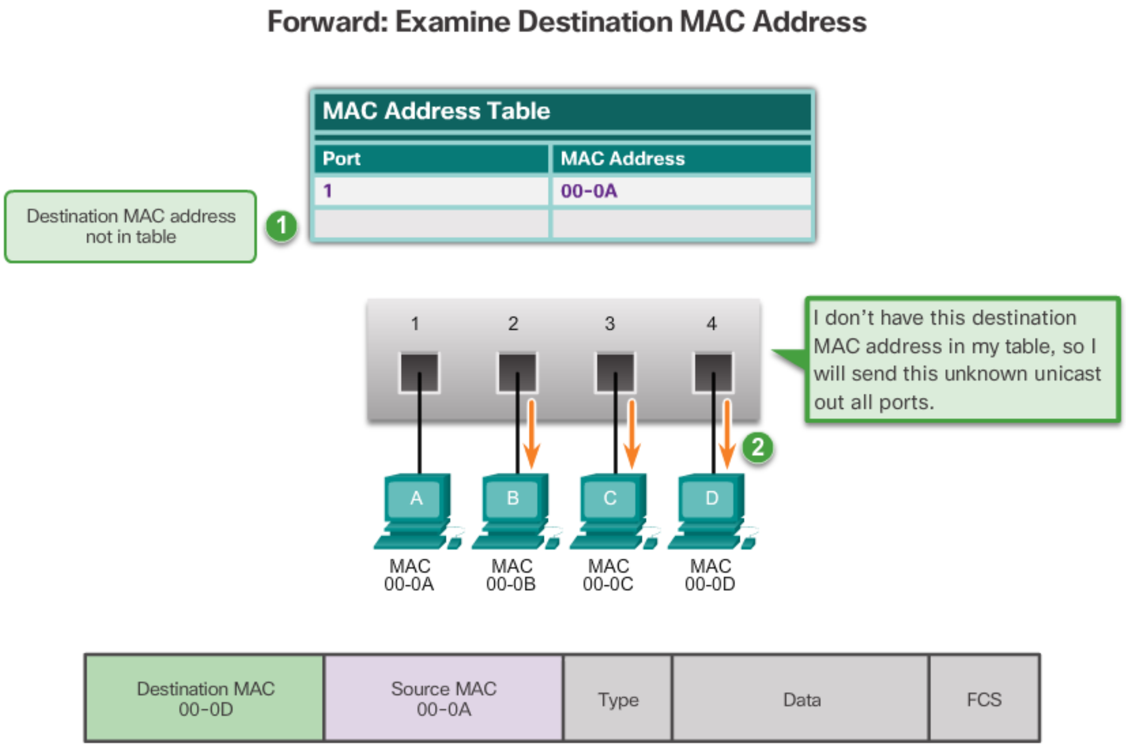


Learn – Examining the Source MAC Address

Every frame that enters a switch is checked for new information to learn. It does this by examining the frame's source MAC address and 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. In Figure 1, PC-A is sending an Ethernet frame to PC-D. The switch adds the MAC address for PC-A to the table.
- 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.

5.2.1.2 Learning MAC Addresses

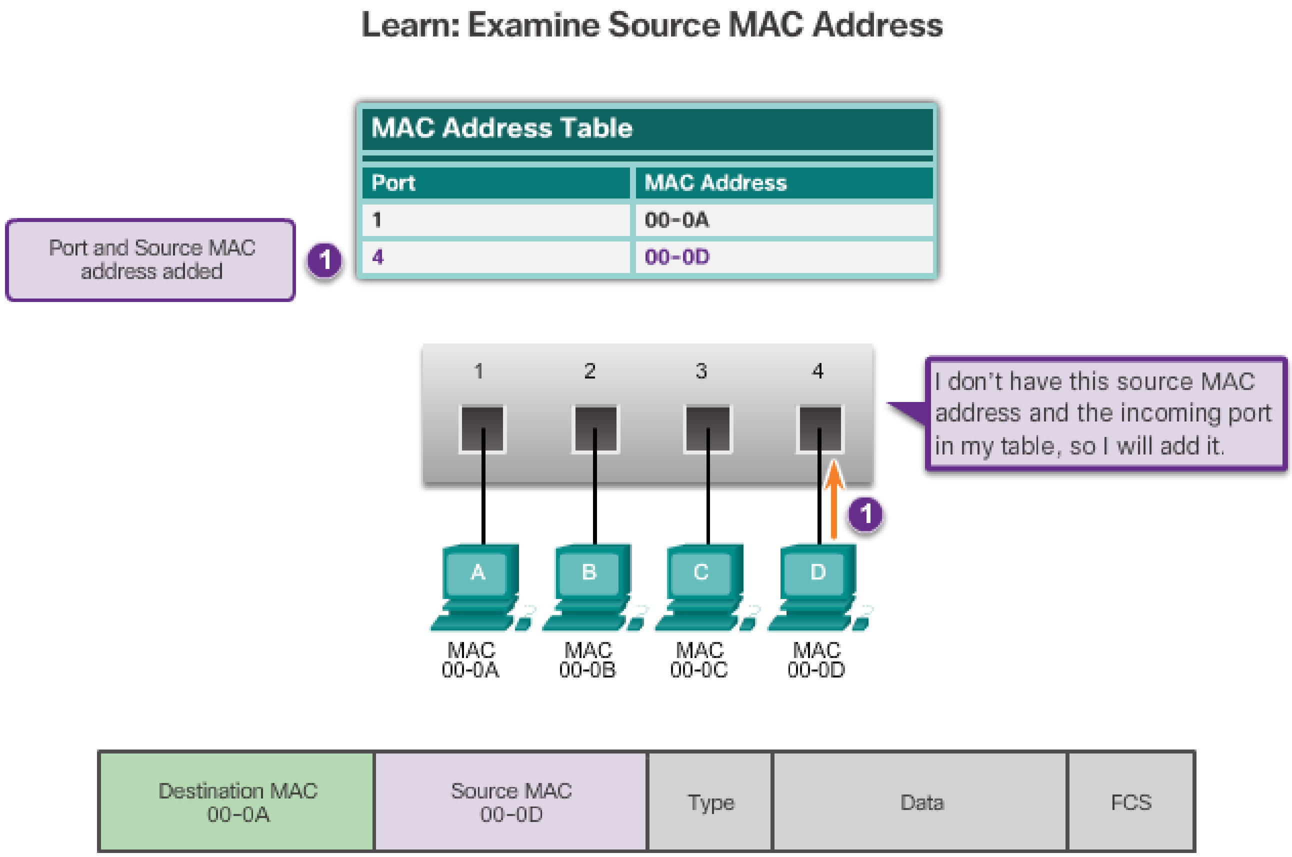


Forward – Examining the Destination MAC Address

Next, 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 known as an unknown unicast. As shown in Figure 2, 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.

5.2.1.3 Filtering Frames



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.

Figures 1 and 2 show PC-D sending a frame back to PC-A. The switch will first learn PC-D's MAC address. Next, because the switch has PC-A's MAC address in its table, it will send the frame only out port 1.

5.2.1.3 Filtering Frames

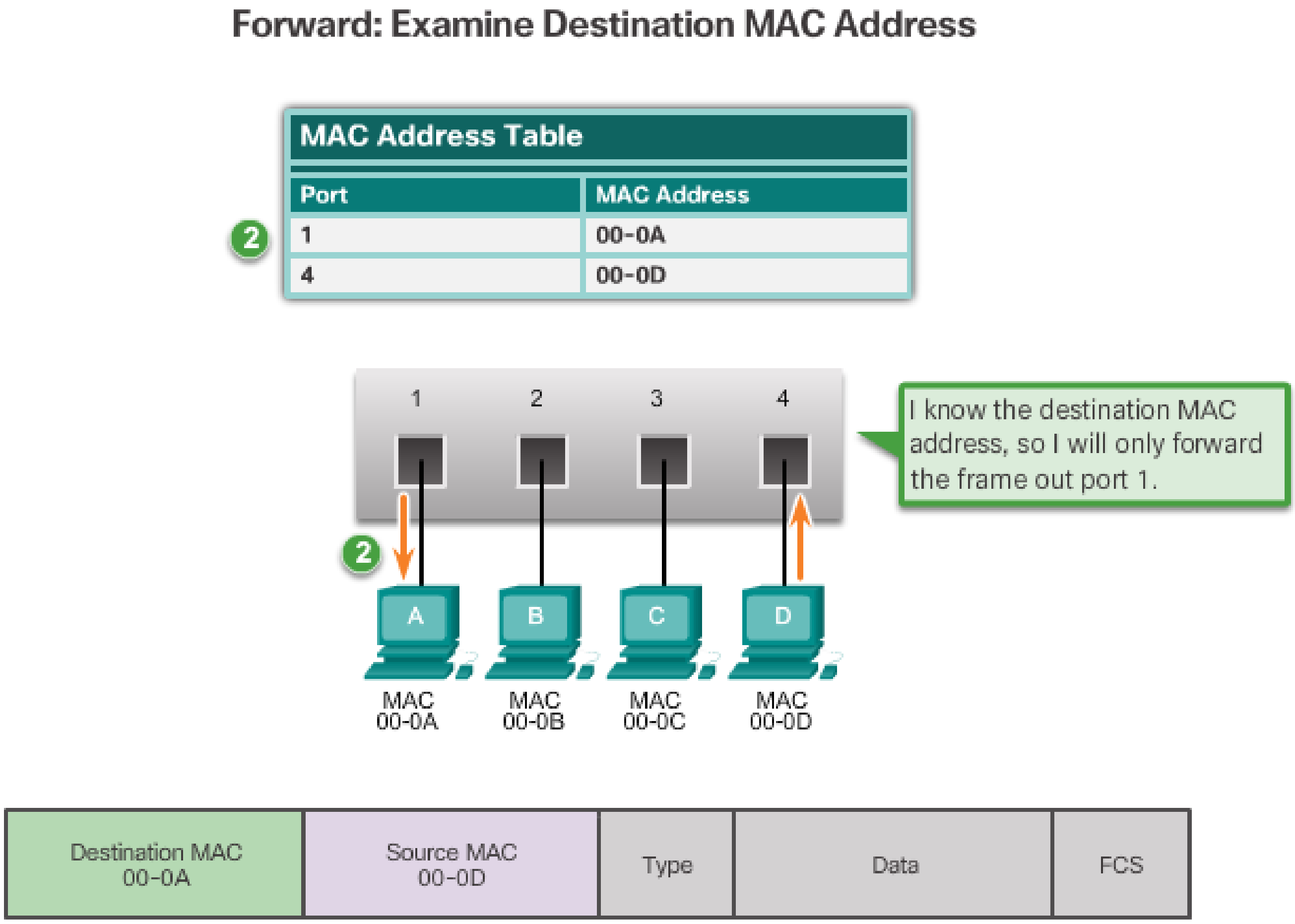


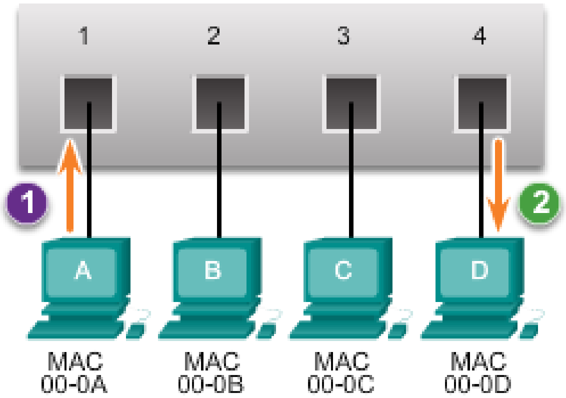
Figure 3 shows PC-A sending another frame to PC-D. The MAC address table already contains PC-A's MAC address, so the five-minute refresh timer for that entry is reset. Next, because the switch's table contains PC-D's MAC address, it sends the frame only out port 4.

5.2.1.3 Filtering Frames

Learn: Examine Source MAC Address

MAC Address Table

Port	MAC Address
1	00-0A
4	00-0D

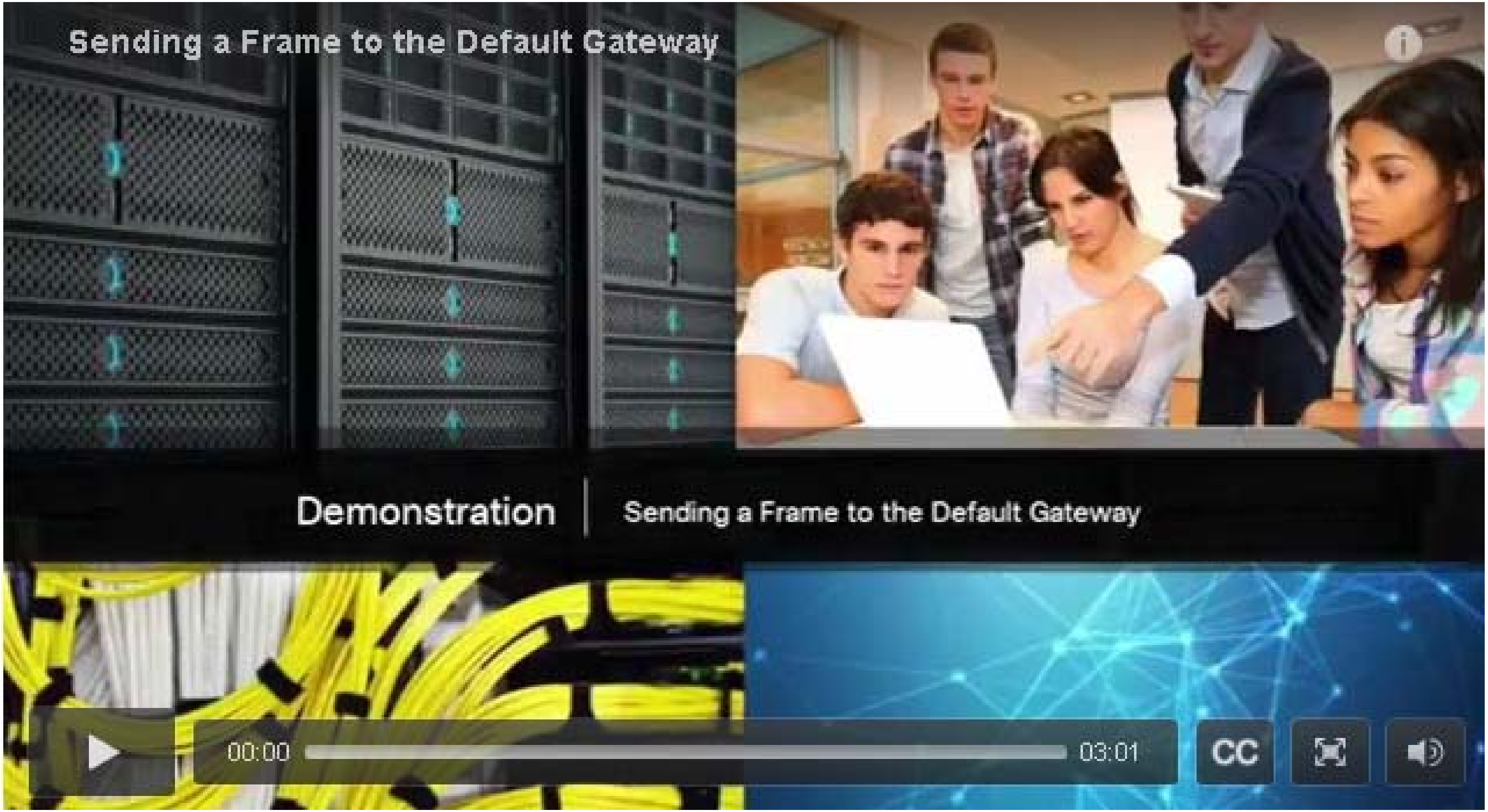


Destination MAC 00-0D	Source MAC 00-0A	Type	Data	FCS

Because the switch's table contains PC-D's MAC address, it sends the frame only out port 4.

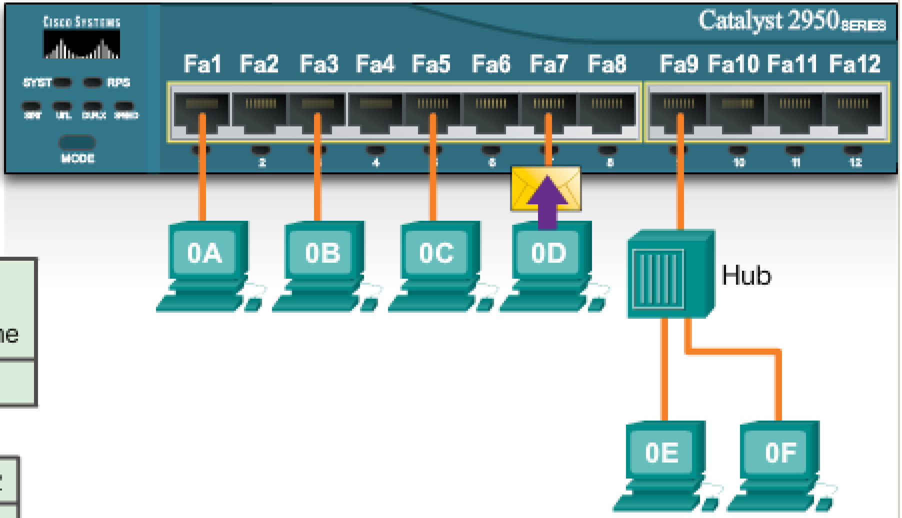
5.2.1.4 Video Demonstration - MAC Address Tables on Connected Switches

5.2.1.5 Video Demonstration - Sending a Frame to the Default Gateway



5.2.1.6 Activity - Switch It!

Activity
Determine how the switch forwards a frame based on the Source MAC and Destination MAC addresses and information in the switch MAC table.
Answer the questions below using the information provided.



Frame

Preamble	Destination MAC	Source MAC	Length Type	Encapsulated Data	End of Frame
	0F	0D			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
				0C		0D		0E 0F			

Question 1 - Where will the switch forward the frame?

- [ ] Fa1 - [ ] Fa2 - [ ] Fa3 - [ ] Fa4 - [ ] Fa5 - [ ] Fa6 - [ ] Fa7 - [ ] Fa8 - [x] Fa9 - [ ] Fa10 - [ ] Fa11 - [ ] Fa12

Question 2 - When the switch forwards the frame, which statement(s) are true?

- [ ] Switch adds the source MAC address to the MAC table.
- [ ] Frame is a broadcast frame and will be forwarded to all ports.
- [x] Frame is a unicast frame and will be sent to specific port only.
- [ ] Frame is a unicast frame and will be flooded to all ports.
- [ ] Frame is a unicast frame but it will be dropped at the switch.

Check

Help

New Problem

5.2.1.7 Lab - Viewing the Switch MAC Address Table

5.2.2.1 Frame Forwarding Methods on Cisco Switches

Switch Packet Forwarding Methods

Store-and-forward

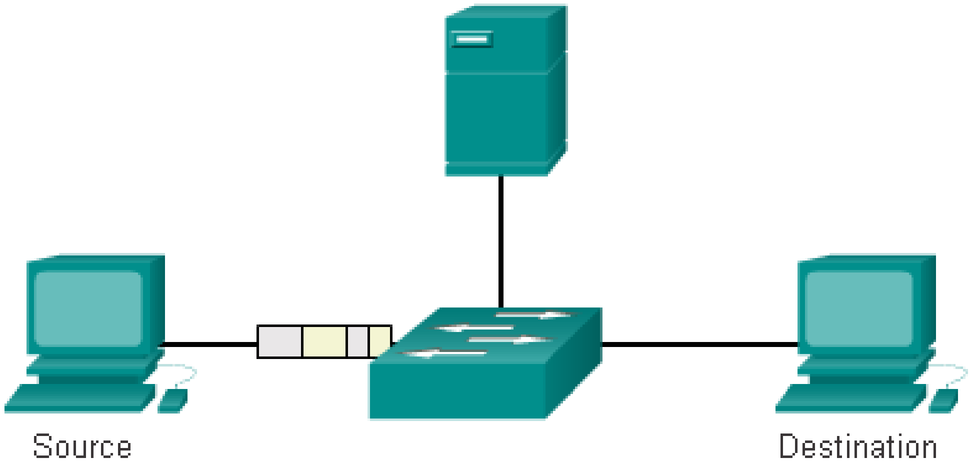
Cut-through

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.

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.

5.2.2.2 Cut-Through Switching

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 - Fast-forward switching offers the lowest level of latency. Fast-forward switching immediately forwards a packet after reading the destination address

Fragment-free switching - In fragment-free switching, the switch stores the first 64 bytes of the frame before forwarding

5.2.2.3 Memory Buffering on Switches

Port-Based and Shared Memory Buffering

Port-based memory	In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.
Shared memory	Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.

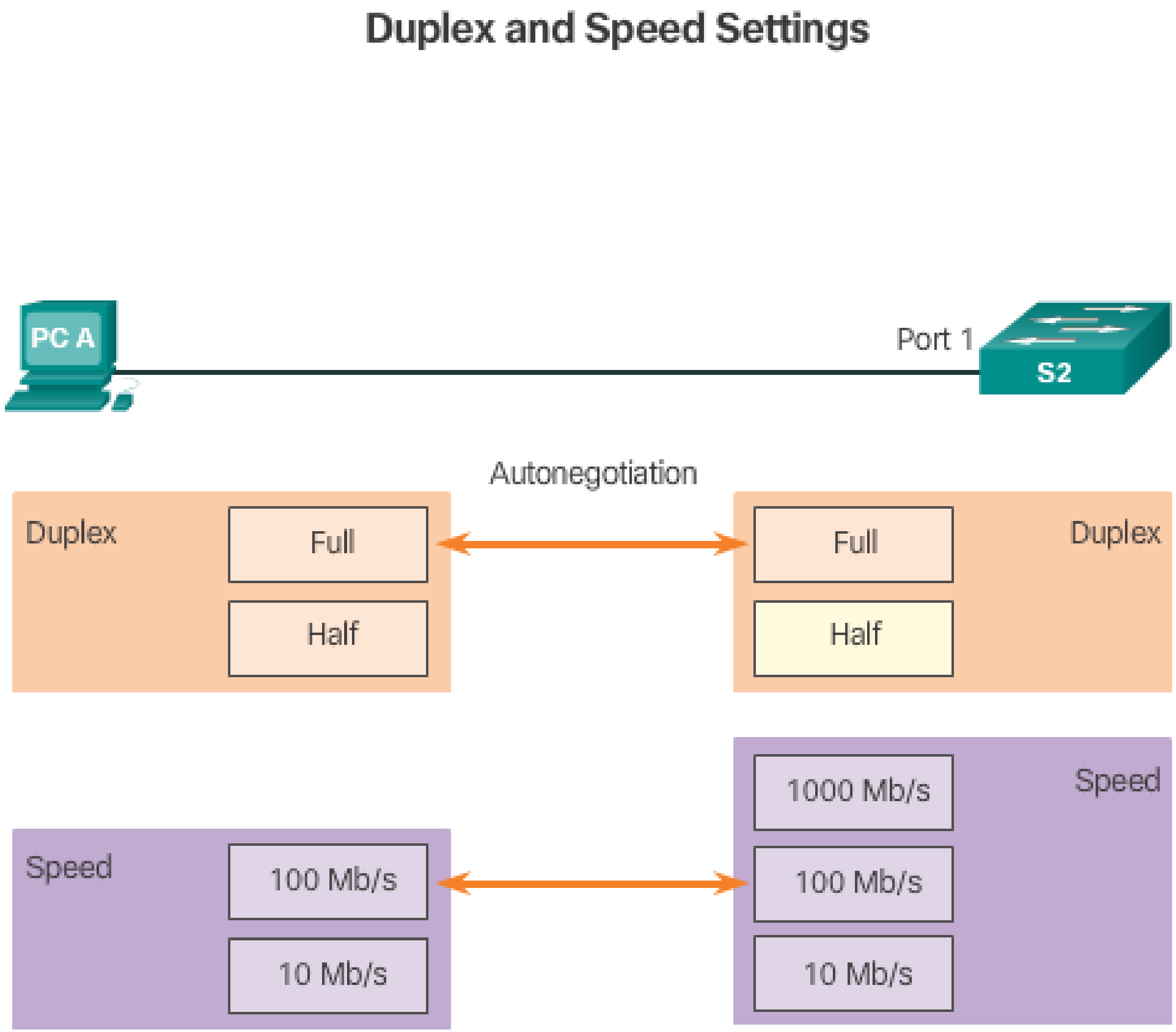
Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store frames before forwarding them. Buffering may also be used when the destination port is busy due to congestion and the switch stores the frame until it can be transmitted.

5.2.2.4 Activity - Frame Forwarding Methods

	Store-and-Forward	Cut-Through
1. Buffers frames until the full frame has been received by the switch.	✓	
2. Checks the frame for errors before releasing it out of its switch ports - if the full frame was not received, the switch discards it.	✓	
3. No error checking on frames is performed by the switch before releasing the frame out of its ports.		✓
4. A great method to use to conserve bandwidth on your network.	✓	
5. The destination network interface card (NIC) discards any incomplete frames using this frame forwarding method.		✓
6. The faster switching method, but may produce more errors in data integrity - therefore, more bandwidth may be consumed.		✓

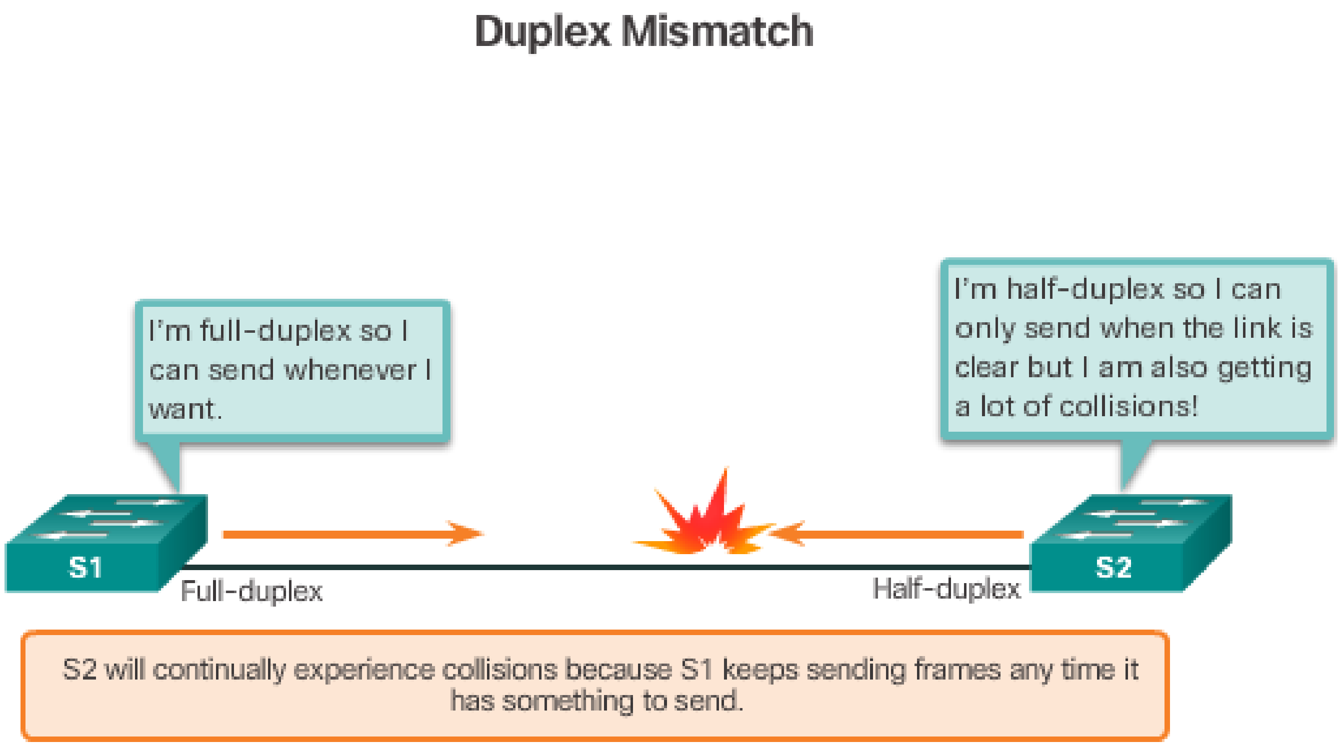
5.2.3.1 Duplex and Speed Settings



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.

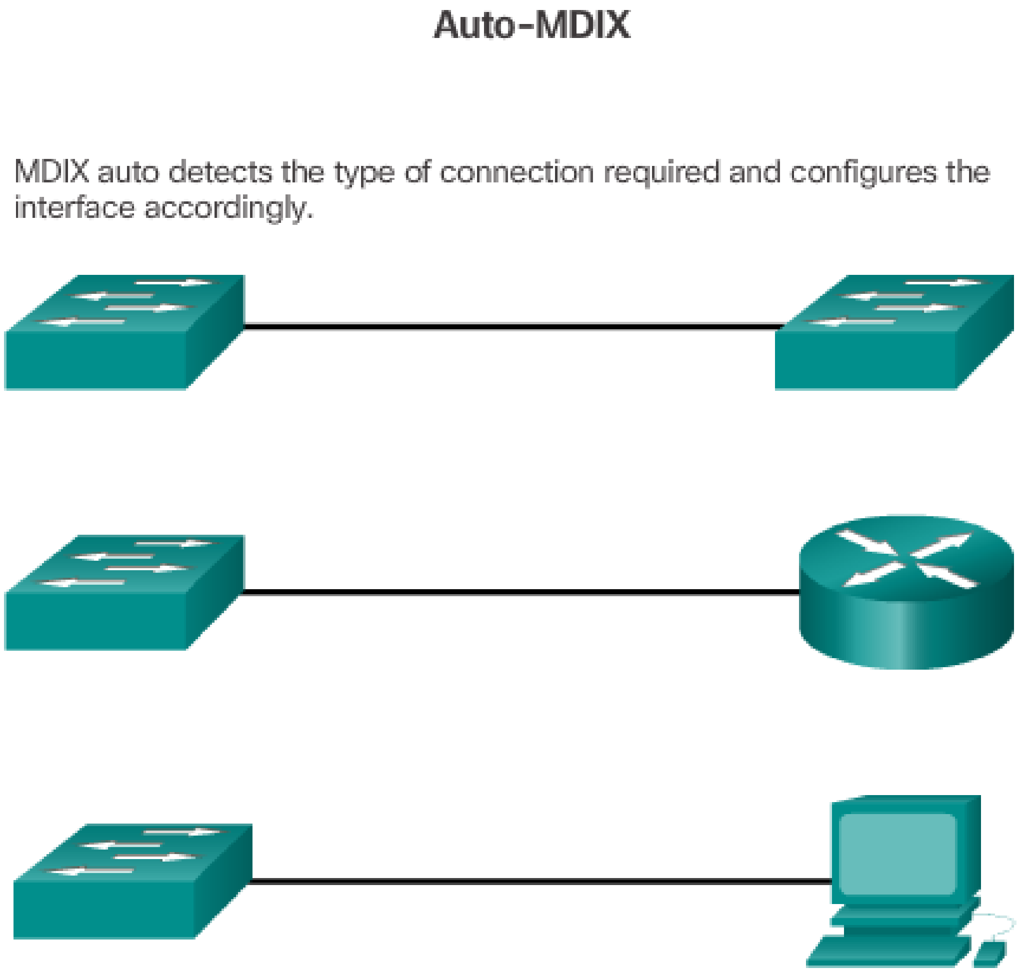
5.2.3.1 Duplex and Speed Settings



One of the most common causes of performance issues on 10/100 Mb/s Ethernet links occurs when one port on the link operates at half-duplex while the other port operates at full-duplex, as shown in Figure 2.

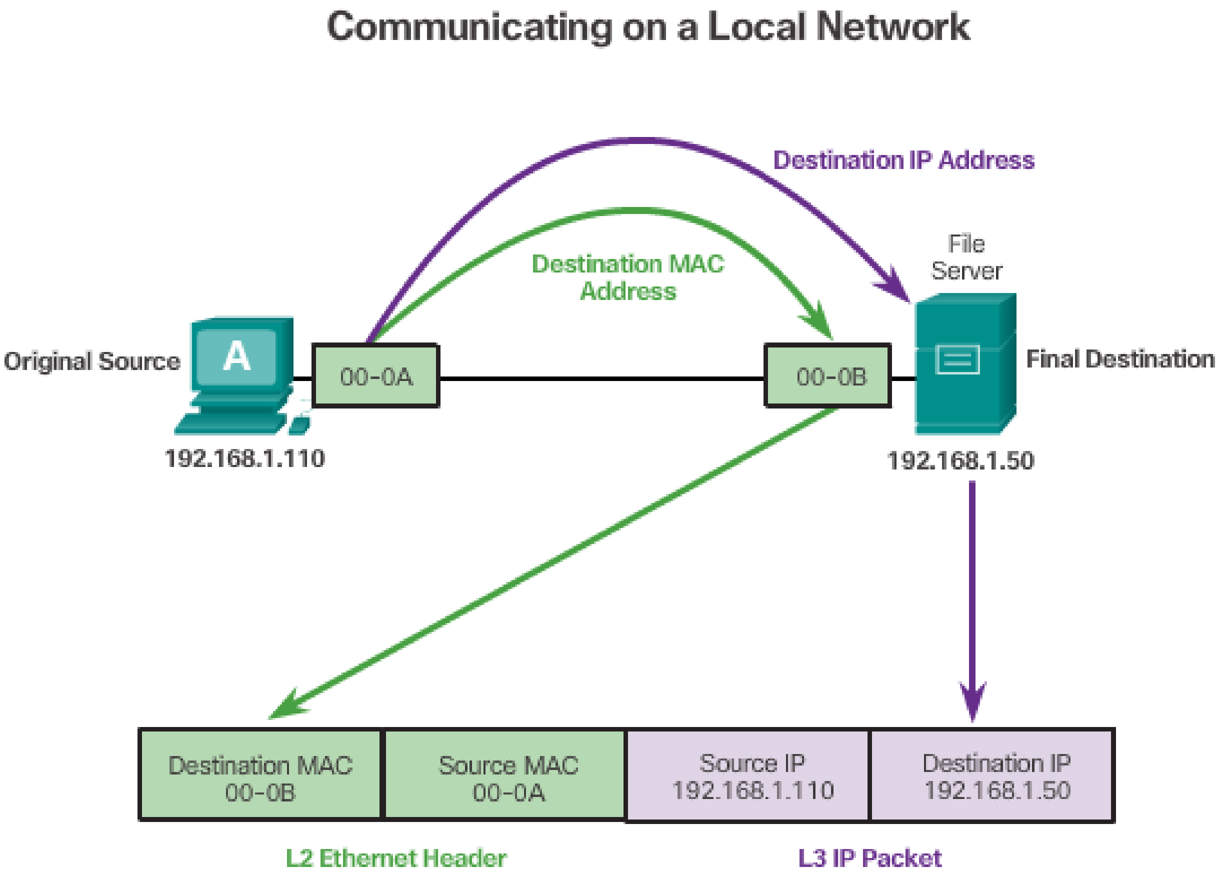
This occurs when one or both ports on a link are reset, and the autonegotiation process does not result in both link partners having the same configuration. It also can occur when users reconfigure one side of a link and forget to reconfigure the other. Both sides of a link should have autonegotiation on, or both sides should have it off.

5.2.3.2 Auto-MDIX



When the auto-MDIX feature is enabled, the switch detects the type of cable attached to the port, and configures the interfaces accordingly. Therefore, you can use either a crossover or a straight-through cable for connections to a copper 10/100/1000 port on the switch, regardless of the type of device on the other end of the connection.

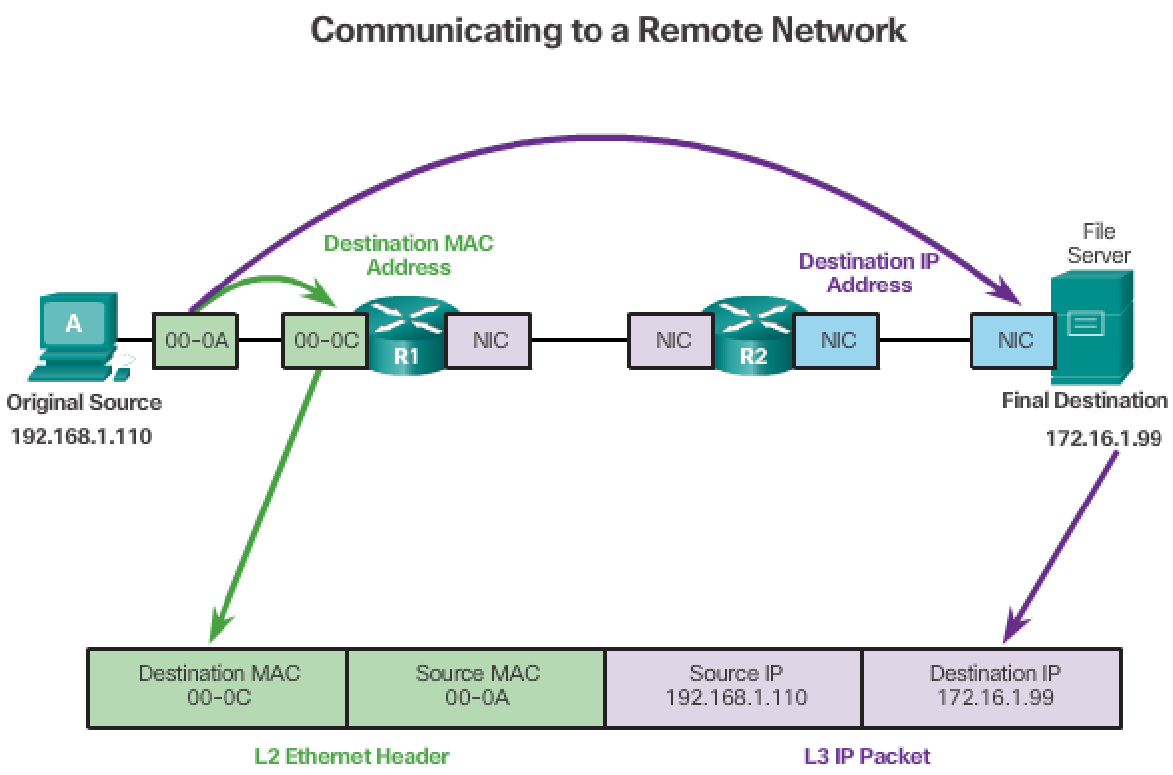
5.3.1.1 Destination on Same Network



There are 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.

5.3.1.2 Destination Remote Network



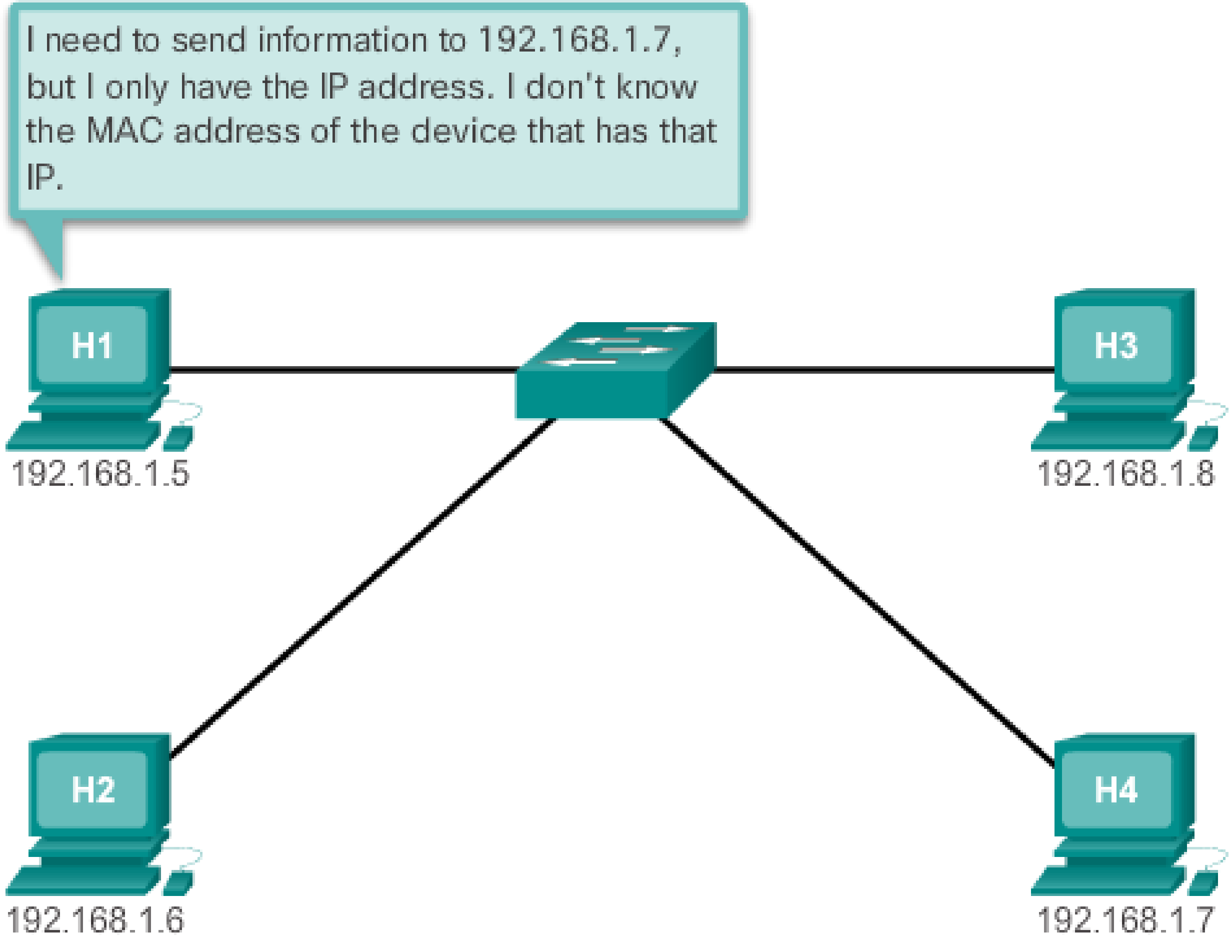
Destination Remote Network

When the destination IP address is on a remote network, the destination MAC address will be the address of the host's default gateway, the router's NIC, as shown in the figure

The figure shows the Ethernet MAC addresses and IP addresses for PC-A sending an IP packet to a web server on a remote network. Routers examine the destination IP address to determine the best path to forward the IP packet. This is similar to how the postal service forwards mail based on the address of the recipient.

5.3.1.3 Packet Tracer – Identify MAC and IP Addresses

5.3.2.1 Introduction to ARP

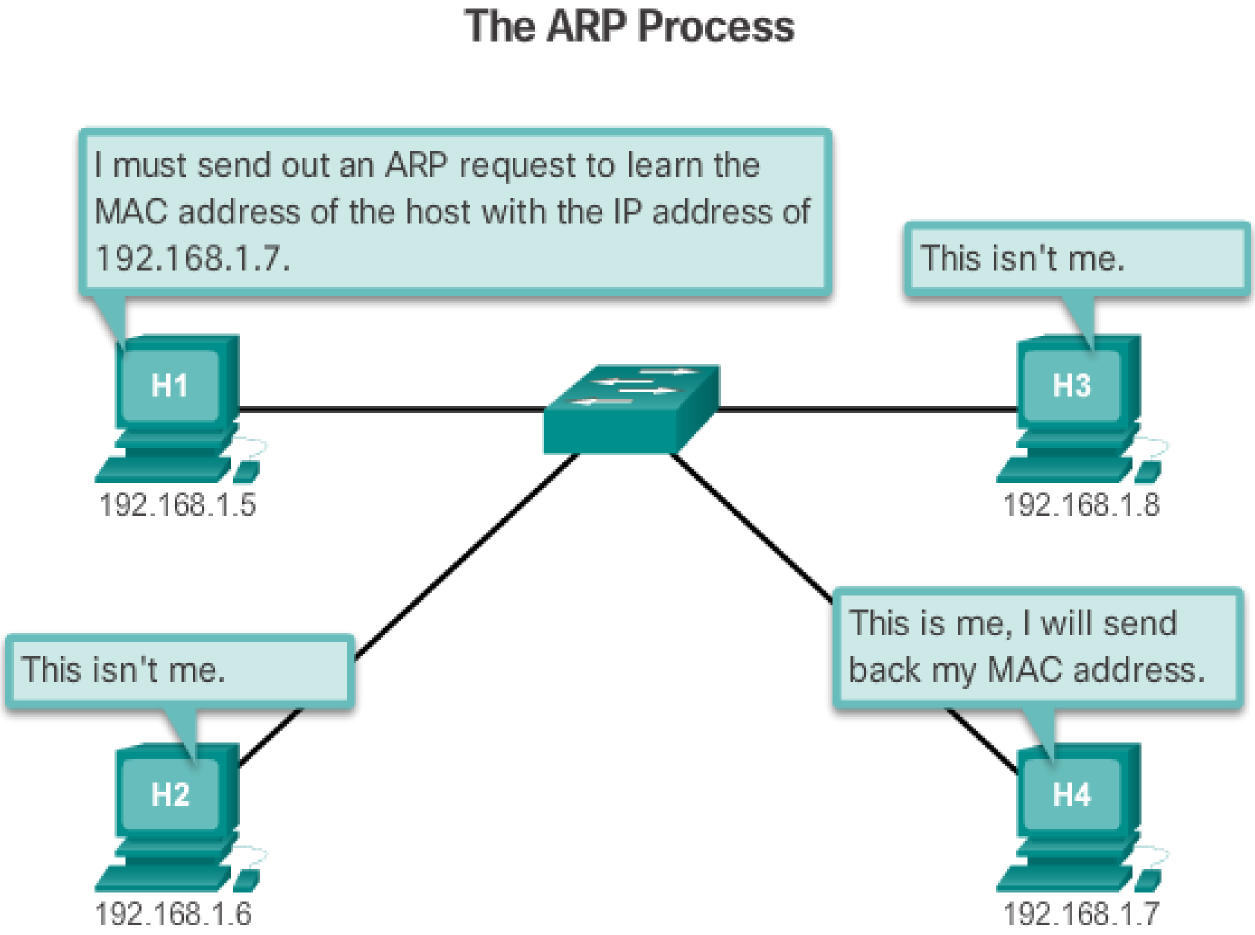


Introduction to ARP

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.

5.3.2.2 ARP Functions



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

- 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.
- 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.

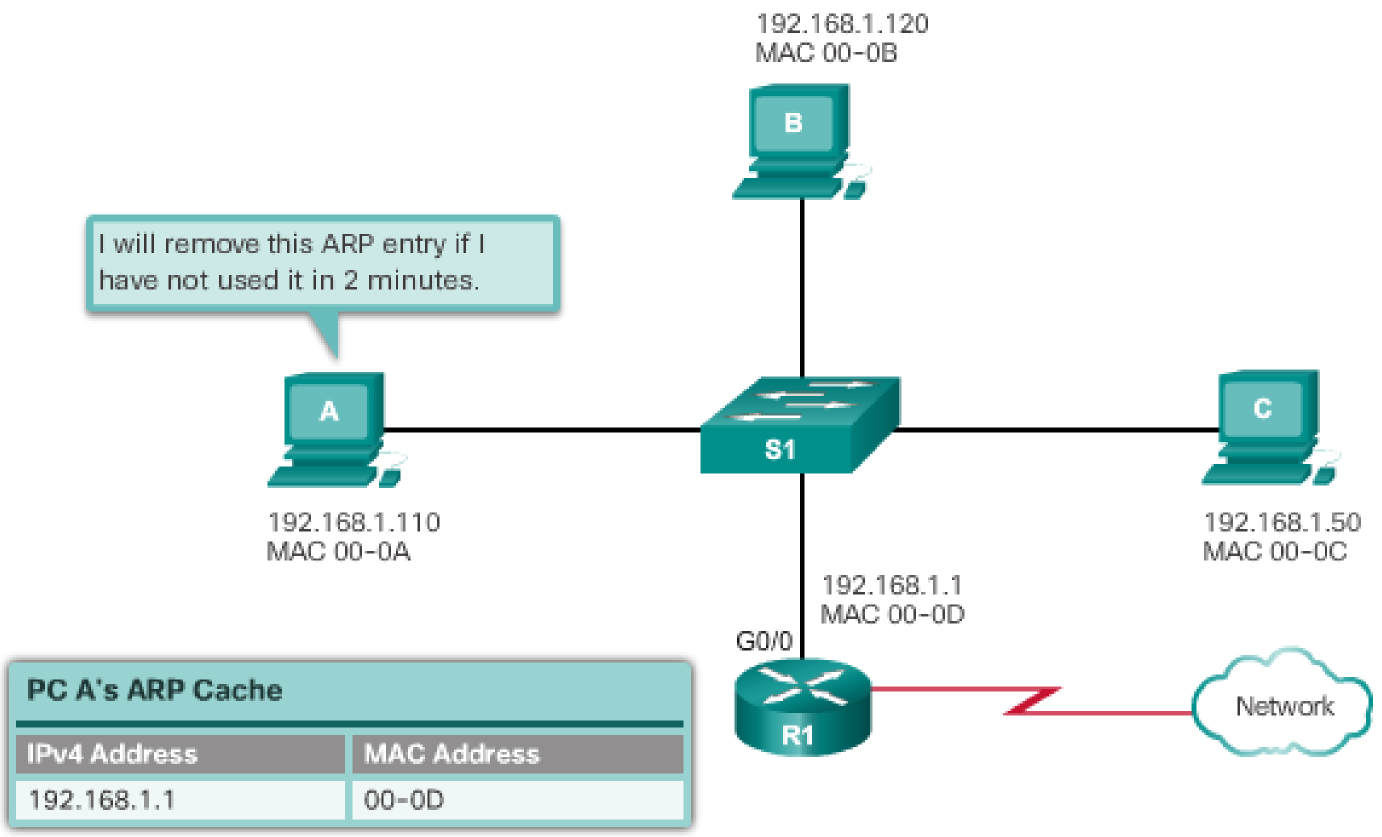
5.3.2.3 Video Demonstration – ARP Request

5.3.2.4 Video Demonstration – ARP Reply

5.3.2.5 Video Demonstration – ARP Role in Remote Communication

5.3.2.6 Removing Entries from an ARP Table

Removing MAC-to-IP Address Mappings



PC A's ARP Cache

IPv4 Address	MAC Address
192.168.1.1	00-0D

MAC addresses are shortened for demonstration purposes.

For each device, an ARP cache timer removes ARP entries that have not been used for a specified period of time. The times differ depending on the device's operating system. For example, some Windows operating systems store ARP cache entries for 2 minutes, as shown in the figure.

5.3.2.7 ARP Tables

Router ARP Table

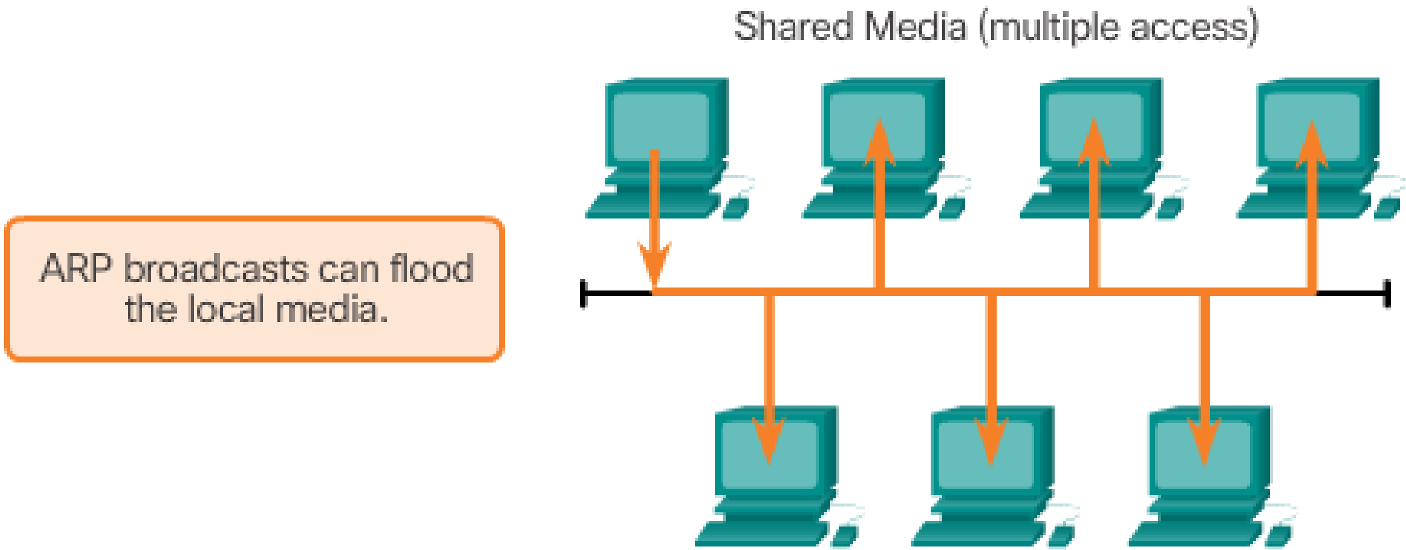
```
Router# show ip arp

                              Age
Protocol   Address            (min)   Hardware Addr    Type    Interface
Internet   172.16.233.229      -      0000.0c59.f892   ARPA    Ethernet0/0
Internet   172.16.233.218      -      0000.0c07.ac00   ARPA    Ethernet0/0
Internet   172.16.168.11       -      0000.0c63.1300   ARPA    Ethernet0/0
Internet   172.16.168.254      9      0000.0c36.6965   ARPA    Ethernet0/0
```

5.3.2.8 Packet Tracer - Examine the ARP Table

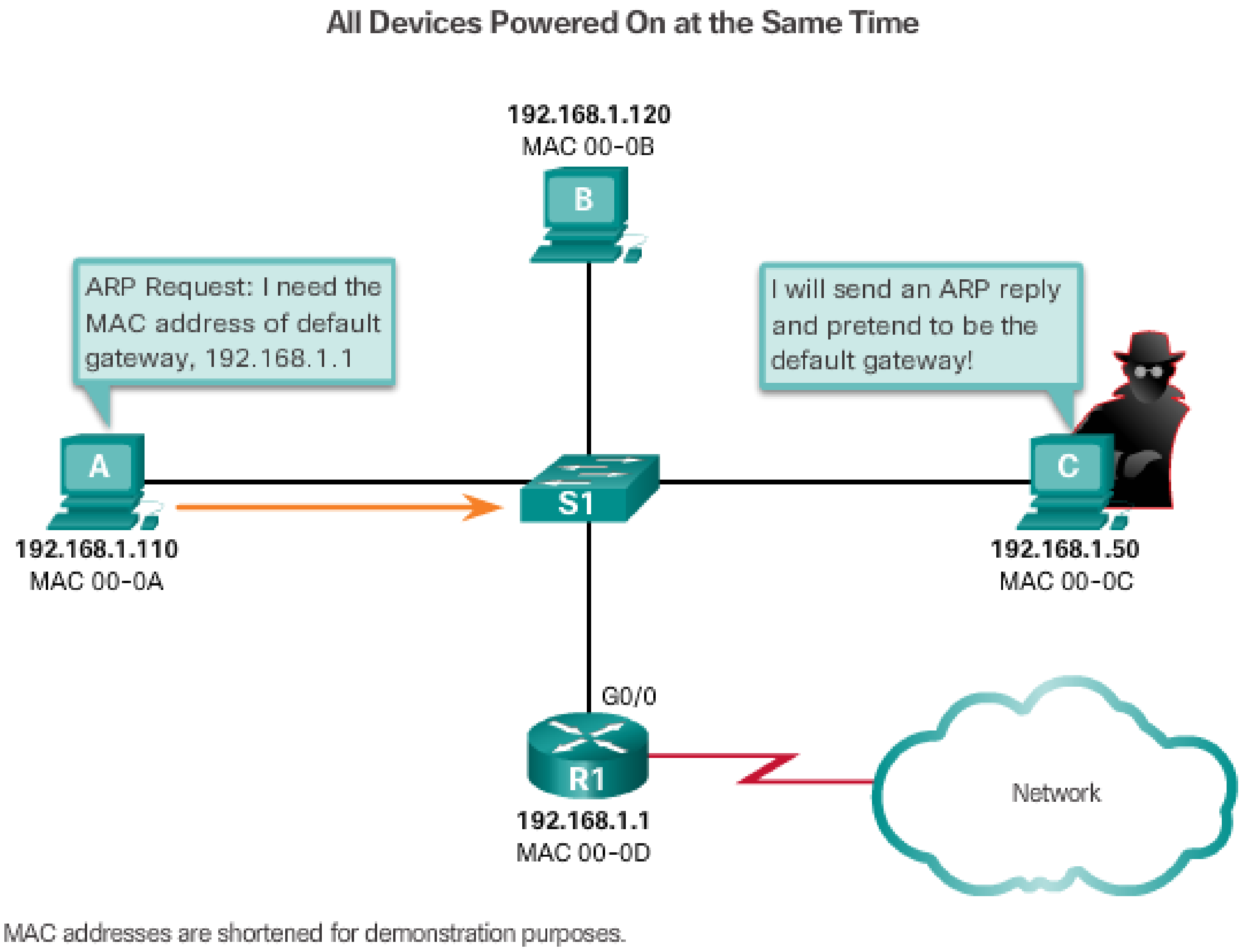
5.3.3.1 ARP Broadcasts

ARP Broadcasts and Security

All devices powered on at the same time



5.3.3.2 ARP Spoofing



In some cases, the use of ARP can lead to a potential security risk known as ARP spoofing or ARP poisoning. This is a technique used by an attacker to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway, as shown in the figure

5.4.1.1 Class Activity - MAC and Choose…

Ethernet uses end and intermediary devices to identify and deliver frames through networks.


Summary
Chapter 5

Thanks!!!

CISCO SYSTEMS

Thank you for your attention!