Cisco Networking Academy

CCNA R&S: Introduction to Networks

Chapter 5:

Ethernet

5.0.1.1 Introduction

Upon completion of this chapter you will be able to:

- Describe the operation of the Ethernet sublayers.
- Identify the major fields of the Ethernet frame.
- Describe the purpose and characteristics of the Ethernet MAC address.
- Describe the purpose of ARP.
- Explain how ARP requests impact network and host performance.
- Explain basic switching concepts.
- Compare fixed configuration and modular switches.
- Configure a Layer 3 switch.

The OSI physical layer provides the means to transport the bits that make up a data link layer frame across the network media.

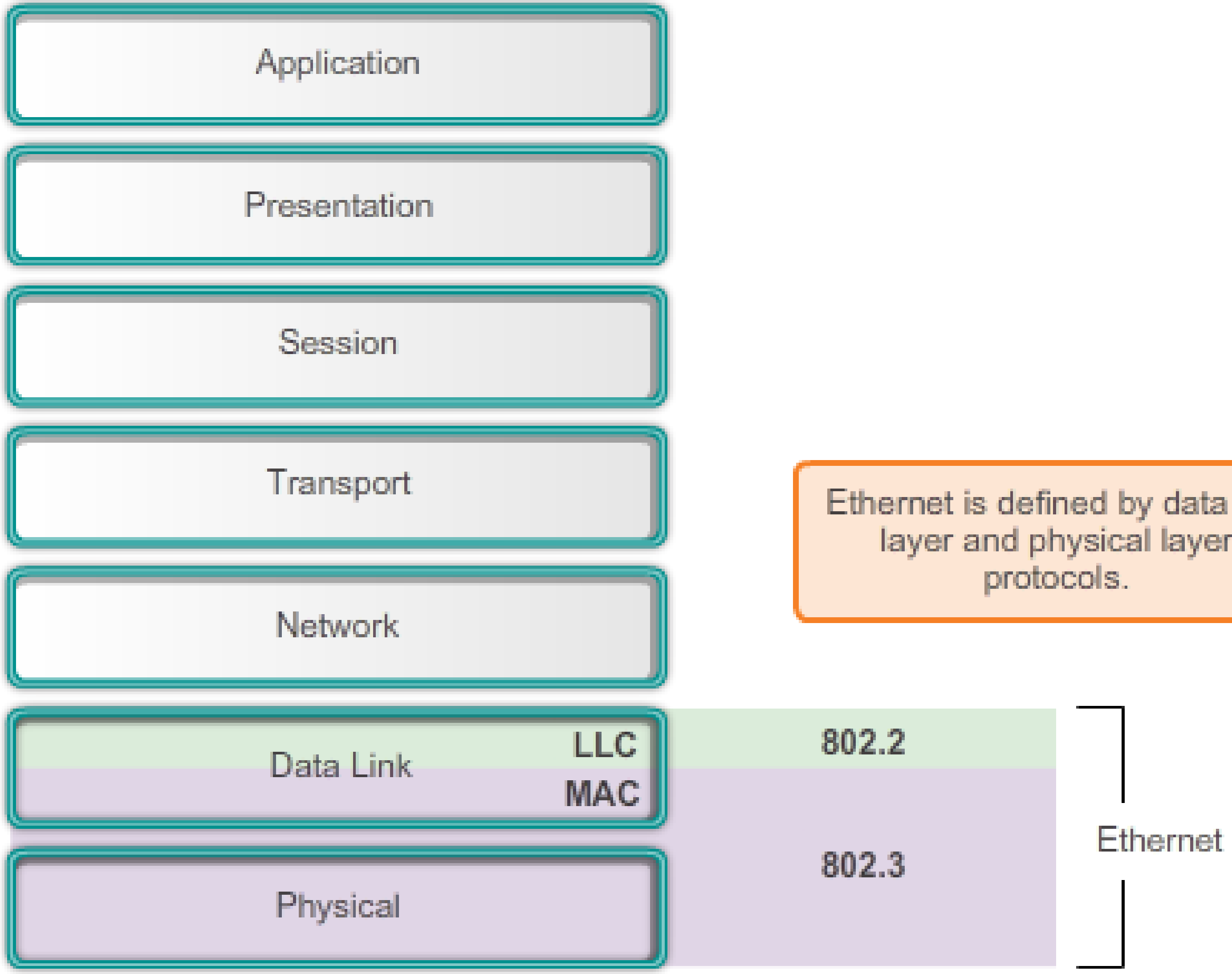
Ethernet is now the predominant LAN technology in the world. Ethernet operates in the data link layer and the physical layer.

5.0.1.2 Activity – Join My Social Circle!

How are communications groups <u>identified</u>?

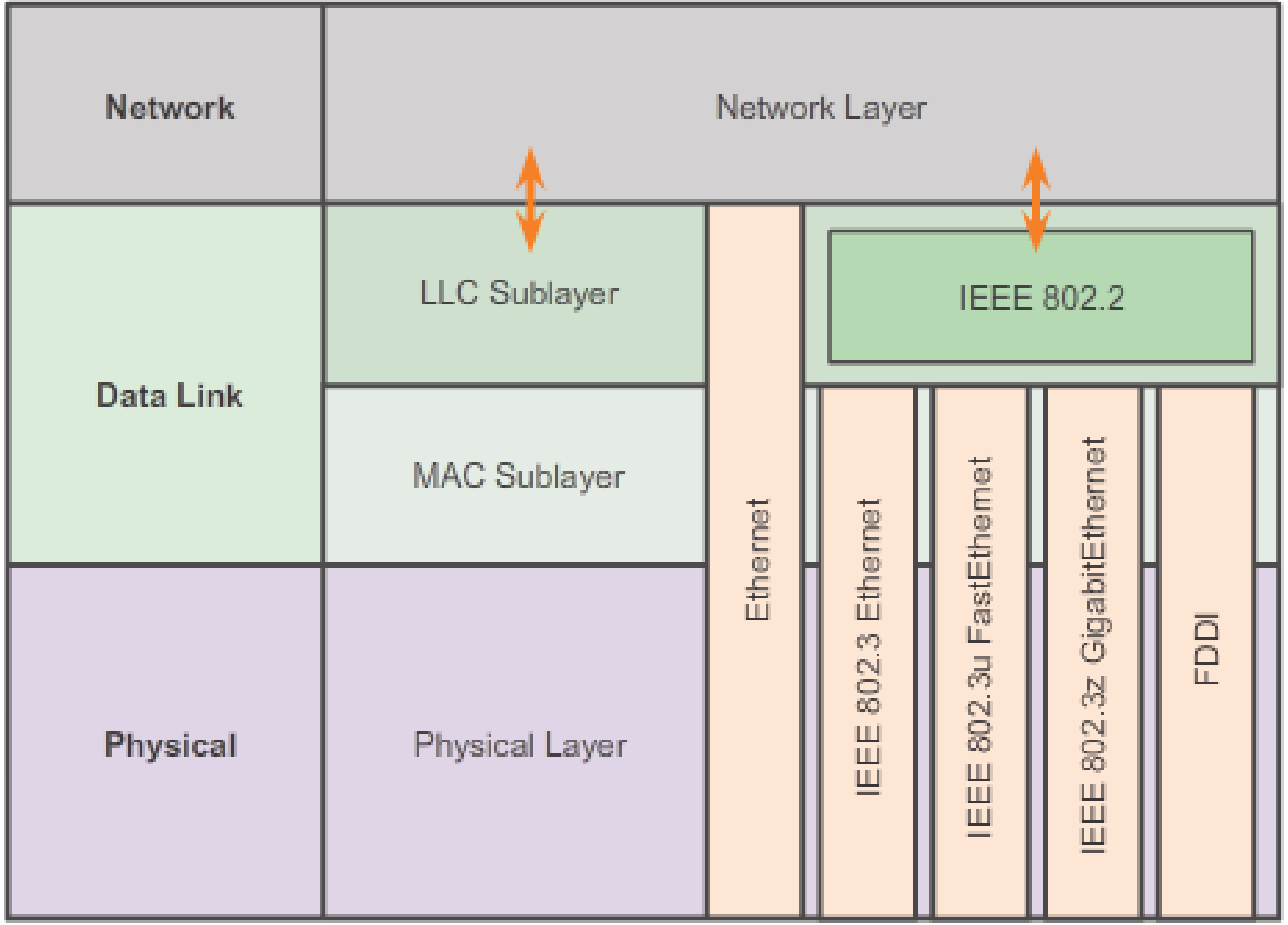
5.1.1.1 LLC and MAC Sublayers

Ethernet

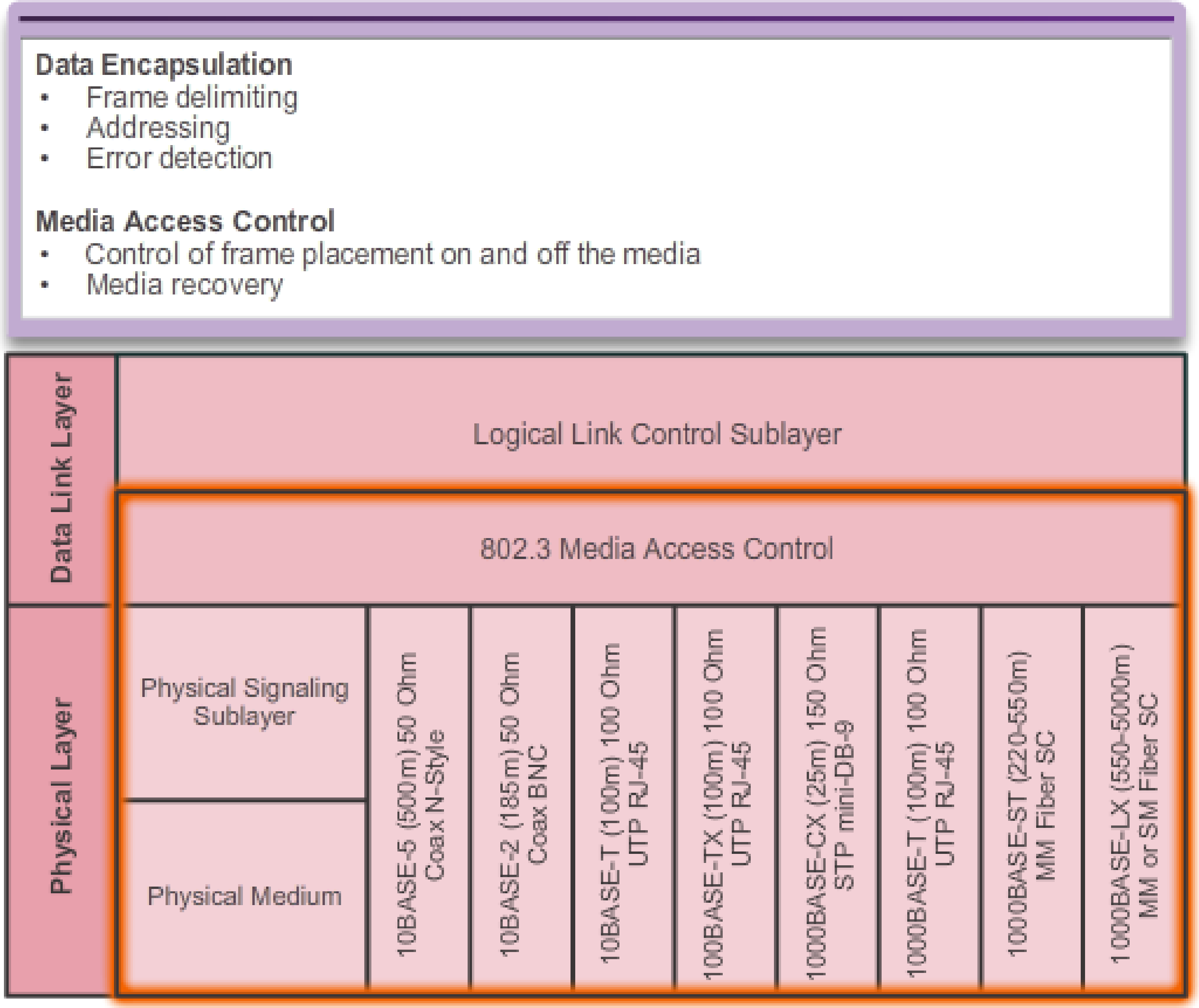


Ethernet is defined by data link layer and physical layer protocols.

5.1.1.1 LLC and MAC Sublayers



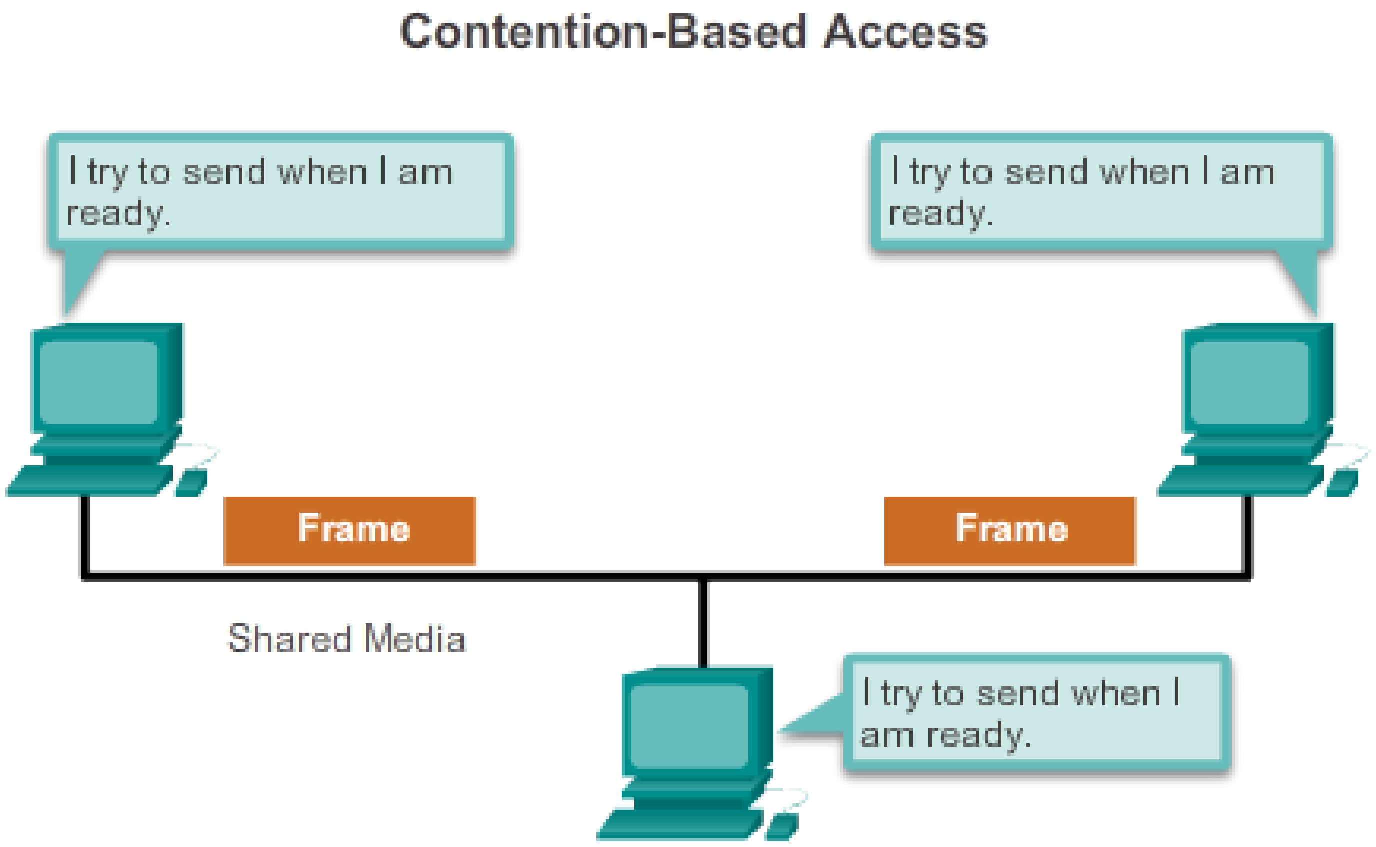
5.1.1.2 MAC Sublayer



Media Access Control

The second responsibility of the MAC sublayer is 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.

5.1.1.3 Media Access Control

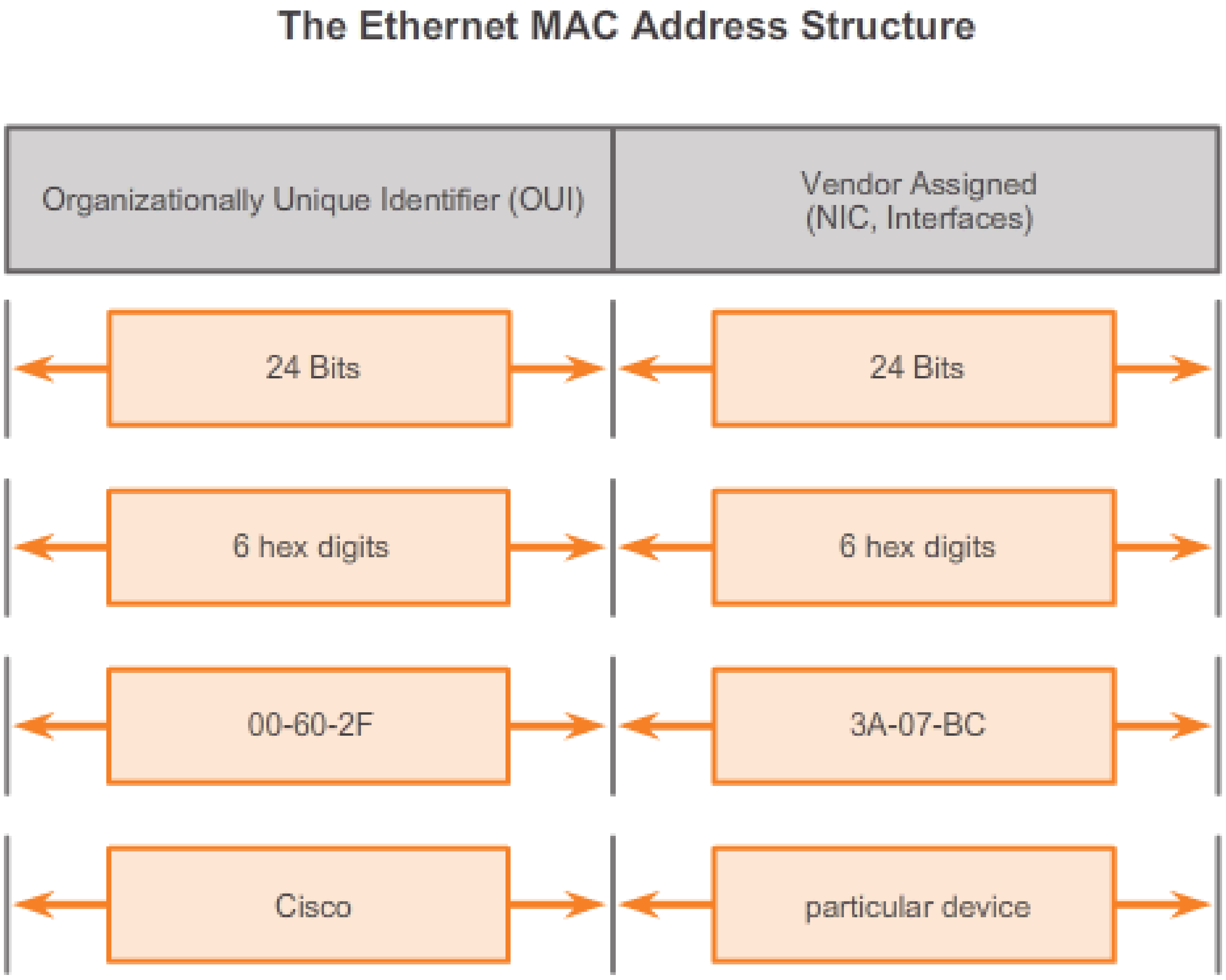


Method	Characteristics	Example

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

The CSMA process is used to first detect if the media is carrying a signal. If a carrier signal on the media from another node is detected, it means that another device is transmitting.

5.1.1.4 MAC Address: Ethernet Identity

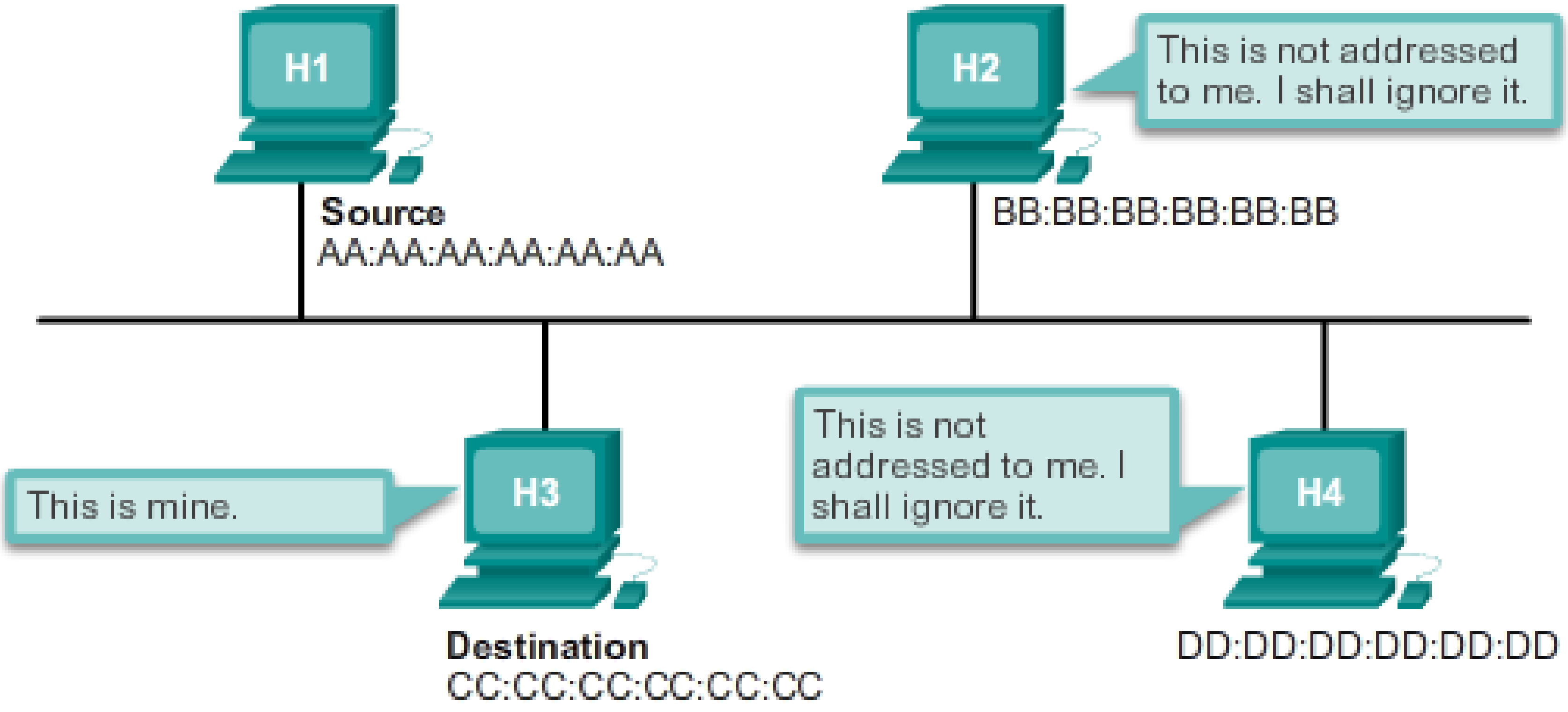


MAC addressing is added as part of a Layer 2 PDU. An Ethernet MAC address is a 48-bit binary value expressed as 12 hexadecimal digits (4 bits per hexadecimal digit).

5.1.1.5 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		



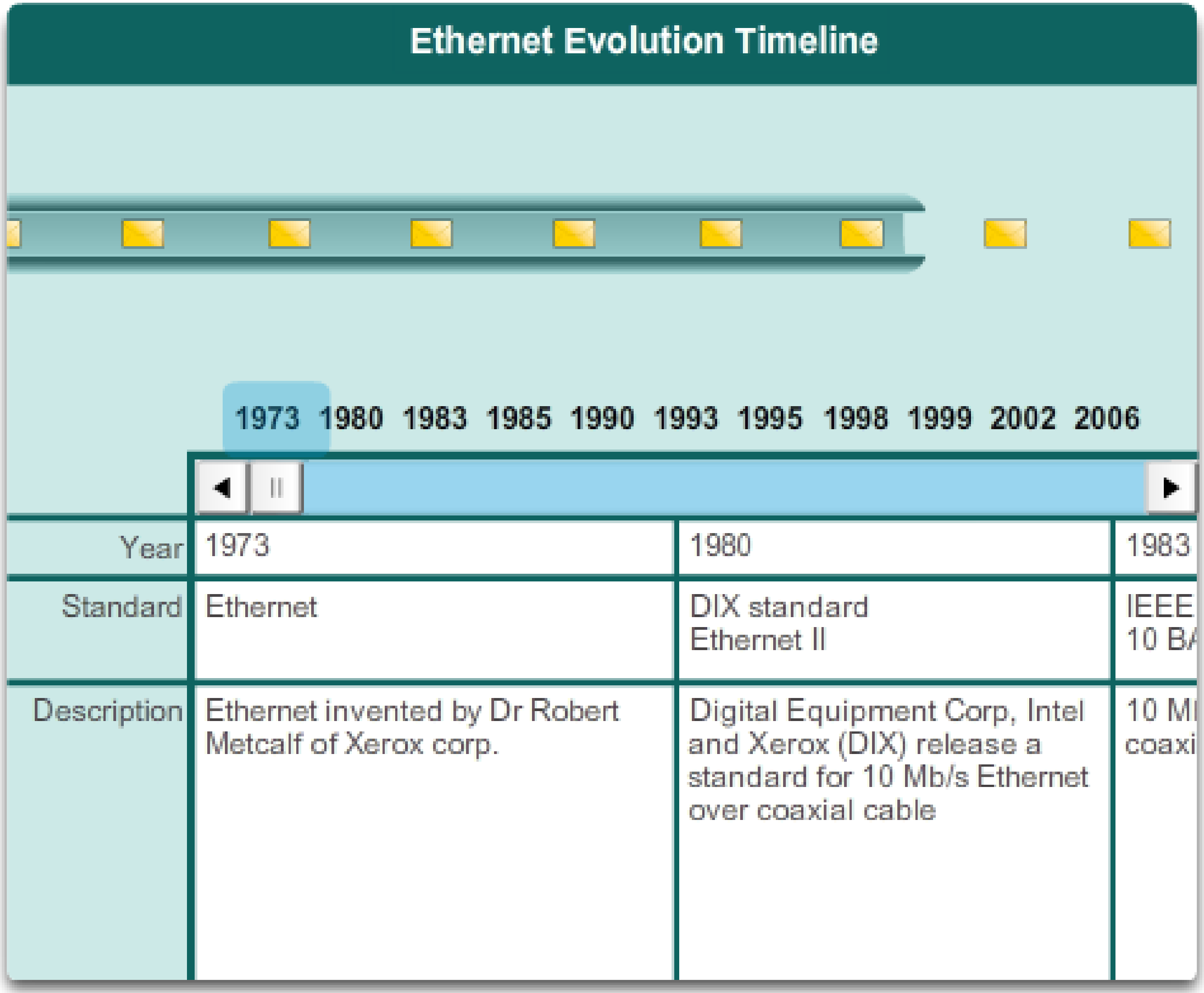
The MAC address is often referred to as a burned-in address (BIA) The address is encoded into the ROM chip permanently - it cannot be changed by software.

It is possible to change the MAC address in software. This is useful when attempting to gain access to a network that filters based on BIA - filtering, or controlling, traffic based on the MAC address is no longer as secure.

5.1.1.6 Activity - MAC and LLC Sublayers

	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 – checks for errors in 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		✓

5.1.2.1 Ethernet Encapsulation



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

5.1.2.1 Ethernet Encapsulation

Comparison of 802.3 and Ethernet II Frame Structures and Field Size

Field size in bytes

IEEE 802.3

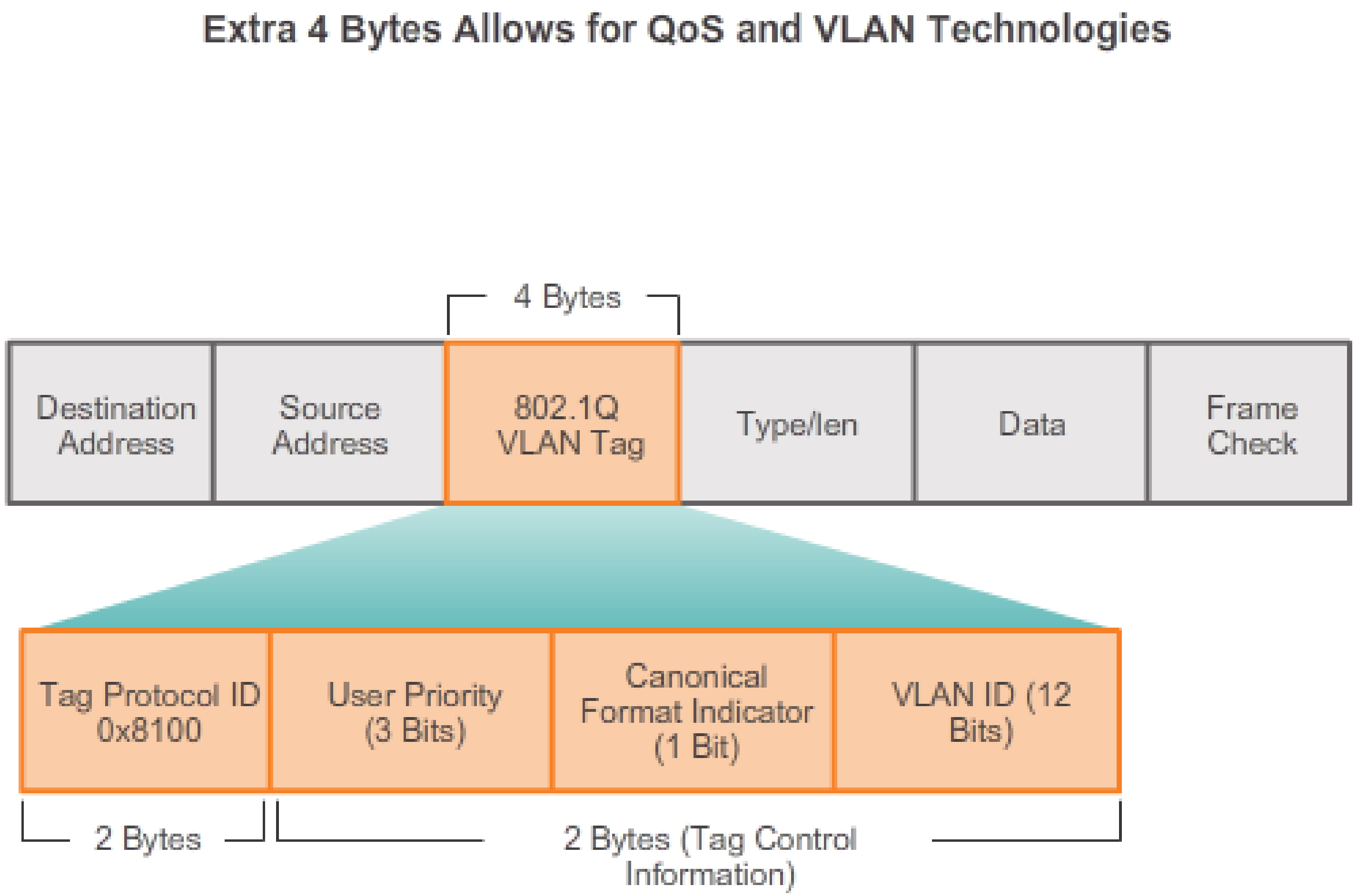
7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destinatio n Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

Ethernet II

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

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

5.1.2.2 Ethernet Frame Size



Both the Ethernet II and IEEE 802.3 standards define the minimum frame size as 64 bytes and the maximum as 1518 bytes. This includes all bytes from the Destination MAC Address field through the Frame Check Sequence (FCS) field. The Preamble and Start Frame Delimiter fields are 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

5.1.2.3 Introduction to the Ethernet Frame

IEEE 802.3

7	1	6	6	2	46 to 1500	4
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

5.1.2.4 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-level 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

IEEE 802.3 Ethernet Frame Fields

7 bytes	1 byte	6 bytes	6 bytes	2 bytes	46-1500 bytes	4 bytes
Preamble	Start of Frame Delimiter	Destination Address	Source Address	Length	802.2 Header and Data	Frame Check Sequence

5.1.3.1 MAC Addresses 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

5.1.3.2 MAC Address Representations

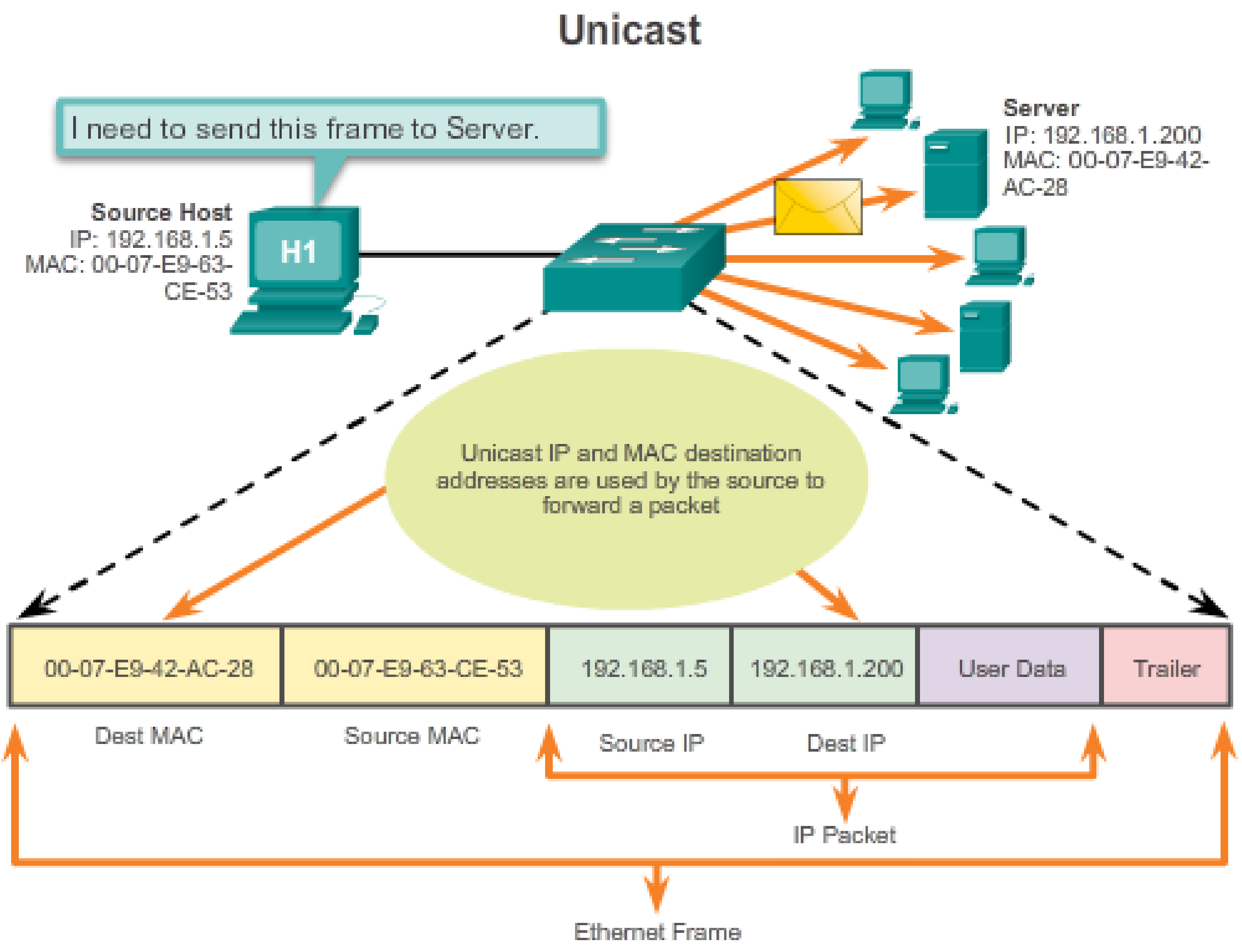
```
C:\>ipconfig/all

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : example.com
   Description . . . . . . . . . . . : Intel(R) Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-18-DE-C7-F3-F8
   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

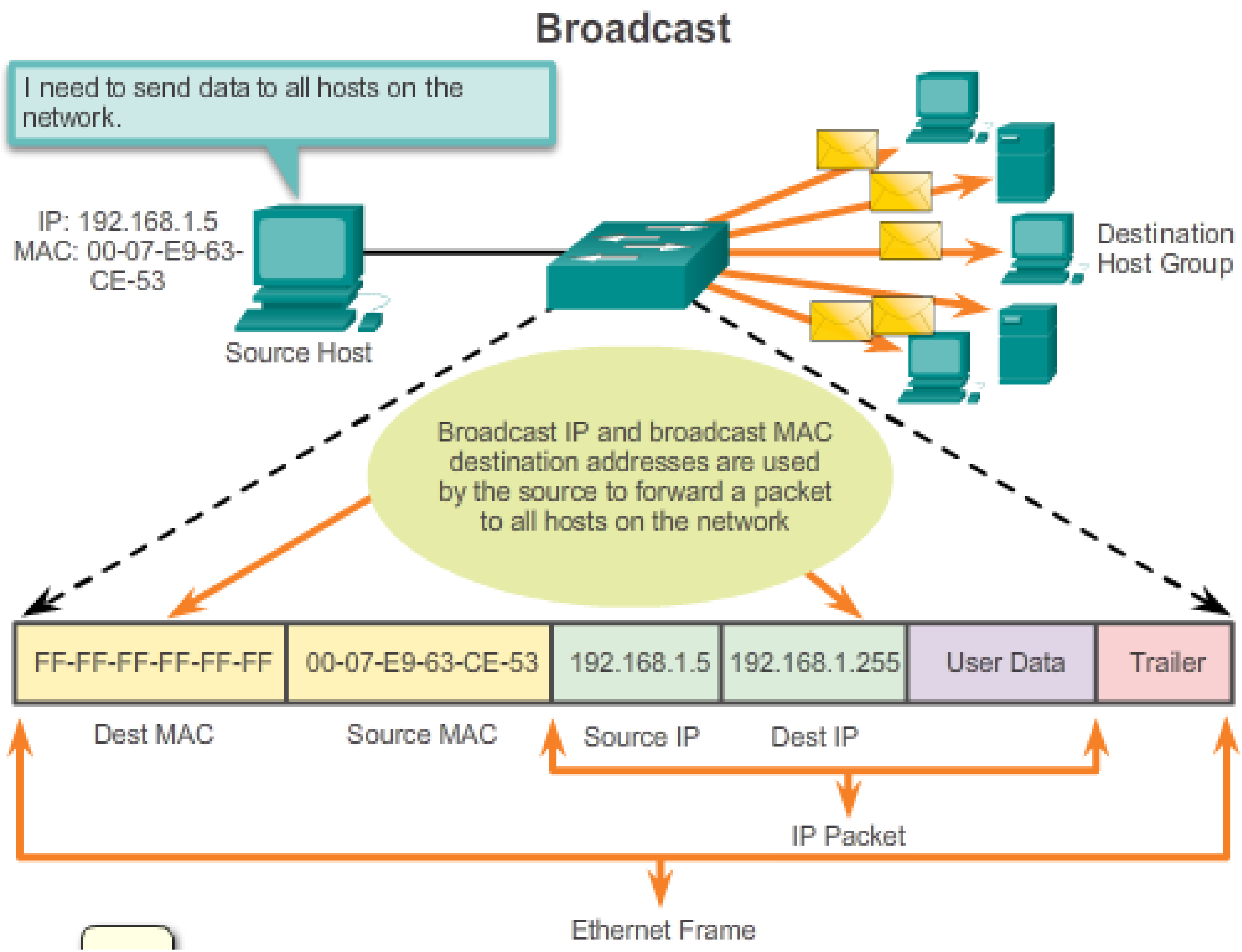
With Periods 0060.2F3A.07BC

5.1.3.3 Unicast MAC Address



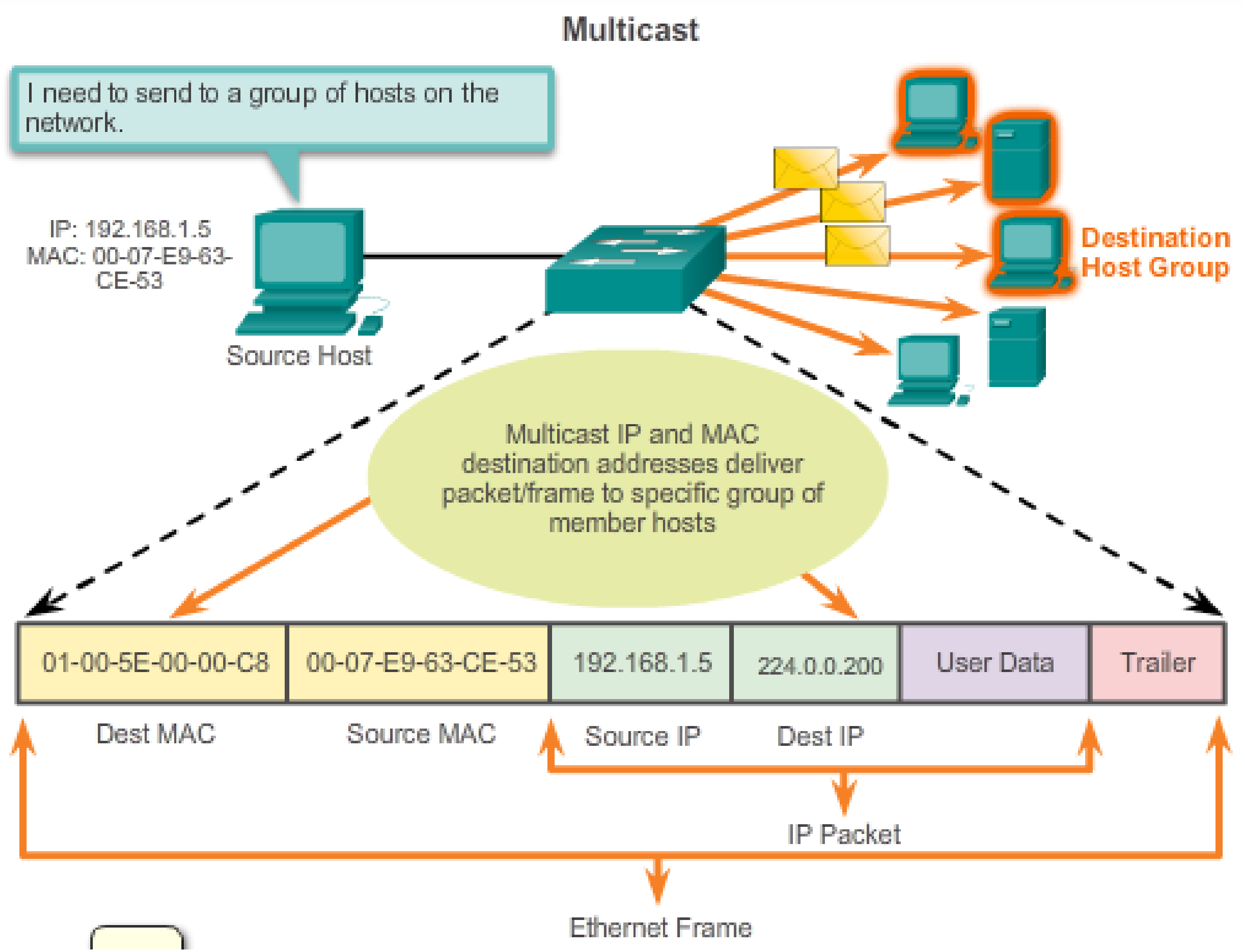
A host with IP address 192.168.1.5 (source) requests a web page from the server at IP address 192.168.1.200. For a unicast packet to be sent and received, a destination IP address must be in the IP packet header. A corresponding destination MAC address must also be present in the Ethernet frame header. The IP address and MAC address combine to deliver data to one specific destination host.

5.1.3.4 Broadcast MAC Address



As shown in the figure, a broadcast IP address for a network needs a corresponding broadcast MAC address in the Ethernet frame. On Ethernet networks, the broadcast MAC address is 48 ones displayed as hexadecimal FF-FF-FF-FF-FF-FF.

5.1.3.5 Multicast MAC Address



As with the unicast and broadcast addresses, the multicast IP address requires a corresponding multicast MAC address to actually deliver frames on a local network. The multicast MAC address is a special value that begins with 01-00-5E in hexadecimal. The remaining portion of the multicast MAC address is created by converting the lower 23 bits of the IP multicast group address into 6 hexadecimal characters.

5.1.3.6 Lab - Viewing 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

5.1.4.1 MAC and IP

Both the physical MAC and logical IP addresses are required for a computer to communicate on a hierarchical network, just like both the name and address of a person are required to send a letter.

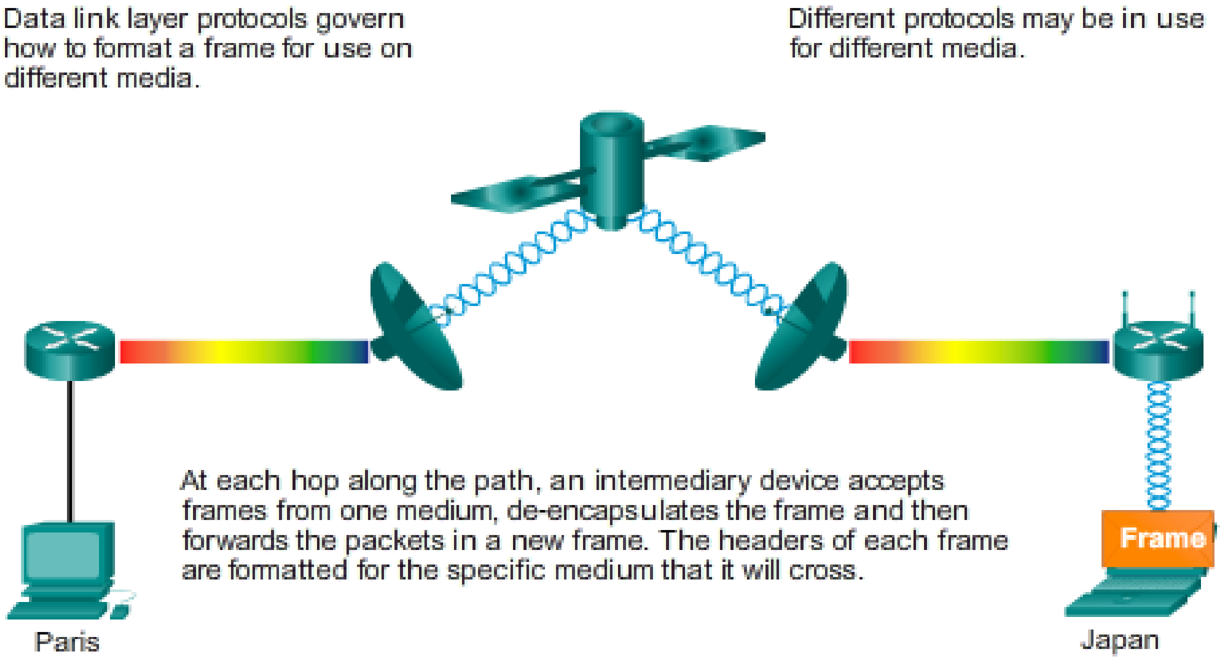
5.1.4.2 End-to-End Connectivity, MAC, and IP

IP Packet Encapsulated in an Ethernet Frame

Destination MAC Address BB:BB:BB:BB:BB:BB	Source MAC Address AA:AA:AA:AA:AA:AA	Source IP Address 10.0.0.1	Destination IP Address 192.168.1.5	Data	Trailer

A router examines IP addresses.

The Data Link Layer



End devices on an Ethernet network do not accept and process frames based on IP addresses, rather, a frame is accepted and processed based on MAC addresses.

On Ethernet networks, MAC addresses are used to identify, at a lower level, the source and destination hosts.

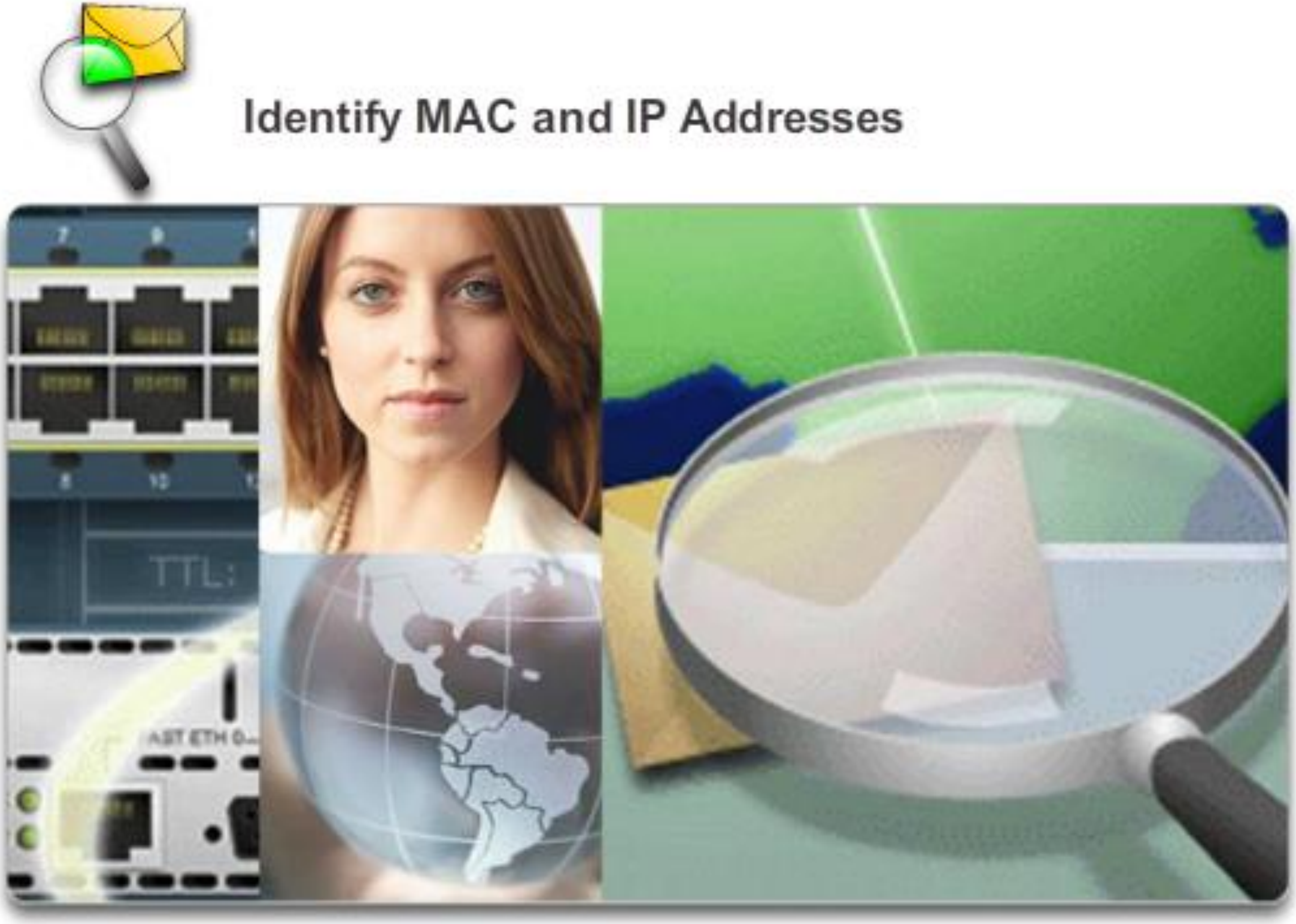
How are the IP addresses of the IP packets in a data flow associated with the MAC addresses on each link along the path to the destination? This is done through a process called Address Resolution Protocol (ARP).

5.1.4.3 Lab - Using Wireshark to Examine Ethernet Frames

In this lab, you will complete the following objectives:

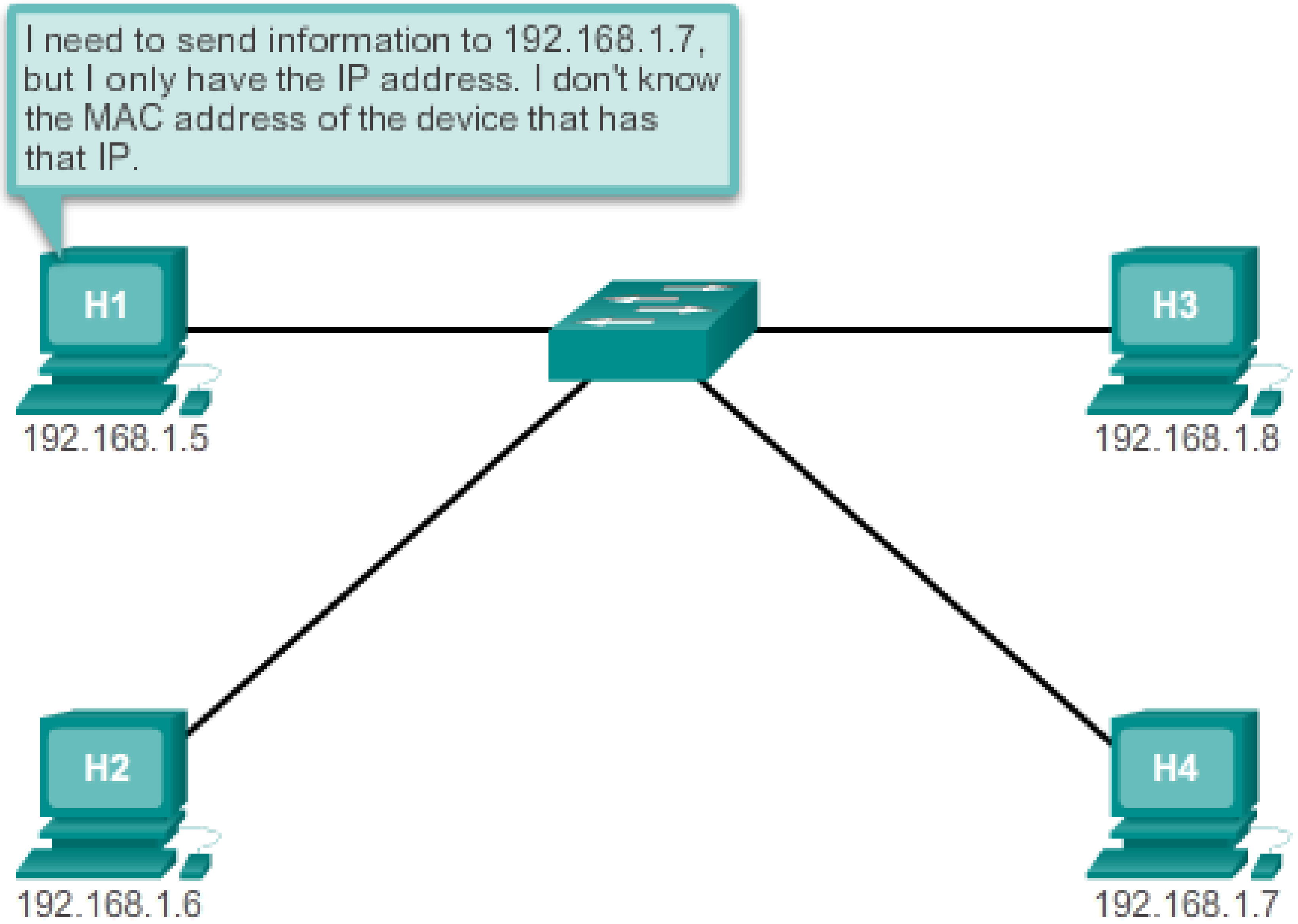
- Examine the Header Fields in an Ethernet II Frame
- Use Wireshark to Capture and Analyze Ethernet Frames

5.1.4.4 Packet Tracer - Identify MAC and IP Addresses



This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

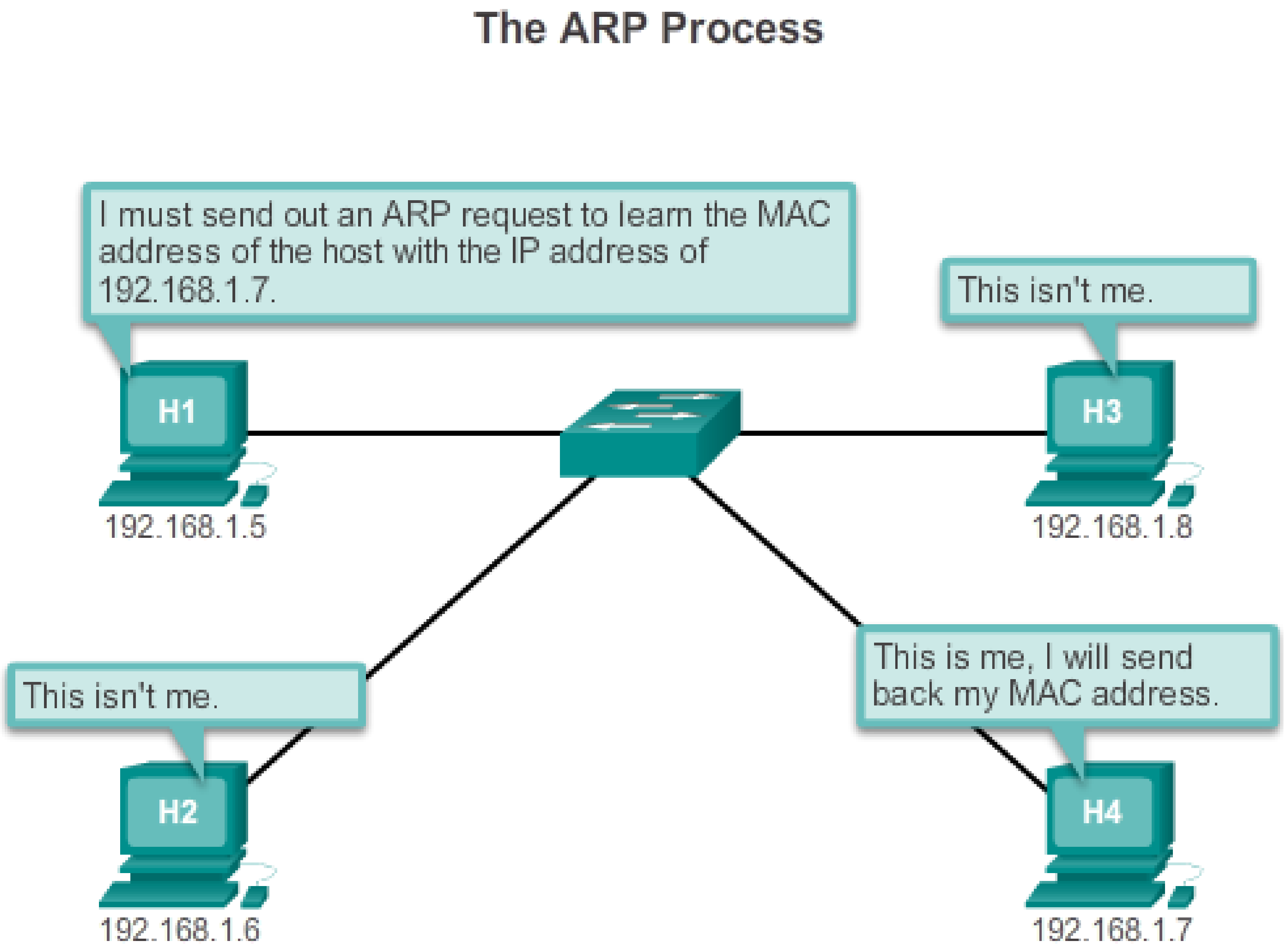
5.2.1.1 Introduction to ARP



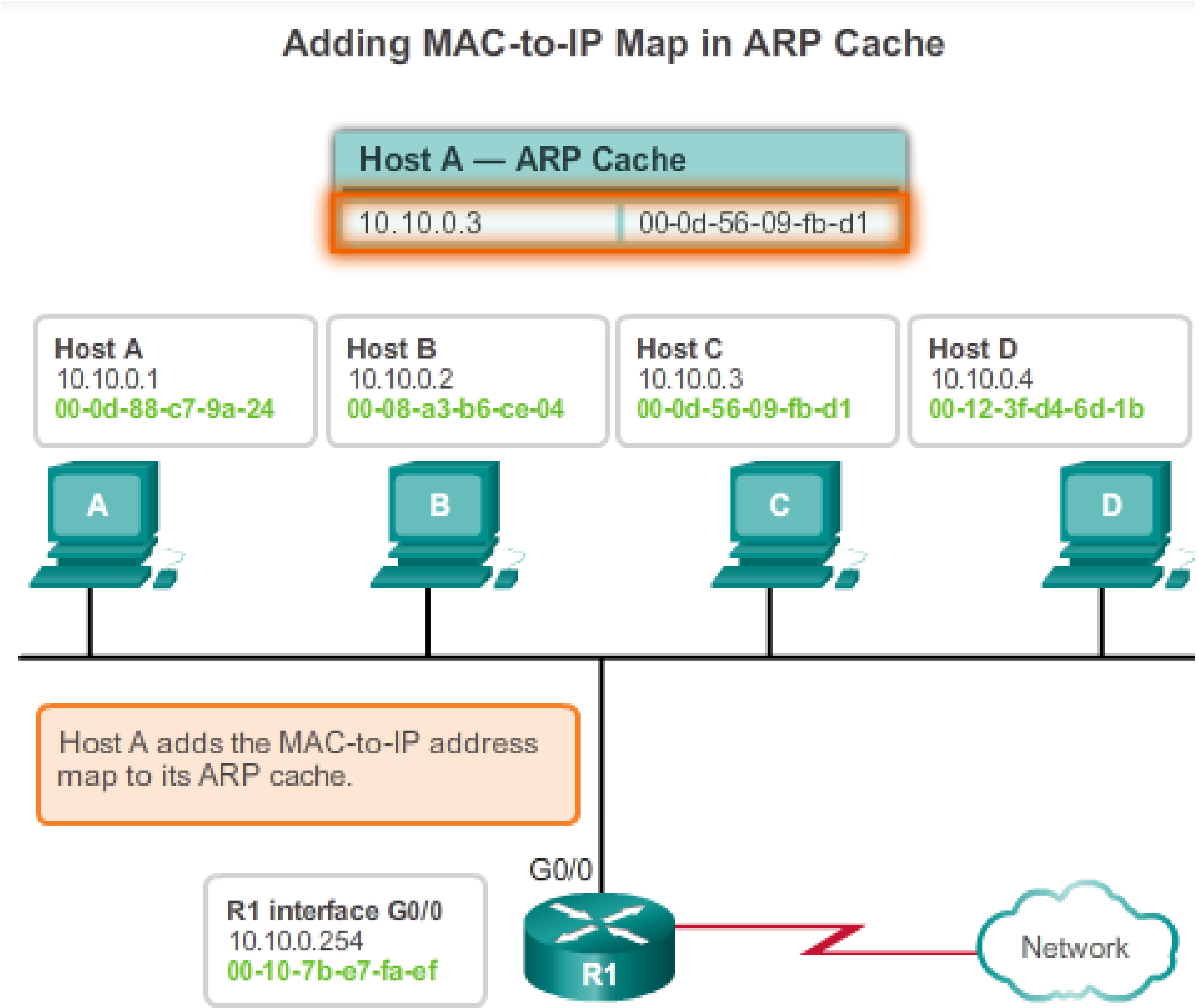
The ARP protocol provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings

5.2.1.2 ARP Functions



5.2.1.3 ARP Operation



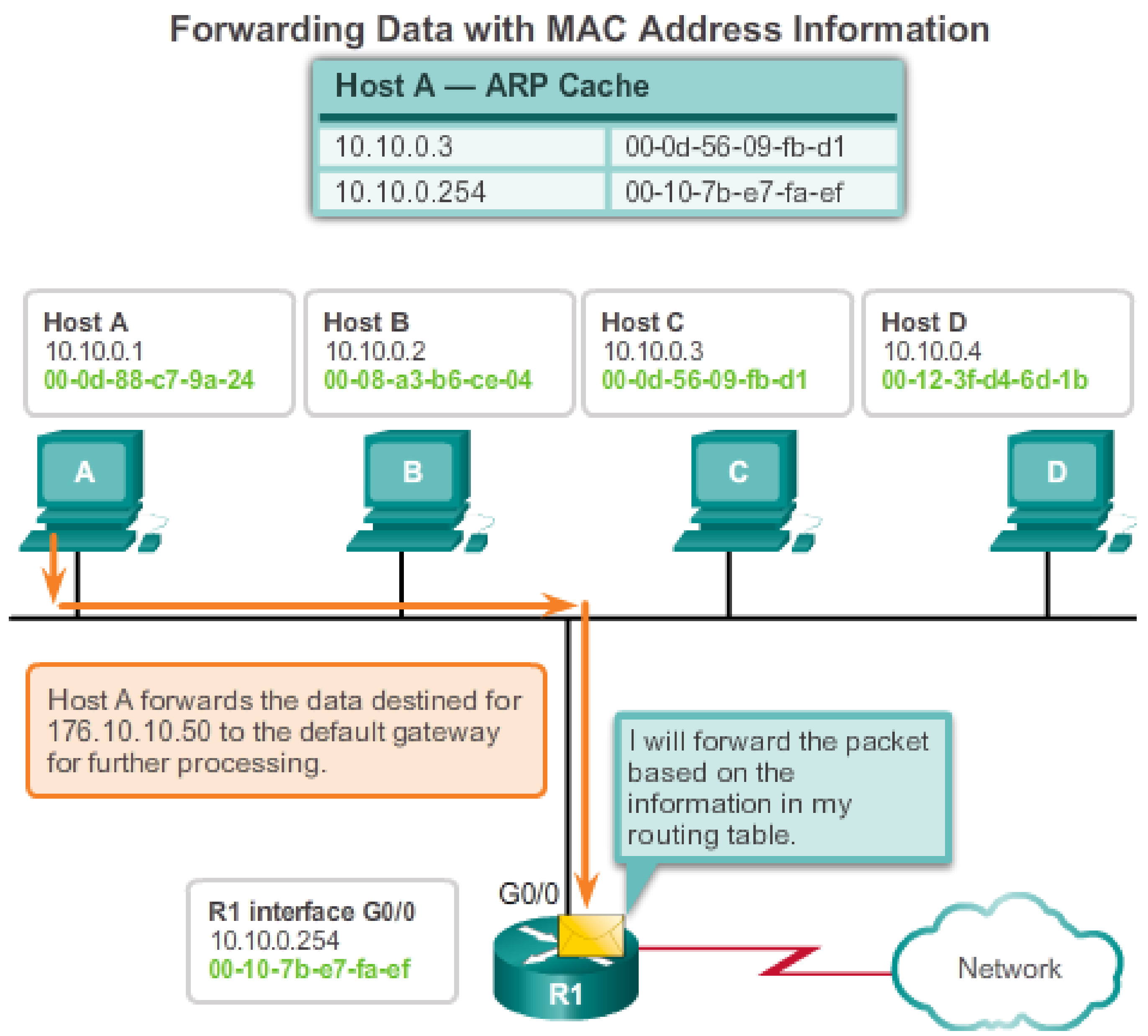
When ARP receives a request to map an IPv4 address to a MAC address, it looks for the cached map in its ARP table.

If an entry is not found, the Layer 2 processes notify ARP that it needs a map.

The ARP processes then send out an ARP request packet to discover the MAC address of the destination device on the local network. If a device receiving the request has the destination IP address, it responds with an ARP reply.

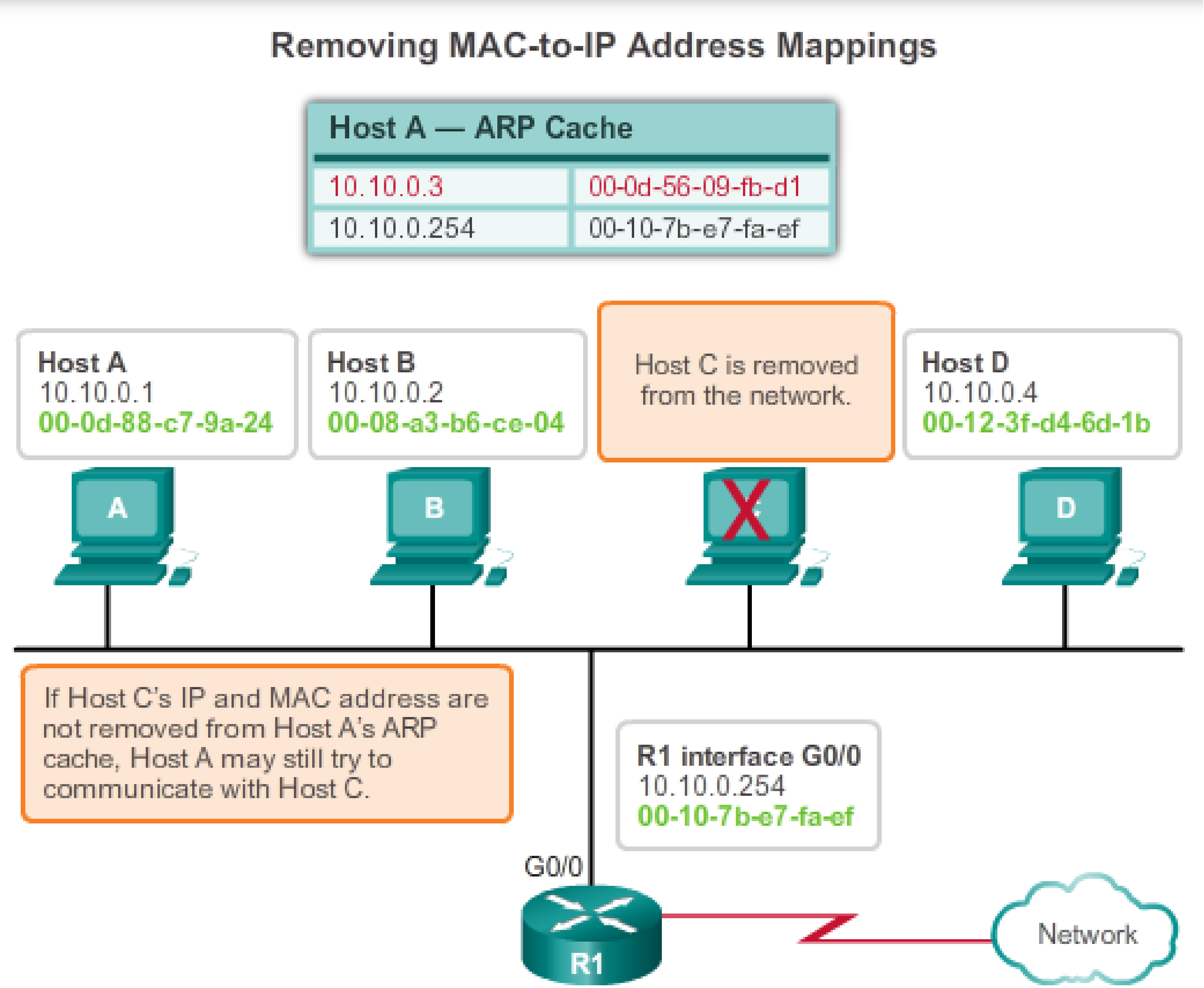
A map is created in the ARP table. Packets for that IPv4 address can now be encapsulated in frames.

5.2.1.4 ARP Role in Remote Communication



If the destination IPv4 host is not on the local network, the source node needs to deliver the frame to the router interface that is the gateway or next hop used to reach that destination. The source node will use the MAC address of the gateway as the destination address for frames containing an IPv4 packet addressed to hosts on other networks.

5.2.1.5 Removing Entries from an ARP Table



Commands may also be used to manually remove all or some of the entries in the ARP table. After an entry has been removed, the process for sending an ARP request and receiving an ARP reply must occur again to enter the map in the ARP table.

5.2.1.6 ARP Tables on Networking Devices

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
```

Host ARP Table
Next

5.2.1.6 ARP Tables on Networking Devices

Host ARP Table

```
C:\>arp -a

Interface: 192.168.1.67 --- 0xa
  Internet Address      Physical Address      Type
  192.168.1.254         64-0f-29-0d-36-91     dynamic
  192.168.1.255         ff-ff-ff-ff-ff-ff     static
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static

Interface: 10.82.253.91 --- 0x10
  Internet Address      Physical Address      Type
  10.82.253.92          64-0f-29-0d-36-91     dynamic
  224.0.0.22            01-00-5e-00-00-16     static
  224.0.0.251           01-00-5e-00-00-fb     static
  224.0.0.252           01-00-5e-00-00-fc     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
```

5.2.1.7 Packet Tracer - Examine the ARP Table

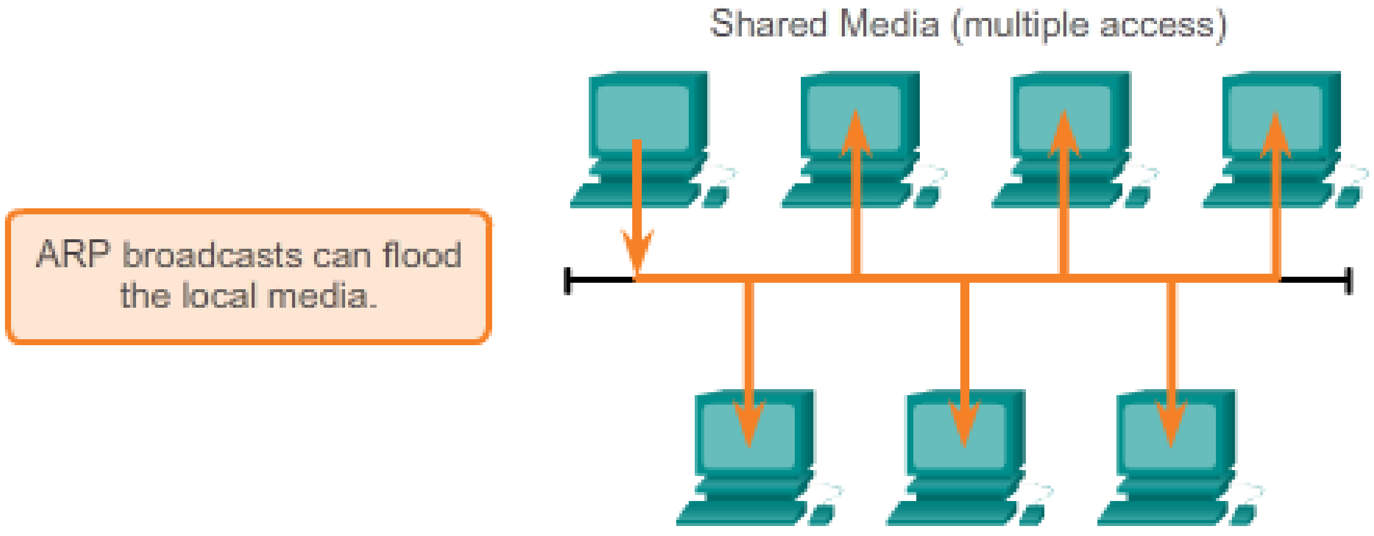
This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

5.2.1.8 Lab - Observing ARP with the Windows CLI, IOS CLI, and Wireshark

In this lab, you will complete the following objectives:

- Part 1: Build and Configure the Network
- Part 2: Use the Windows ARP Command
- Part 3: Use the IOS Show ARP Command
- Part 4: Use Wireshark to Examine ARP Exchanges

5.2.2.1 How ARP Can Create Problems



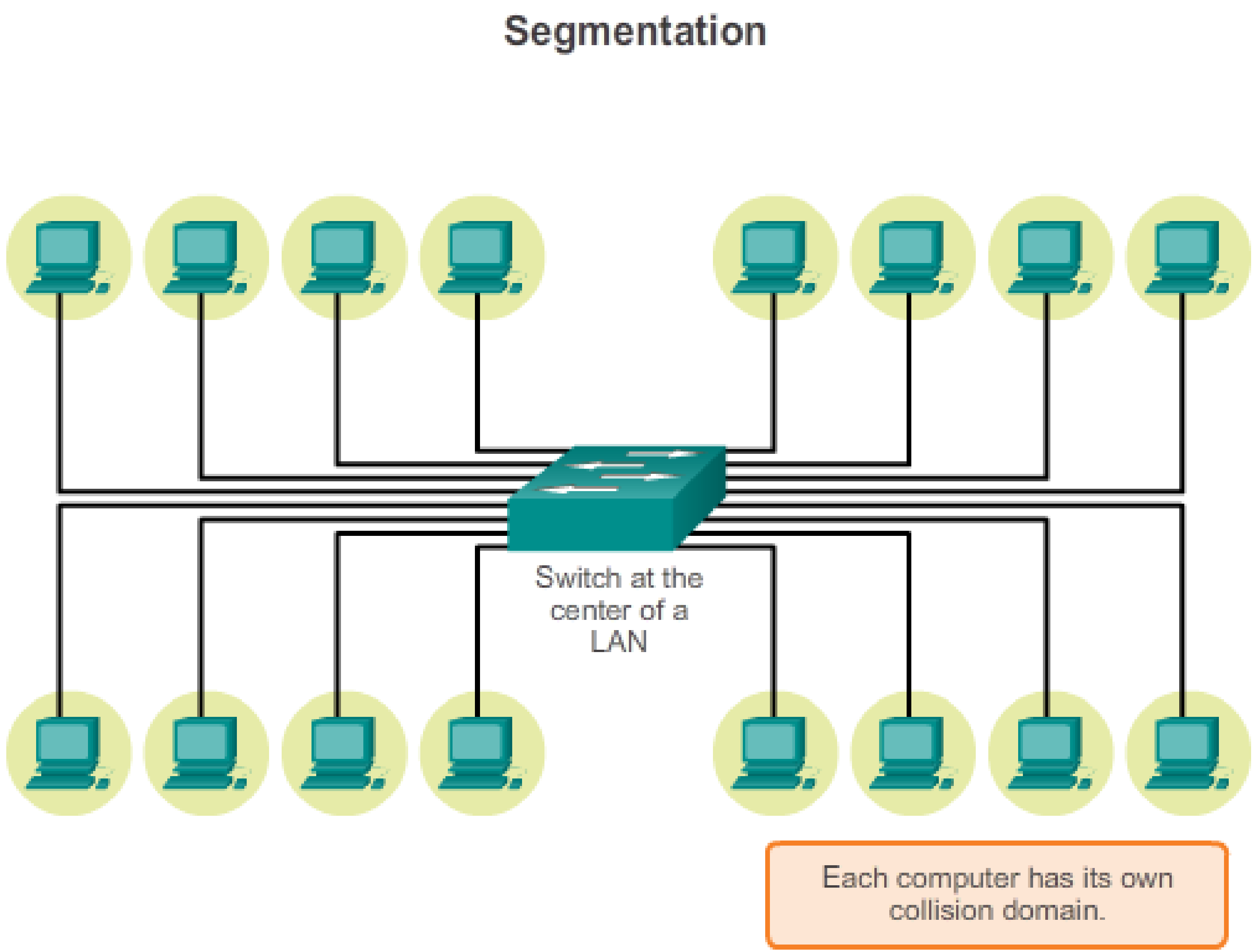
ARP Issues:
- Broadcasts, overhead on the media
- Security

A false ARP message can provide an incorrect MAC address that will then hijack frames using that address (called a spoof).

In some cases, the use of ARP can lead to a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association into a network by issuing fake ARP replies. An attacker forges the MAC address of a device and then frames can be sent to the wrong destination.

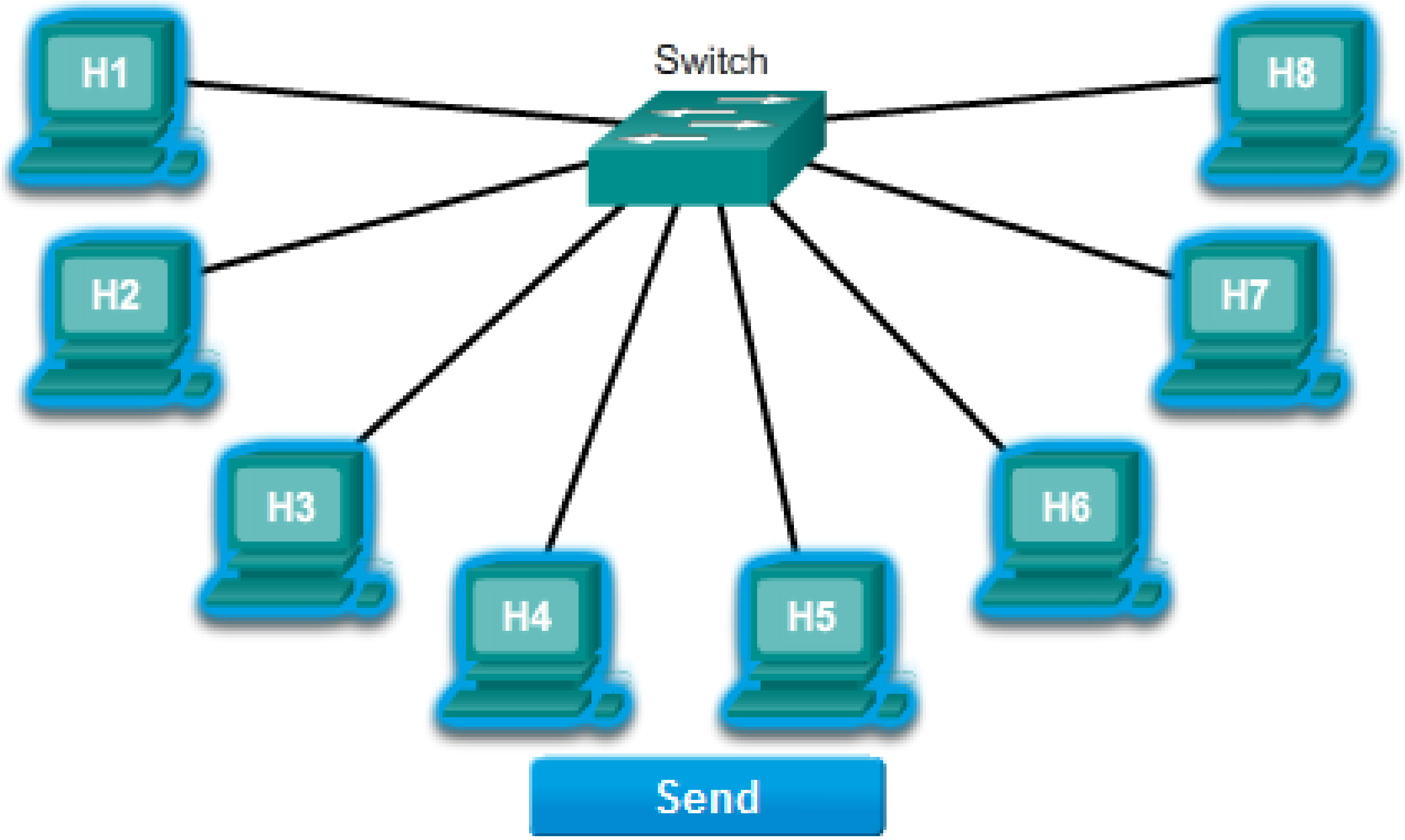
Manually configuring static ARP associations is one way to prevent ARP spoofing. Authorized MAC addresses can be configured on some network devices to restrict network access to only those devices listed.

5.2.2.2 Mitigating ARP Problems



Switches provide segmentation of a LAN, dividing the LAN into independent collision domains. Each port on a switch represents a separate collision domain and provides the full media bandwidth to the node or nodes connected on that port.

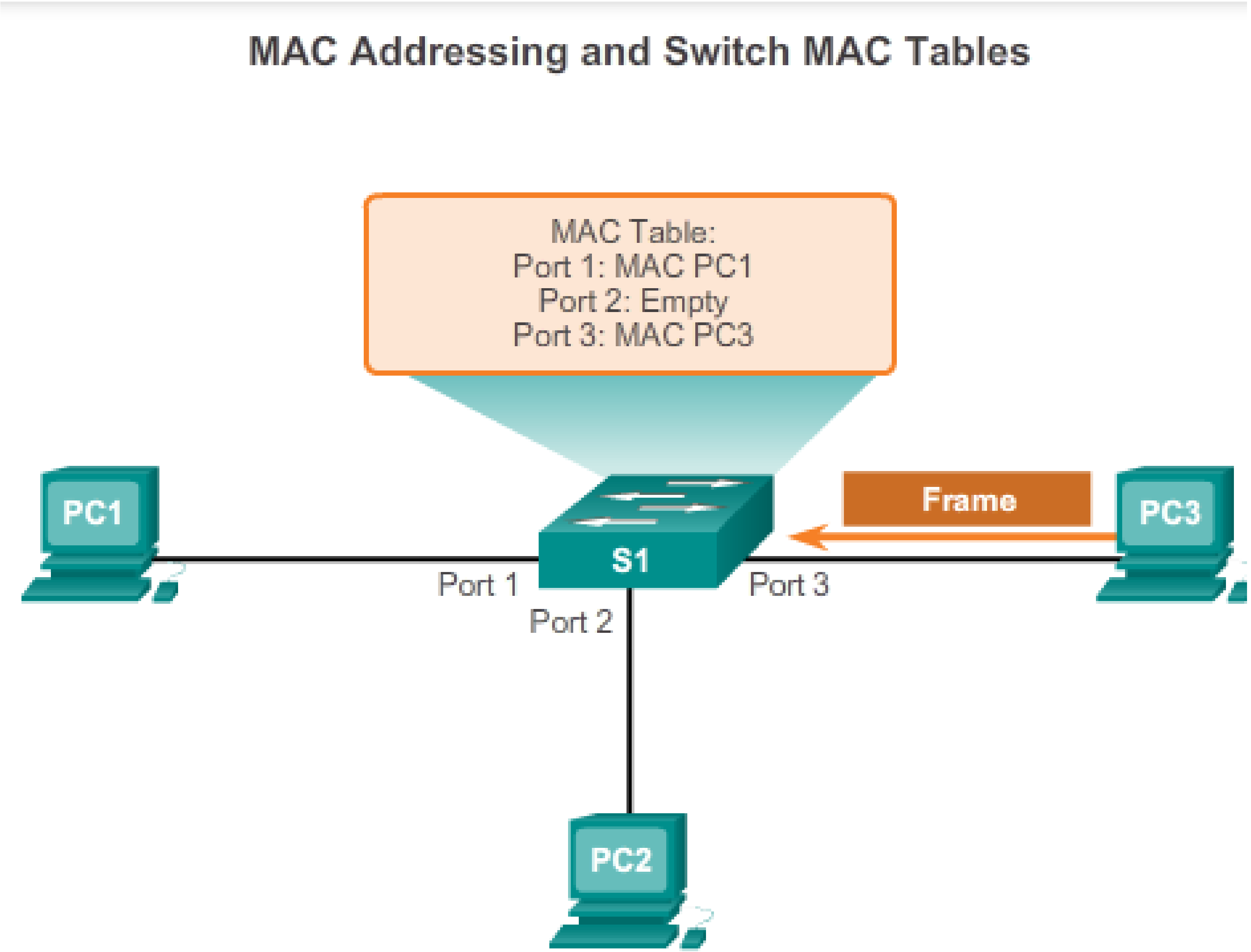
5.3.1.1 Switch Port Fundamentals



Click a source host and a destination host, then click **Send** to see how switches deliver messages.

A Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address. A switch is completely transparent to network protocols and user applications. 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.

5.3.1.2 Switch MAC Address Table

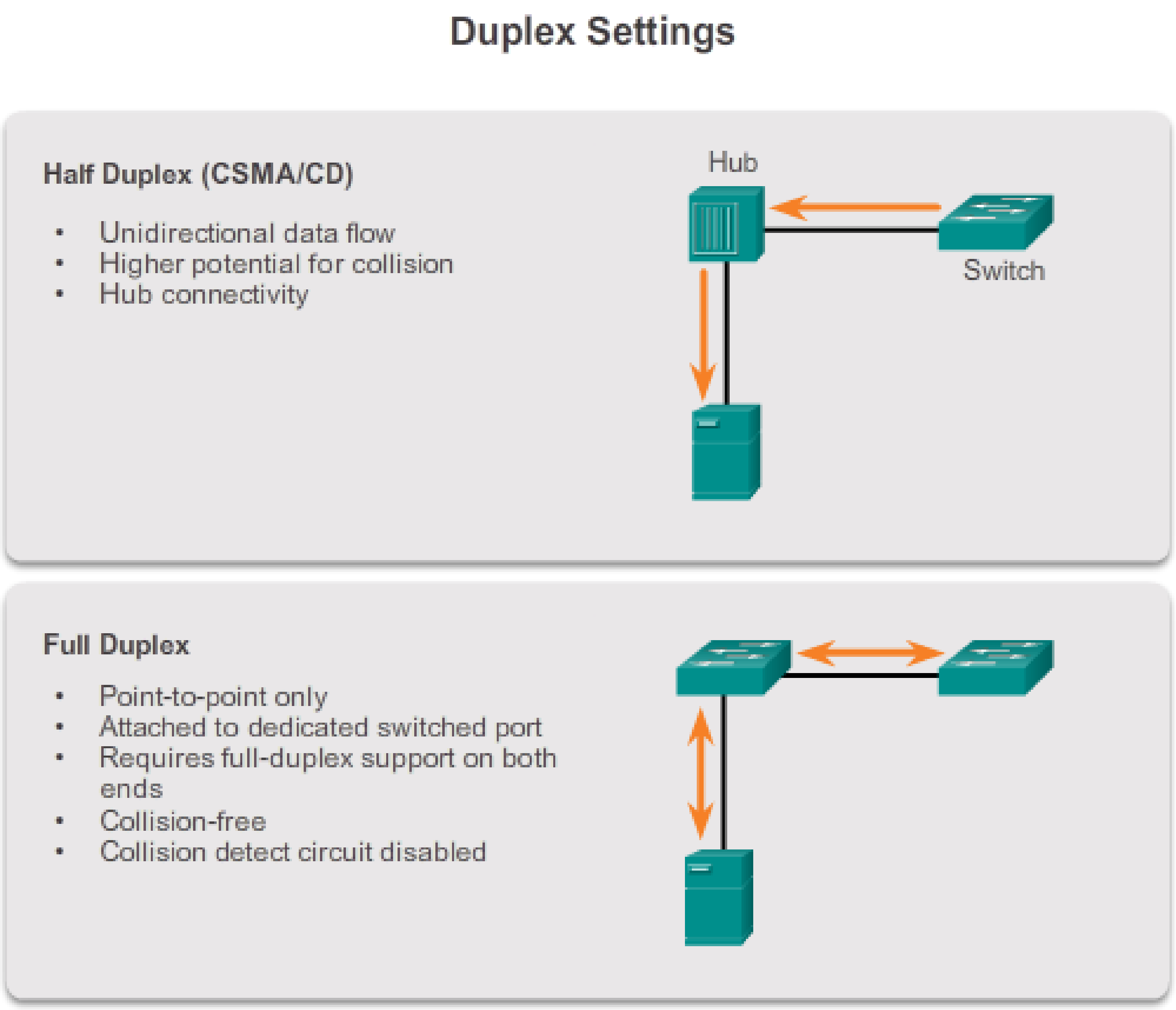


Switches use MAC addresses to direct network communications through their switch fabric to the appropriate port toward the destination node.

The switch fabric is the integrated circuits and the accompanying machine programming that allows the data paths through the switch to be controlled.

For a switch to know which port to use to transmit a unicast frame, it must first learn which nodes exist on each of its ports.

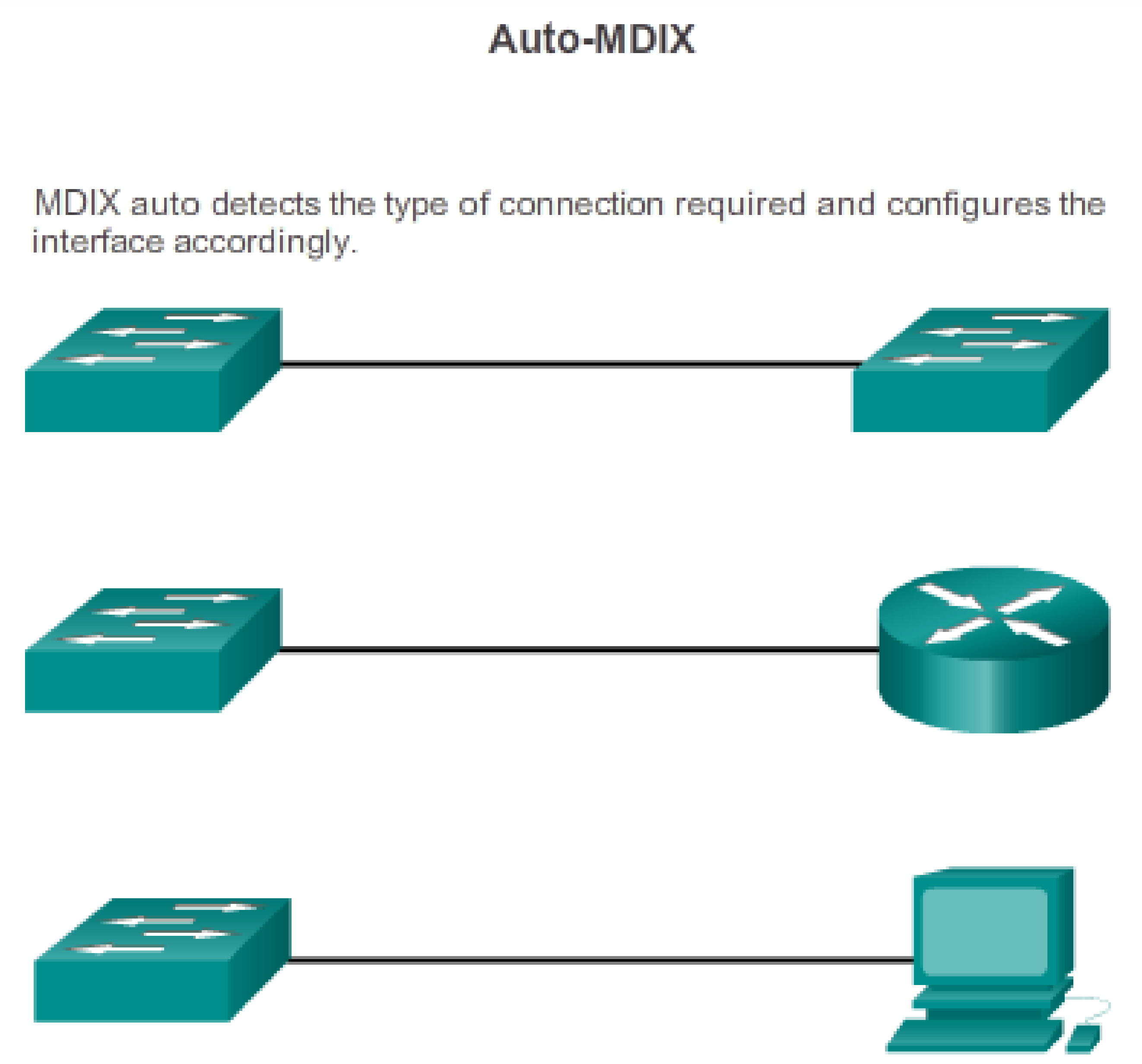
5.3.1.3 Duplex Settings



Half-duplex communication relies on unidirectional data flow where sending and receiving data are not performed at the same time.

In full-duplex communication, data flow is bidirectional, so data can be sent and received at the same time. The bidirectional support enhances performance by reducing the wait time between transmissions. Most Ethernet, Fast Ethernet, and Gigabit Ethernet NICs sold today offer full-duplex capability. In full-duplex mode, the collision detect circuit is disabled.

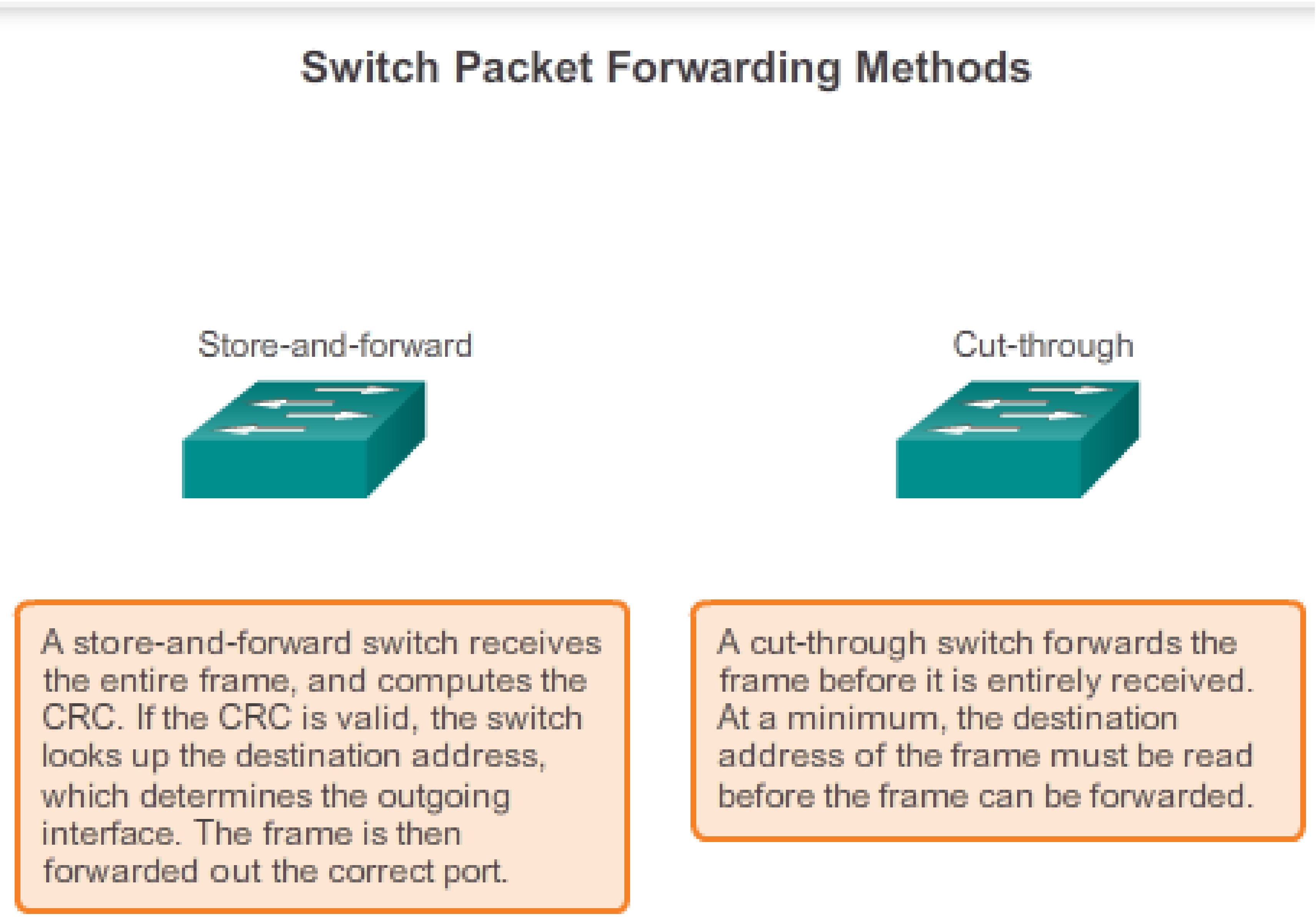
5.3.1.4 Auto-MDIX



Switch detects the required cable type for copper Ethernet connections 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.

The auto-MDIX feature is enabled by default on switches running Cisco IOS Release 12.2(18)SE or later. For releases between Cisco IOS Release 12.1(14)EA1 and 12.2(18)SE, the auto-MDIX feature is disabled by default.

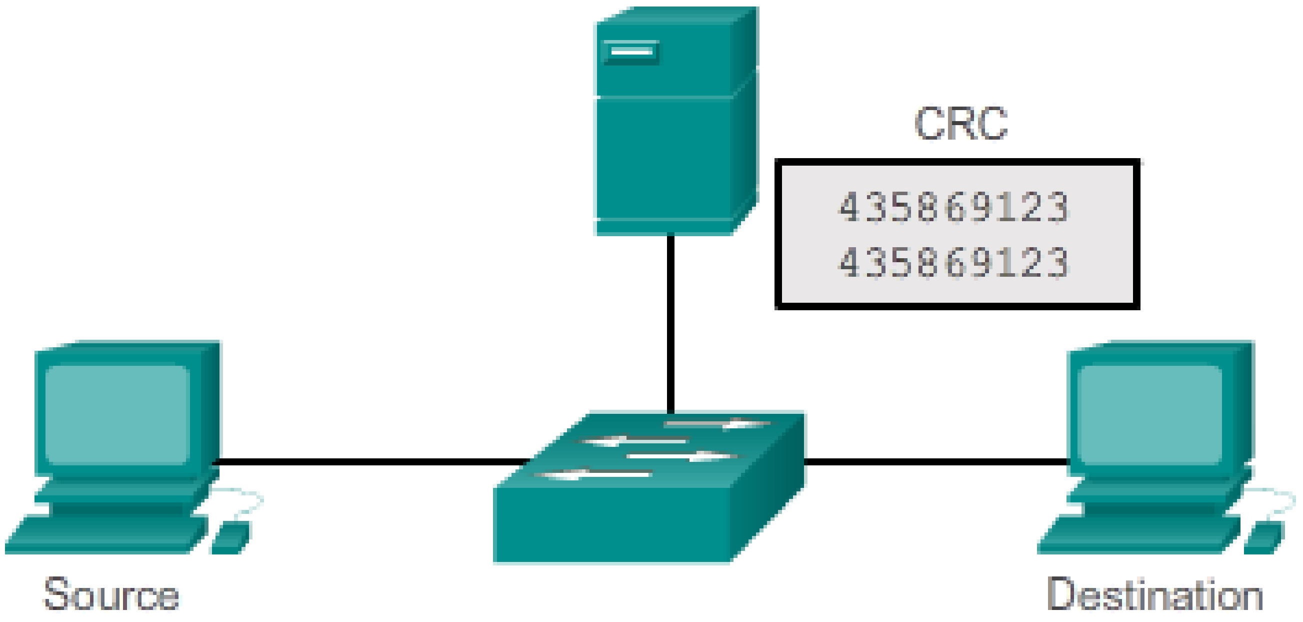
5.3.1.5 Frame Forwarding Methods on Cisco Switches



In store-and-forward switching, when the switch receives the frame, it stores the data in buffers until the complete frame has been received. During the storage process, the switch analyzes the frame for information about its destination. In this process, the switch also performs an error check using the Cyclic Redundancy Check (CRC) trailer portion of the Ethernet frame.

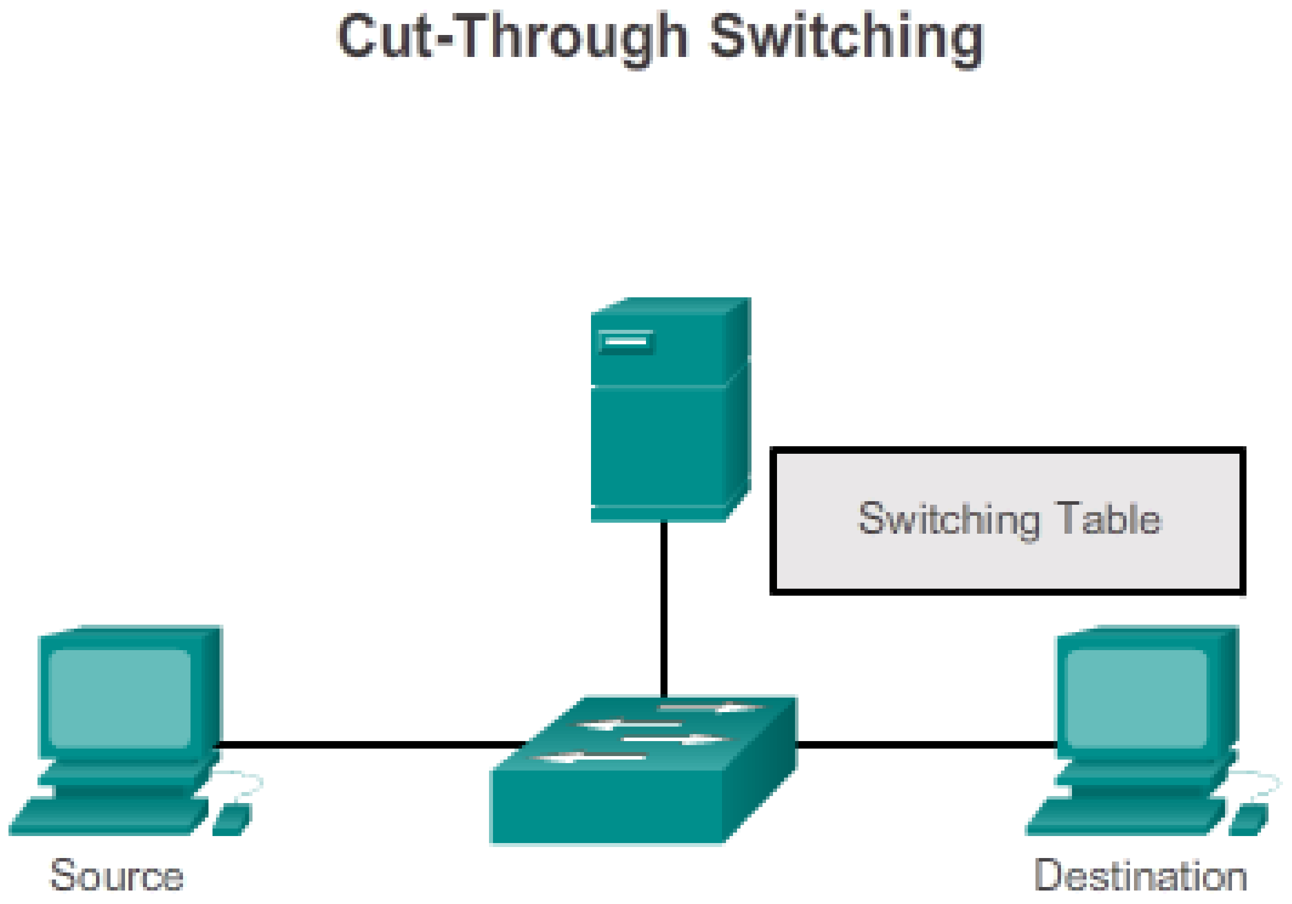
5.3.1.5 Frame Forwarding Methods on Cisco Switches

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.

5.3.1.6 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.

In cut-through switching, the switch acts upon the data as soon as it is received, even if the transmission is not complete. 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 destination MAC address is located in the first 6 bytes of the frame following the preamble

5.3.1.6 Cut-Through Switching

Fast-forward switching:

- offers the lowest level of latency.
- immediately forwards a packet after reading the destination address.
- there may be times when packets are relayed with errors.
- This occurs infrequently, and the destination network adapter discards the faulty packet upon receipt.
- latency is measured from the first bit received to the first bit transmitted.

Fragment-free switching:

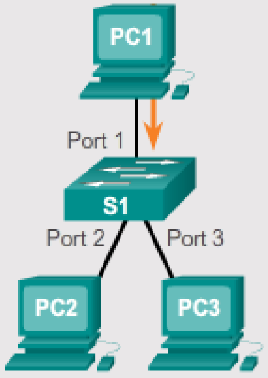
- switch stores the first 64 bytes of the frame before forwarding.
- compromise between store-and-forward switching and fast-forward switching.
- most network errors and collisions occur during the first 64 bytes.
- error check on the first 64 bytes of the frame to ensure that a collision has not occurred
- Fragment-free switching is a compromise between the high latency and high integrity of store-and-forward switching, and the low latency and reduced integrity of fast-forward switching.

5.3.1.7 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.		

Activity
Read the scenario based on the topology shown. Identify how the frames will be processed by dragging your answers to the appropriate fields provided in the table. All answers will not be used.

✓ Straight-through	Cabling used in this topology will be ____.
✓ Broadcast	To find where PC2 is located, PC1 will send out a ____ data frame.
✓ Unicast	PC2 will respond back to PC1 by sending back a ____ message.
✓ Discard it	If PC2 receives only half of the data in the frame, it will ____.
✓ Store-and-forward	If PC2 receives many damaged frames on Port 2, S1 likely will change back to ____ switching.



- S1 is a brand new switch. PC1 is sending data to PC2.
- S1 is using full-duplex, MDIX, and fast-forward as a frame switching method.

5.3.1.8 Memory Buffering on Switches

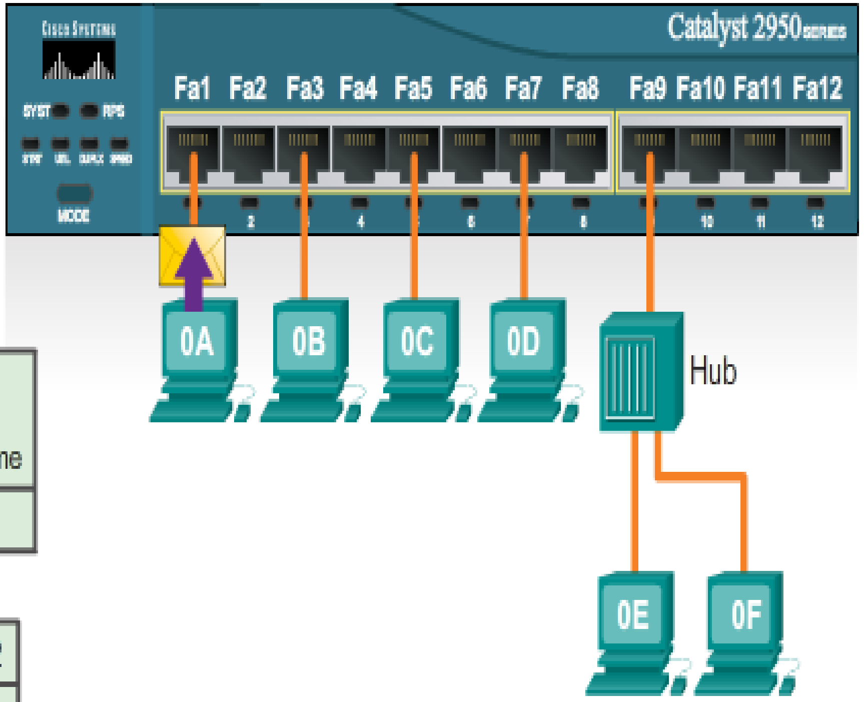
Port-Based and Shared Memory Buffering

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.

As discussed, a switch analyzes some or all of a packet before it forwards it to the destination host. 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.

5.3.1.9 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
	0C	0A			

MAC Table

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

Question 1 - Where will the switch forward the frame?

☐ Fa1 ☐ Fa2 ☐ Fa3 ☐ Fa4 ☐ Fa5 ☐ Fa6 ☐ Fa7 ☐ Fa8 ☐ 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.
☐ 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

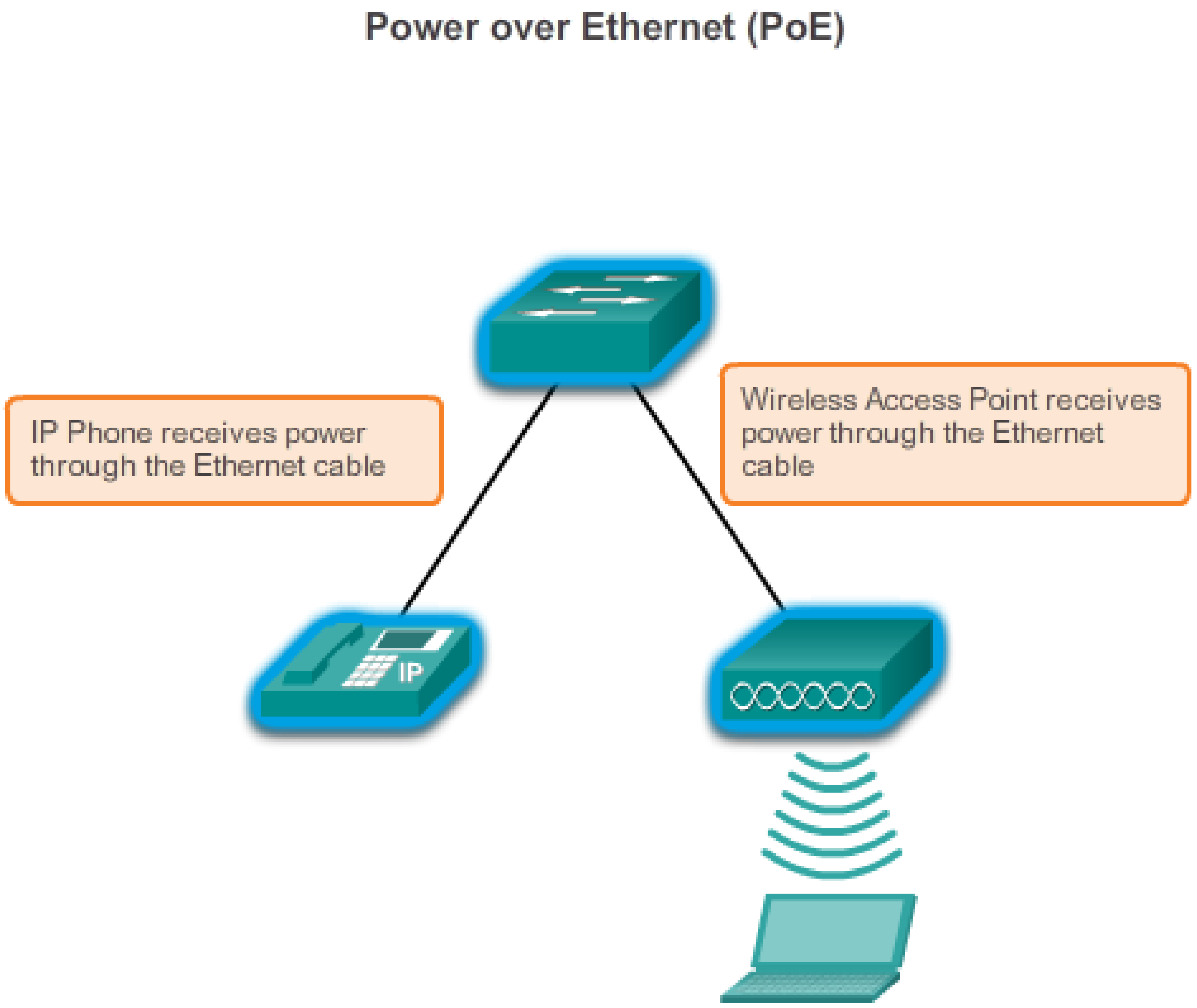
New Problem

5.3.1.10 Lab - Viewing 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

5.3.2.1 Fixed versus Modular Configuration



Fixed configuration switches are fixed in their configuration. What that means is that you cannot add features or options to the switch beyond those that originally came with the switch. The particular model you purchase determines the features and options available.

Modular switches offer more flexibility in their configuration. Modular switches typically come with different sized chassis that allow for the installation of different numbers of modular line cards. The line cards actually contain the ports.

5.3.2.1 Fixed versus Modular Configuration

Switch Form Factors

Fixed Configuration Switches
Features and options are limited to those that originally come with the switch.

Modular Configuration Switches
The chassis accepts line cards that contain the ports.

Stackable Configuration Switches
Stackable switches, connected by a special cable, effectively operate as one large switch.

5.3.2.2 Module Options for Cisco Switch Slots

SFP Modules

Cisco Optical Gigabit Ethernet SFP

Cisco 1000BASE-T Copper SFP

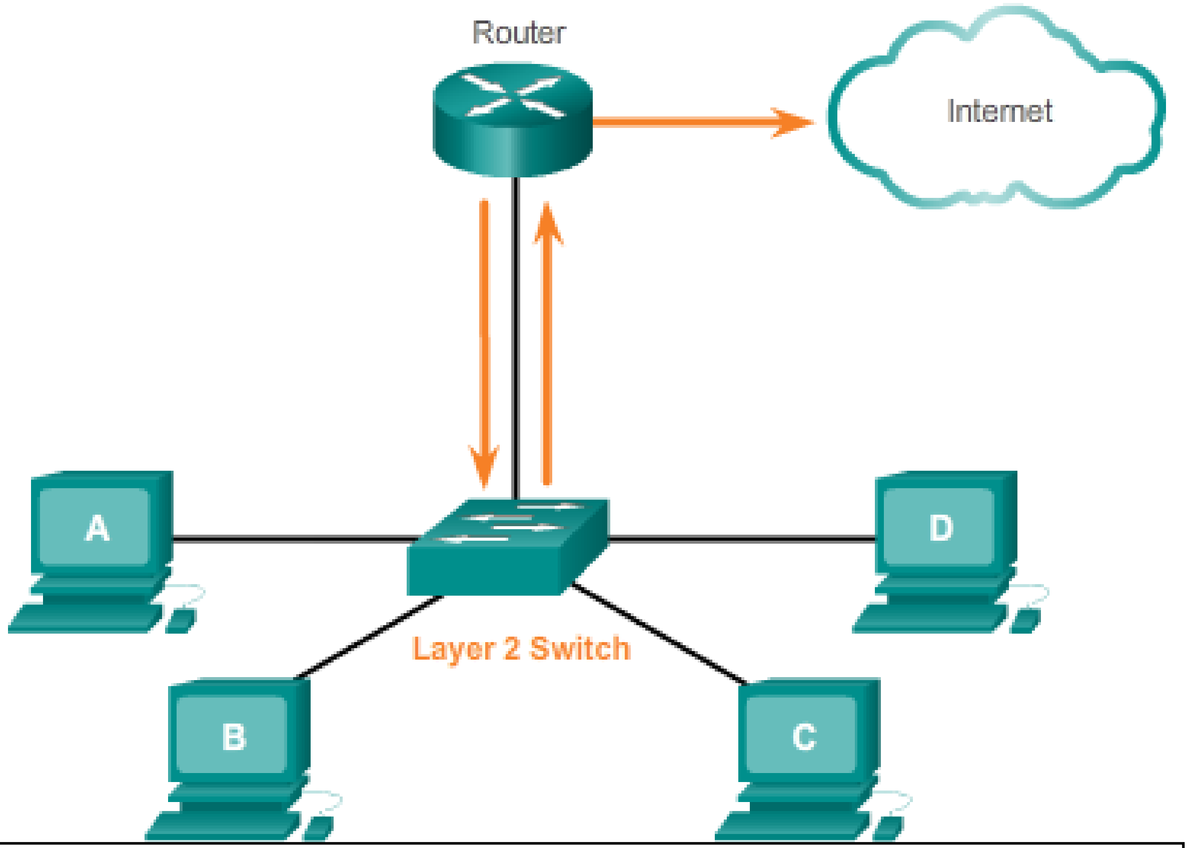
Cisco 2-channel 1000BASE-BX
Optical SFP

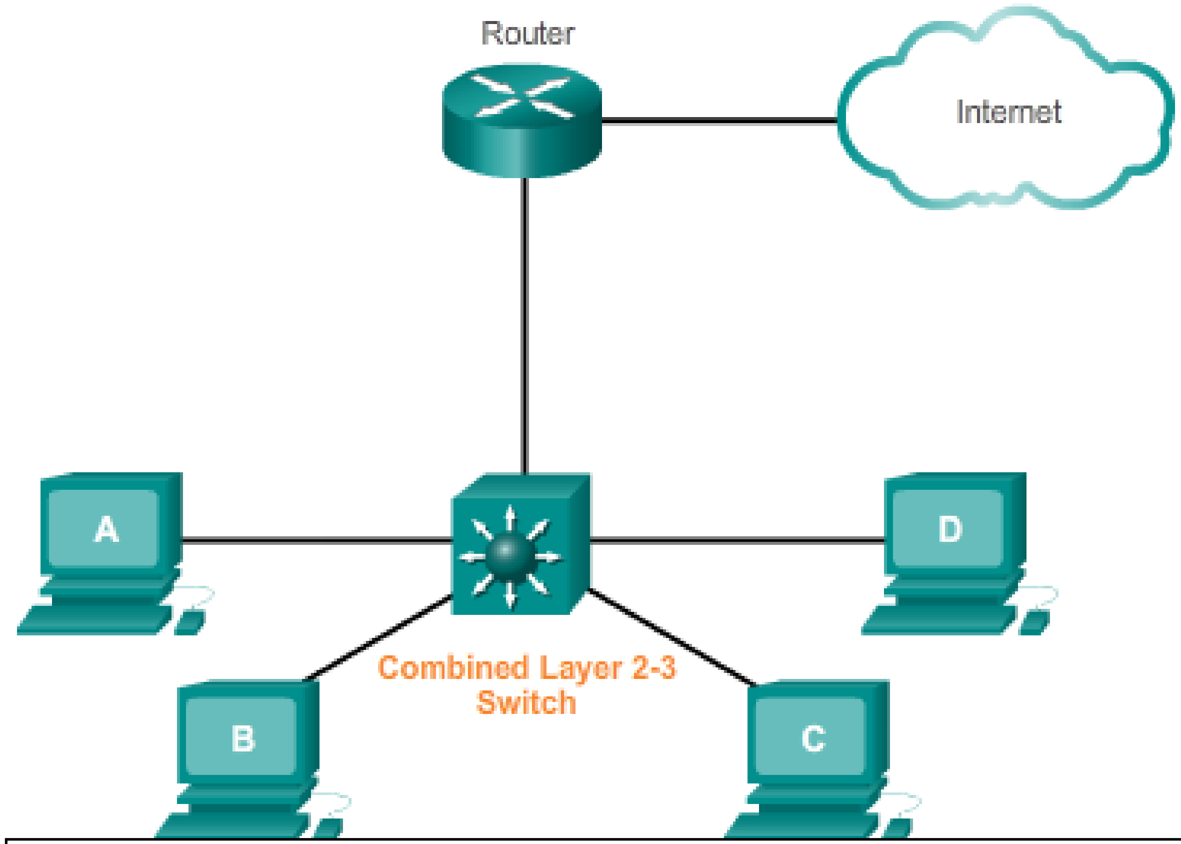
Fast Ethernet SFP Modules –

Gigabit Ethernet SFP Modules –

10 Gigabit Ethernet SFP Modules –

5.3.3.1 Layer 2 versus Layer 3 Switching

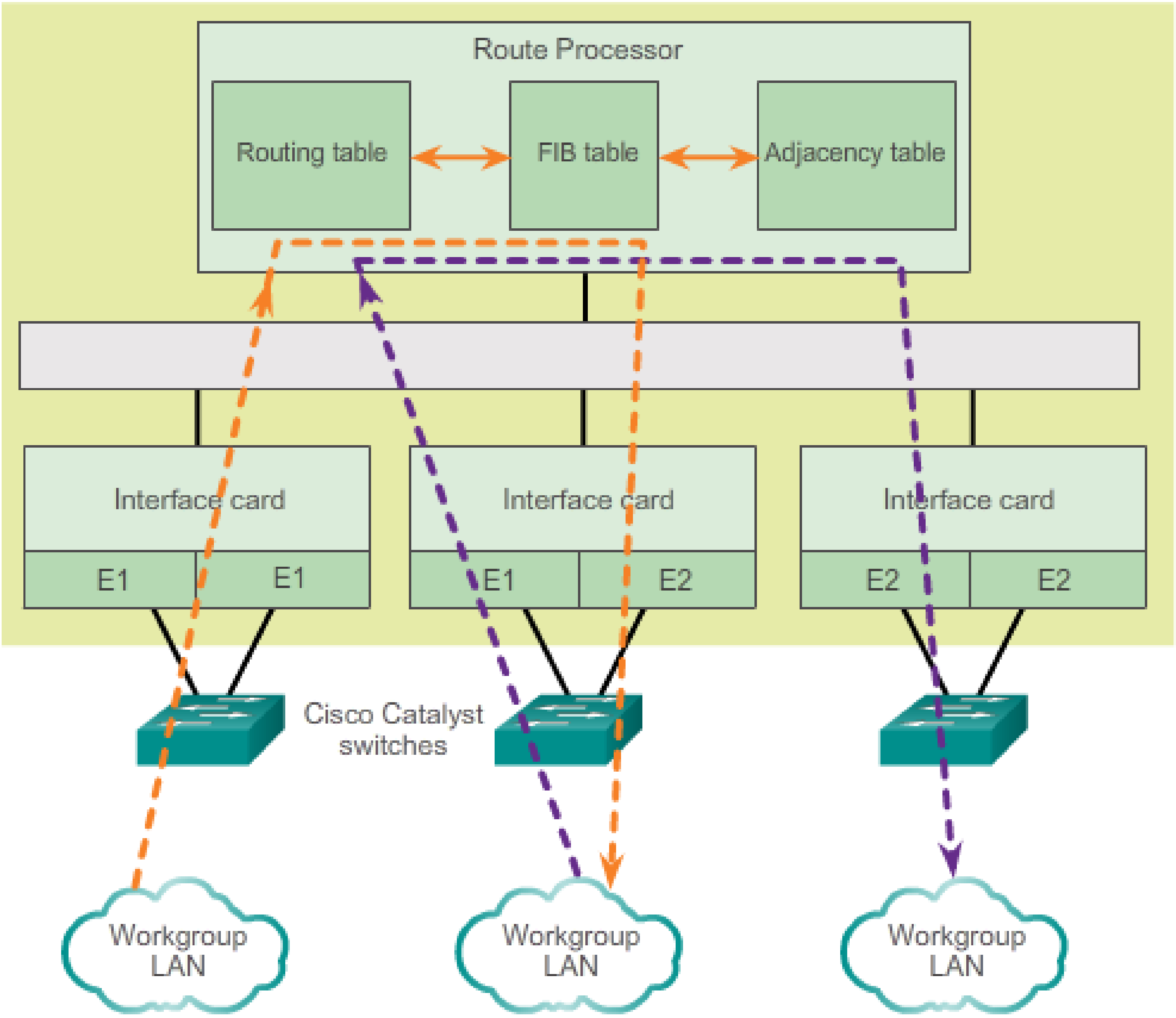




Layer 2 LAN switch performs switching and filtering based only on the OSI data link layer (Layer 2) MAC address and depends upon routers to pass data between independent IP subnetworks

a Layer 3 switch can also learn which IP addresses are associated with its interfaces. This allows the Layer 3 switch to direct traffic throughout the network based on IP address information as well.

5.3.3.2 Cisco Express Forwarding



Cisco Express Forwarding (CEF)

CEF decouples the usual strict interdependence between Layer 2 and Layer 3 decision

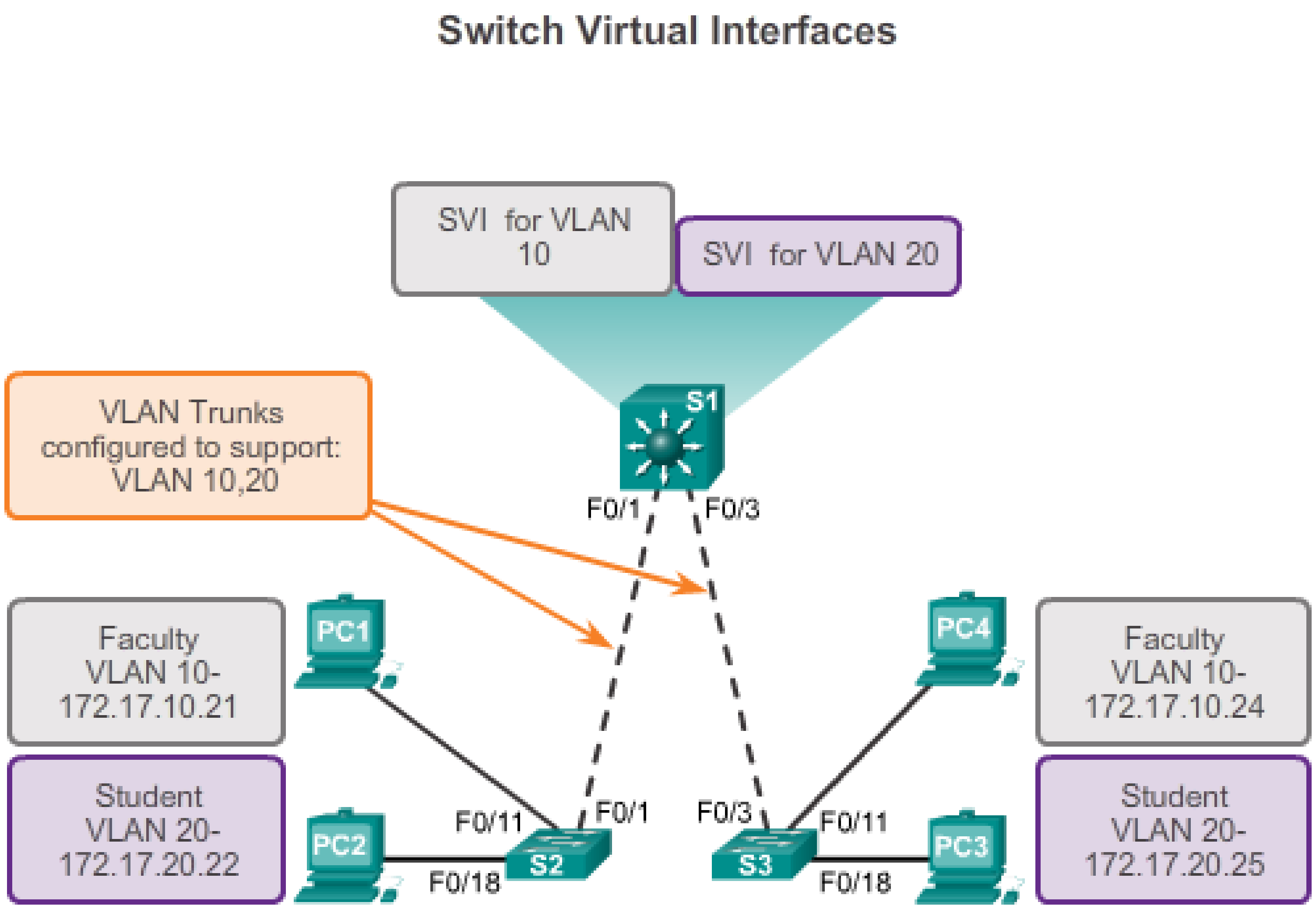
Forwarding IP packets can be slow

- the constant referencing back-and-forth between Layer 2 and Layer 3 constructs

The two main components of CEF operation Forwarding Information

- Base (FIB)
- Adjacency tables

5.3.3.3 Types of Layer 3 Interfaces



Cisco networking devices support a number of distinct types of Layer 3 interfaces. A Layer 3 interface is one that supports forwarding IP packets toward a final destination based on the IP address.

The major types of Layer 3 interfaces are:

- Switch Virtual Interface (SVI) - Logical interface on a switch associated with a virtual local area network (VLAN).
- Routed Port - Physical port on a Layer 3 switch configured to act as a router port.
- Layer 3 EtherChannel - Logical interface on a Cisco device associated with a bundle of routed ports.

5.3.3.4 Configuring a Routed Port on a Layer 3 Switch

Routed Port Configuration

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar  1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief
Interface         IP-Address     OK? Method Status                Protocol
Vlan1             unassigned     YES unset  administratively down down
FastEthernet0/1   unassigned     YES unset  down                  down
FastEthernet0/2   unassigned     YES unset  down                  down
FastEthernet0/3   unassigned     YES unset  down                  down
FastEthernet0/4   unassigned     YES unset  down                  down
FastEthernet0/5   unassigned     YES unset  down                  down
FastEthernet0/6   192.168.200.1  YES manual up                    up
FastEthernet0/7   unassigned     YES unset  up                    up
FastEthernet0/8   unassigned     YES unset  up                    up
<output omitted>
```

A switch port can be configured to be a Layer 3 routed port and behave like a regular router interface.

Specifically, a routed port:

- Is not associated with a particular VLAN.
- Can be configured with a Layer 3 routing protocol.
- Is a Layer 3 interface only and does not support Layer 2 protocol.

Configure routed ports by putting the interface into Layer 3 mode with the no switchport interface configuration command. Then assign an IP address to the port. That's it!

5.3.3.5 Packet Tracer - Configure Layer 3 Switches

Configure Layer 3 Switches

The Network Administrator is replacing the current router and switch with a new Layer 3 switch. As the Network Technician, it is your job to configure the switch and place it into service. You will be working after hours to minimize disruption to the business.

5.4.1.1 Activity - MAC and Choose…

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

Please view the video located at the following link:

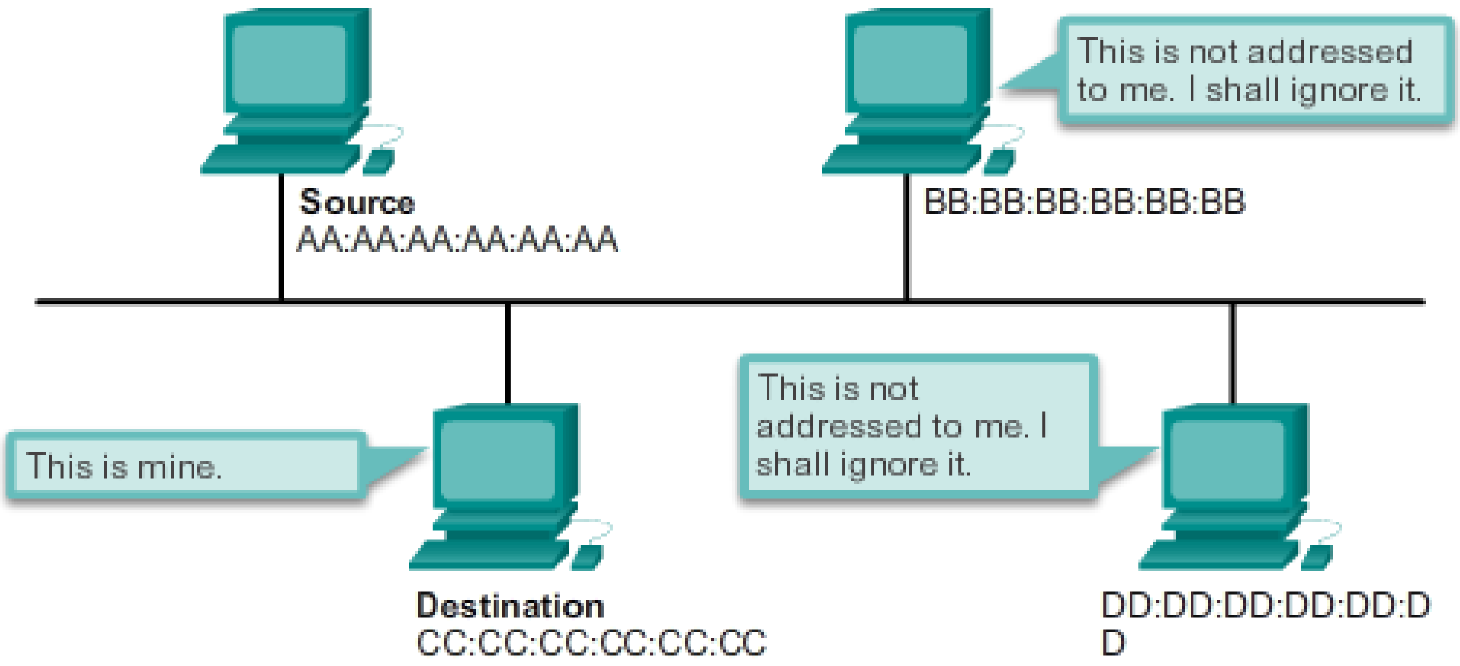
http://www.netevents.tv/video/bob-metcalfe-the-history-of-ethernet

Topics discussed include not only where we have come from in Ethernet development, but where we are going with Ethernet technology (a futuristic approach).

5.4.1.2 Summary

Frame Forwarding

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



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

Thanks

Thanks for your attention!!