PXL IT

CISCO CCNA1

CCNA Routing and Switching: Introduction to Networks

HOOFDSTUK 5

Ethernet

DE HOGESCHOOL MET HET NETWERK

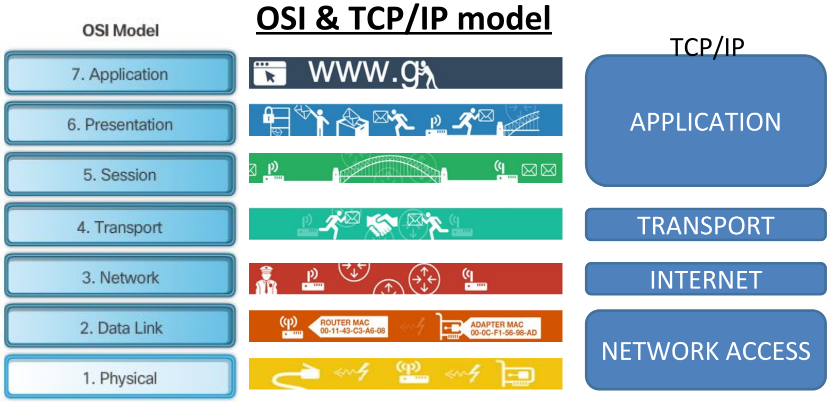
Hogeschool PXL – Elfde-Liniestraat 24 – B-3500 Hasselt
www.pxl.be - www.pxl.be/facebook

CCNA1 - Overzicht

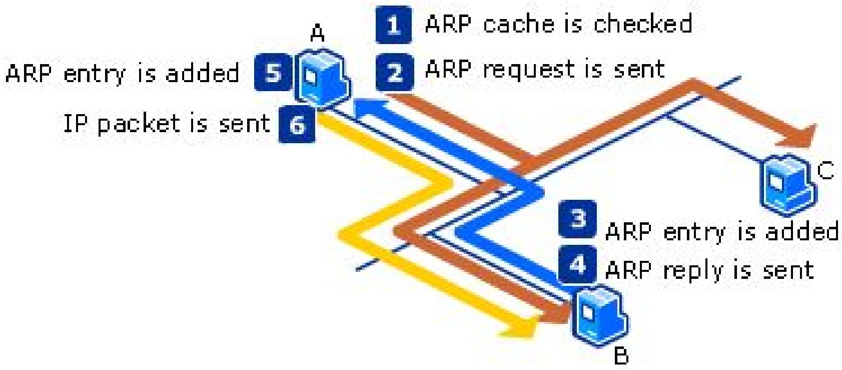
- OSI model en de belangrijkste (LAN) protocollen.
- Data Flow in een LAN
  (verklaring volgens het OSI model).
- IP en subnetting.
- Het toepassen en onderzoeken van bovenstaande 3 in Packettrace oefeningen.

CCNA1 - Overzicht

1. OSI model en de belangrijkste (LAN) protocollen.



2. Data Flow in een LAN   (verklaring volgens het OSI model)



3. IP en subnetting

Situering hoofdstuk 5

Chapter 5 behandelt het ethernet protocol, het MAC adres, de switch, ARP en de default gateway. Dit zijn belangrijke principes voor het begrijpen van de dataflow in een LAN.
Allereerst wordt het ethernetframe besproken, daarna het MAC adres (5.1).
Het MAC adres (=data link adres = fysiek adres = burned in address) wordt gebruikt voor data verkeer in een lokaal netwerk. Switches sturen frames door op basis van het data link adres! ARP wordt gebruikt voor het vinden van MAC adressen (via een IP adres) en de gateway wordt gebruikt voor communicatie buiten het netwerk. Al deze begrippen vormen de basis van 'dataflow in een netwerk'. In dit hoofdstuk wordt deze dataflow stap voor stap doorlopen.

Doelstellingen:

- Kent het Ethernet frame (PDU velden). 5.1.1.6
- Weet wat een MAC adres is en hoe het gebruikt wordt. (5.1.2)
- Mac unicast, -mulitcast, -broadcast (5.1.2)
- Werking van een switch (5.2.1.6).
- CLI commando's m.b.t. mac-address-table (show/clear).
- ARP (packet trace oefening!)
- Dataflow "same network vs remote network"
- Verklaar de gebruikte protocollen (ARP, ICMP)
- Verklaar op elk punt de PDU (gebruikt IP, MAC)
- Packettrace oefeningen!!
- Wat is een default gateway!
- DATA FLOW in een LAN !!

Activity & PT

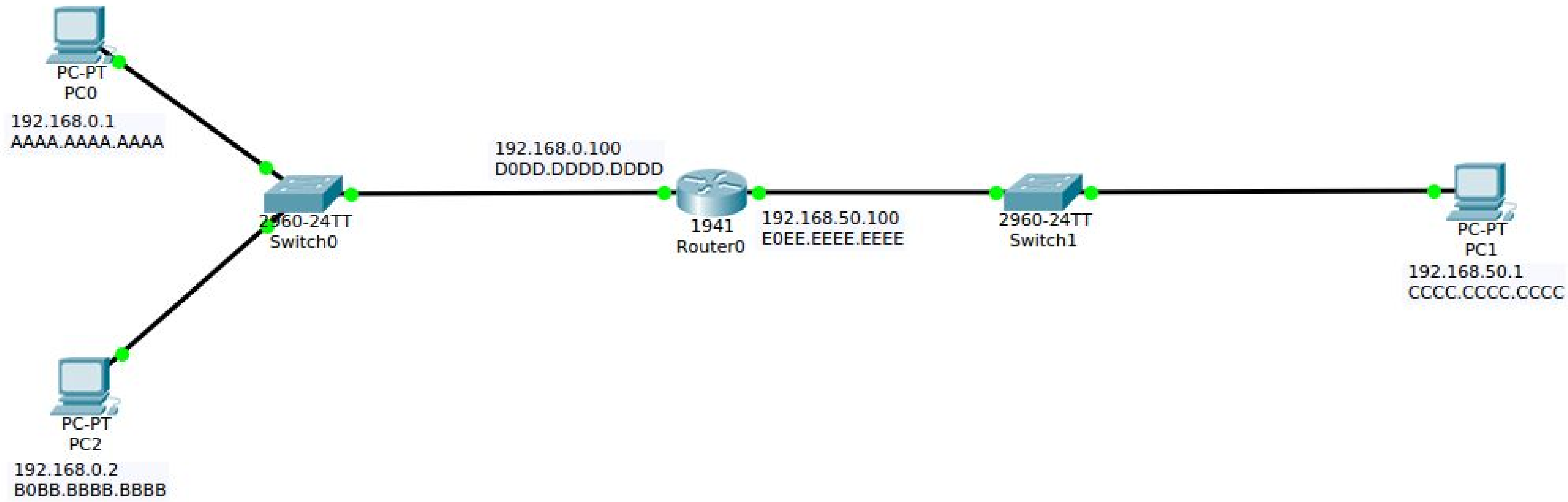
- 5.1.1.6 Ethernet Frame Fields
- 5.2.1.6 Switch it
- PT 5.3.1.3 PT Identify MAC and IP addresses
- PT 5.3.2.8 Examine the ARP table
- Zie ook dataflowoefening.

Zie leerpad op blackboard!

Leertip:

Belangrijk in dit hoofdstuk is de data flow oefening, activity 5.2.1.6 (Switch it) en de PT 5.3.2.8 (begrijpen van ARP).

Inleidende PT oefening



Cisco Networking Academy
Mind Wide Open

Chapter 5: Ethernet

Introduction to Networks v5.1

Chapter Outline

5.0 Introduction

5.1 Ethernet Protocol

5.2 LAN Switches

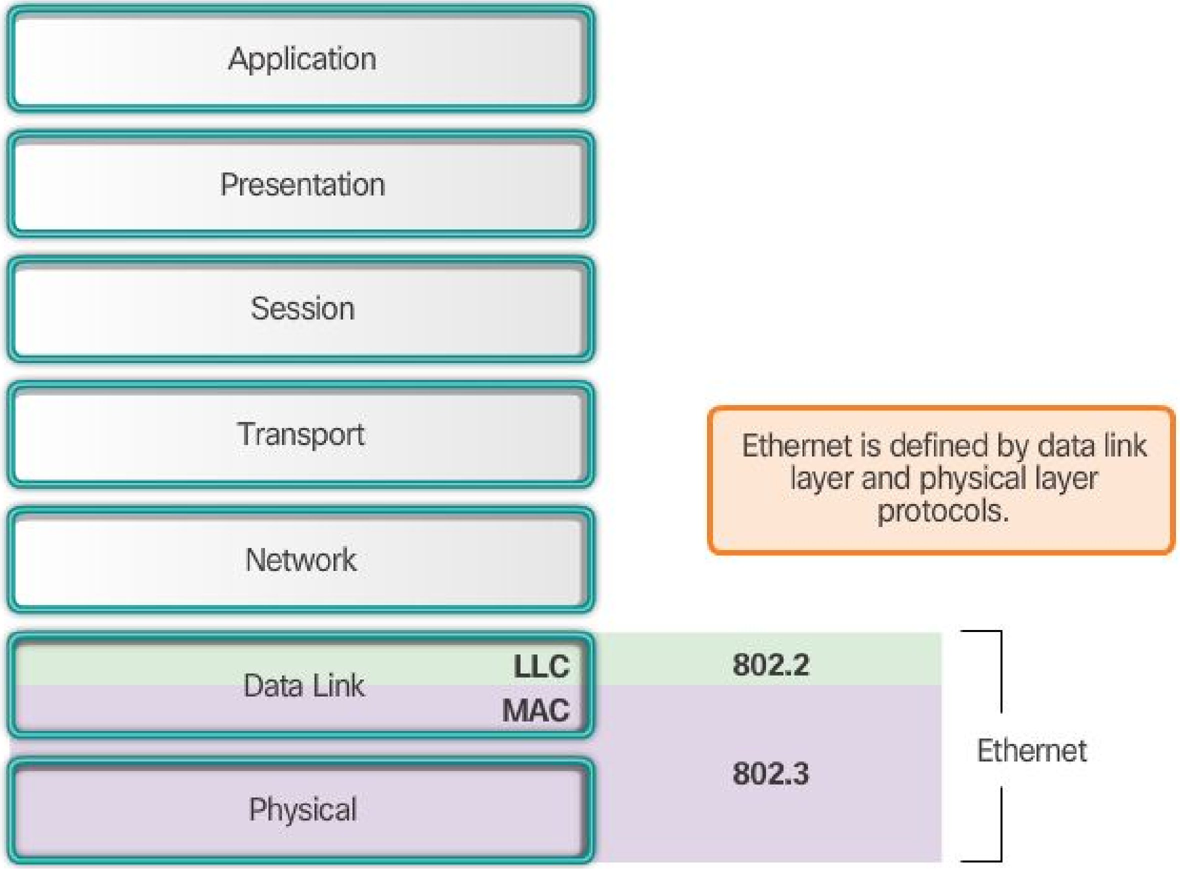
5.3 Address Resolution Protocol

5.4 Summary

Section 5.1: Ethernet Protocol

- 5.1.1: Ethernet Frame
- 5.1.2: Ethernet MAC Address

5.1.1: Ethernet Frame
5.1.1.1 Ethernet Encapsulation



5.1.1.1 Ethernet Encapsulation (cont.)

Ethernet

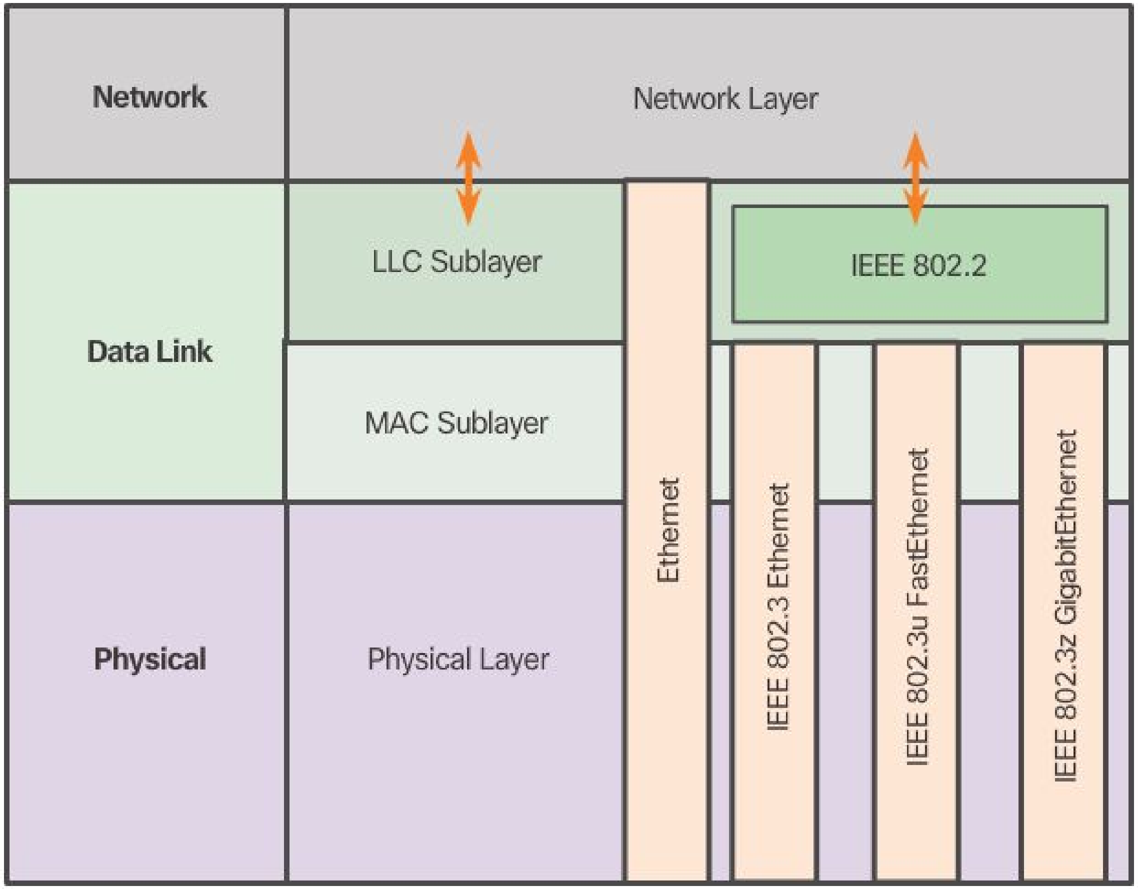
- Most widely used LAN technology
- Operates in the data link layer and the physical layer
- Family of networking technologies that are defined in the IEEE 802.2 and 802.3 standards
- Supports data bandwidths of 10, 100, 1000, 10,000, 40,000, and 100,000 Mbps (100 Gbps)

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

5.1.1: Ethernet Frame

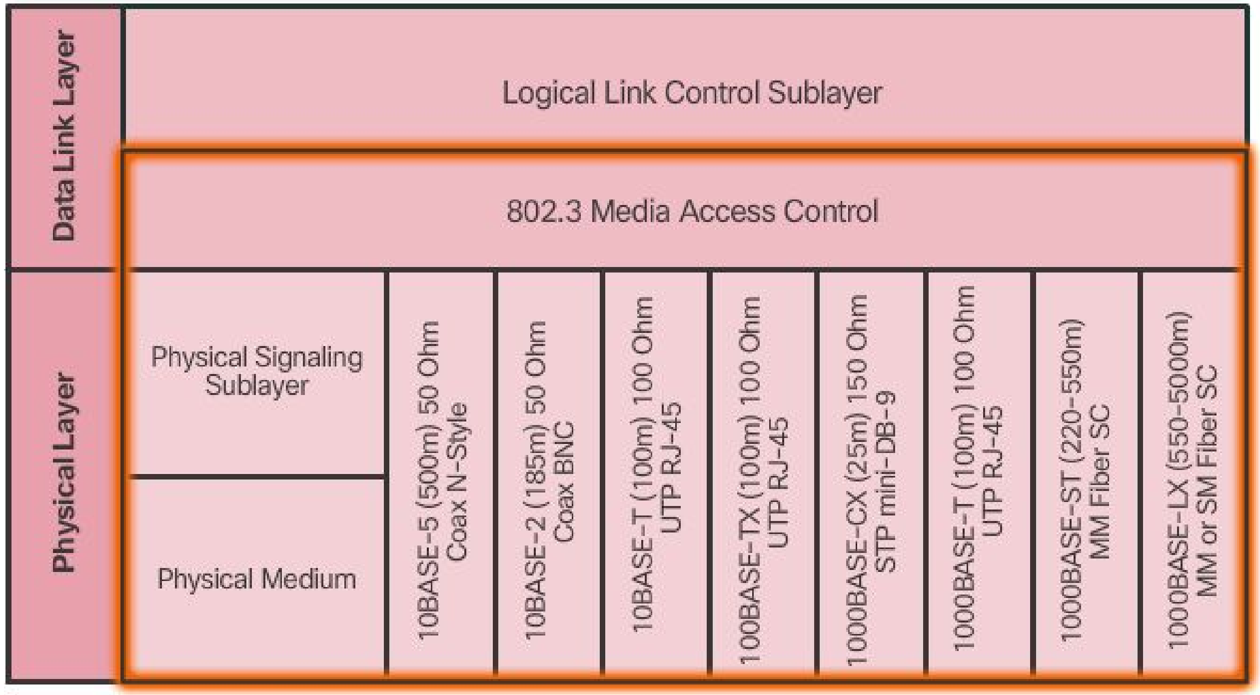
5.1.1.1 Ethernet Encapsulation(cont.)



5.1.1: Ethernet Frame
5.1.1.2 Mac Sublayer

Primary responsibilities:

- Data encapsulation
- Media access control



5.1.1: Ethernet Frame
5.1.1.3 Ethernet Evolution

Ethernet II Frame Structure and Field Size

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

5.1.1: Ethernet Frame
5.1.1.4 Ethernet II Frame Fields

- Minimum Ethernet frame size is 64 bytes (Collision Frame or Runt)
- Maximum Ethernet frame size is 1518 bytes (Jumbo or Baby Giant)

Preamble	Destination MAC Address	Source MAC Address	EtherType	Data	FCS

Preamble and Start Frame Delimiter Fields

The Preamble (7 bytes) and Start Frame Delimiter (SFD), also called the Start of Frame (1 byte), fields are used for synchronization between the sending and receiving devices. These first eight bytes of the frame are used to get the attention of the receiving nodes. Essentially, the first few bytes tell the receivers to get ready to receive a new frame.

Destination MAC Address Field

This 6-byte field is the identifier for the intended recipient. As you will recall, this address is used by Layer 2 to assist devices in determining if a frame is addressed to them. The address in the frame is compared to the MAC address in the device. If there is a match, the device accepts the frame. Can be a unicast, multicast or broadcast address.

Source MAC Address Field

This 6-byte field identifies the frame's originating NIC or interface. Must be a unicast address.

5.1.1: Ethernet Frame
5.1.1.4 Ethernet II Frame Fields (cont.)

Preamble	Destination MAC Address	Source MAC Address	EtherType	Data	FCS

EtherType 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

This field (46 - 1500 bytes) contains the encapsulated data from a higher layer, which is a generic Layer 3 PDU, or more commonly, 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.

Frame Check Sequence Field

The Frame Check Sequence (FCS) field (4 bytes) is used to detect errors in a frame. It uses a cyclic redundancy check (CRC). The sending device includes the results of a CRC in the FCS field of the frame. The receiving device receives the frame and generates a CRC to look for errors. If the calculations match, no error occurred. Calculations that do not match are an indication that the data has changed; therefore, the frame is dropped. A change in the data could be the result of a disruption of the electrical signals that represent the bits.

5.1.1: Ethernet Frame

5.1.1.5 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 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.		

5.1.1: Ethernet Frame
5.1.1.5 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 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.		✓

5.1.1: Ethernet Frame

5.1.1.6 Activity - Ethernet Frame Fields

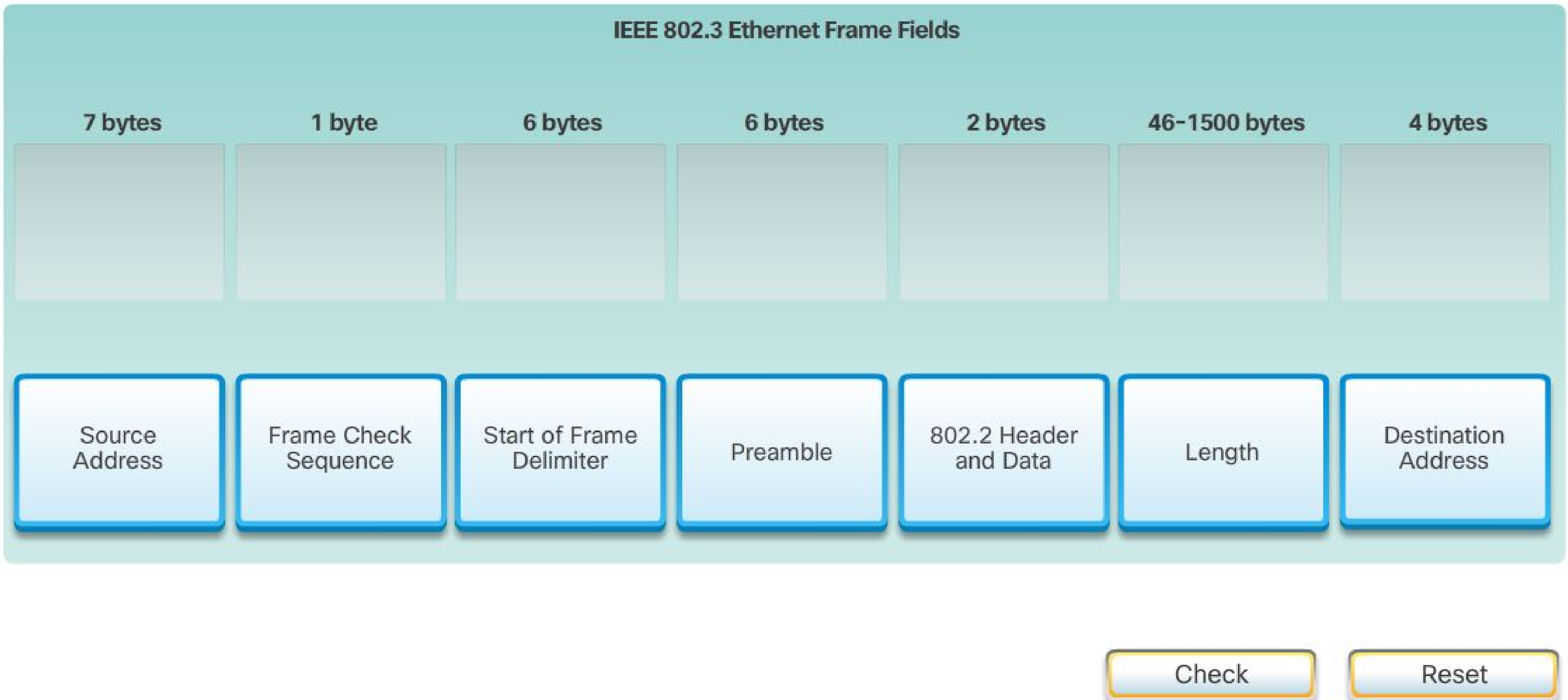
- 802.2 Header and Data
- Frame Check Sequence
- Type
- Start of Frame Delimiter
- Destination Address
- Preamble
- Source Address

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

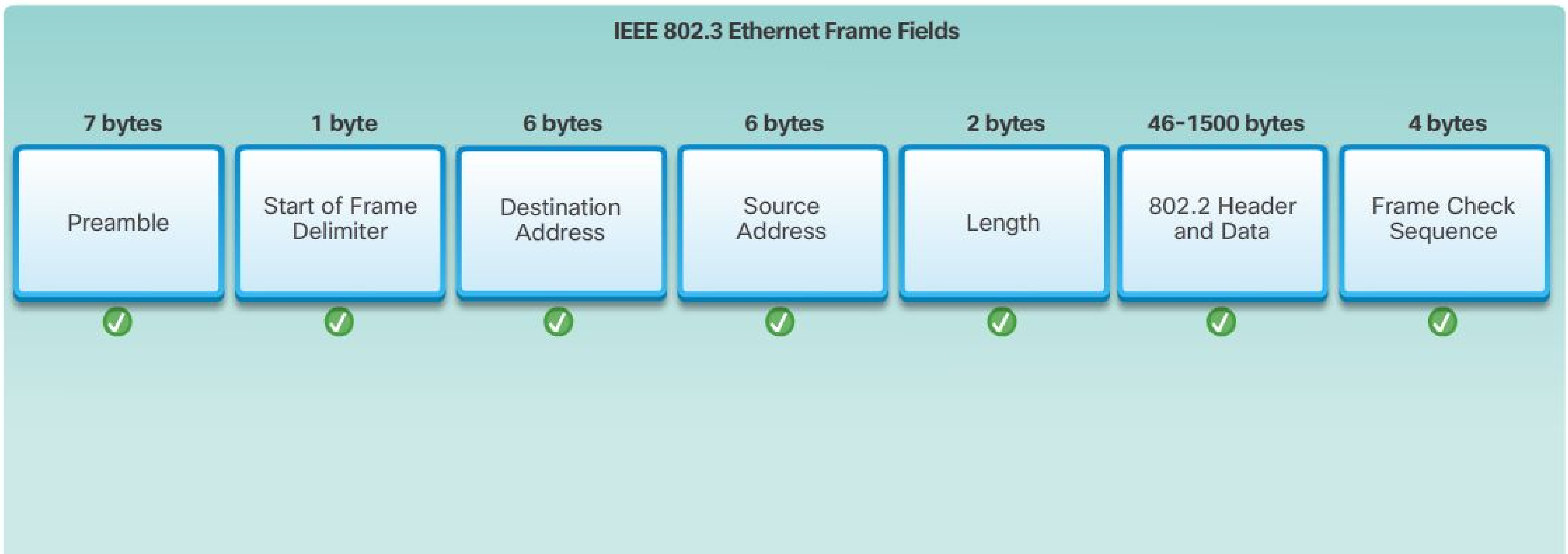
5.1.1: Ethernet Frame
5.1.1.6 Activity - Ethernet Frame Fields

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: Ethernet Frame
5.1.1.6 Activity - Ethernet Frame Fields



5.1.1: Ethernet Frame
5.1.1.6 Activity - Ethernet Frame Fields



5.1.2: Ethernet MAC Address

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

5.1.2: Ethernet MAC Address

5.1.2.1MAC Address and Hexadecimal (cont.)

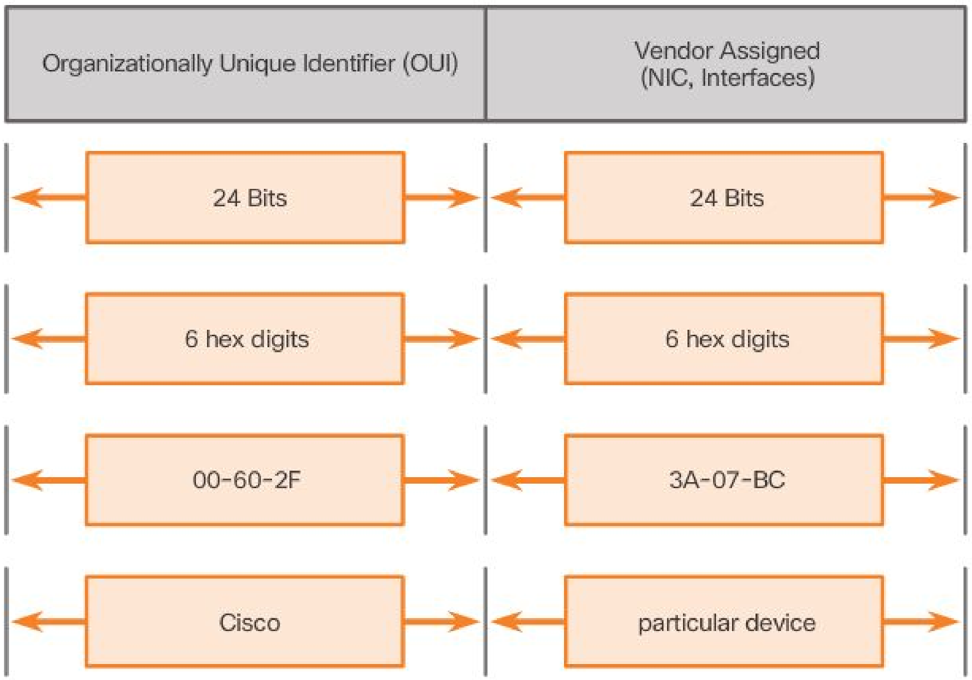
Hexadecimal Numbering

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

5.1.2.2 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 two simple rules:
  - Must use that vendor's assigned OUI as the first three bytes.
  - All MAC addresses with the same OUI must be assigned a unique value in the last three bytes.



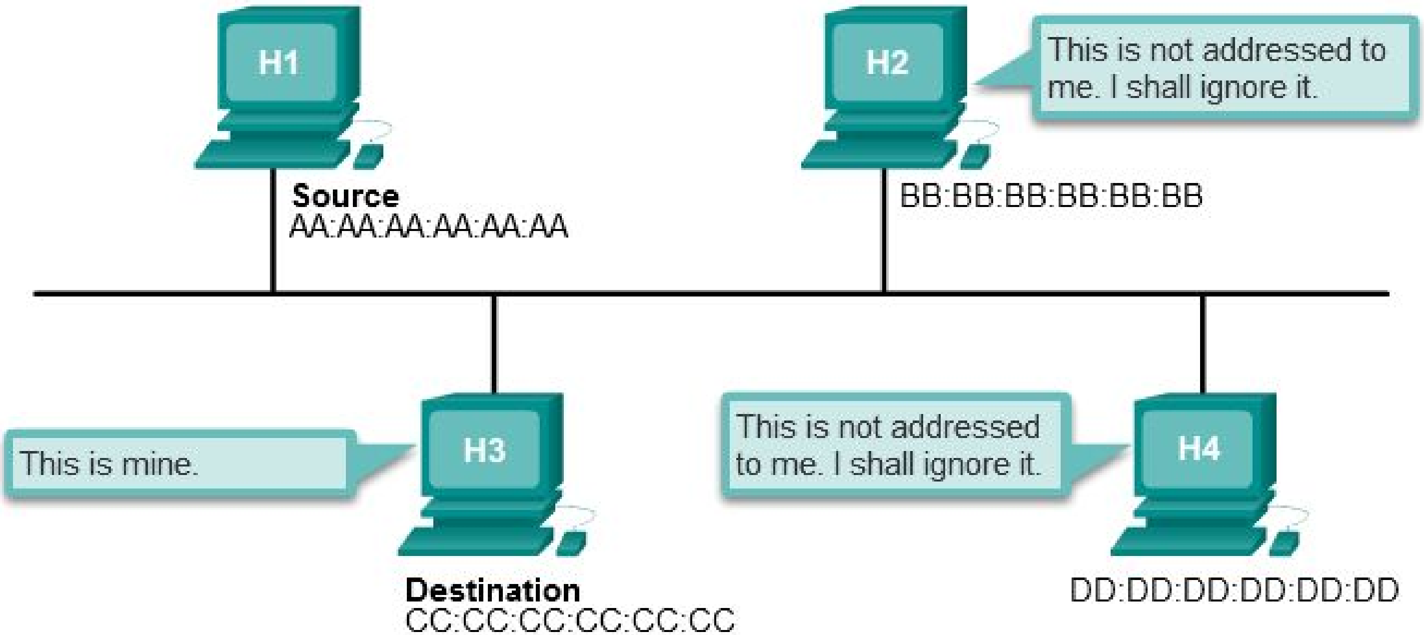
5.1.2: Ethernet MAC Address

5.1.2.3 Frame Processing

see animation online

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: Ethernet MAC Address
5.1.2.3 Frame Processing (cont.)

- The NIC views information to see if the destination MAC address in the frame matches the device's physical MAC address stored in RAM.
- If there is no match, the device discards the frame.
- If there is a match, the NIC passes the frame up the OSI layers, where the de-encapsulation process takes place.

5.1.2: Ethernet MAC Address
5.1.2.4 MAC Address Representations

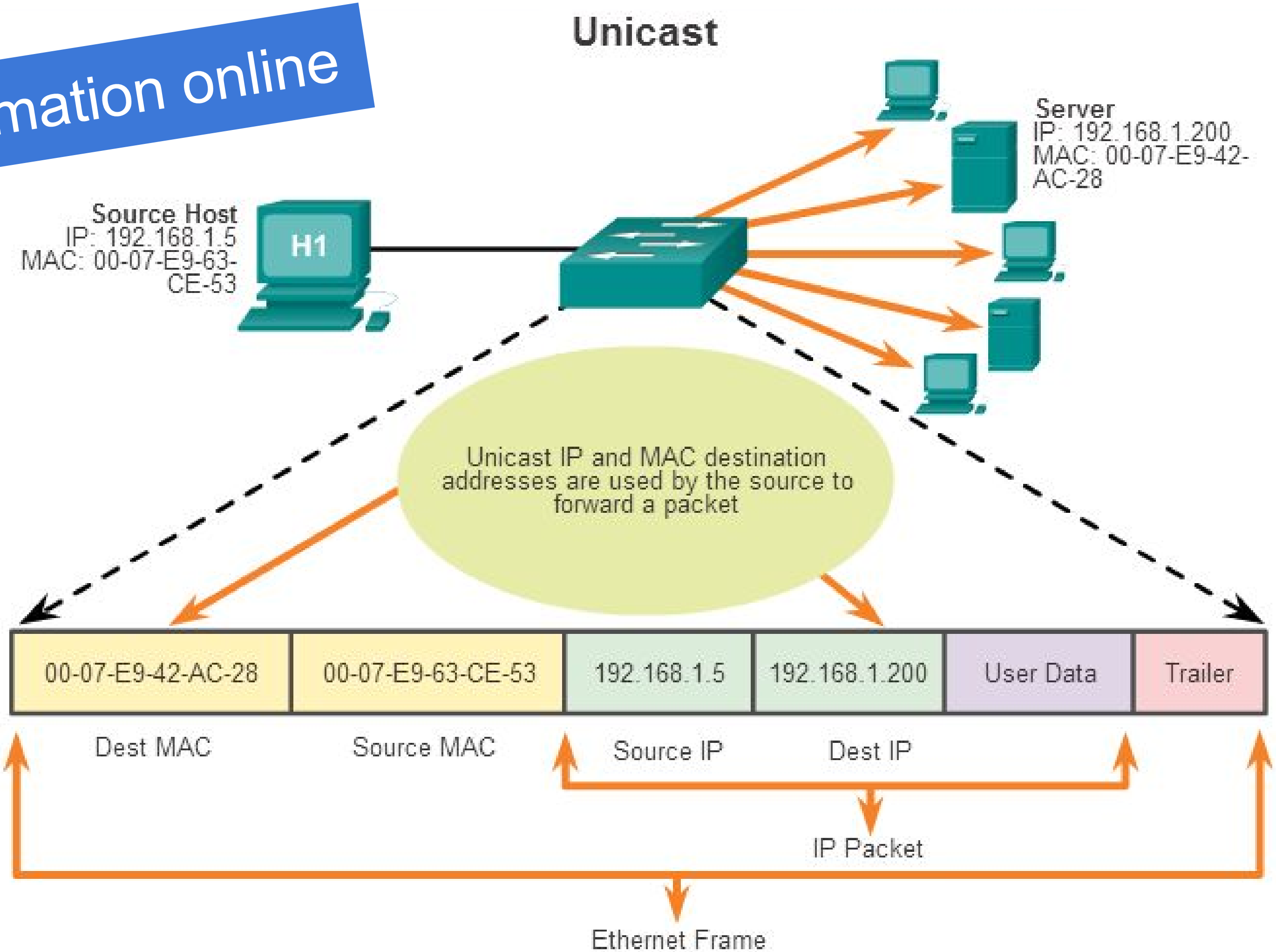
With Dashes	00-60-2F-3A-07-BC
With Colons	00:60:2F:3A:07:BC
With Periods	0060.2F3A.07BC

```
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: Ethernet MAC Address

5.1.2.5 Unicast MAC Address

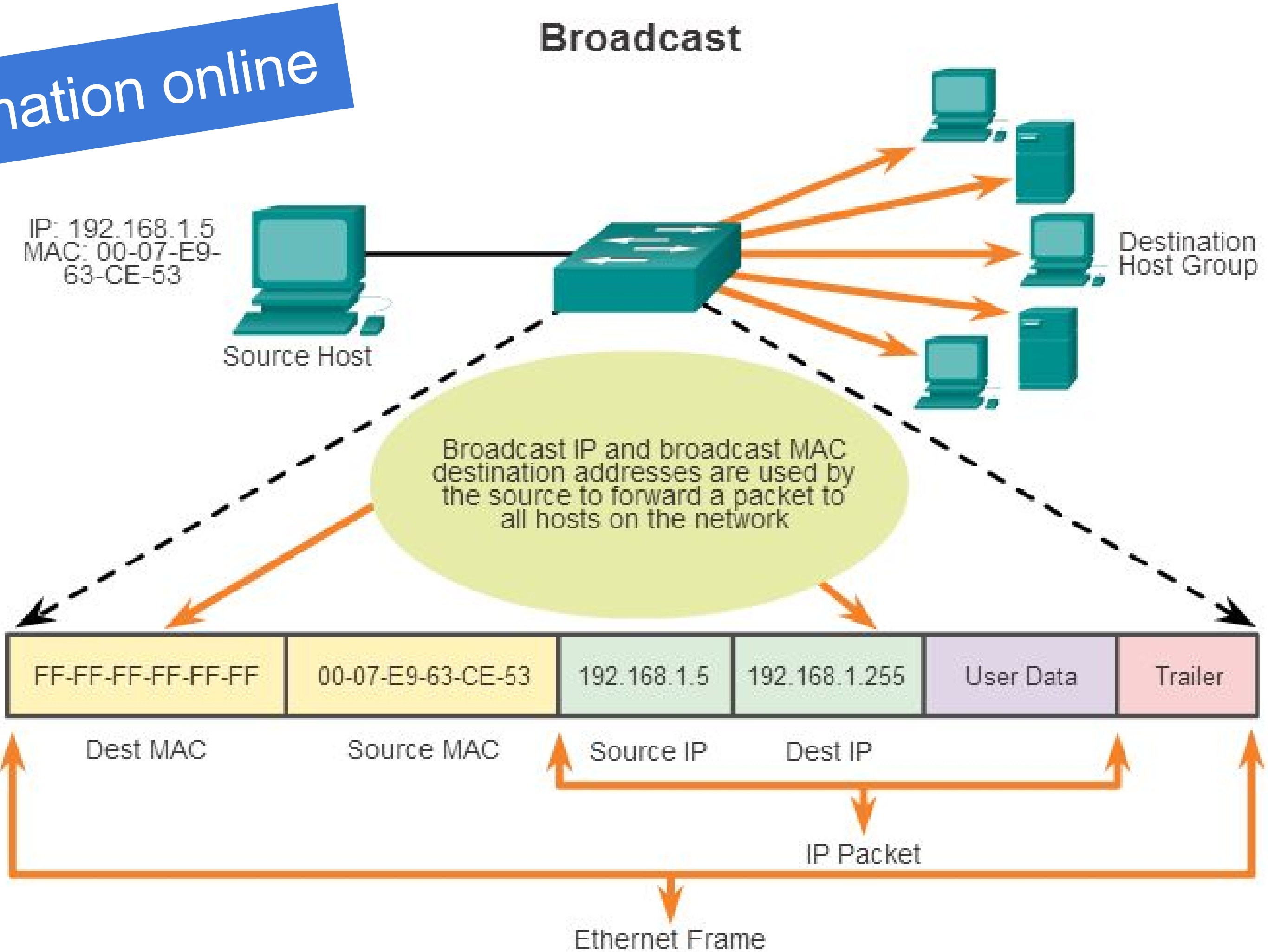
see animation online



5.1.2: Ethernet MAC Address

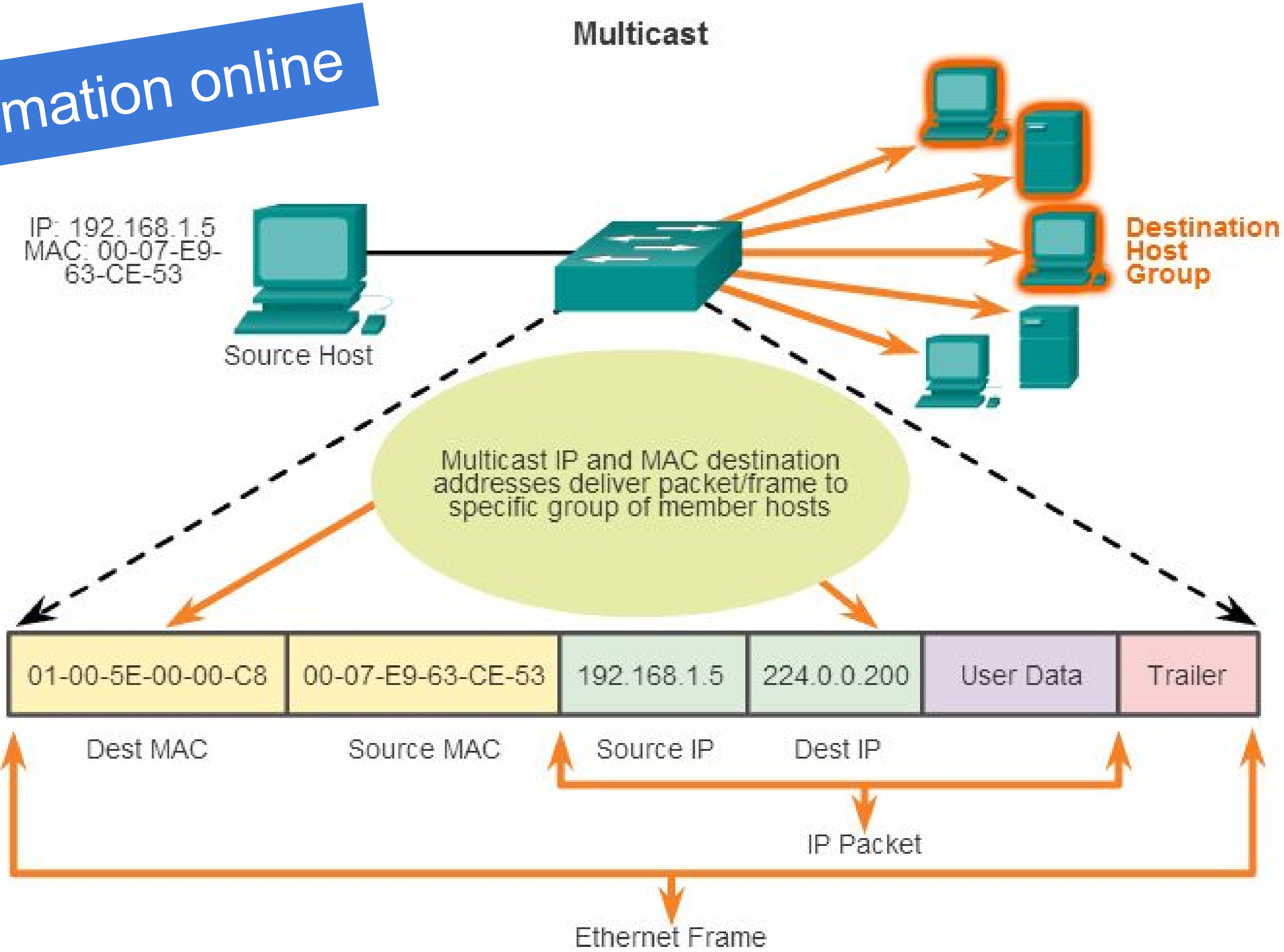
5.1.2.6 Broadcast MAC Address

see animation online



5.1.2: Ethernet MAC Address
5.1.2.7 Multicast MAC Address

see animation online



Section 5.2: LAN Switches

- 5.2.1: MAC Address Table
- 5.2.2: Switch Forwarding Methods
- 5.2.3: Switch Port Settings

5.2.1: MAC Address Table

5.2.1.1 Switch Fundamentals

- An Ethernet Switch is a Layer 2 device.
- It uses MAC addresses to make forwarding decisions.
- The MAC address table is sometimes referred to as a content addressable memory (CAM) table.

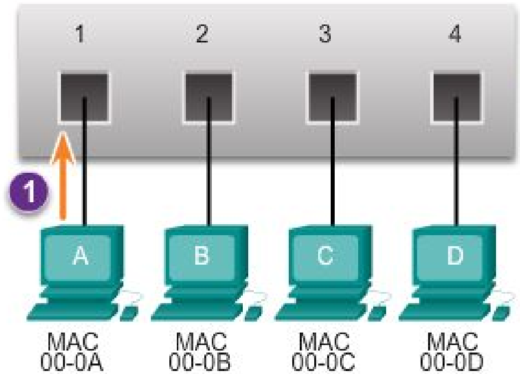
5.2.1: MAC Address Table
5.2.1.2 Learning MAC Addresses

Learn: Examine Source MAC Address

Port and Source MAC address added 2

MAC Address Table	
Port	**MAC Address**
1	00-0A

1



I don’t have this source MAC address and the incoming port in my table, so I will add it.

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

MAC addresses are shortened for demonstration purposes.

5.2.1: MAC Address Table
5.2.1.2 Learning MAC Addresses (cont.)

Forward: Examine Destination MAC Address

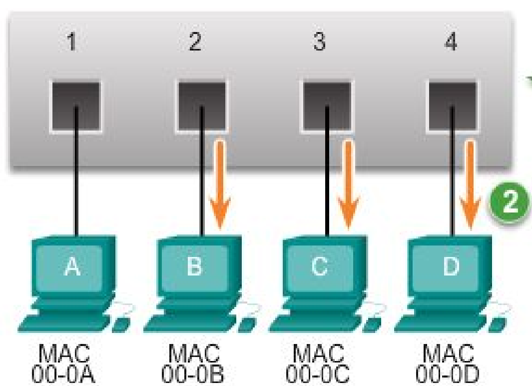
MAC Address Table	
Port	**MAC Address**
1	00-0A

Destination MAC address not in table

1

I don't have this destination MAC address in my table, so I will send this unknown unicast out all ports.

2



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

MAC addresses are shortened for demonstration purposes.

5.2.1: MAC Address Table
5.2.1.3 Filtering Frames

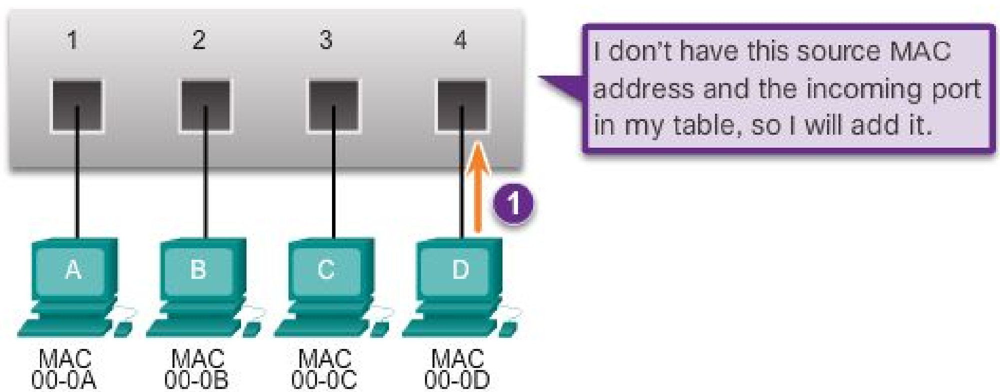
PC-D sends a frame back to PC-A and the switch learns PC-D's MAC address.

Port and Source MAC address added

1

MAC Address Table

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



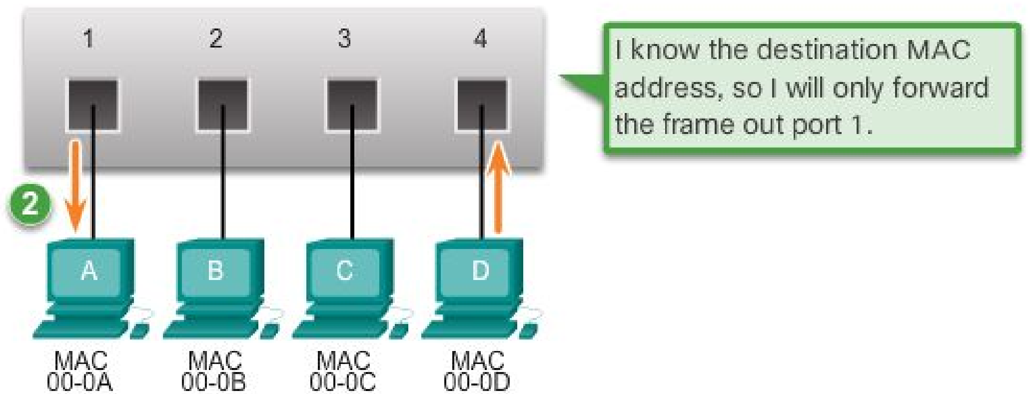
Destination MAC 00-0A	Source MAC 00-0D	Type	Data	FCS

5.2.1: MAC Address Table
5.2.1.3 Filtering Frames (cont.)

Since the Switch MAC Address table contains PC-A’s MAC Address, it sends the frame out only port 1.

MAC Address Table

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



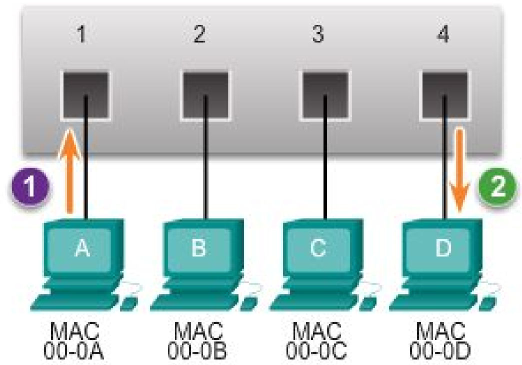
Destination MAC 00-0A	Source MAC 00-0D	Type	Data	FCS

5.2.1: MAC Address Table
5.2.1.3 Filtering Frames (cont.)

PC-A sends another frame to PC-D. The switch's table now contains PC-D's MAC address, so it sends the frame out only port 4.

MAC Address Table

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



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

5.2.1: MAC Address Table

5.2.1.4 Video Demonstration - MAC Address Tables on Connected Switches

- A switch can have multiple MAC addresses associated with a single port.
- This occurs when the switch is connected to another switch.
- See VIDEO DEMONSTRATION

5.2.1.5 Video Demonstration - Sending a Frame to the Default Gateway

- When a device has an IP address that is on a remote network, the Ethernet frame cannot be sent directly to the destination device.
- The Ethernet frame is sent to the MAC address of the default gateway, which is the router.
- See VIDEO DEMONSTRATION

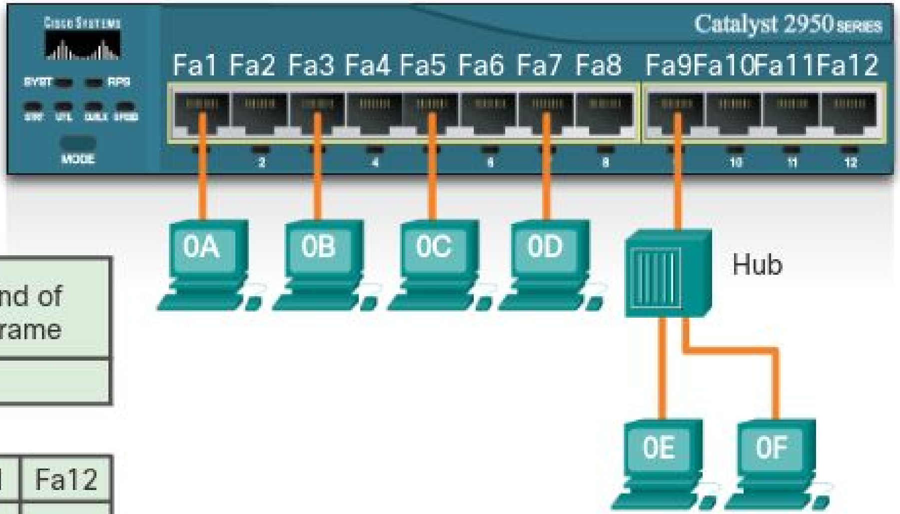
5.2.1: MAC Address Table

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
	0C	**0F**			

MAC Table

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

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

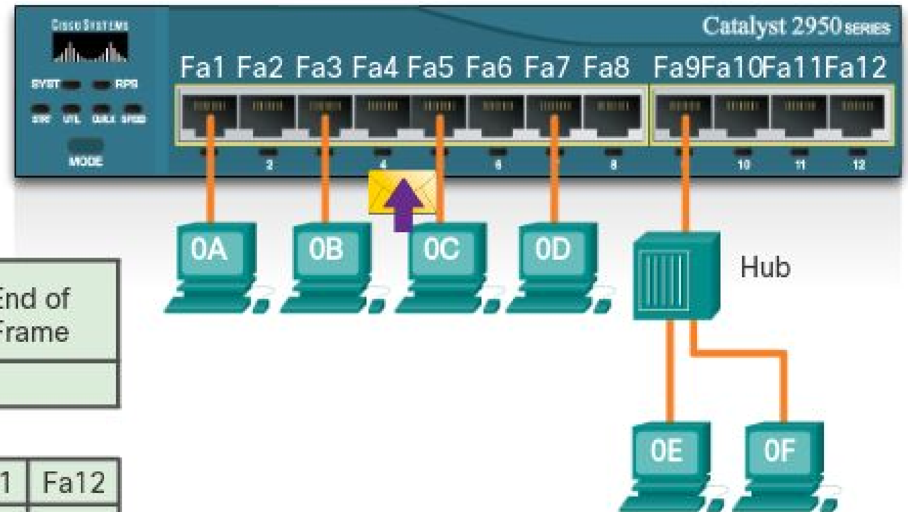
5.2.1: MAC Address Table

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
	0D	0A			

MAC Table

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

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.

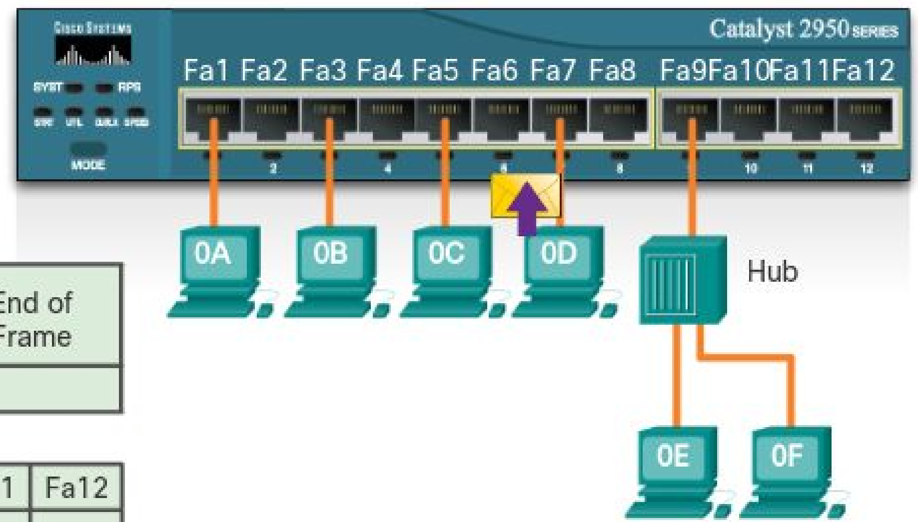
Check

Help

New Problem

5.2.1: MAC Address Table
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
	FF	0B			

MAC Table

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

Question 1 – Where will the switch forward the frame?

- [x] Fa1
- [ ] Fa2
- [ ] Fa3
- [ ] Fa4
- [x] Fa5
- [ ] Fa6
- [x] 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.
- [x] 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.

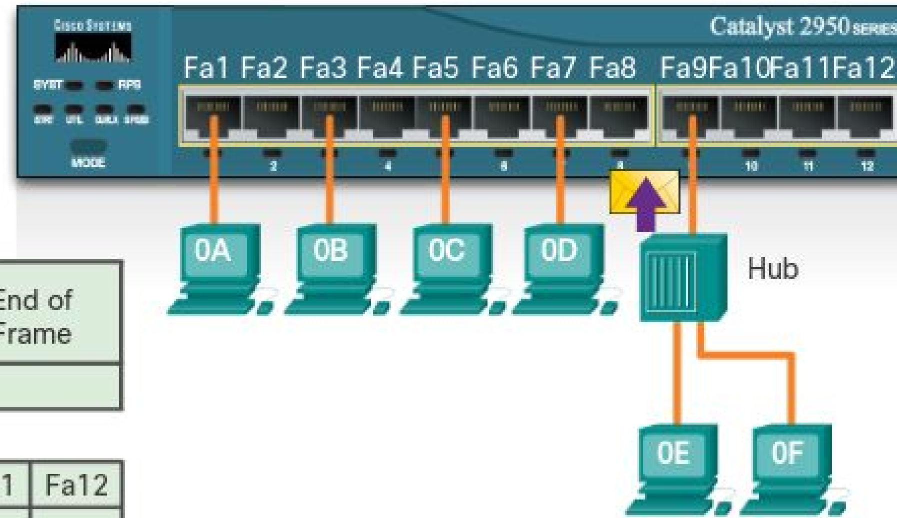
Check

Help

New Problem

5.2.1: MAC Address Table
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
	0E	**0C**			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0B									

Question 1 - Where will the switch forward the frame?

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

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

- [x] 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.
- [x] 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.

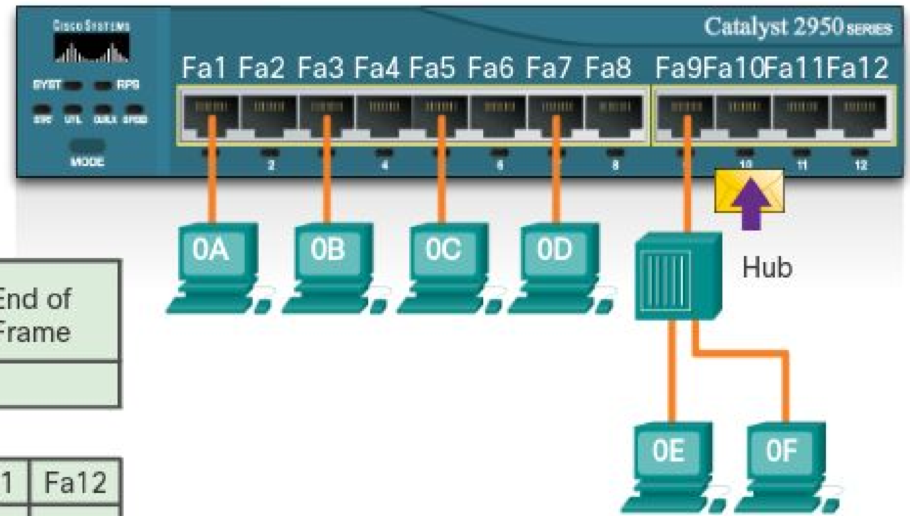
Check

Help

New Problem

5.2.1: MAC Address Table
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
	0E	0D			

MAC Table

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

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?

- [x] 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

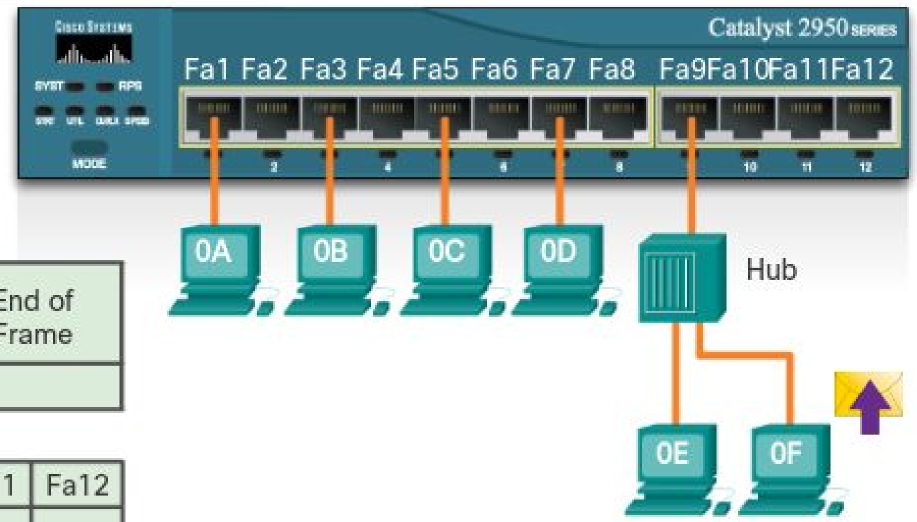
5.2.1: MAC Address Table

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	0E			

MAC Table

Fa1	Fa2	Fa3	Fa4	Fa5	Fa6	Fa7	Fa8	Fa9	Fa10	Fa11	Fa12
		0B						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

5.2.2: Switch Forwarding Methods

5.2.2.1 Frame Forwarding Methods on Cisco Switches

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.

see animation online

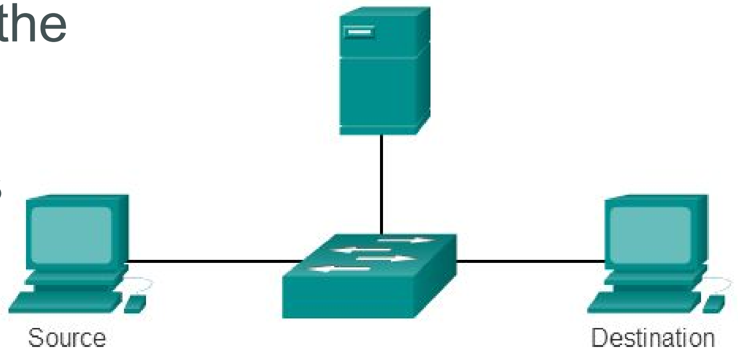
5.2.2: Switch Forwarding Methods
5.2.2.2 Cut-Through Switching

Fast-forward switching:

- Lowest level of latency immediately forwards a packet after reading the destination address.
- Typical cut-through method of switching.

Fragment-free switching:

- Switch stores the first 64 bytes of the frame before forwarding.
- Most network errors and collisions occur during the first 64 bytes.



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.

see animation online

5.2.2: Switch Forwarding Methods
5.2.2.3 Memory Buffering on Switches

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.

5.2.2: Switch Forwarding Methods

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.		

5.2.2: Switch Forwarding Methods

5.2.2.4 Activity - Frame Forwarding Methods

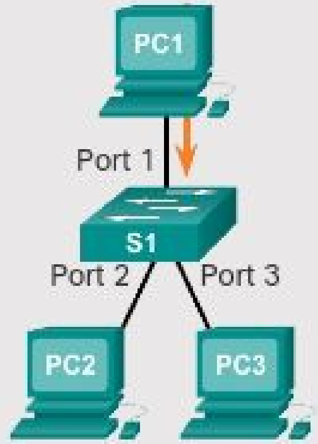
	Store-and-Forward	Cut-Through
1. Buffers frames until the full frame has been received by the switch.	✓	
2. Checks the frame for errors before releasing it out of its switch ports - if the full frame was not received, the switch discards it.	✓	
3. No error checking on frames is performed by the switch 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.		✓

5.2.2: Switch Forwarding Methods
5.2.2.4 Activity - Frame Forwarding Methods

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.

	Cabling used in this topology will be ____.
	To find where PC2 is located, PC1 will send out a ____ data frame.
	PC2 will respond back to PC1 by sending back a ____ message.
	If PC2 receives only half of the data in the frame, it will ____.
	If PC2 receives many damaged frames on Port 3, 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.

Straight-through | Cut-through | Unicast

Store-and-forward | Broadcast | Discard it | Reply back to PC1

Check | Reset

5.2.2: Switch Forwarding Methods

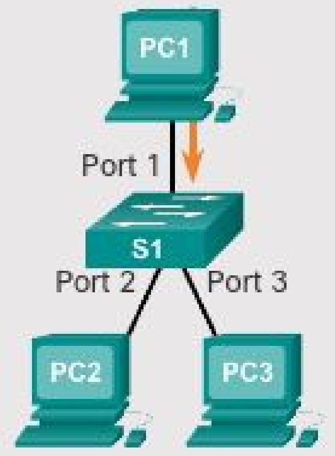
5.2.2.4 Activity - Frame Forwarding Methods

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 3, S1 likely will change back to ____ switching.

Cut-through



- 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.

Reply back to PC1

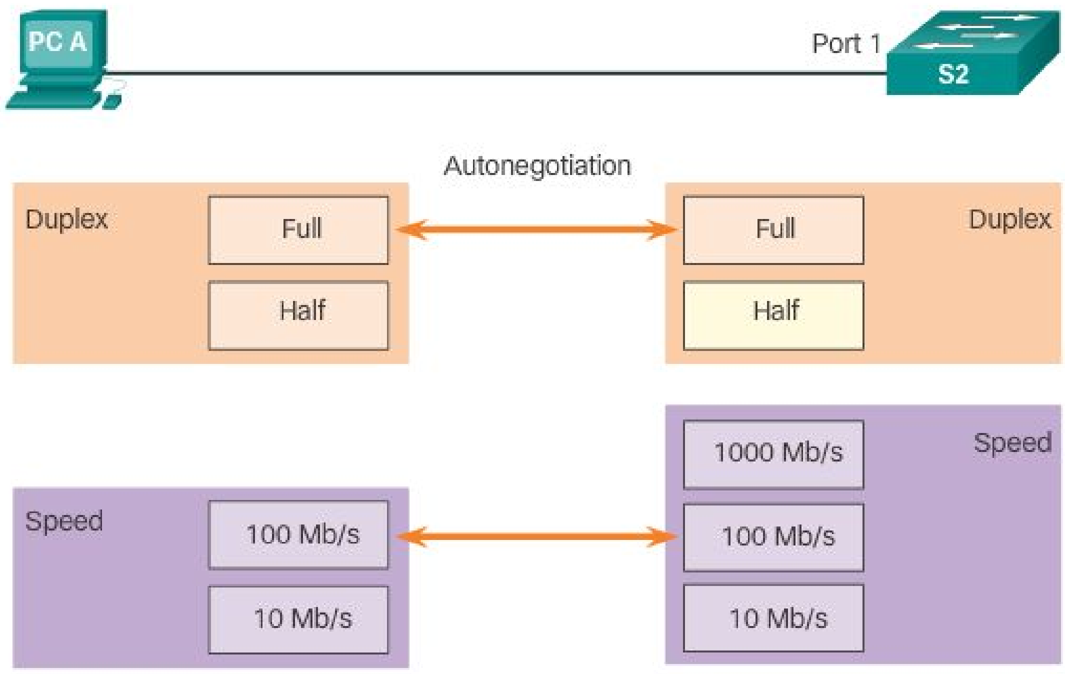
Check

Reset

5.2.3: Switch Port Settings

5.2.3.1 Duplex and Speed Settings

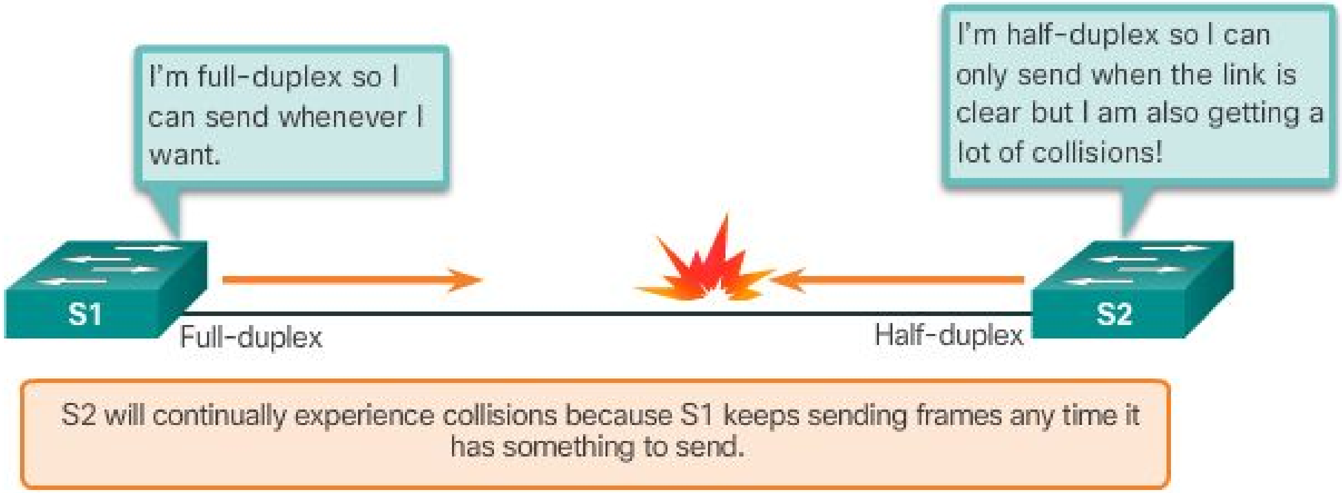
- Full-duplex – Both ends of the connection can send and receive simultaneously.
- Half-duplex – Only one end of the connection can send at a time.



5.2.3: Switch Port Settings

5.2.3.1 Duplex and Speed Settings (cont.)

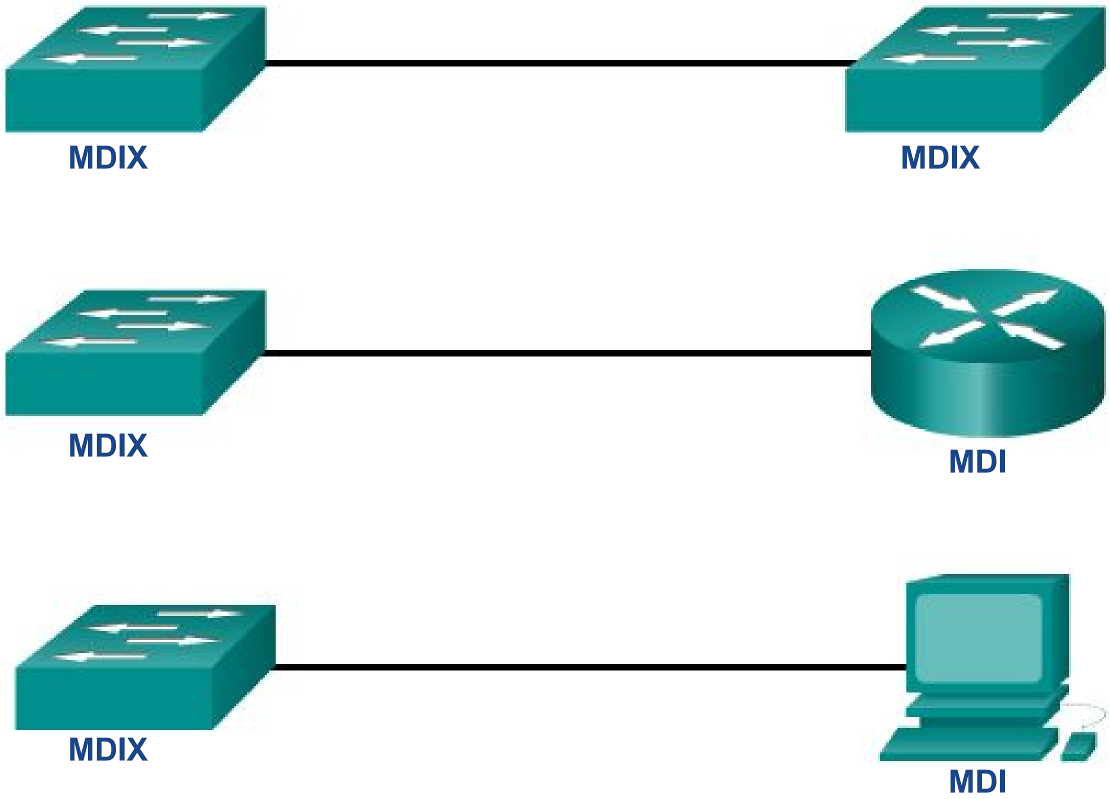
A common cause of performance issues on 10/100 Mb/s Ethernet links is when one port on the link operates at half-duplex and the other on full-duplex.



5.2.3: Switch Port Settings

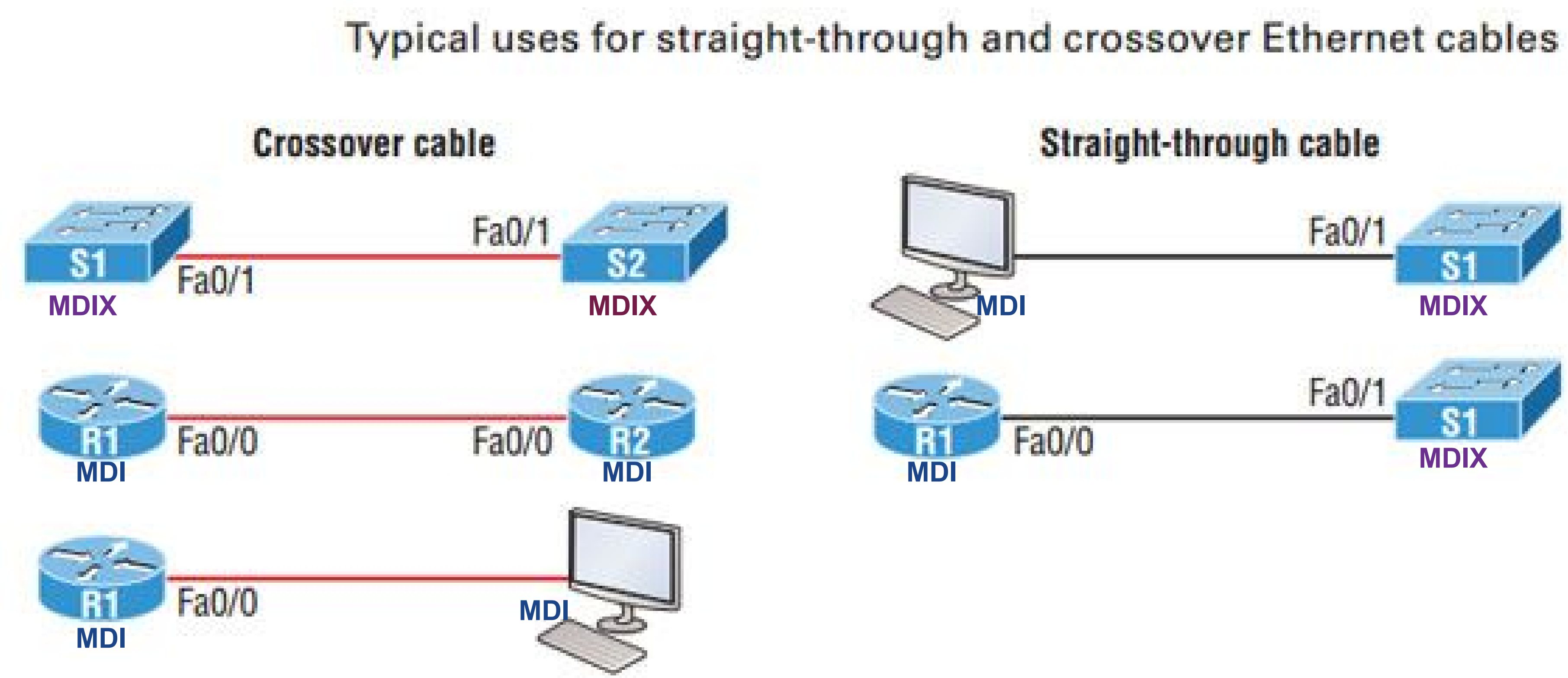
5.2.3.2 Auto-MDIX

MDIX auto detects the type of connection required and configures the interface accordingly.



5.2.3: Switch Port Settings

5.2.3.2 Without Auto-MDIX



Section 5.3: Address Resolution Protocol

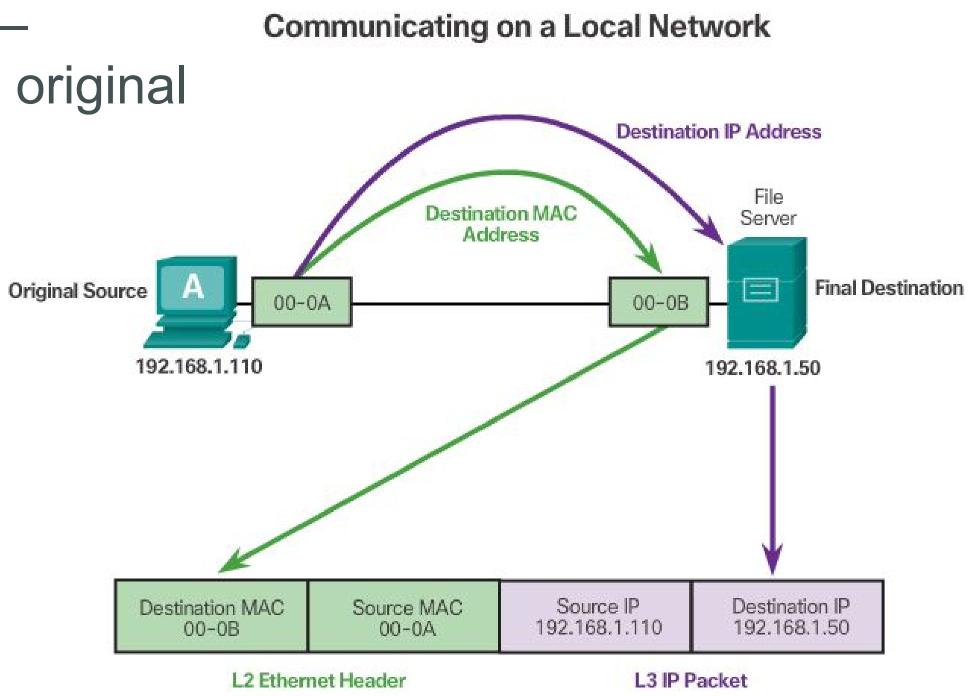
- 5.3.1: MAC and IP
- 5.3.2: ARP
- 5.3.3: ARP Issues

5.3.1: MAC and IP

5.3.1.1 Destination on the Same Network

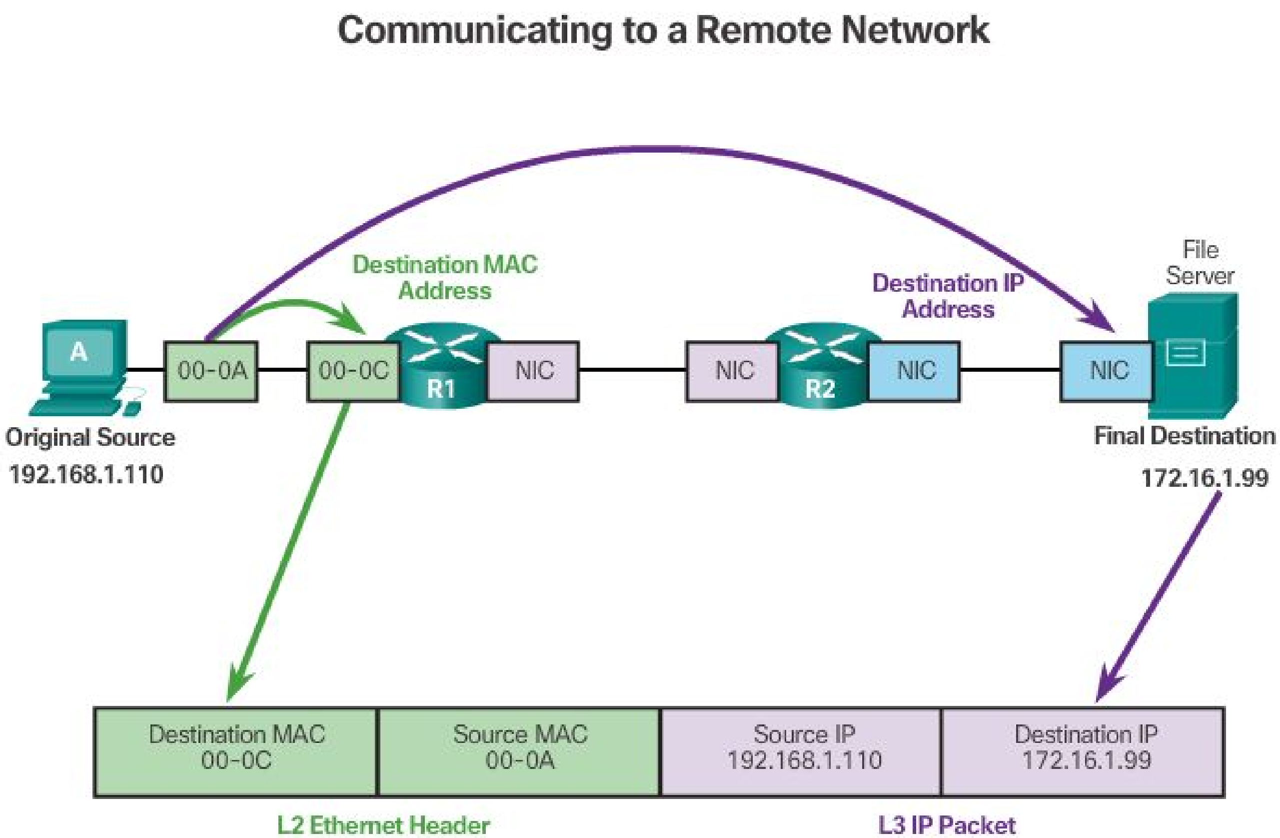
There are two primary addresses assigned to a device on an Ethernet LAN:

- 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.



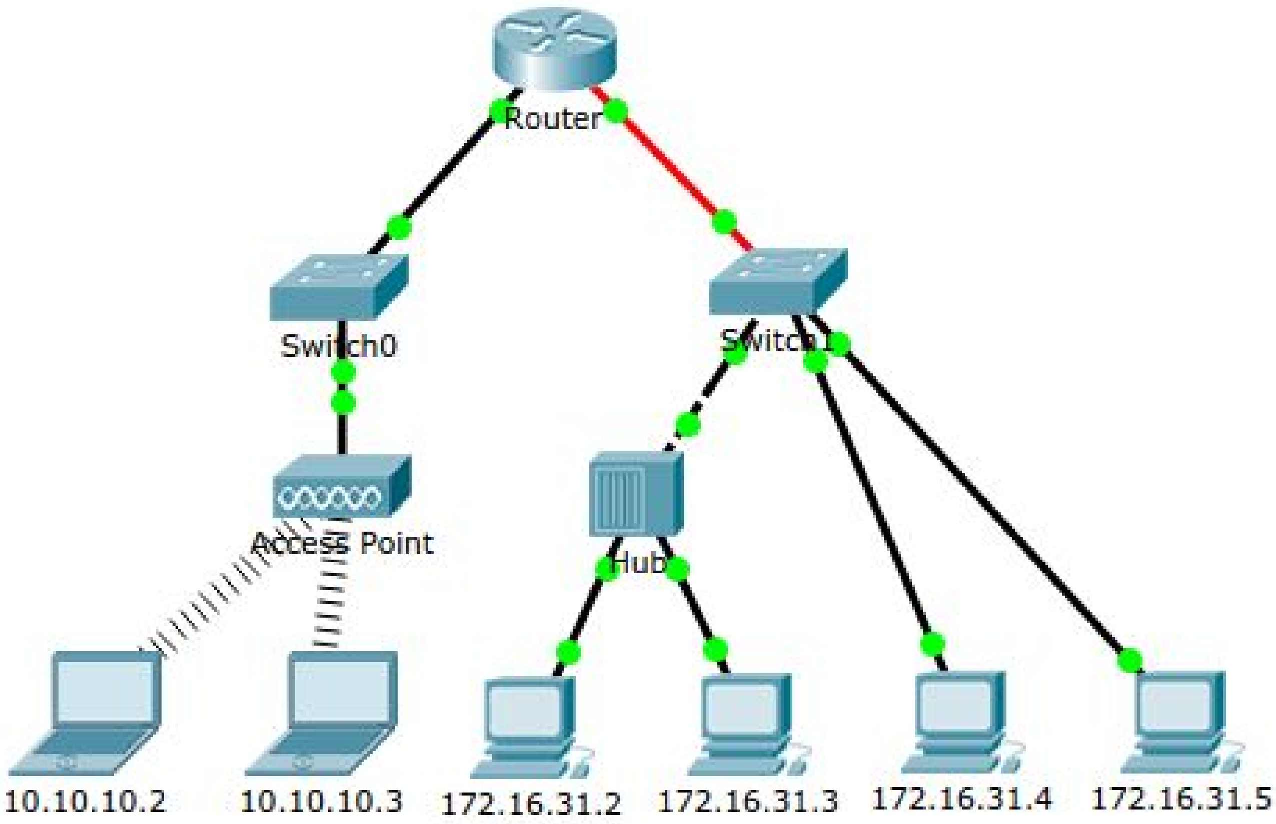
5.3.1: MAC and IP

5.3.1.2 Destination on a Remote Network

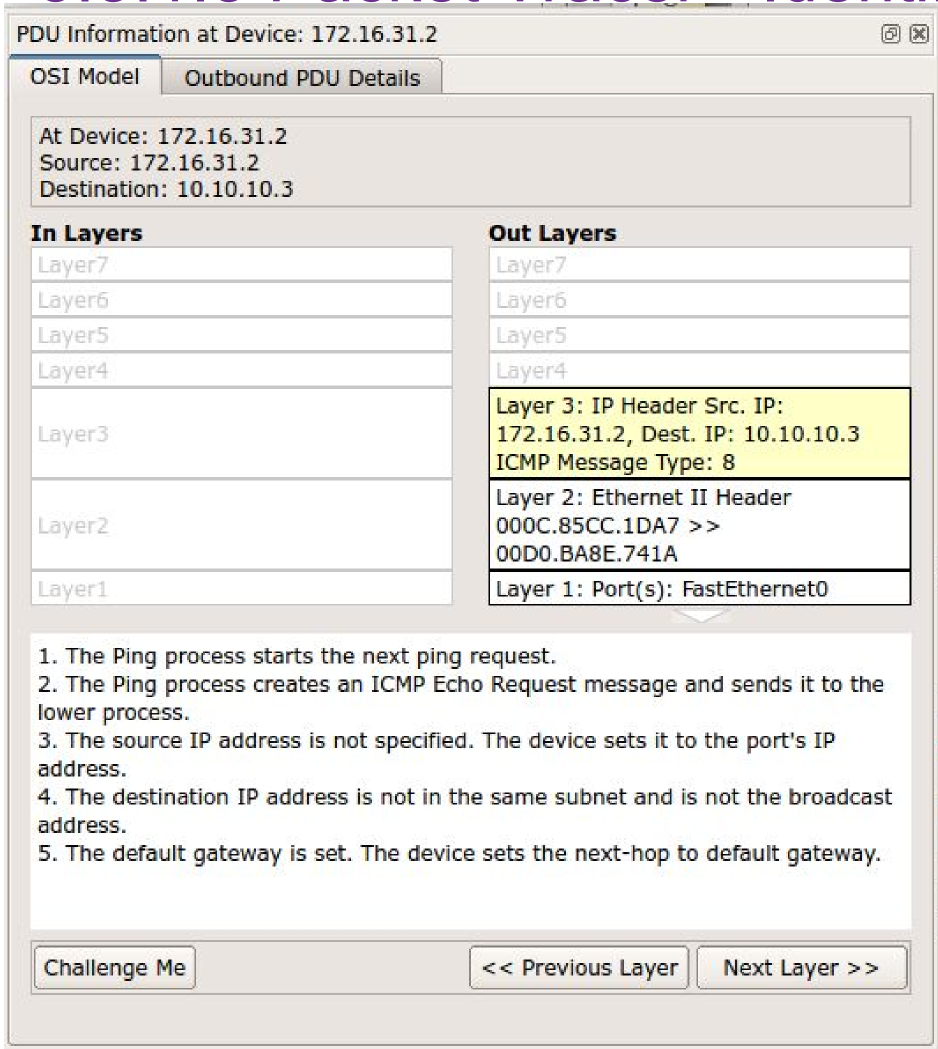


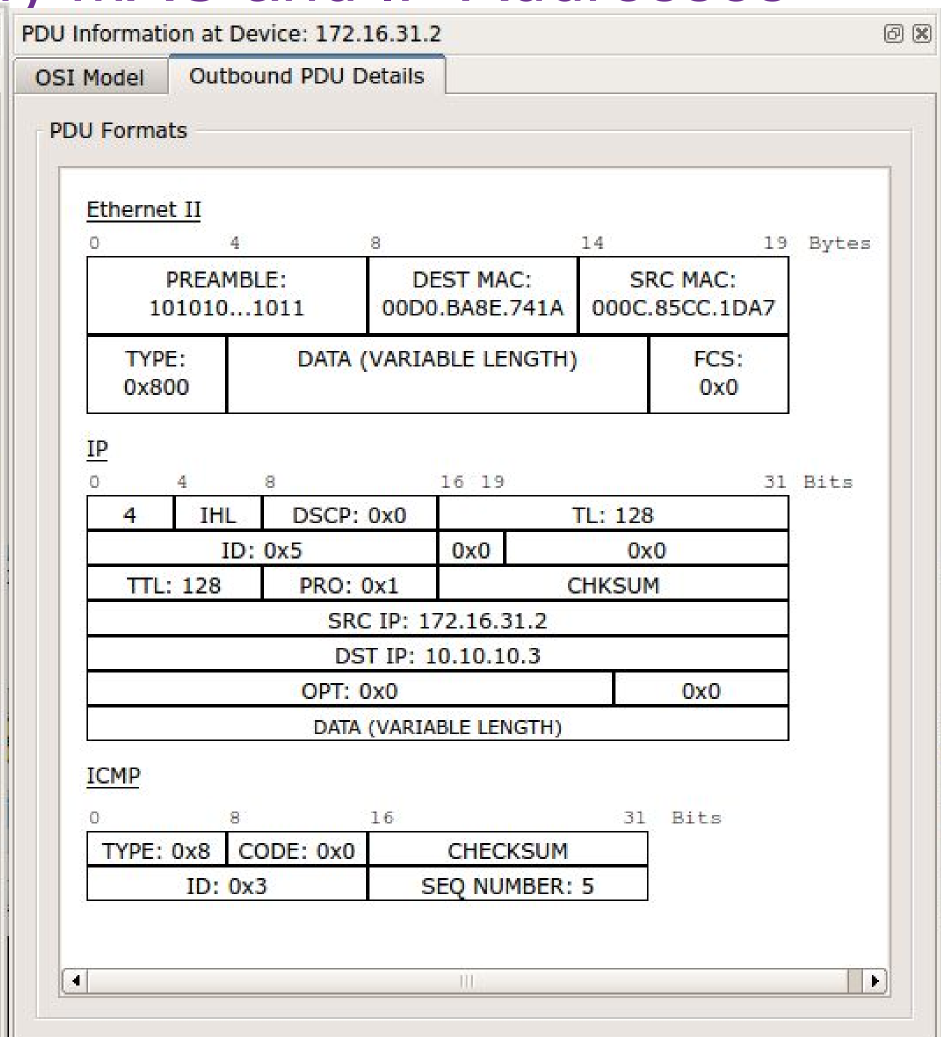
MAC addresses are shortened for demonstration purposes.

5.3.1: MAC and IP
5.3.1.3 Packet Tracer - Identify MAC and IP Addresses



5.3.1: MAC and IP
5.3.1.3 Packet Tracer - Identify MAC and IP Addresses

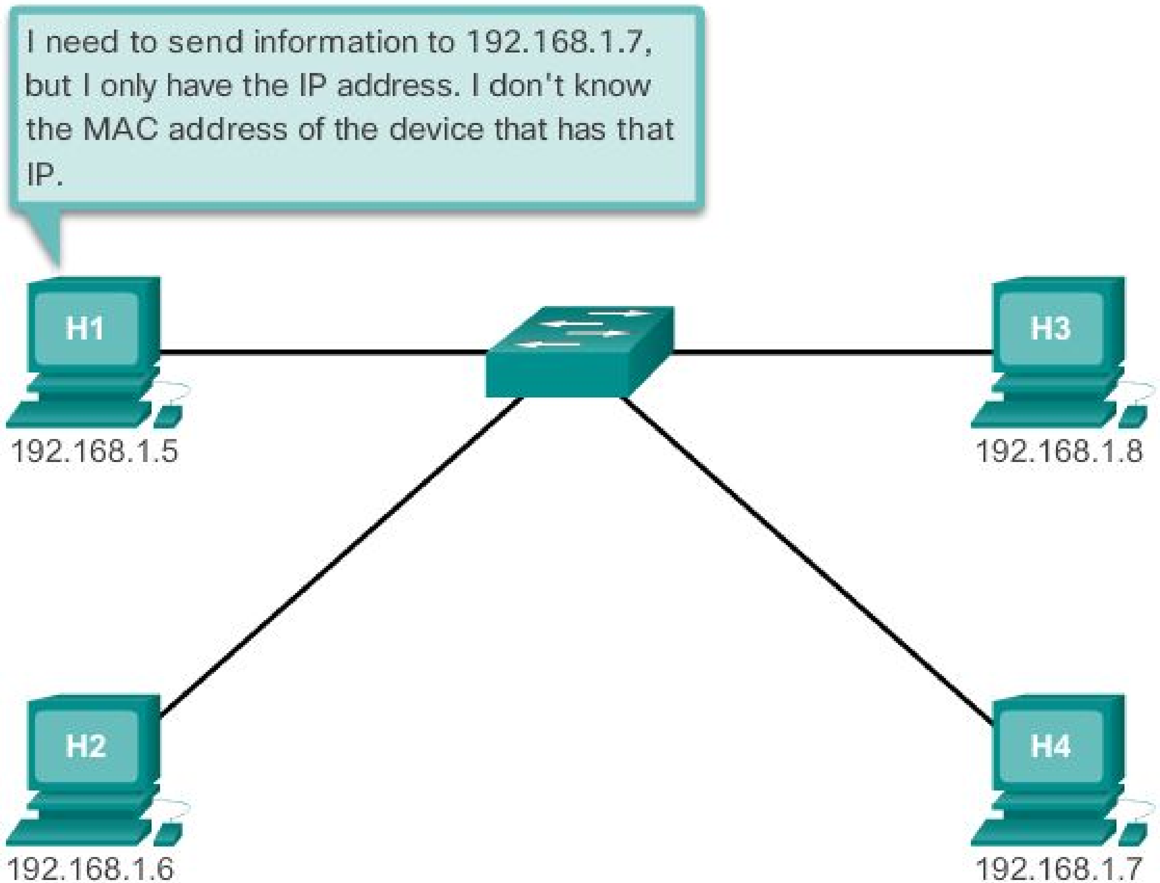




5.3.1: MAC and IP
5.3.1.3 Packet Tracer - Identify MAC and IP Addresses

Test	At Device	Dest. MAC	Src MAC	Src IPv4	Dest IPv4
Ping from 172.16.31.2 to 10.10.10.3	172.16.31.2	00D0:BA8E:741A	000C:85CC:1DA7	172.16.31.2	10.10.10.3
	Hub	--	--	--	--
	Switch1	00D0:BA8E:741A	000C:85CC:1DA7	--	--
	Router	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3
	Switch0	0060:4706:572B	00D0:588C:2401	--	--
	Access Point	--	--	--	--
	10.10.10.3	0060:4706:572B	00D0:588C:2401	172.16.31.2	10.10.10.3

5.3.2: ARP
5.3.2.1 Introduction to ARP



5.3.2: ARP
5.3.2.2 ARP Functions

see animation online

ARP Table

- Used to find the MAC address that is mapped to the destination IPv4 address.
- If the destination IPv4 address is on the same network as the source IPv4, the device will search the ARP table for the destination IPv4 address.
- If the destination IPv4 address is on a different network, the device will search for the IPv4 address of the default gateway.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.
- If no entry is found, then an ARP request is sent.

5.3.2.3 ARP Request

- Sent when a device needs a MAC address associated with an IPv4 address, and it does not have an entry in its ARP table.
- The ARP request message includes:

  Target IPv4 address – This is the IPv4 address that requires a corresponding MAC address.

  Target MAC address – This is the unknown MAC address and will be empty in the ARP request message.

- The ARP request is encapsulated in an Ethernet frame using the following header information:

  Destination MAC address – This is a broadcast address requiring all Ethernet NICs on the LAN to accept and process the ARP request.

  Source MAC address – This is the sender's MAC address.

  Type – ARP messages have a type field of 0x806.

- See VIDEO DEMONSTRATION

5.3.2: ARP
5.3.2.4 ARP Reply

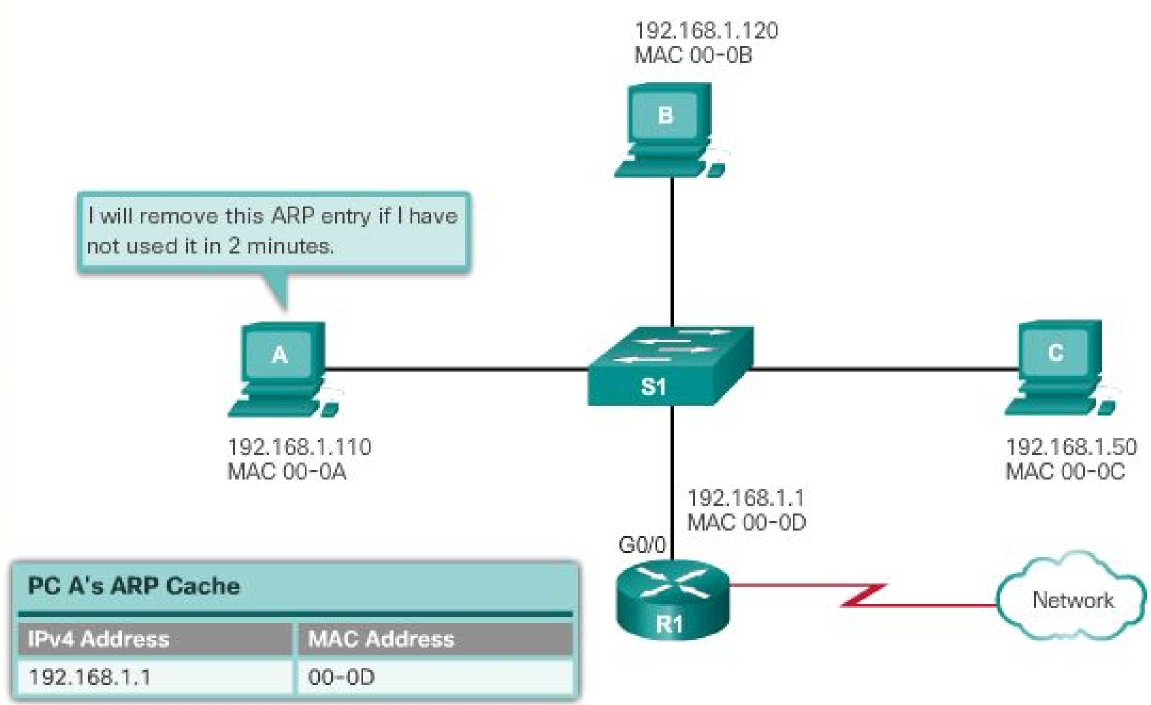
- The device with the target IPv4 address in the ARP request will respond with an ARP reply. The ARP reply message includes:
  - Sender's IPv4 address – This is the IPv4 address of the sender, the device whose MAC address was requested.
  - Sender's MAC address – This is the MAC address of the sender, the MAC address needed by the sender of the ARP request.
- The ARP reply is encapsulated in an Ethernet frame using the following header information:
  - Destination MAC address – This is the MAC address of the sender.
  - Source MAC address – This is the sender of the ARP reply's MAC address.
  - Type – ARP messages have a type field of 0x806.
- See VIDEO DEMONSTRATION

5.3.2.5 Video Demonstration – ARP Role in Remote Communication

- When the destination IPv4 address is not on the same network as the source IPv4 address, the source device needs to send the frame to its default gateway.
- The source checks its ARP table for an entry with the IPv4 address of the default gateway.
- If there is not an entry, it uses the ARP process to determine the MAC address of the default gateway.
- See VIDEO DEMONSTRATION

5.3.2: ARP
5.3.2.6 Removing Entries from an ARP Table

- ARP cache timer removes ARP entries that have not been used for a specified period of time.
- Commands may also be used to manually remove all or some of the entries in the ARP table.



5.3.2.7 ARP Tables on Networking Devices

Router ARP Table

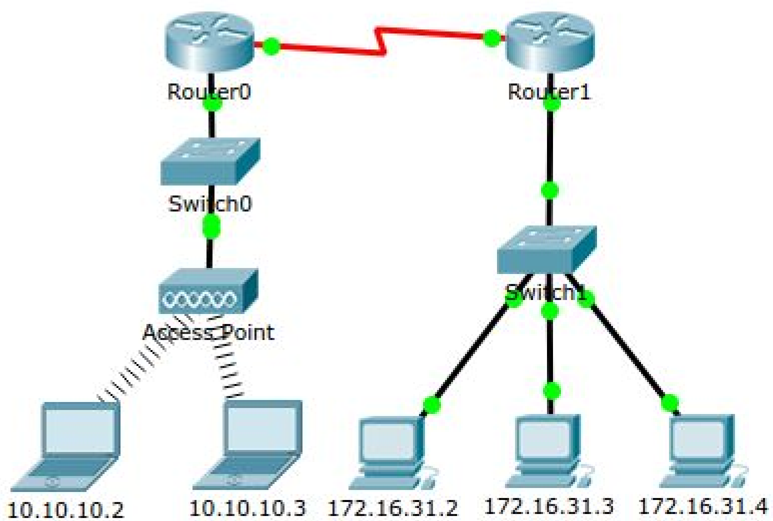
```
Router# show ip arp

                                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
```

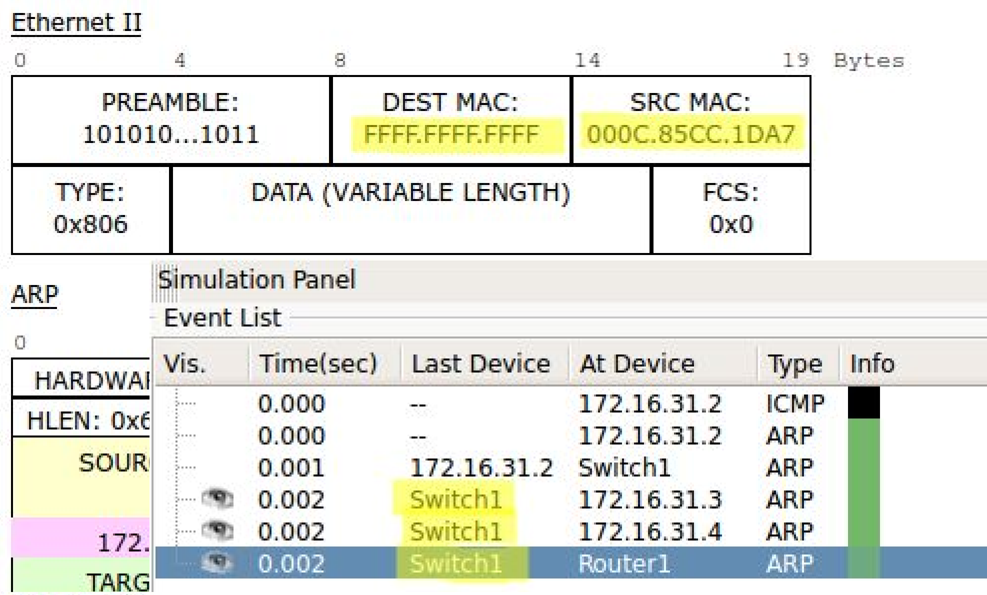
5.3.2: ARP
5.3.2.7 ARP Tables on Networking Devices (cont.)

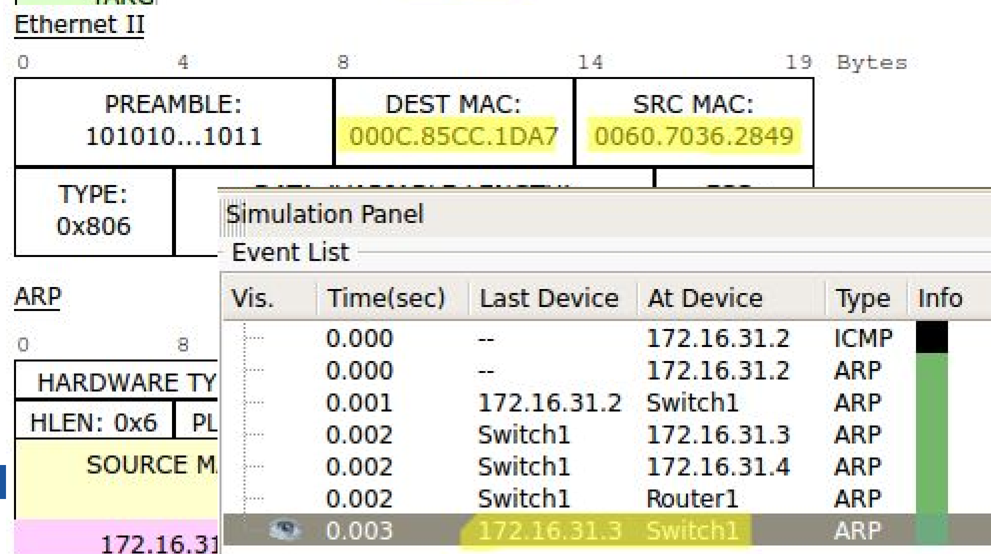
Host ARP Table

```
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
```

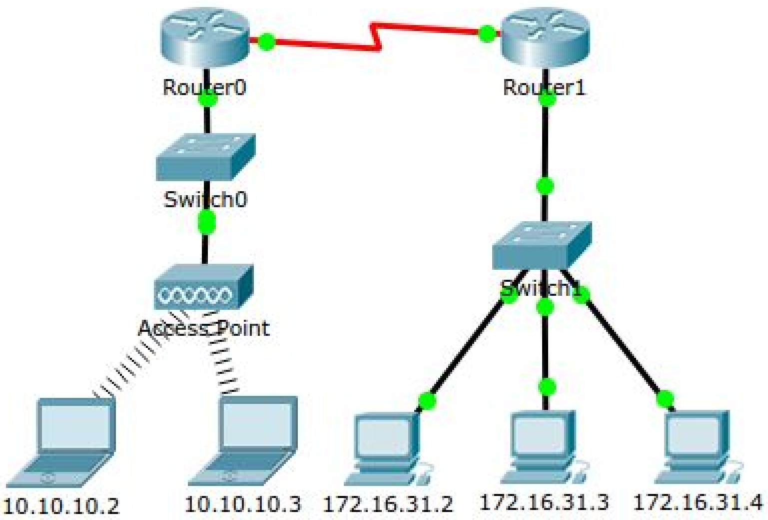
5.3.2: ARP
5.3.2.8 Packet Tracer - Examine the ARP Table





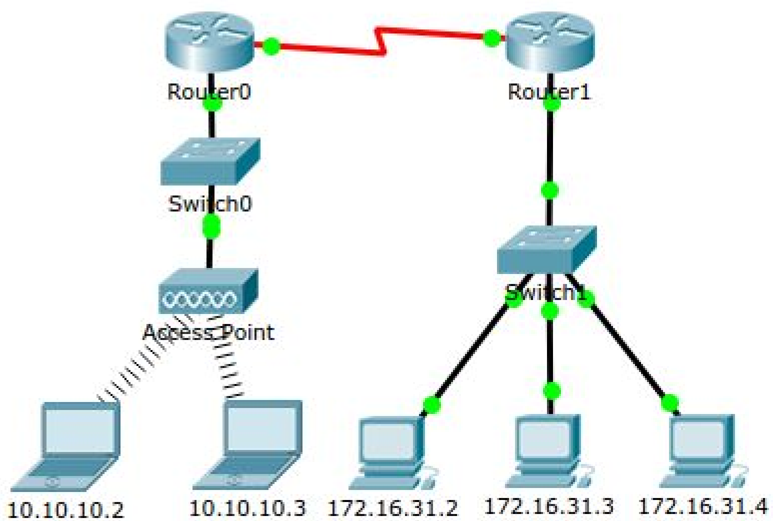


5.3.2: ARP
5.3.2.8 Packet Tracer - Examine the ARP Table




```
Packet Tracer PC Command Line 1.0
PC>arp -d
PC>ping 172.16.31.3

Pinging 172.16.31.3 with 32 bytes of data:

Reply from 172.16.31.3: bytes=32 time=7ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms TTL=128
Reply from 172.16.31.3: bytes=32 time=0ms TTL=128

Ping statistics for 172.16.31.3:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 7ms, Average = 1ms

PC>arp -a
  Internet Address      Physical Address      Type
  172.16.31.3           0060.7036.2849        dynamic
```

5.3.2: ARP
5.3.2.8 Packet Tracer - Examine the ARP Table

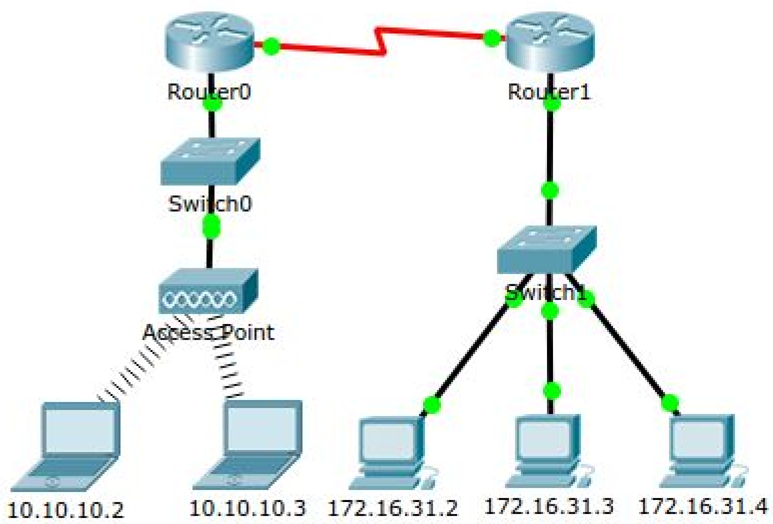


Generate additional traffic to populate the switch MAC address table.

```
Switch>show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

   1    0002.1640.8d75    DYNAMIC     Fa0/3
   1    000c.85cc.1da7    DYNAMIC     Fa0/1
   1    00e0.f7b1.8901    DYNAMIC     Gig0/1
```

Device	Interface	MAC Address	Switch Interface
Router0	Gg0/0	0001.6458.2501	G0/1
	S0/0/0	N/A	N/A
Router1	G0/0	00E0.F7B1.8901	G0/1
	S0/0/0	N/A	N/A
10.10.10.2	Wireless	0060.2F84.4AB6	F0/2
10.10.10.3	Wireless	0060.4706.572B	F0/2
172.16.31.2	F0	000C.85CC.1DA7	F0/1
172.16.31.3	F0	0060.7036.2849	F0/2
172.16.31.4	G0	0002.1640.8D75	F0/3

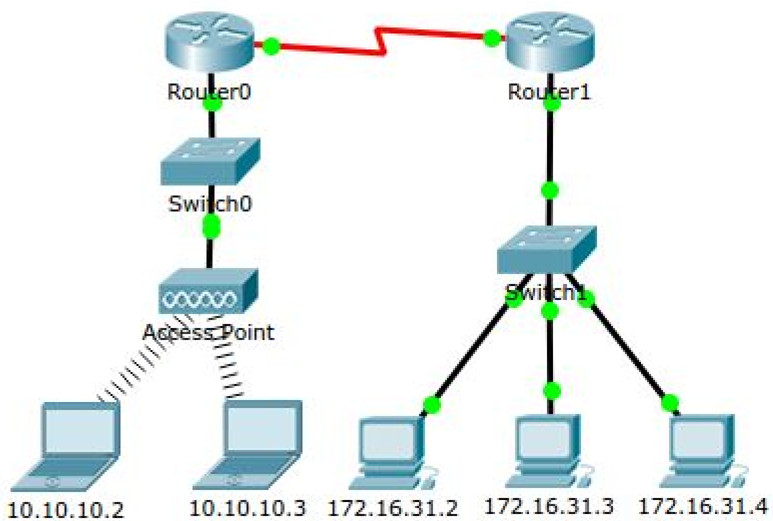
5.3.2: ARP
5.3.2.8 Packet Tracer - Examine the ARP Table




```
PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:

Reply from 10.10.10.1: bytes=32 time=1ms TTL=254
Reply from 10.10.10.1: bytes=32 time=9ms TTL=254
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254
Reply from 10.10.10.1: bytes=32 time=1ms TTL=254

Ping statistics for 10.10.10.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 9ms, Average = 3ms

PC>arp -a
  Internet Address      Physical Address      Type
  172.16.31.1           00e0.f7b1.8901        dynamic
  172.16.31.3           0060.7036.2849        dynamic
  172.16.31.4           0002.1640.8d75        dynamic

PC>arp -d
PC>ping 10.10.10.1

Pinging 10.10.10.1 with 32 bytes of data:
```

Simulation mode

5.3.2: ARP
5.3.2.8 Packet Tracer - Examine the ARP Table



Ethernet II

0 4 8 14 19 Bytes

PREAMBLE: 101010...1011	DEST MAC: FFFF.FFFF.FFFF	SRC MAC: 000C.85CC.1DA7
TYPE: 0x806	DATA (VARIABLE LENGTH)	FCS: 0x0

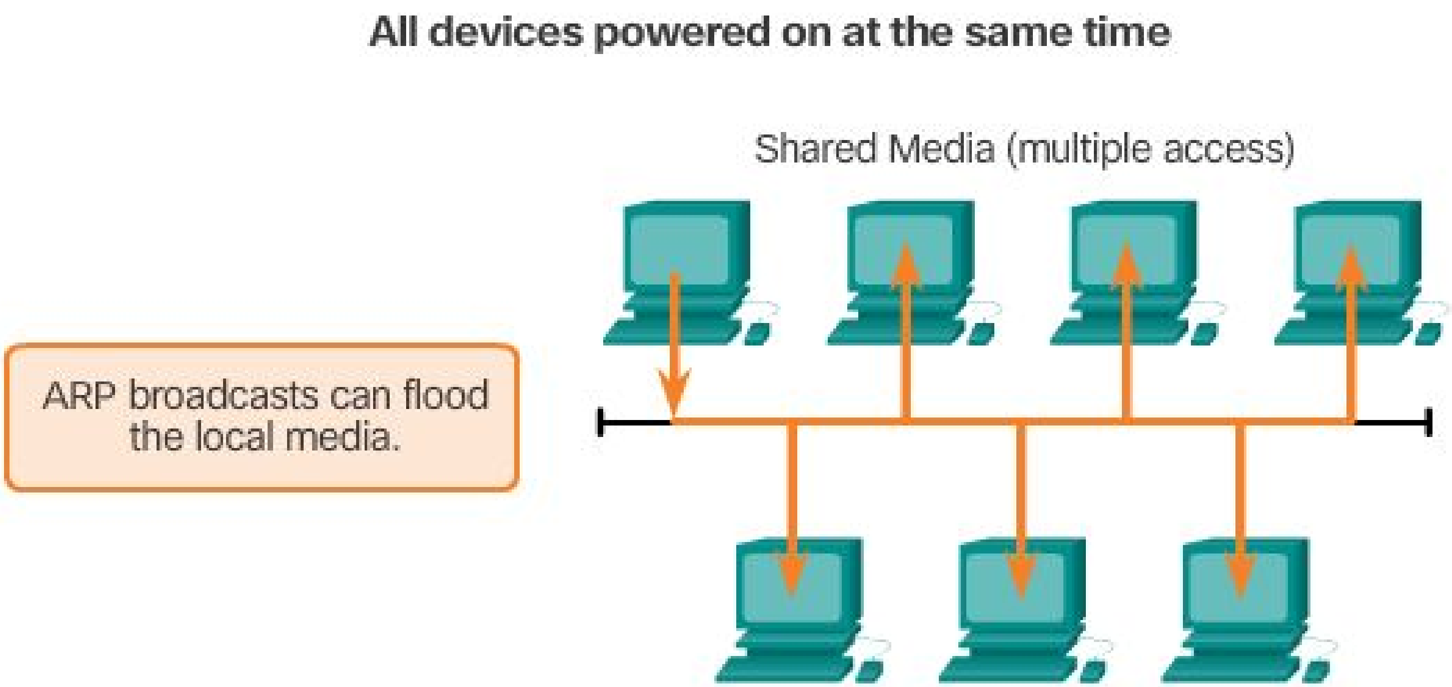
ARP

0 8 16 31 Bits

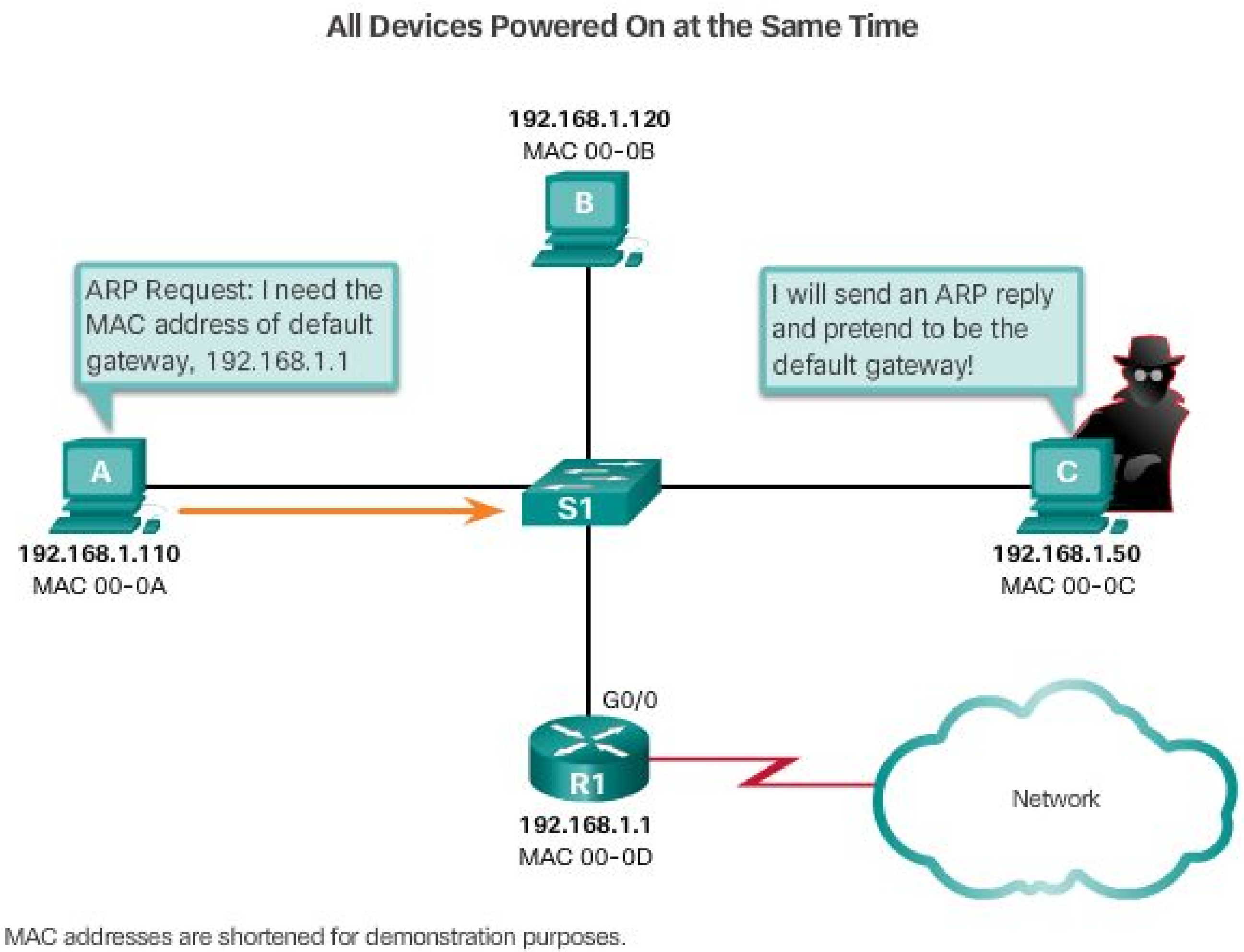
HARDWARE TYPE: 0x1		PROTOCOL TYPE: 0x800
HLEN: 0x6	PLEN: 0x4	OPCODE: 0x1
SOURCE MAC: 000C.85CC.1DA7 (48 bits)		
		SOURCE IP (32 bits) ==>
172.16.31.2		
TARGET MAC: 0000.0000.0000 (48 bits)		
TARGET IP: 172.16.31.1 (32 bits)		

```
Router>enable
Router#show mac-address-table
          Mac Address Table
-------------------------------------------

Vlan    Mac Address       Type        Ports
----    -----------       --------    -----

Router#show arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  172.16.31.1             -   00E0.F7B1.8901  ARPA   GigabitEthernet0/0
Internet  172.16.31.2             2   000C.85CC.1DA7  ARPA   GigabitEthernet0/0
```

5.3.3: ARP Issues
5.3.3.1 ARP Broadcasts

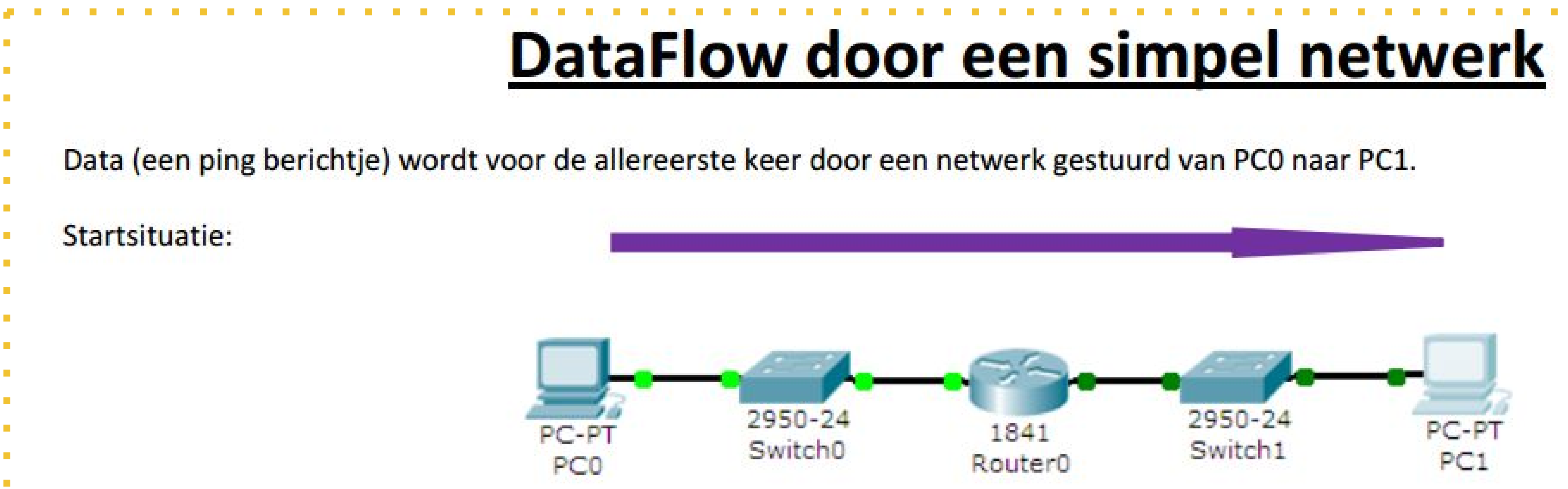


5.3.3: ARP Issues
5.3.3.2 ARP Spoofing



Data Flow - extra

- Check out pdf and packet tracer file: **DataFlow**
- Complete explanation of what happens in a simple network when sending data from A to B, using ‘*normal*’ L2 switch and L3 router (using the OSI reference model)
  - → Watch the ARP tables, Routing tables, MAC tables



DataFlow door een simpel netwerk

Data (een ping berichtje) wordt voor de allereerste keer door een netwerk gestuurd van PC0 naar PC1.

Startsituatie:

Thank you.

Cisco Networking Academy
Mind Wide Open