Cisco Networking Academy
Mind Wide Open

Chapter 5: Ethernet

Introduction to Networks v5.1

Chapter Outline

1. Introduction
2. Ethernet Protocol
3. LAN Switches
4. Address Resolution Protocol
5. Summary

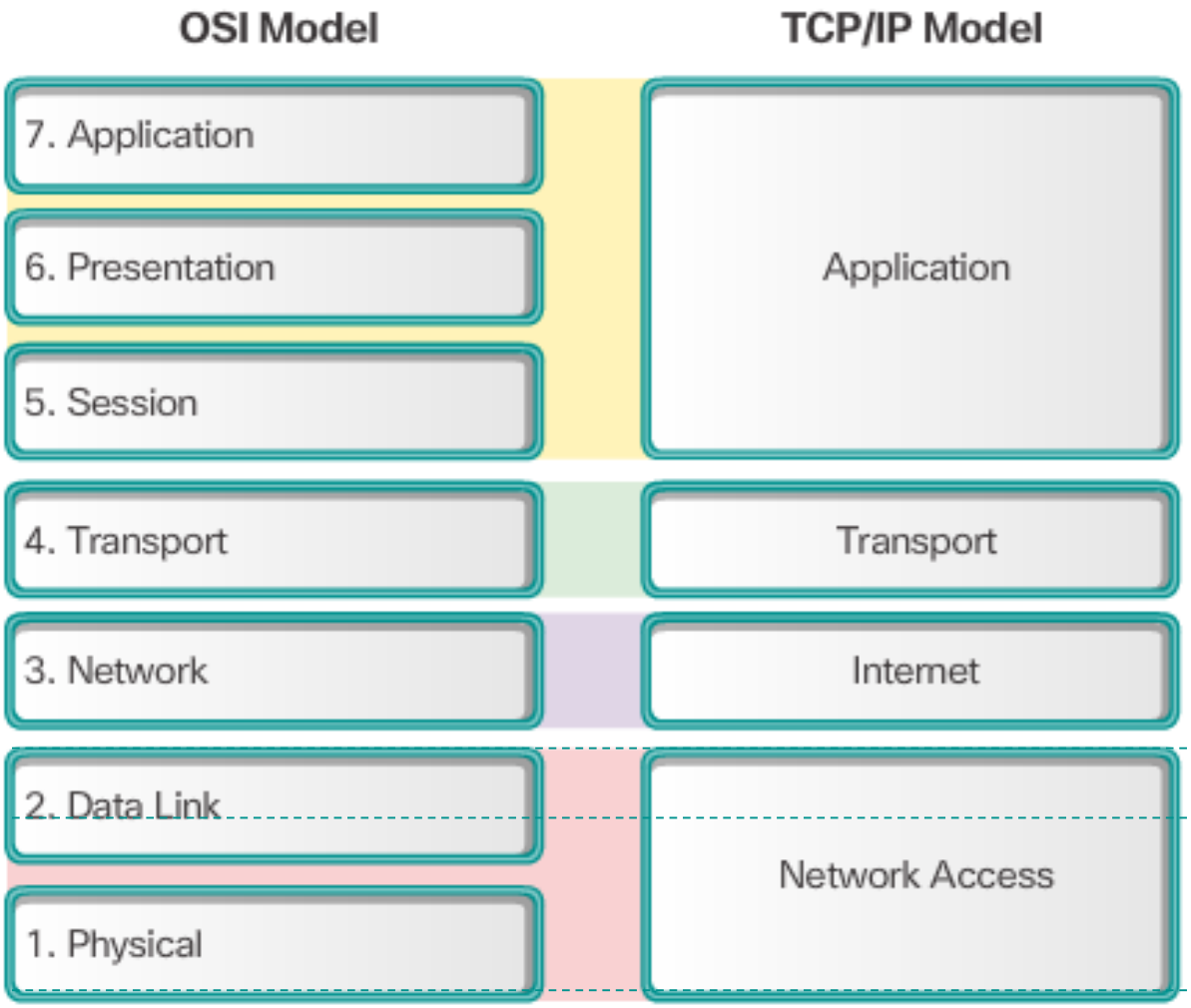
Section 5.1: Ethernet Protocol

Upon completion of this section, you should be able to:

- Explain how the Ethernet sublayers are related to the frame fields.
- Describe the Ethernet MAC address.

Topic 5.1.1: Ethernet Frame

Ethernet Protocol



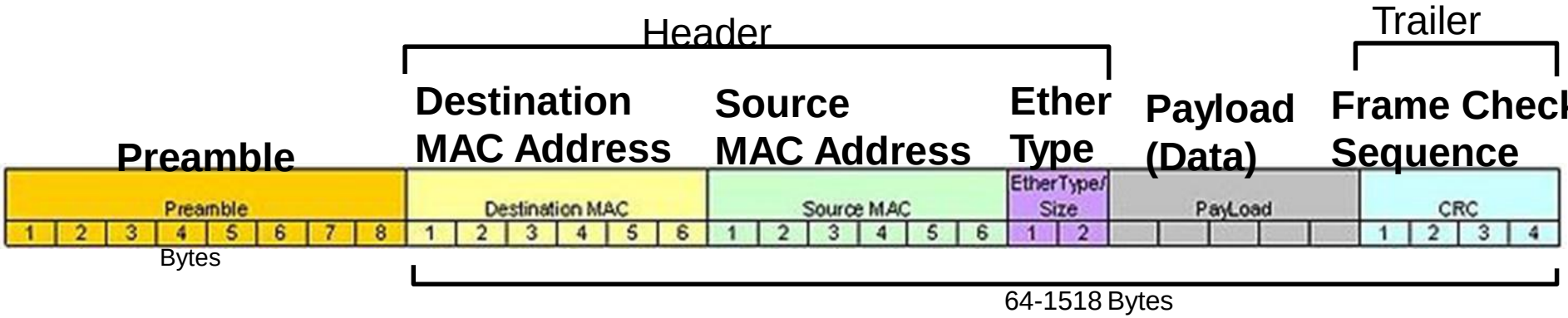
Ethernet

Logical Link Control - LLC

Media Access Control
MAC

Ethernet Encapsulation

IEEE 802.3 Standard / Ethernet II

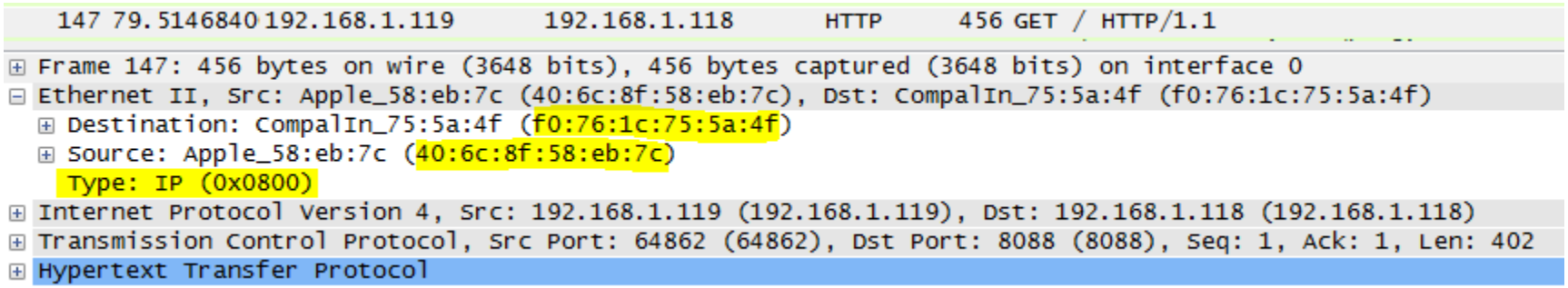


Preamble: sequence of 10101 for bit synchronization
Destination and Source MAC Address:
EtherType: Identifies upper layer Protocol, see table below for examples
Frame Check Sequence: Redundant information for error detection

EtherType for some notable protocols

EtherType	Protocol
0x0800	Internet Protocol version 4 (IPv4)
0x0806	Address Resolution Protocol (ARP)
0x0842	Wake-on-LAN[6]
0x22F3	IETF TRILL Protocol
0x6003	DECnet Phase IV
0x8035	Reverse Address Resolution Protocol

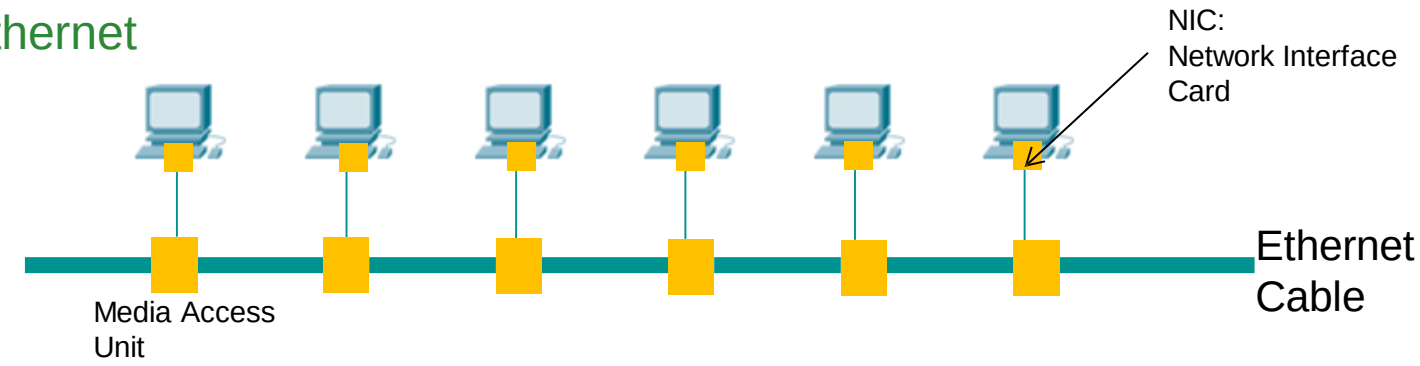
Wireshark Capture



Media Access Control

- Media Access Control Protocol:
  - CSMA/CD: Carrier Sense Multiple Access / Collision Detection
- Ethernet is a “Local Area Network”
  - It is a layer 2 protocol intended for multiple user access

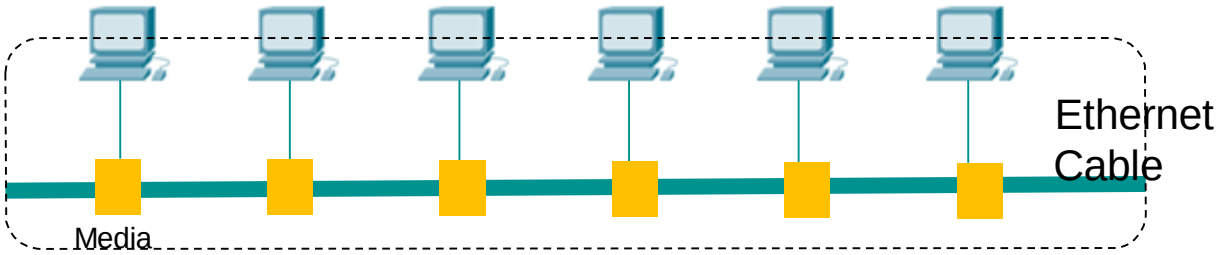
Legacy Ethernet



- Each station is electrically attached to the shared Ethernet cable using a MAU
- Ethernet CSMA/CD Protocol
  1. A station listens for a signal on the Ethernet Cable
  2. If no signal is heard then the station transmits the frame and listens for collisions
  3. If a collision occurs, then delay a random backoff wait-time and retry
  4. End device whose MAC Addresses matches the Destination Address reads the frame

Collision Domain & Broadcast Domain: Ethernet Cable and Hubs

Legacy Ethernet



Collision Domain = Broadcast Domain

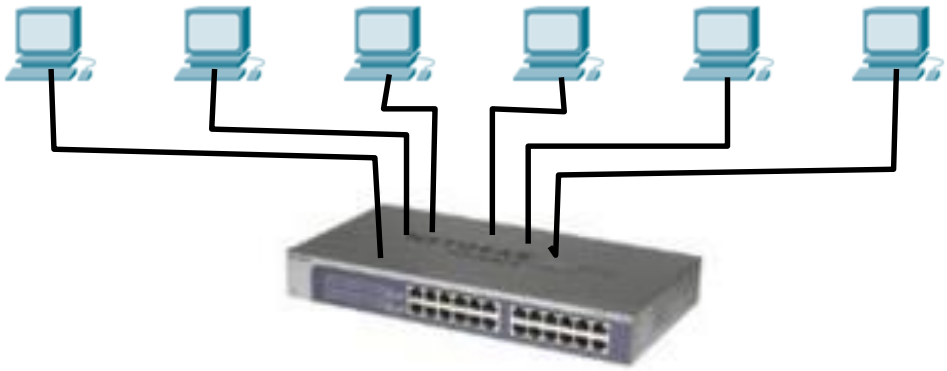
Collision Domain:

- When a device sends **any frame** (excluding broadcast), the collision domain is the extent of the network to which the frame reaches including the interfaces of end devices. If two end devices in the same collision domain send a frame at the same time, they will collide and interfere with each other. The end devices will need to resend the frame.

Broadcast Domain:

- When a device sends a **broadcast frame**, the broadcast domain is the extent of the network to which the frame reaches including the interfaces of end devices. If two end devices in the same broadcast domain send a broadcast frame at the same time, they will collide and interfere with each other. The end devices will need to resend the frame.

Ethernet Evolution



1. Ethernet Hub replaces Ethernet Cable
   Hub operation is nearly identical to Ethernet Cable with MAUs

2. Ethernet Switch replaces Ethernet Hub
   Switch operation explained in later slides

Topic 5.1.2:
Ethernet MAC Address

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

4 bits = 1 nibble
8 bits = 1 byte
8 bits = 1 octet
4 bits = 1 hex digit

MAC Address and Hexadecimal (cont.)

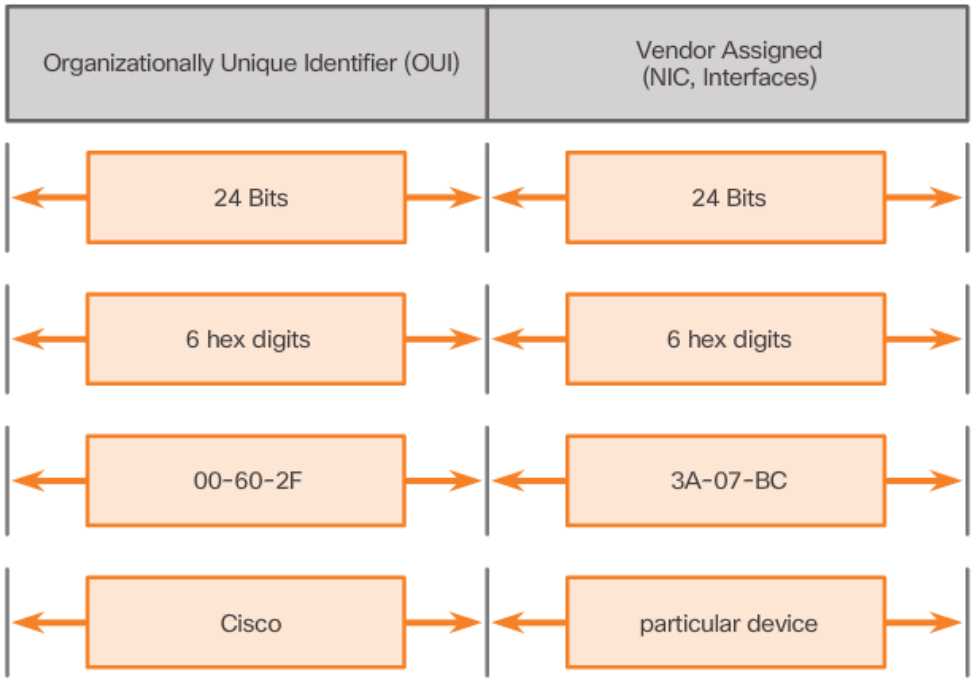
Hexadecimal Numbering

Selected Decimal, Binary, and Hexadecimal equivalents

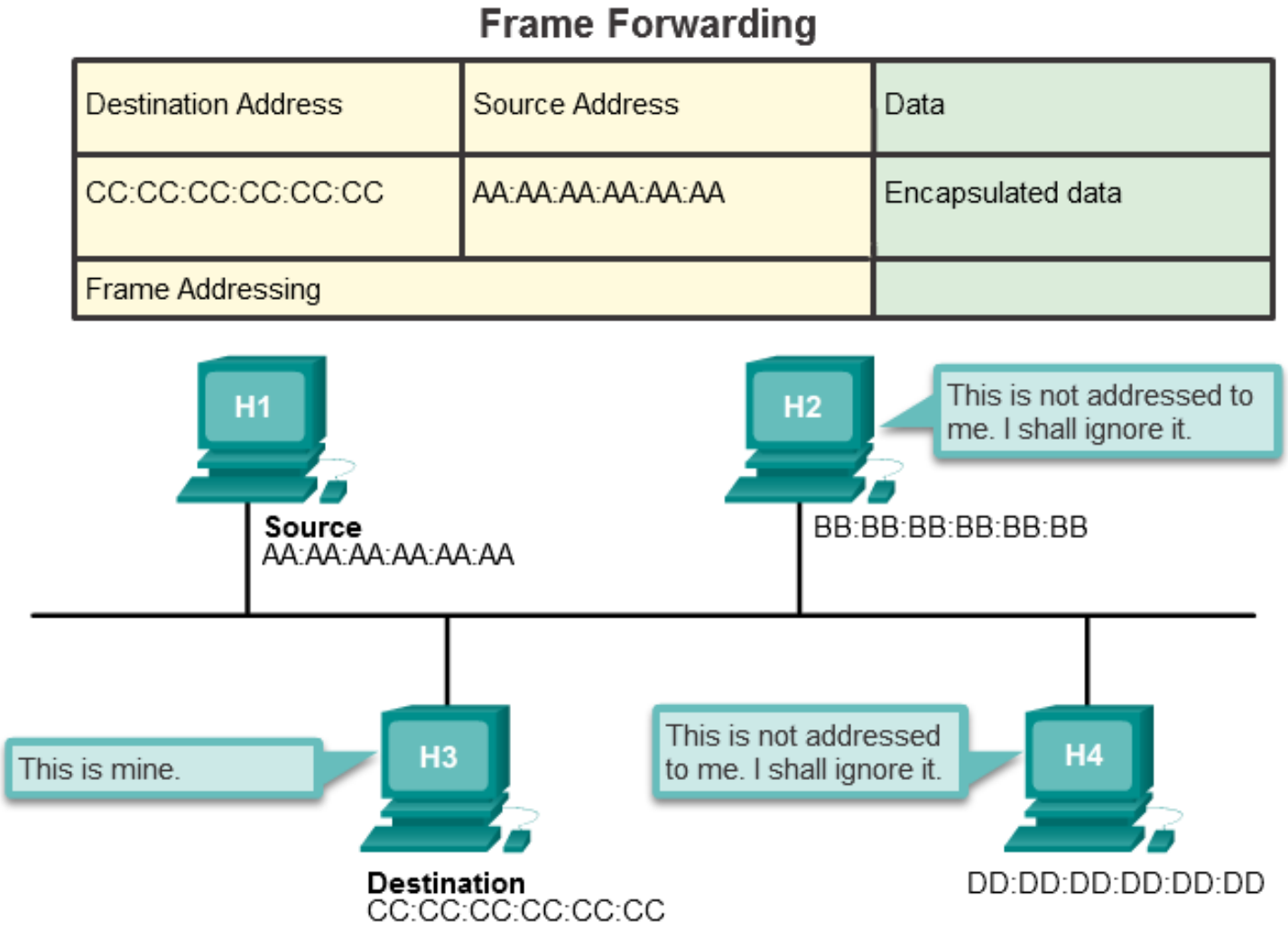
Decimal	Binary	Hexadecimal
0	0000 0000	00
1	0000 0001	01
2	0000 0010	02
3	0000 0011	03
4	0000 0100	04
5	0000 0101	05
6	0000 0110	06
7	0000 0111	07
8	0000 1000	08
10	0000 1010	0A
15	0000 1111	0F
16	0001 0000	10
32	0010 0000	20
64	0100 0000	40
128	1000 0000	80
192	1100 0000	C0
202	1100 1010	CA
240	1111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

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.



Frame Processing



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.

MAC Address Representations

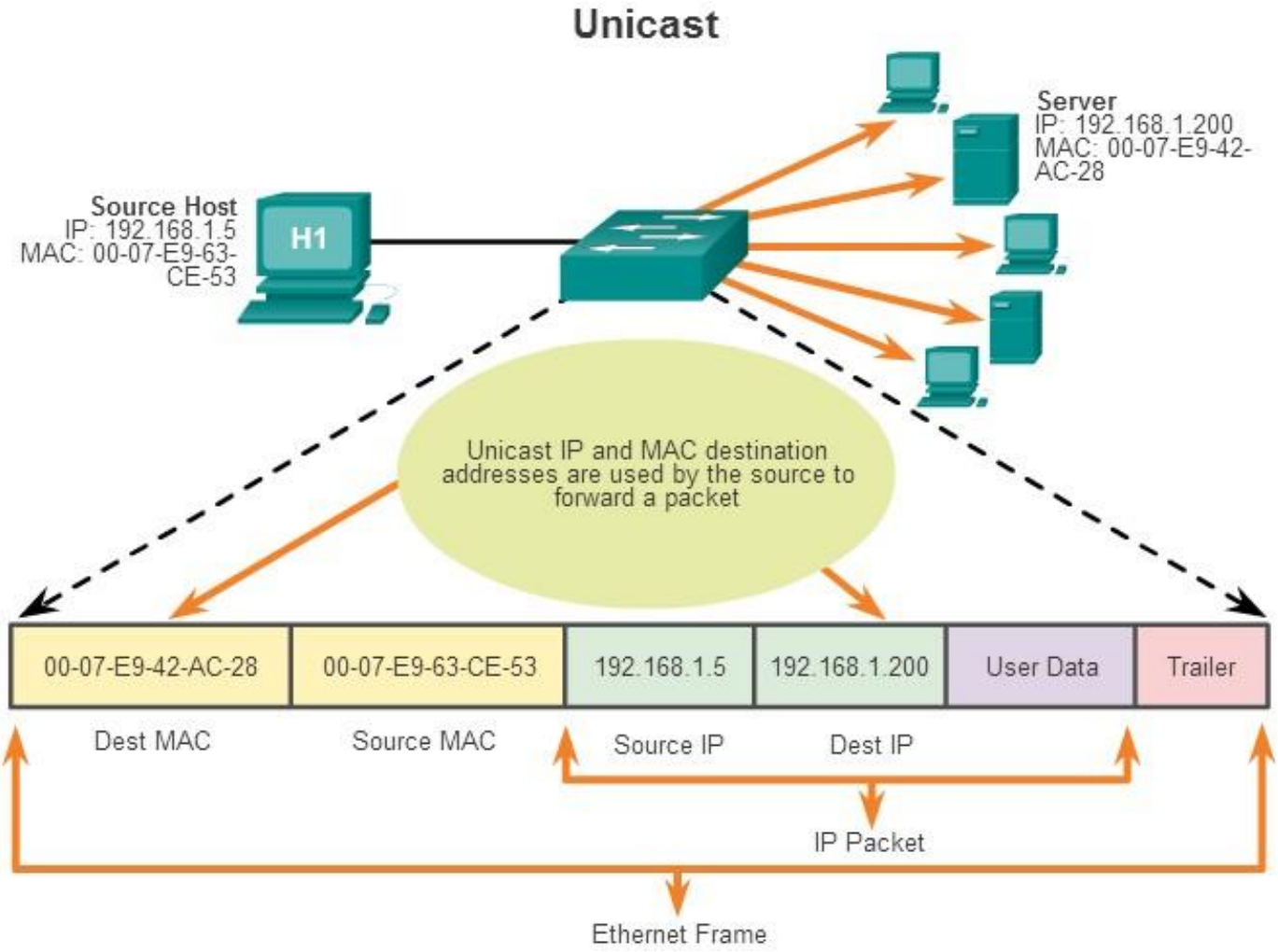
With Dashes 00-60-2F-3A-07-BC

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

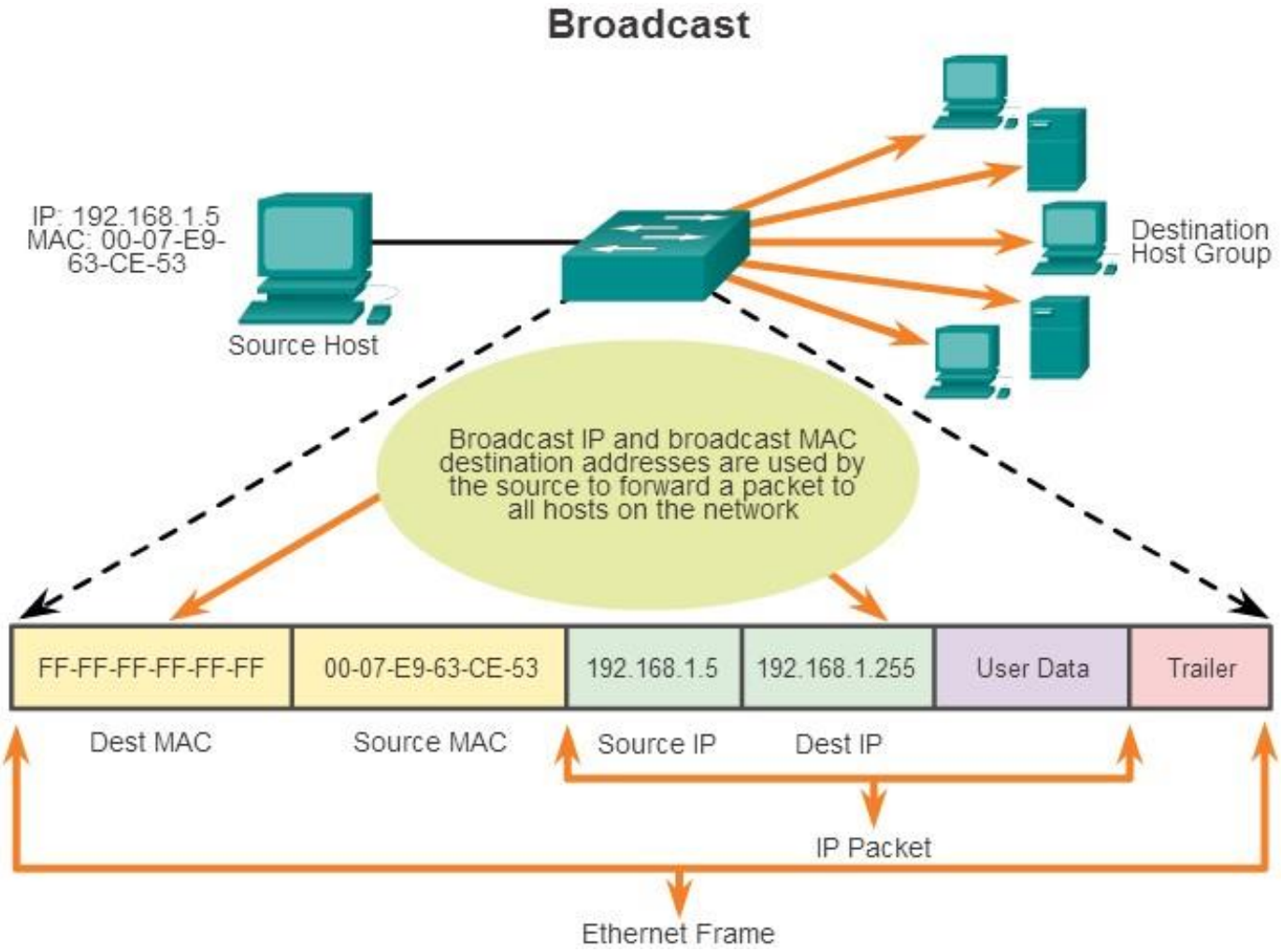
With Periods 0060.2F3A.07BC

```
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
```

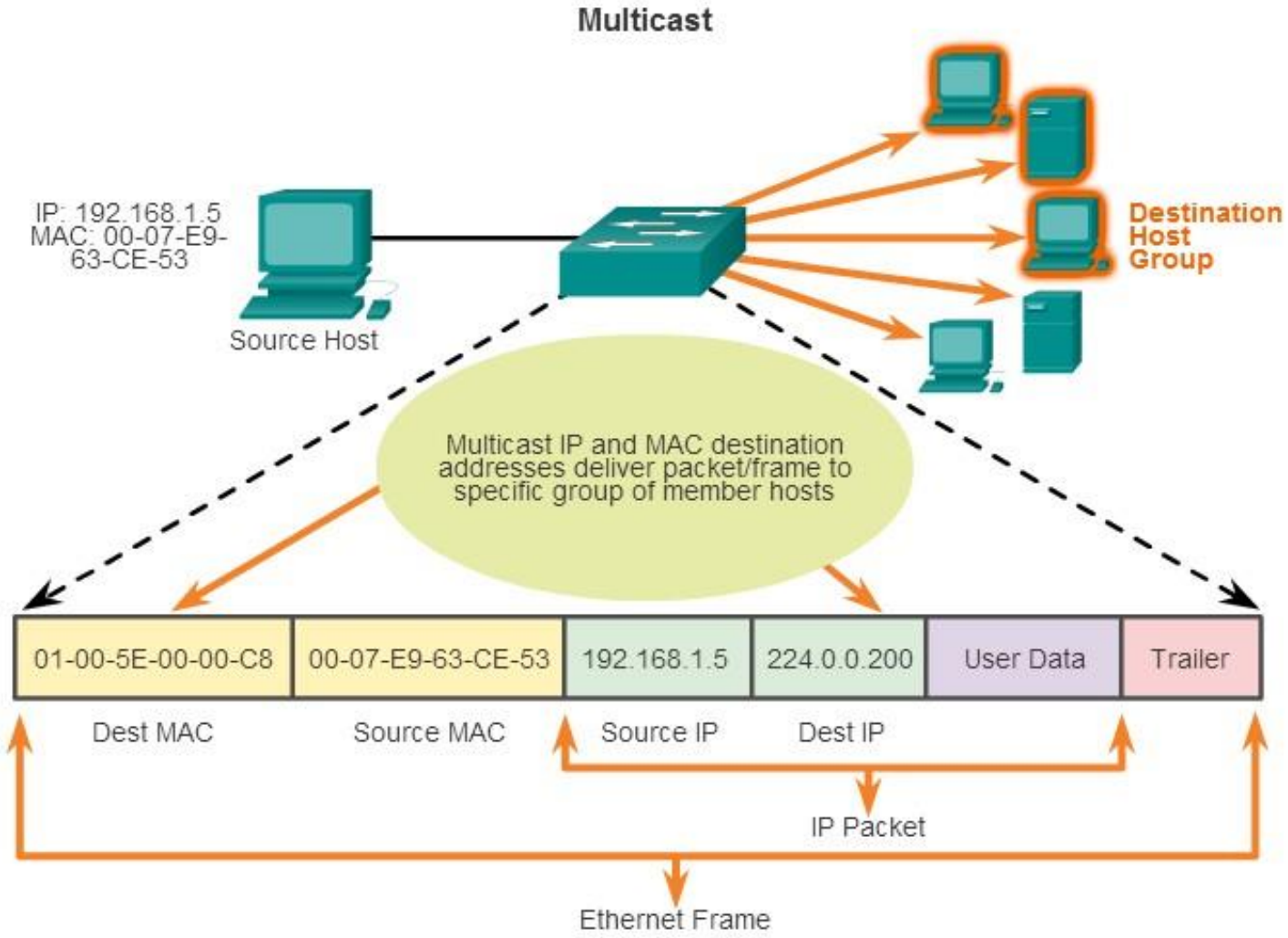
Unicast MAC Address



Broadcast MAC Address



Multicast MAC Address



Section 5.2: LAN Switches

Upon completion of this section, you should be able to:

- Explain how a switch operates.
- Explain how a switch builds its MAC address table and forwards frames.
- Describe switch forwarding methods.
- Describe the types of port settings available for Layer 2 switches.

Topic 5.2.1:
MAC Address Table

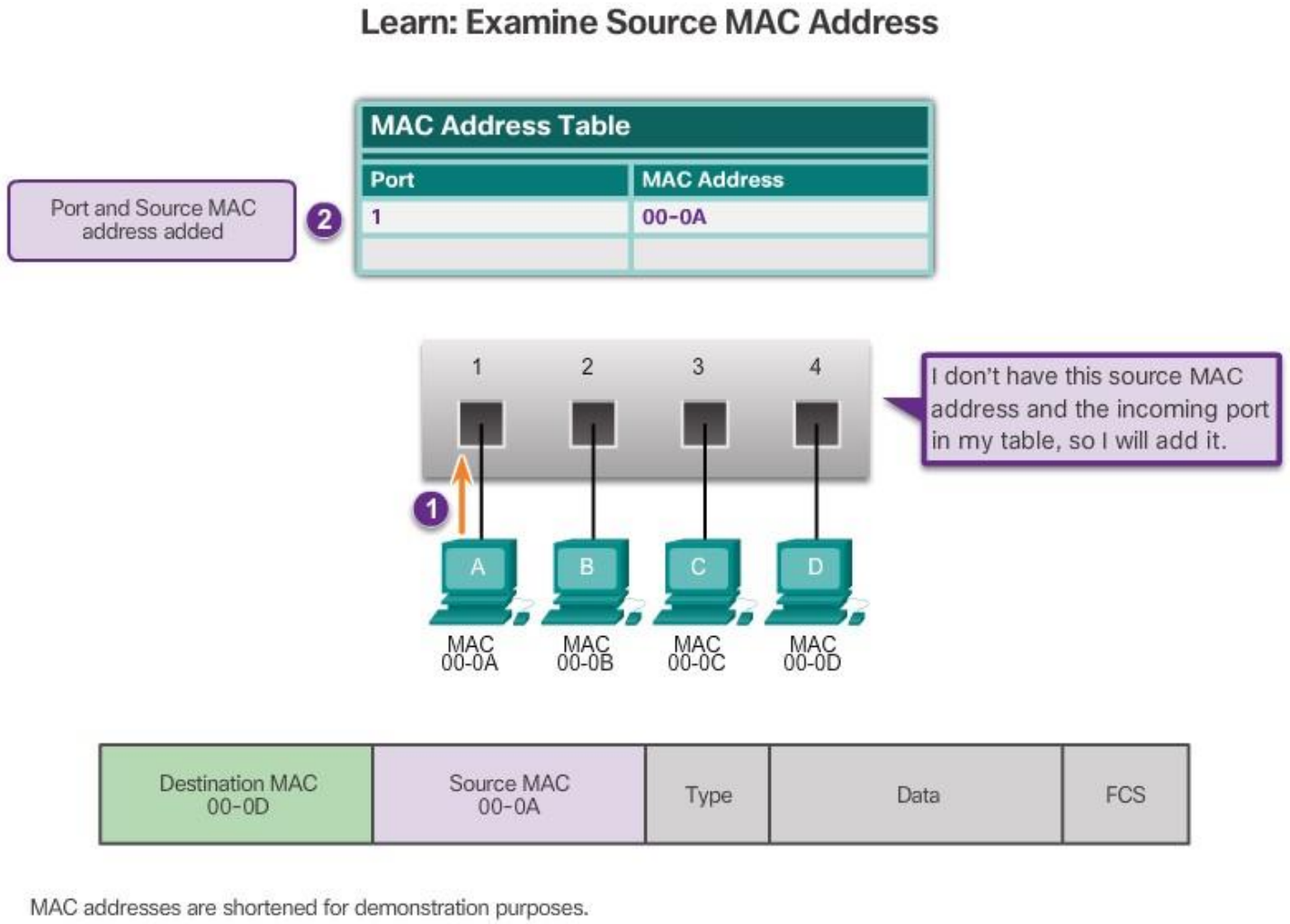
Switch Fundamentals

- 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.

Frame Forwarding = transferring an incoming to the correct outgoing port
Switching = Learning + Frame Forwarding (non standard definition)

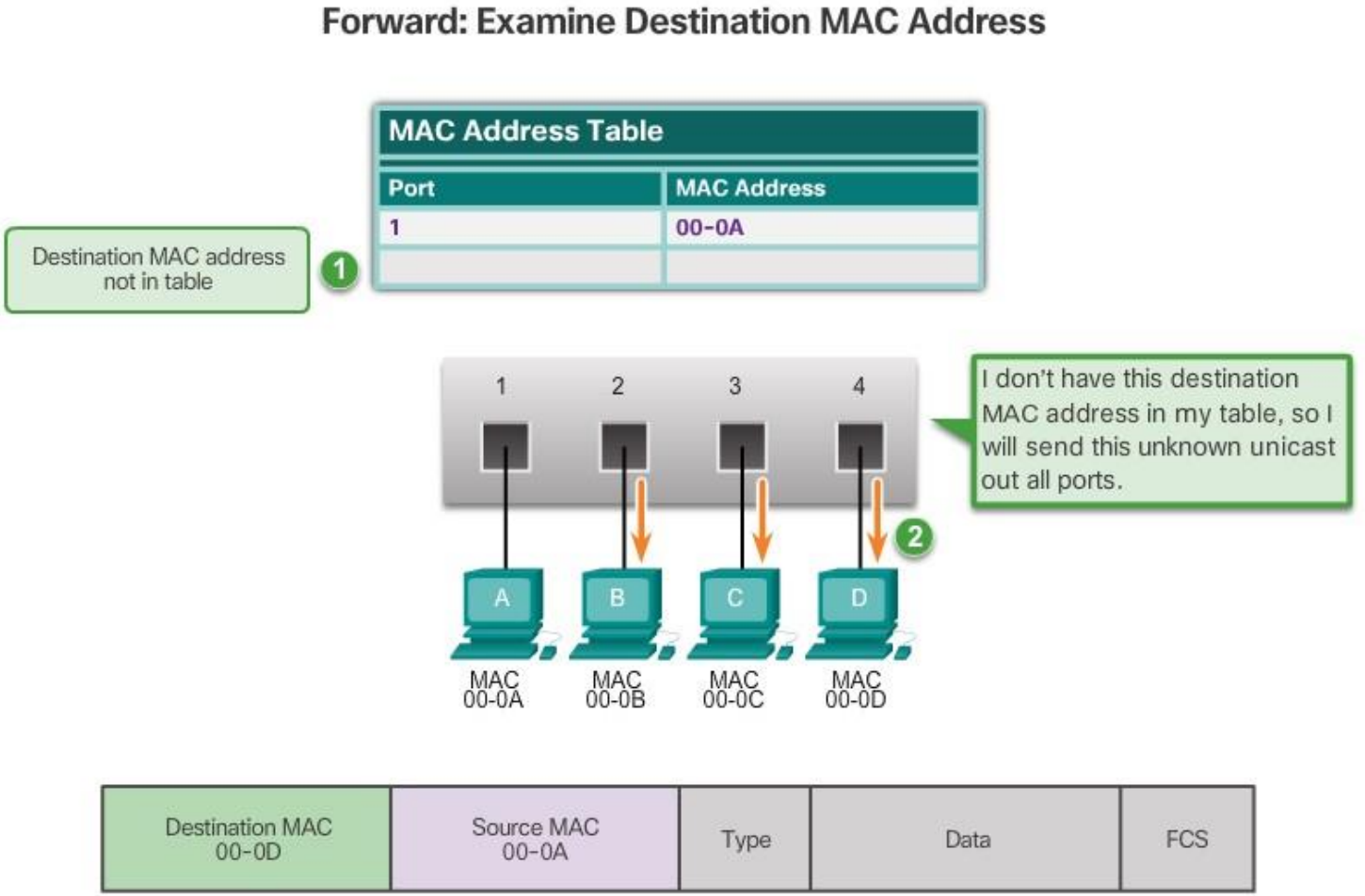
Layer 2 Switching - 1

Step 1: Learn MAC Address



Layer 2 Switching - 2

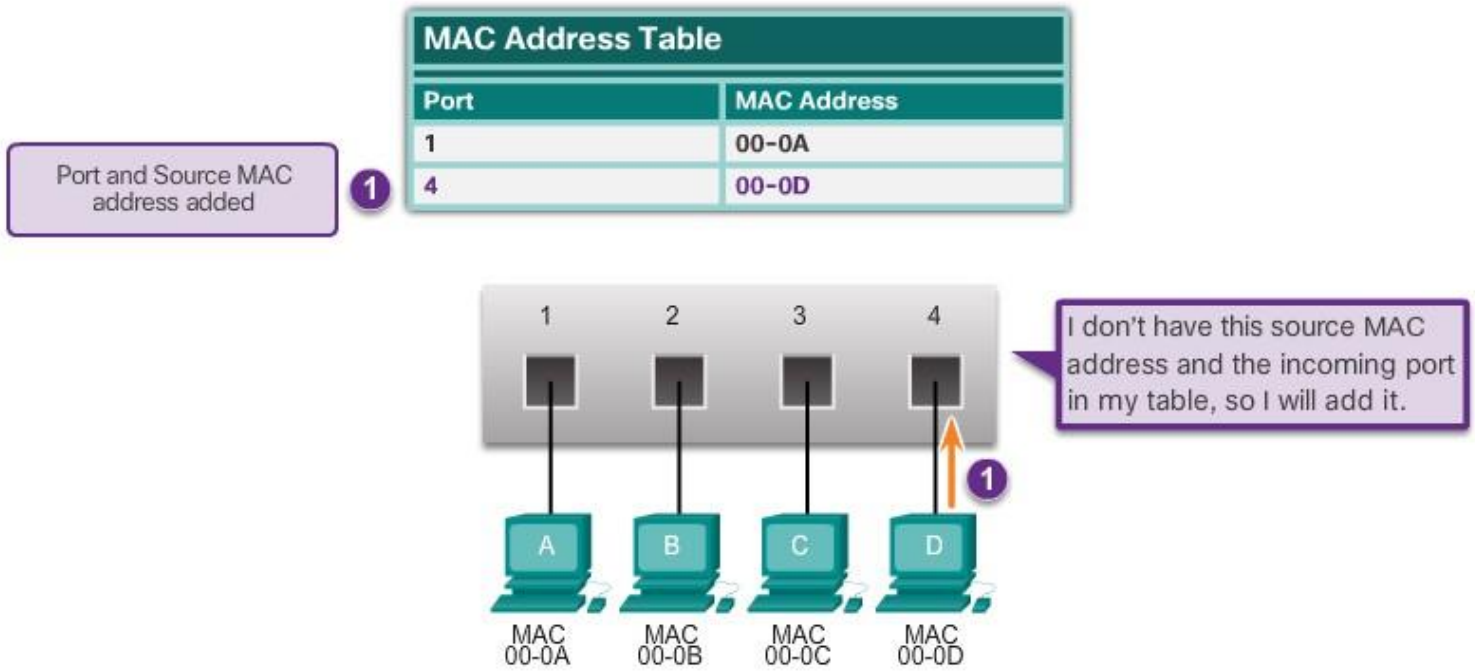
Step 2: Forward the Frame

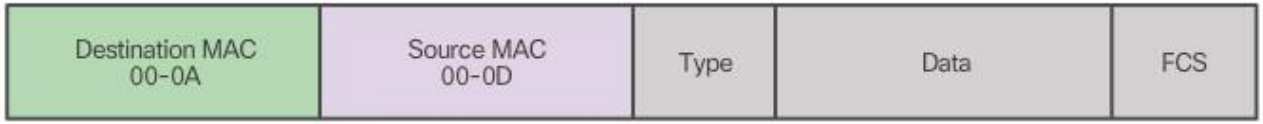


Layer 2 Switching – 3

Step 1: Learn MAC Address

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

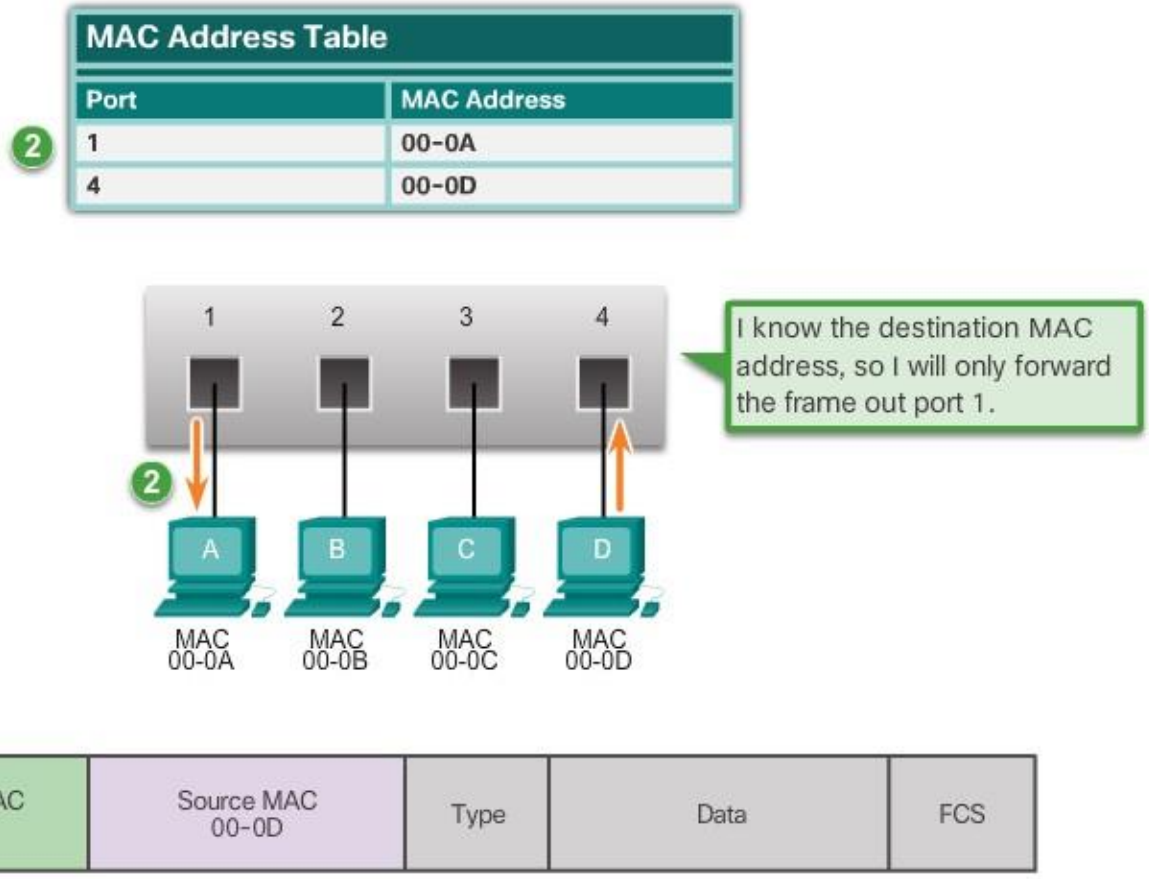




Layer 2 Switching - 4

Step 1: Forward the Frame

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

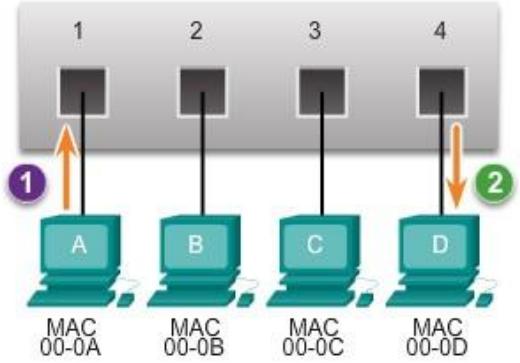


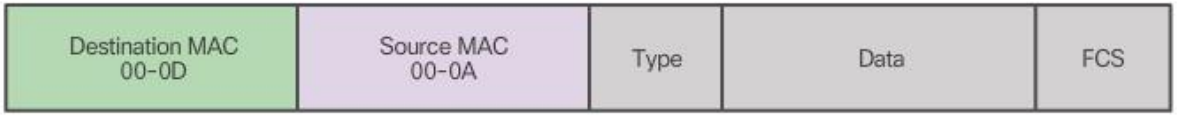
Layer 2 Switching – Forward Only

Step 1: Forward the Frame

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





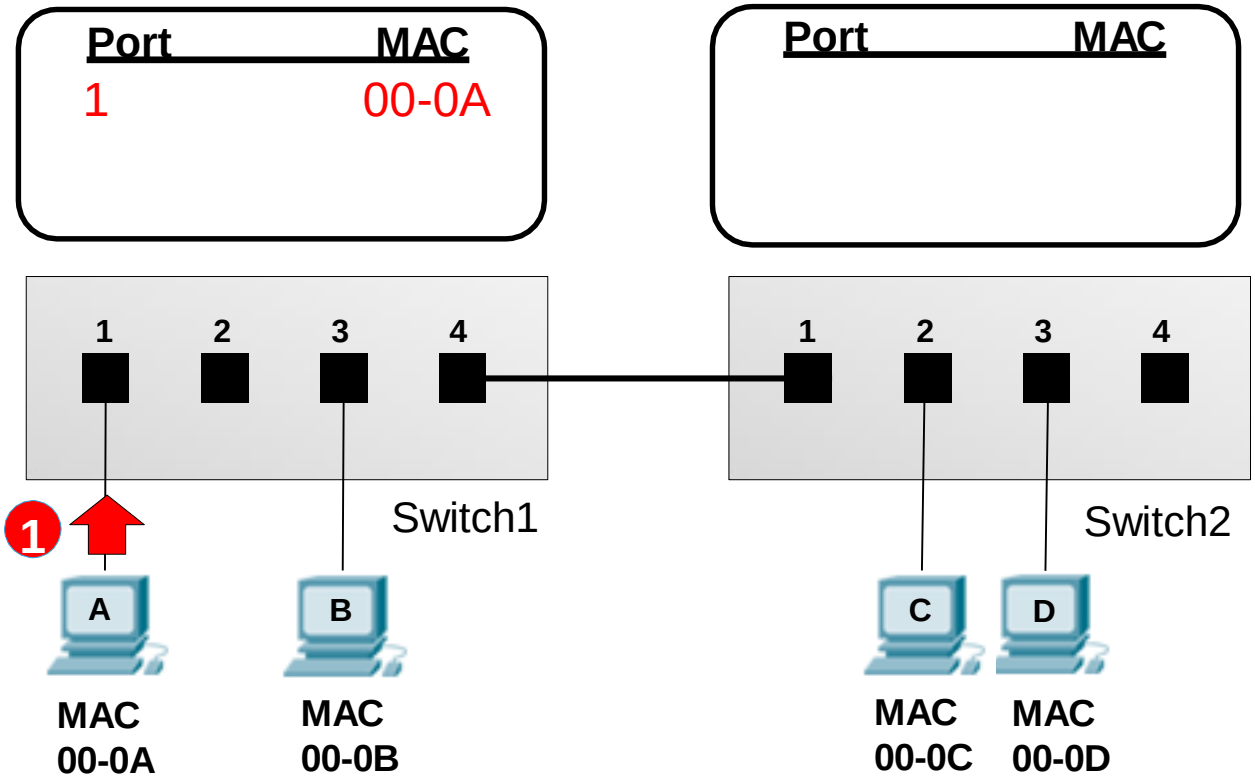
Video Demonstration – MAC Address Tables on Connected Switch

- 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 on Network Academy Book

  Section 5.2.1.4

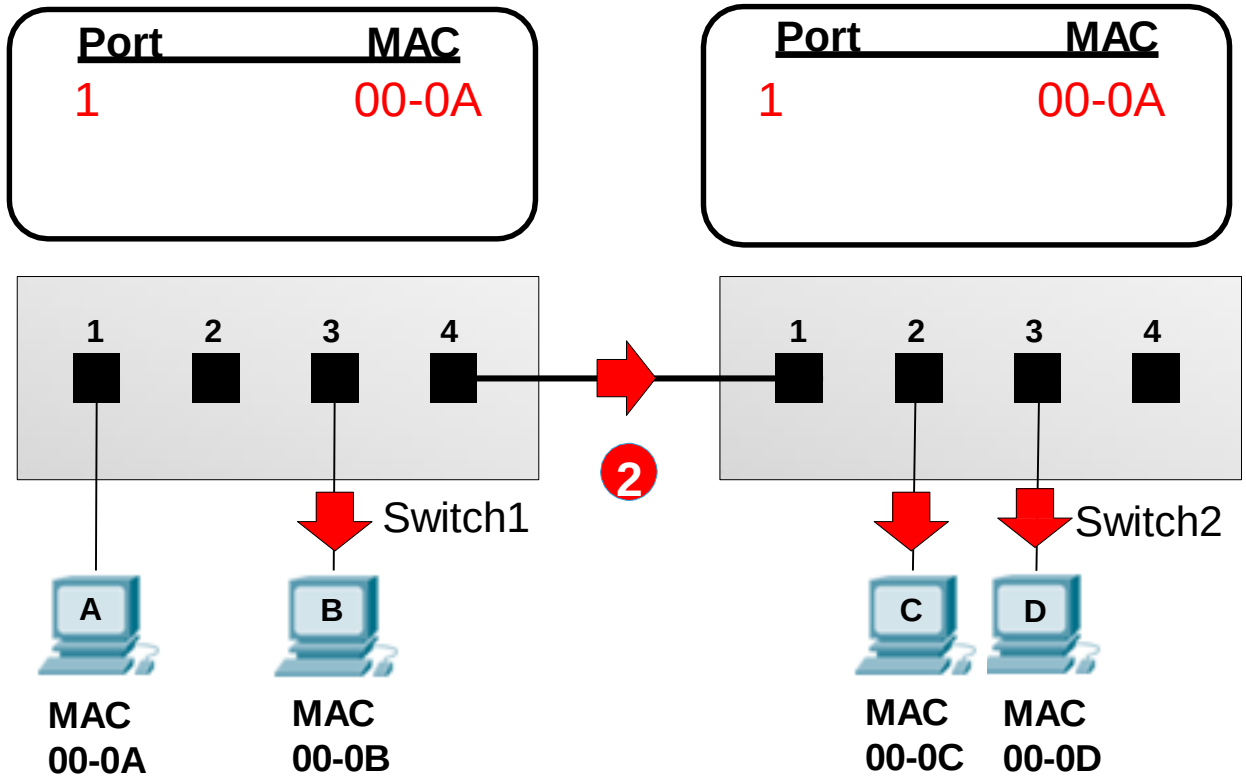
Layer 2 Switching to Connected Switch - 1

- PC-A sends a Frame to PC-C,
- If Switch1 does not have the source MAC Addr in its MAC Address Table
  - Then Switch1 learns the Addr and adds it to its MAC Address Table,



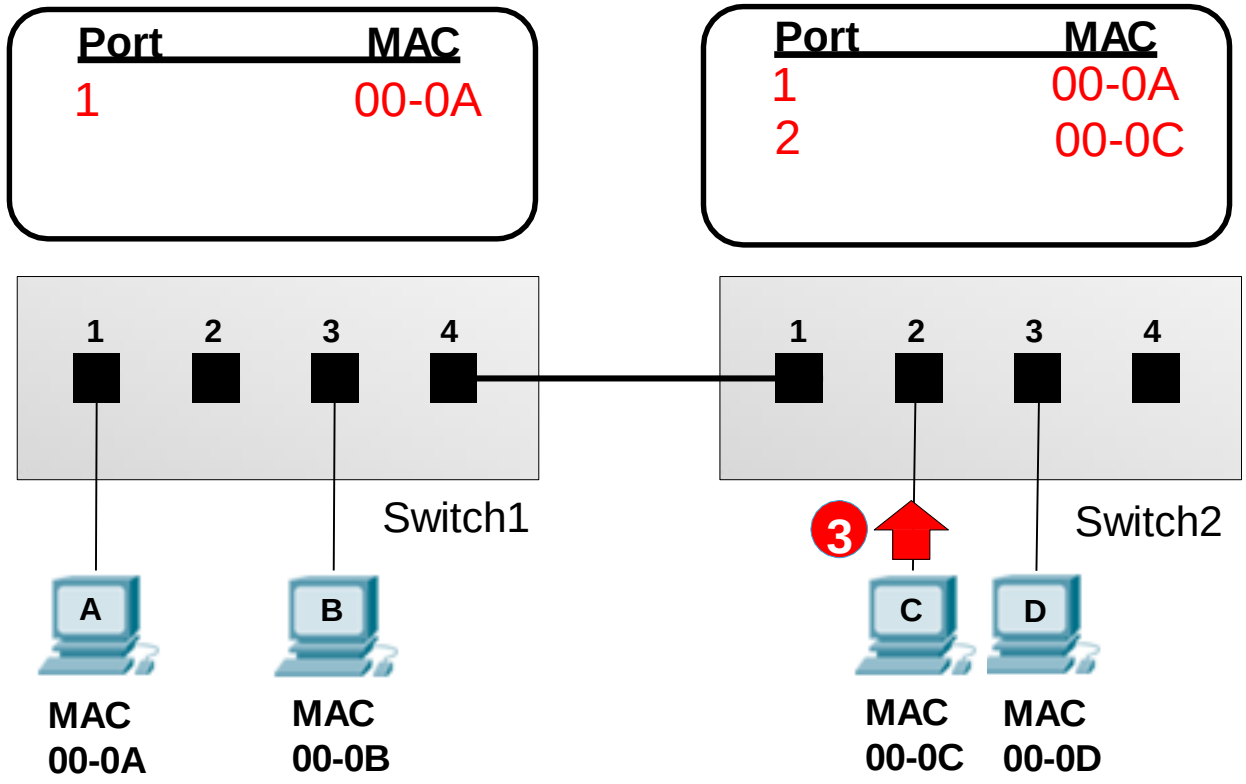
Layer 2 Switching to Connected Switch - 2

- Switch1 does not have the destination MAC in its MAC Address Table,
- Switch1 floods the frame out all ports except source port,
- Switch2 learns the MAC Addr and adds it to its MAC Address Table
- PC-C reads the frame and other PCs ignore the frame.



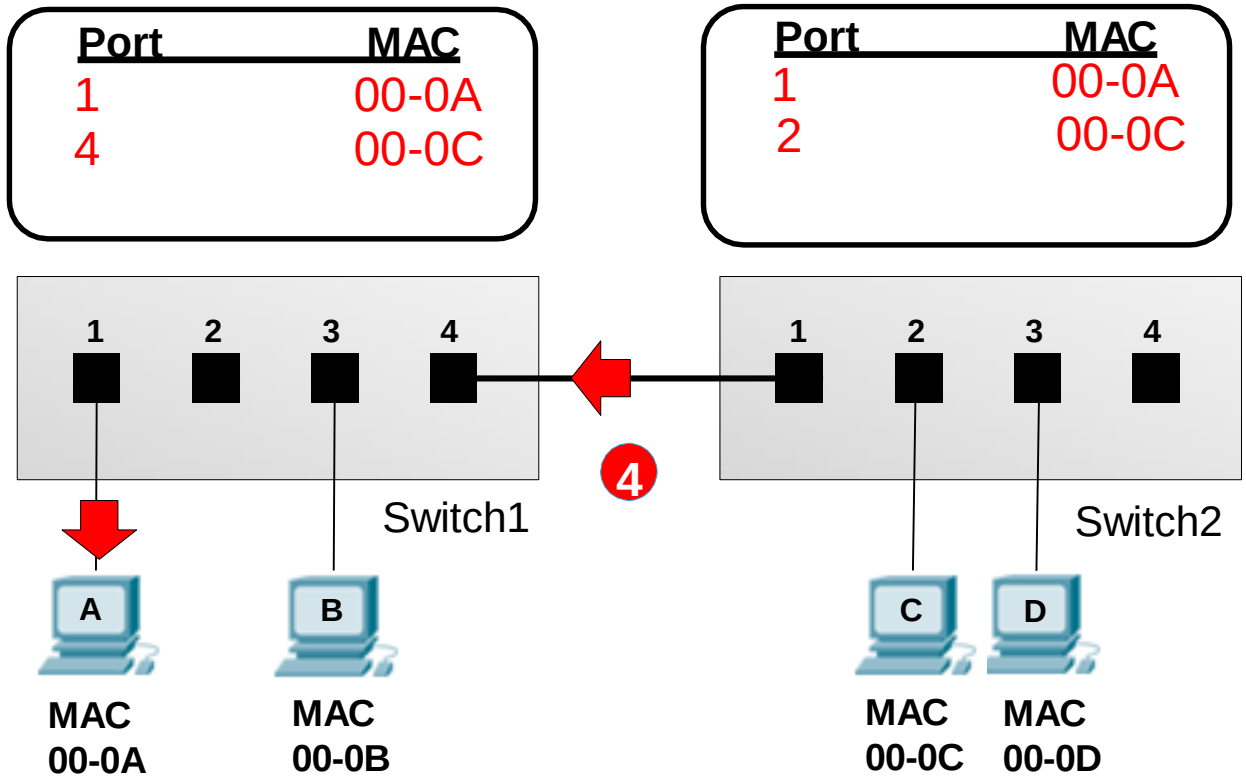
Layer 2 Switching to Connected Switch - 3

- PC-C sends a reply frame to PC-A,
- If Switch2 does not have the source MAC in its MAC Address Table
  - Switch2 adds it to its MAC Address Table,



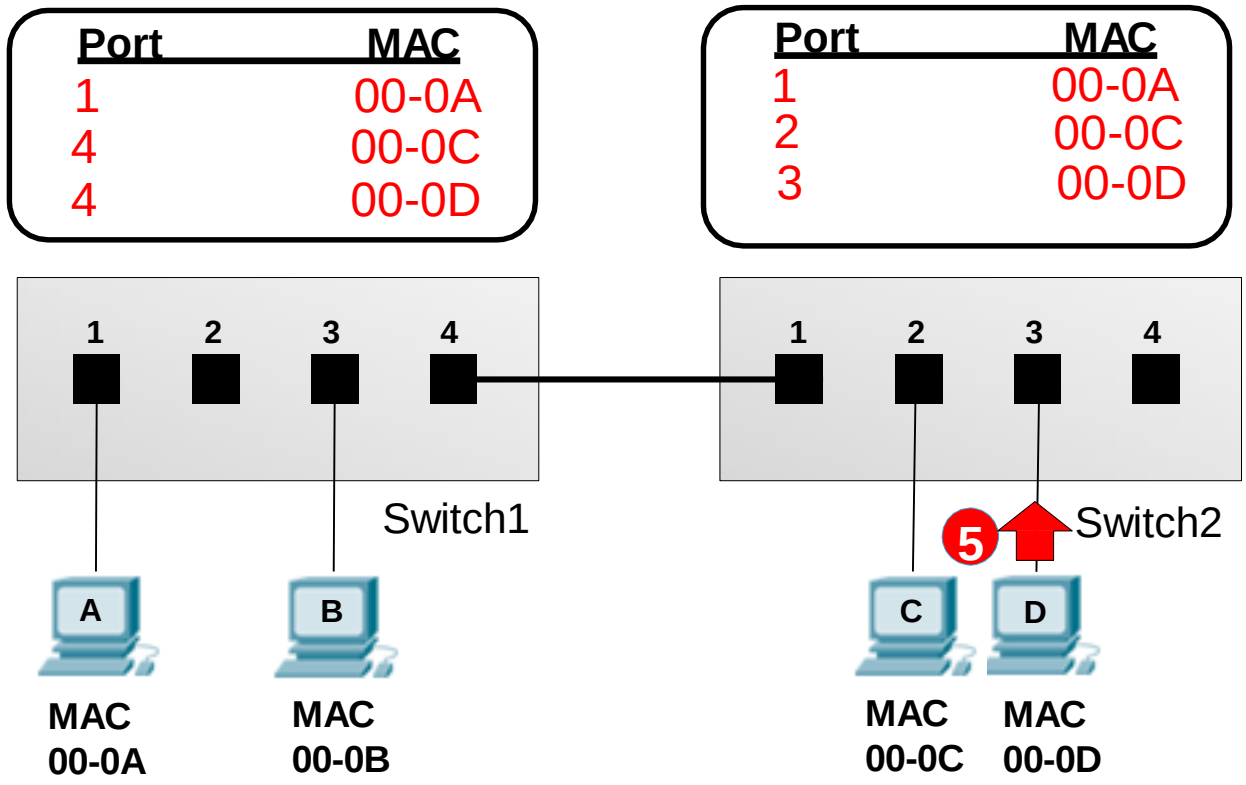
Layer 2 Switching to Connected Switch - 4

- Switch2 has the destination MAC Addr in its MAC Address Table
- Switch1 learns of PC-C and adds the MAC Addr to its MAC Address Table
- PC-A reads the frame



Layer 2 Switching to Connected Switch - 5

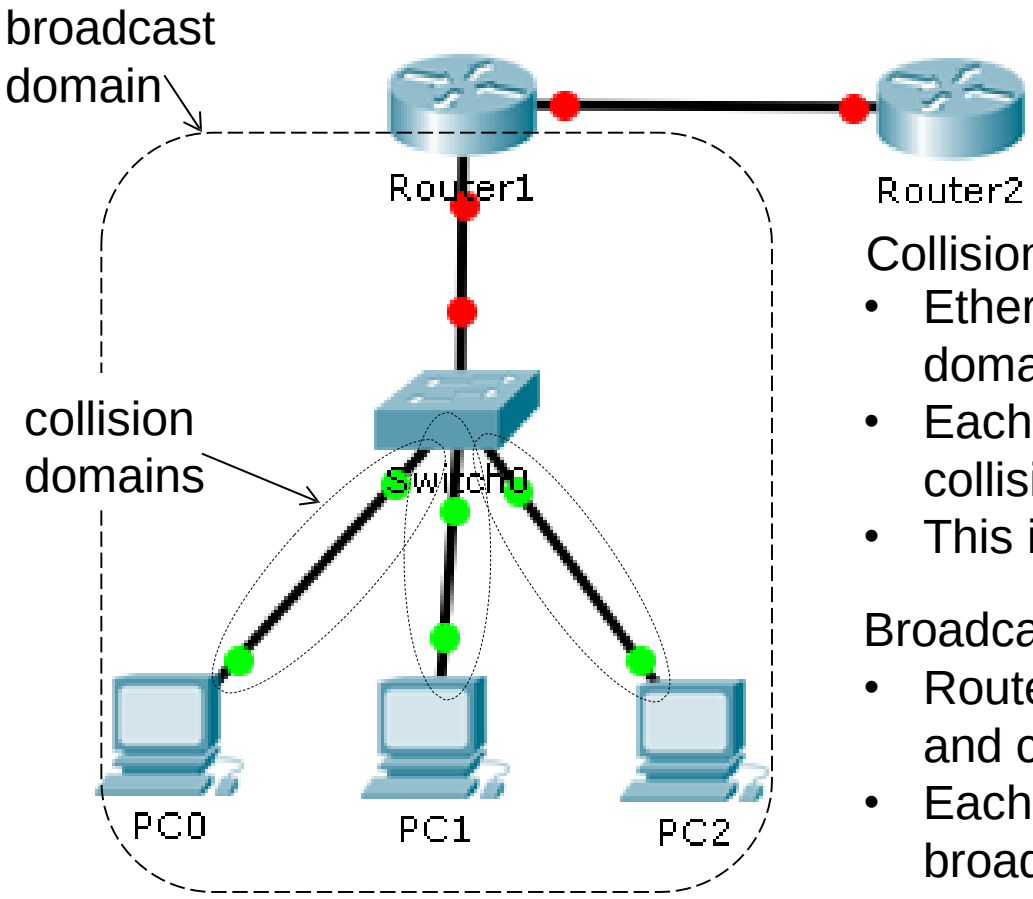
- If PC-D sends a frame to PC-A, then Switch1 will have two entries for port 4



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

Collision Domain & Broadcast Domain: Ethernet Switched Network



Collision Domain:

- Ethernet Switches break up collision domains into point-to-point links.
- Each Switch port forms a separate collision domain
- This is due to the switching function

Broadcast Domain:

- Routers break up broadcast domains and collision domains
- Each Router port forms a separate broadcast domain
- Routers do not forward broadcasts
- The switch prevents collisions in the broadcast domain.

This is important for capacity planning

Topic 5.2.2:
Switch Forwarding Methods

Frame Forwarding Methods on Cisco Switches

Store-and-forward

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

Cut-through

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

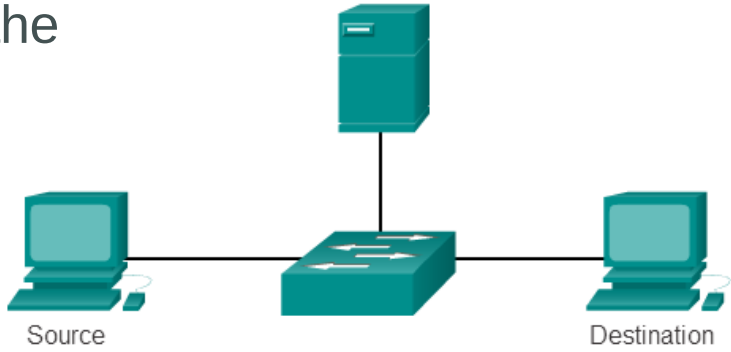
Cut-Through Switching

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.

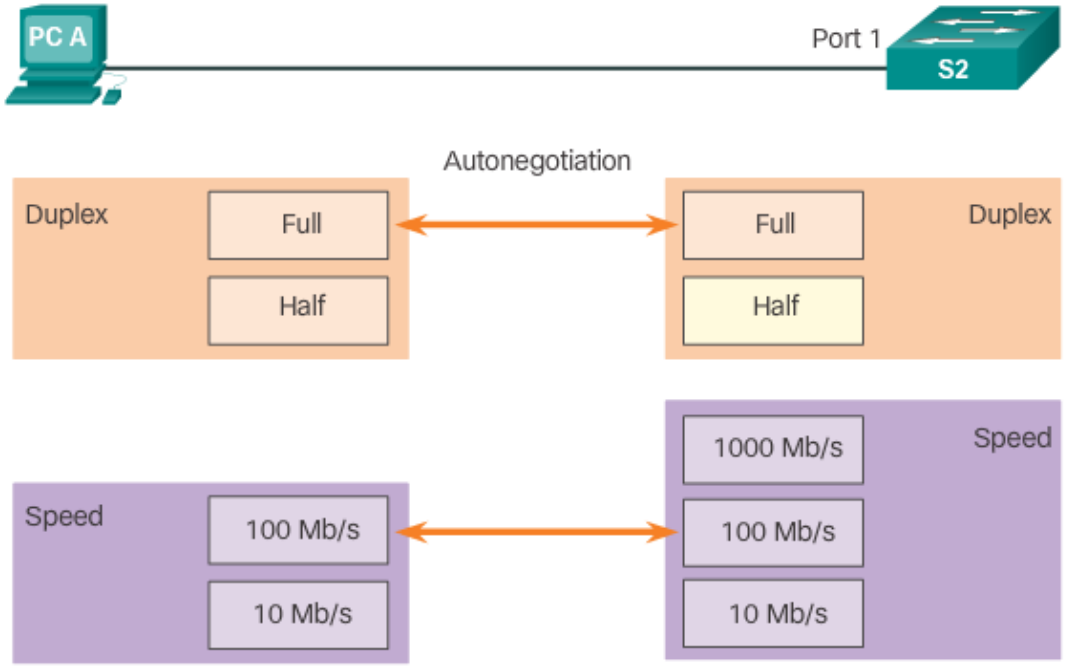


A cut-through switch forwards the frame before it is entirely received. At a minimum, the destination address of the frame must be read before the frame can be forwarded.

Topic 5.2.3:
Switch Port Settings

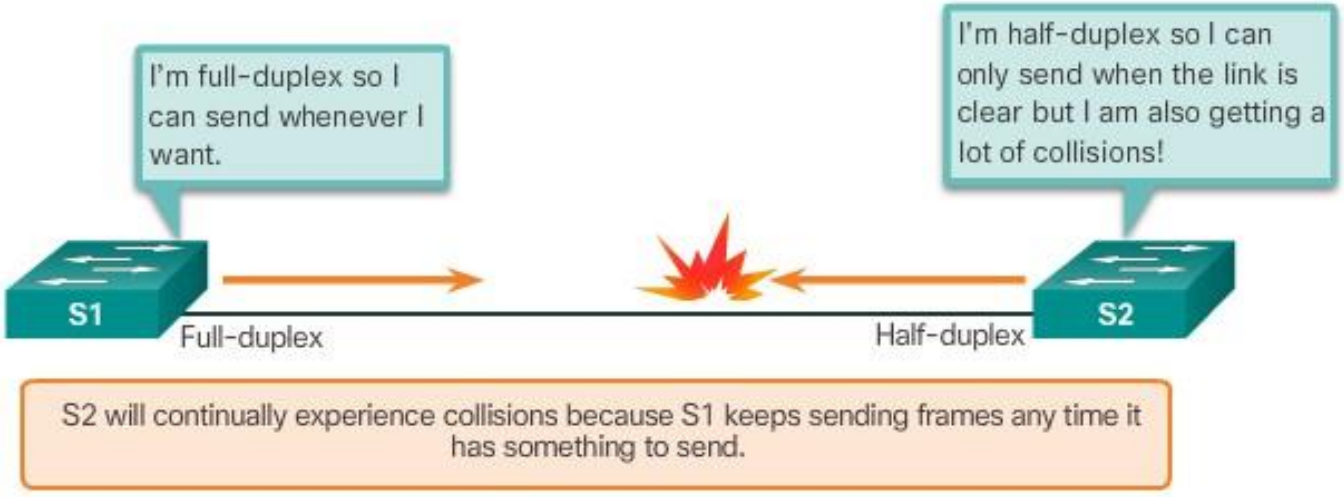
Duplex and Speed Settings

- 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.



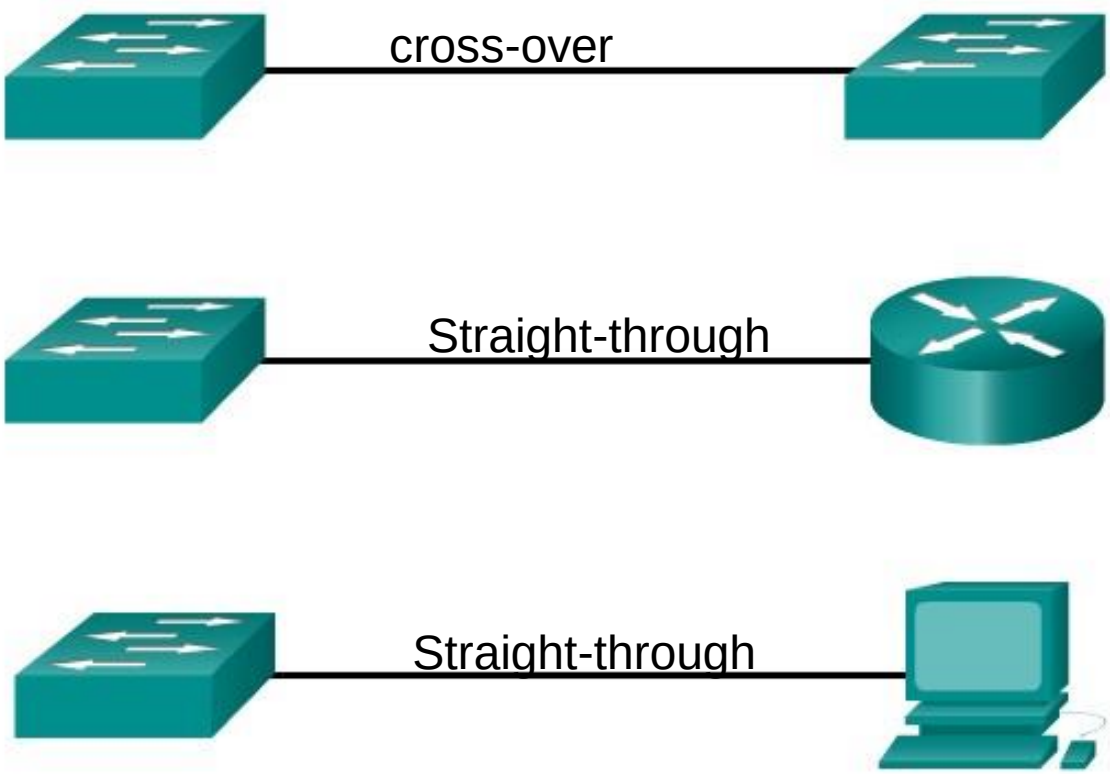
Duplex and Speed Settings (cont.)

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.



Auto-MDIX (Media Dependent Interface Exchange)

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



Section 5.3: Address Resolution Protocol

Upon completion of this section, you should be able to:

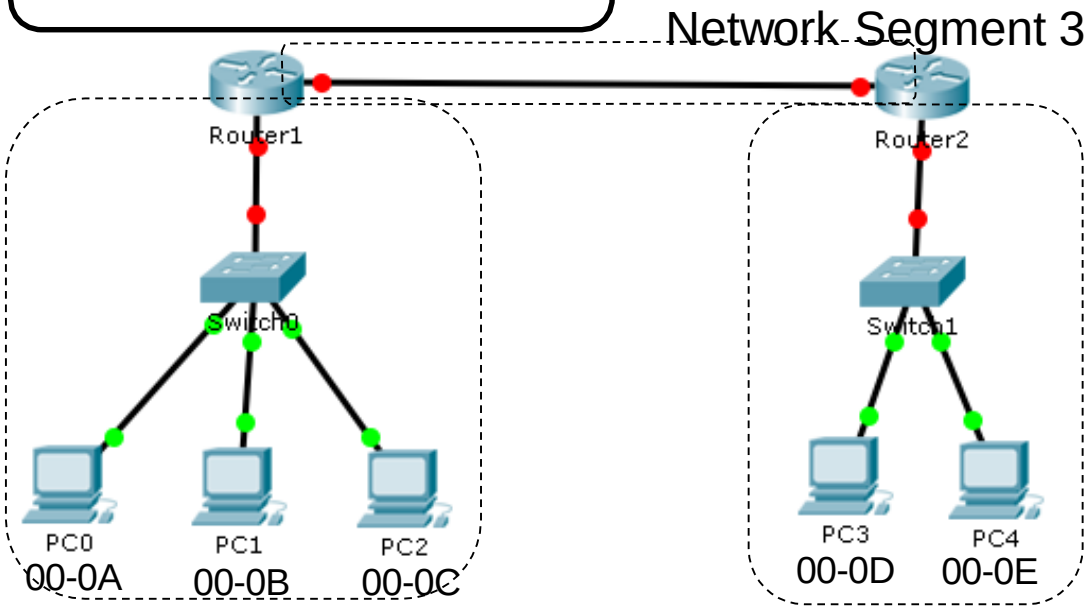
- Compare the roles of the MAC address and the IP address.
- Describe the purpose of ARP.
- Explain how ARP requests impact network and host performance.

Topic 5.3.1: MAC and IP

IP Packet Forwarding

Routing Table

Dest Network	Next Hop
192.168.2.0/24	IPAddr of Rtr i/f



Network Segment 1

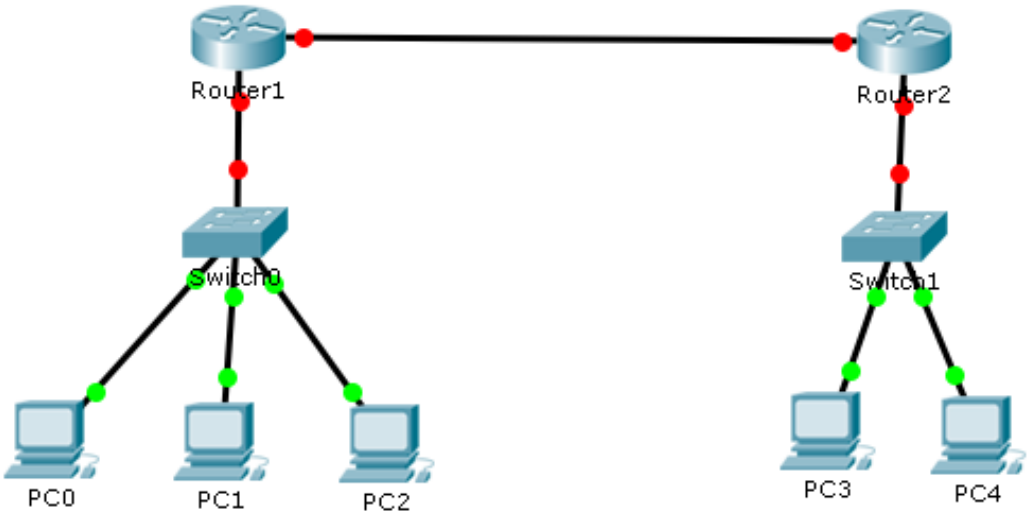
IP Network Address:
192.168.**1**.0
255.255.255.0

Network Segment 2

IP Network Address:
192.168.**2**.0
255.255.255.0

- Ethernet Switches forward frames between end devices that are on the same network segment using MAC addresses.
- Routers forward packets to remote networks and network segments using IP Addresses.
- Router interfaces define a network segment.
- Each end device will have an IP Address whose Network Address is the same as the Network segment.
- End devices with the same network address are on the same network segment.

Question



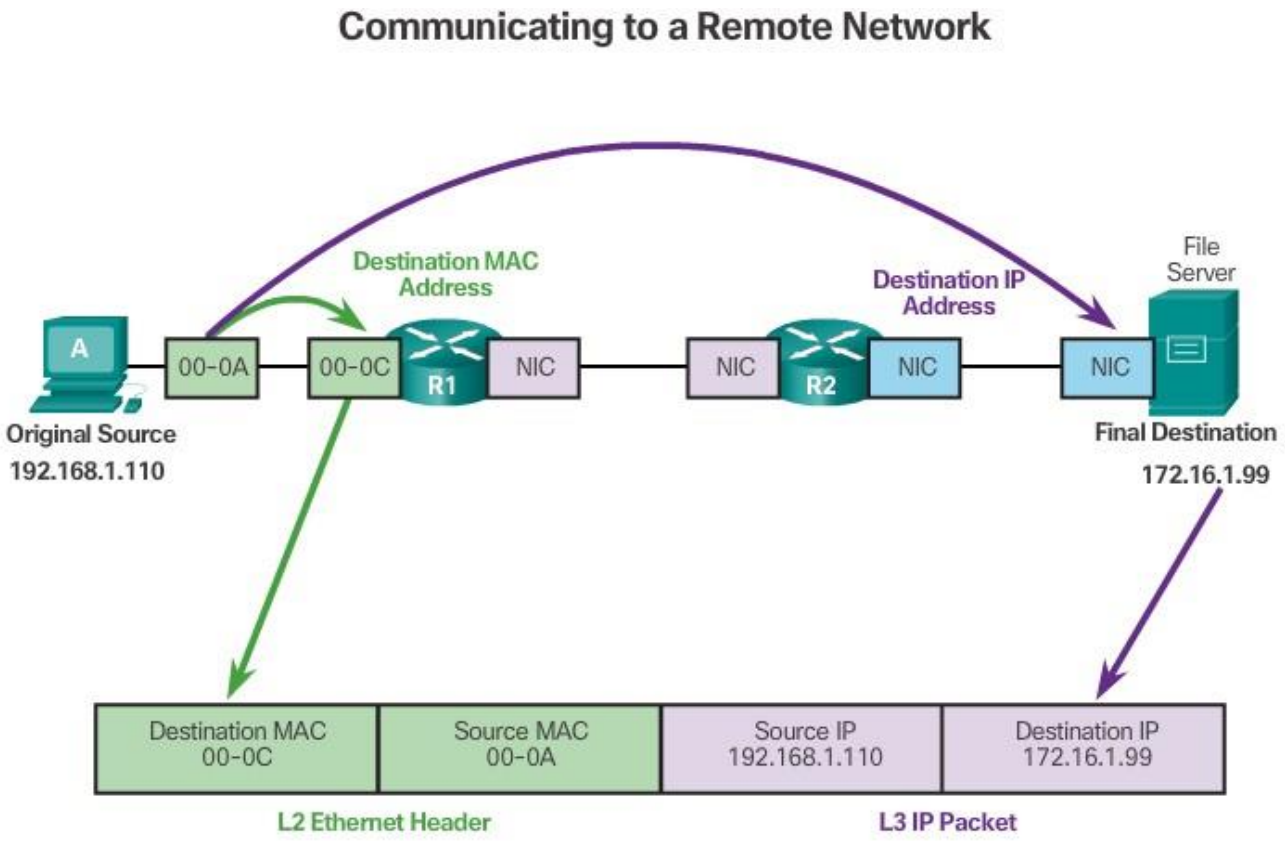
How many collision domains are in the network?

A) 3
B) 5
C) 7
D) 8

How many broadcast domains are in the network?

A) 3
B) 5
C) 7
D) 8

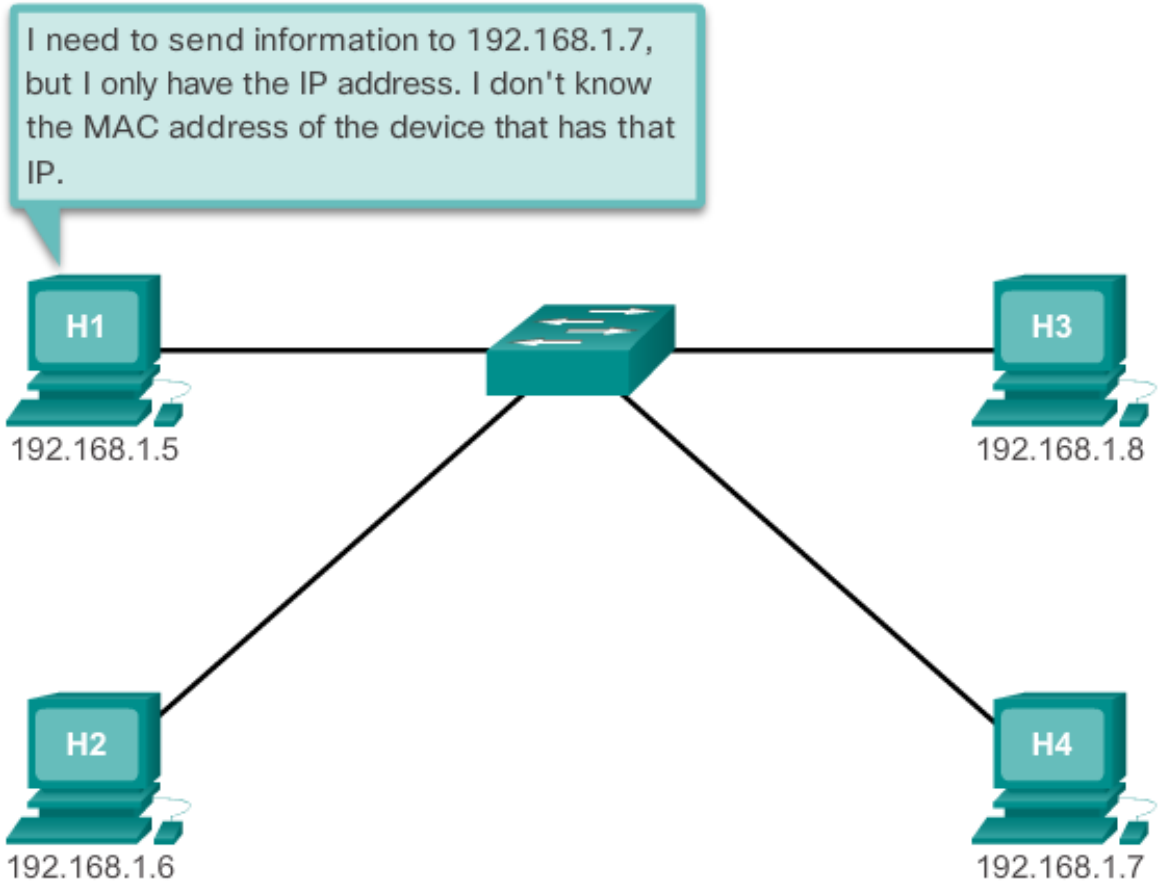
Destination on a Remote Network



MAC addresses are shortened for demonstration purposes.

Topic 5.3.2: ARP

Introduction to ARP



ARP Functions

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.

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 in section 5.3.2.3.

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.

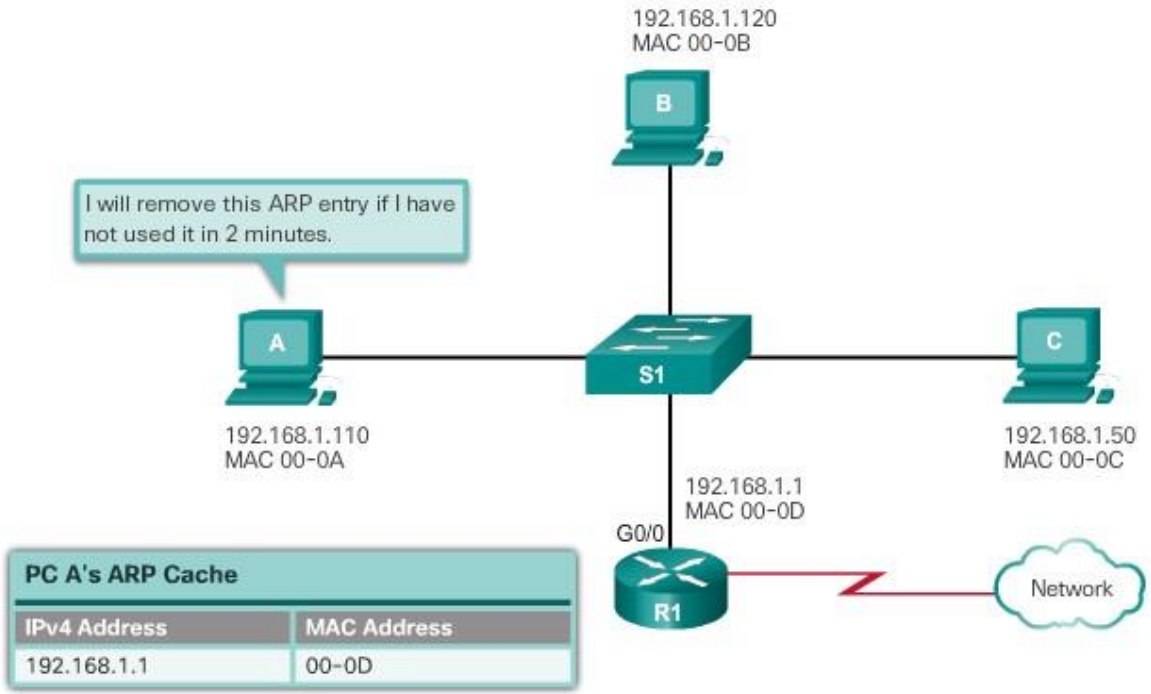
- See VIDEO DEMONSTRATION 5.3.2.4

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 5.3.2.5.

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.



ARP Tables on Networking Devices (cont.)

Host ARP Table

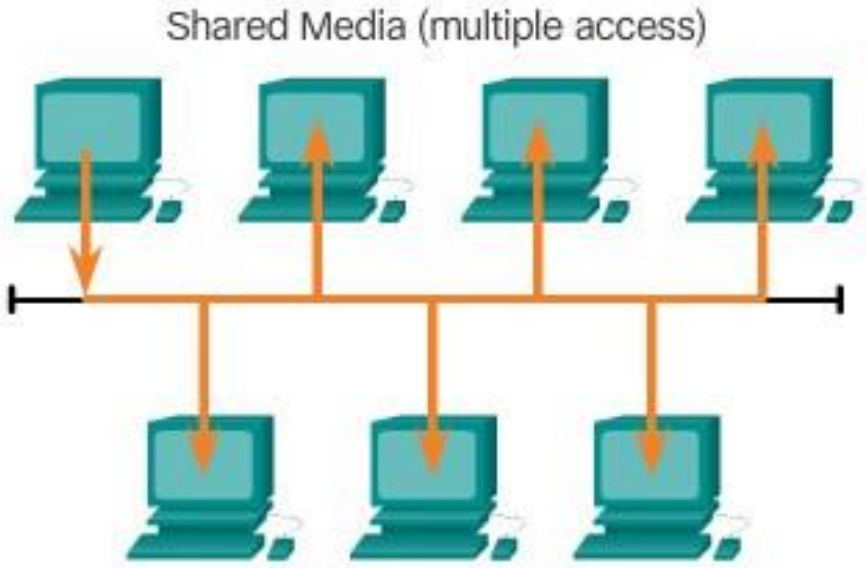
```
C:\> arp -a

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
```

Topic 5.3.3: ARP Issues

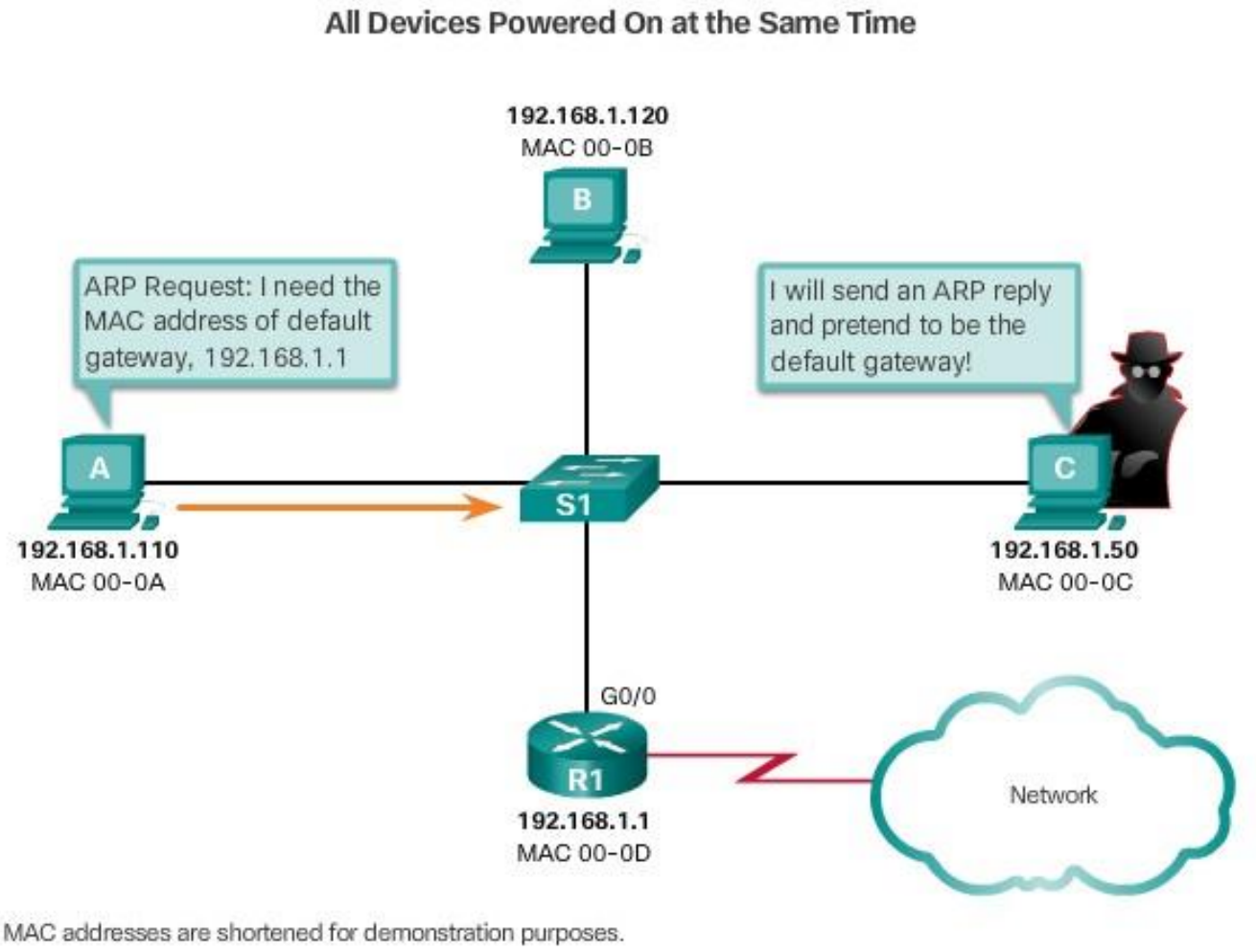
ARP Broadcasts

All devices powered on at the same time

ARP broadcasts can flood the local media.



ARP Spoofing



Section 5.4: Summary

Chapter Objectives:

- Explain the operation of Ethernet.
- Explain how a switch operates.
- Explain how the address resolution protocol enables communication on a network.

Thank you.

Cisco Networking Academy

Mind Wide Open