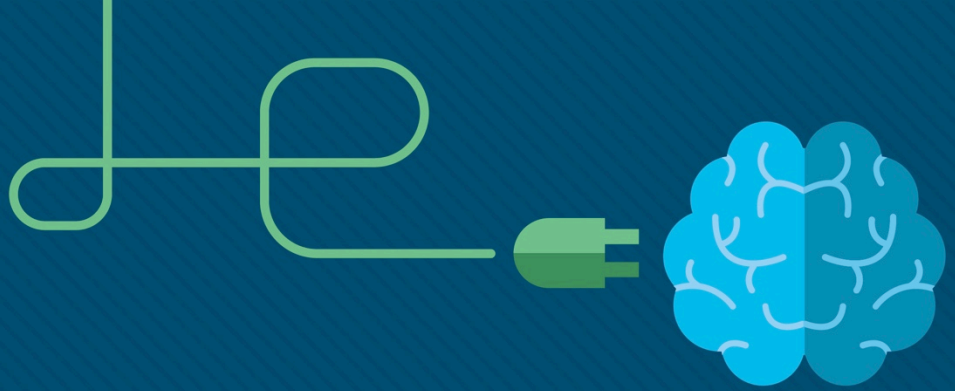


Chapter 5: Ethernet

CCNA Routing and Switching

Introduction to Networks v6.0

Chapter 5 - Sections & Objectives

- 5.1 Ethernet Protocol
  - Explain the operation of Ethernet.
    - Explain how the Ethernet sublayers are related to the frame fields.
    - Describe the Ethernet MAC address
- 5.2 LAN Switches
  - Explain how a switch operates.
    - Explain how a switch builds its MAC address table and forwards frames.
    - Describe switch forwarding methods and port settings available on Layer 2 switch ports.
- 5.3 Address Resolution Protocol
  - Explain how the address resolution protocol enables communication on a network.
    - 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.

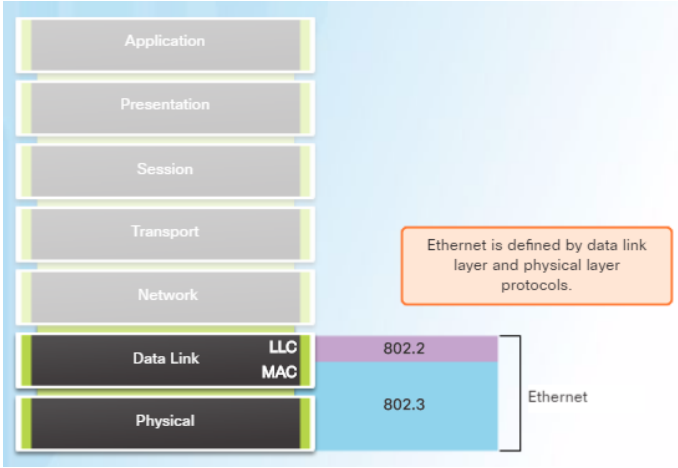
5.1 Ethernet Protocol

Ethernet Encapsulation

- Ethernet is the most widely used LAN technology today.
  - Defined in the IEEE 802.2 and 802.3 standards.
  - It supports data bandwidths of 10 Mb/s, 100 Mb/s, 1000 Mb/s (1 Gb/s), 10,000 Mb/s (10 Gb/s), 40,000 Mb/s (40 Gb/s), and 100,000 Mb/s (100 Gb/s).

- Ethernet operates in the data link layer and the physical layer.

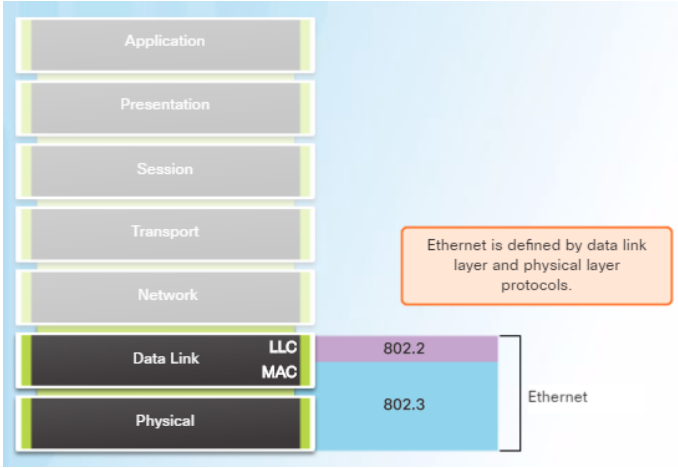
- Ethernet relies on the two separate sublayers of the data link layer to operate, the Logical Link Control (LLC) and the MAC sublayers.



Ethernet Encapsulation (Cont.)

- The Ethernet LLC sublayer handles the communication between the upper layers and the lower layers. It is implemented in software, and its implementation is independent of the hardware.

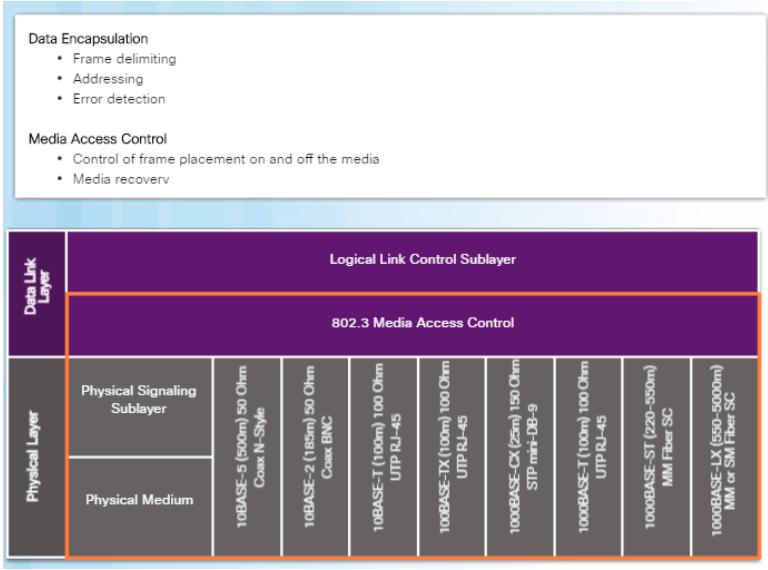
- The MAC sublayer constitutes the lower sublayer of the data link layer. MAC is implemented by hardware, typically in the computer NIC.



MAC Sublayer

- The MAC sublayer has two primary responsibilities:
  - Data encapsulation
  - Media access control

- Data encapsulation provides three primary functions:
  - Frame delimiting
  - Addressing
  - Error detection



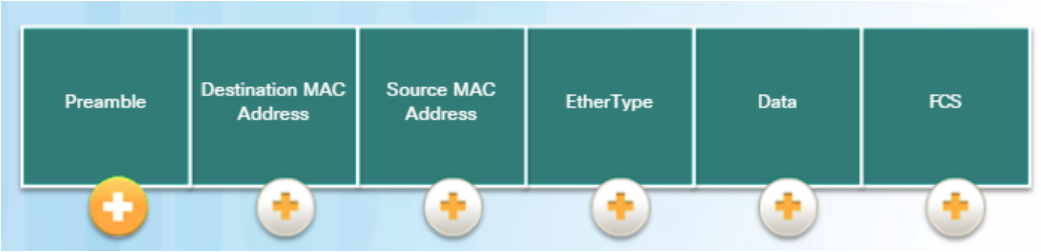
- Media access control is responsible for the placement of frames on the media and the removal of frames from the media. This sublayer communicates directly with the physical layer.

Ethernet Evolution

- Since 1973, Ethernet standards have evolved specifying faster and more flexible versions of the technology.
- Early versions of Ethernet were relatively slow at 10 Mbps.
- The latest versions of Ethernet operate at 10 Gigabits per second and faster.

Ethernet Frame Fields

- The minimum Ethernet frame size from Destination MAC address to FCS is 64 bytes and the maximum is 1518 bytes.



- Frames less than 64 bytes are called a “collision fragment” or “runt frame” and are automatically discarded by receiving stations. Frames greater than 1500 bytes of data are considered “jumbo” or “baby giant frames”.

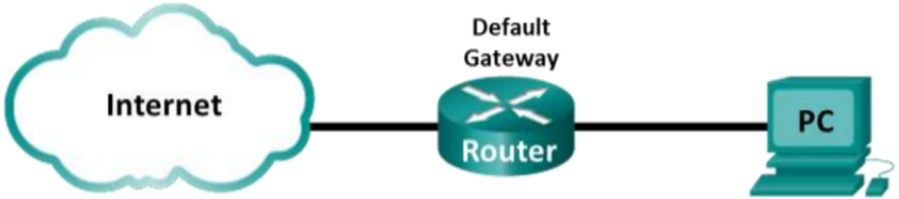
- If the size of a transmitted frame is less than the minimum or greater than the maximum, the receiving device drops the frame.

Lab - Using Wireshark to Examine Ethernet Frames

Cisco Networking Academy® Mind Wide Open™

Lab – Using Wireshark to Examine Ethernet Frames

Topology



Objectives

Part 1: Examine the Header Fields in an Ethernet II Frame

Part 2: Use Wireshark to Capture and Analyze Ethernet Frames

Background / Scenario

When upper layer protocols communicate with each other, data flows down the Open Systems Interconnection (OSI) layers and is encapsulated into a Layer 2 frame. The frame composition is dependent on the media access type. For example, if the upper layer protocols are TCP and IP and the media access is Ethernet, then the Layer 2 frame encapsulation will be Ethernet II. This is typical for a LAN environment.

When learning about Layer 2 concepts, it is helpful to analyze frame header information. In the first part of this lab, you will review the fields contained in an Ethernet II frame. In Part 2, you will use Wireshark to capture and analyze Ethernet II frame header fields for local and remote traffic.

MAC Addresses and Hexadecimal

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

- Hexadecimal is used to represent Ethernet MAC addresses and IP Version 6 addresses.
  - Hexadecimal is a base sixteen system using the numbers 0 to 9 and the letters A to F.
  - It is easier to express a value as a single hexadecimal digit than as four binary bits.
  - Hexadecimal is usually represented in text by the value preceded by 0x (E.g., 0x73).

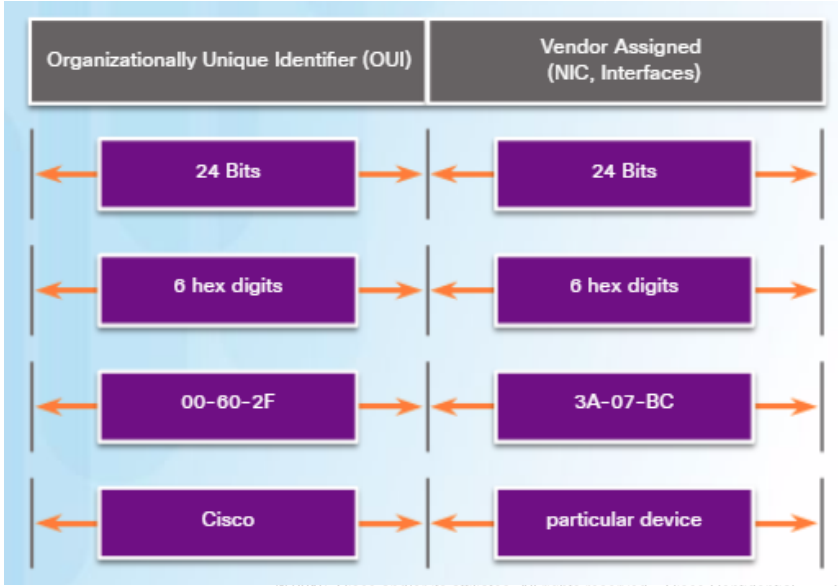
Decimal	Binary	Hexadecimal
0	0000	0
1	0001	1
2	0010	2
3	0011	3
4	0100	4
5	0101	5
6	0110	6
7	0111	7
8	1000	8
9	1001	9
10	1010	A
11	1011	B
12	1100	C
13	1101	D
14	1110	E
15	1111	F

- Convert the decimal or hexadecimal value to binary, and then to convert the binary value to either decimal or hexadecimal as needed.

MAC Addresses: Ethernet Identity

- MAC addresses were created to identify the actual source and destination.
  - The MAC address rules are established by IEEE.
  - The IEEE assigns the vendor a 3-byte (24-bit) code, called the Organizationally Unique Identifier (OUI).

- IEEE requires a vendor to follow two simple rules:
  - All MAC addresses assigned to a NIC or other Ethernet device must use that vendor's assigned OUI as the first 3 bytes.
  - All MAC addresses with the same OUI must be assigned a unique value in the last 3 bytes.

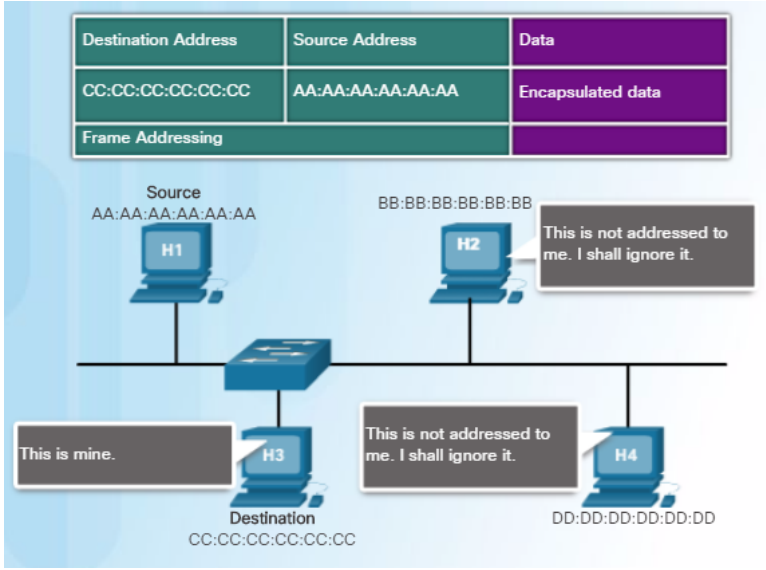


Frame Processing

- The MAC address is often referred to as a burned-in address (BIA) meaning the address is encoded into the ROM chip permanently. When the computer starts up, the first thing the NIC does is copy the MAC address from ROM into RAM.

- When a device is forwarding a message to an Ethernet network, it attaches header information to the frame.

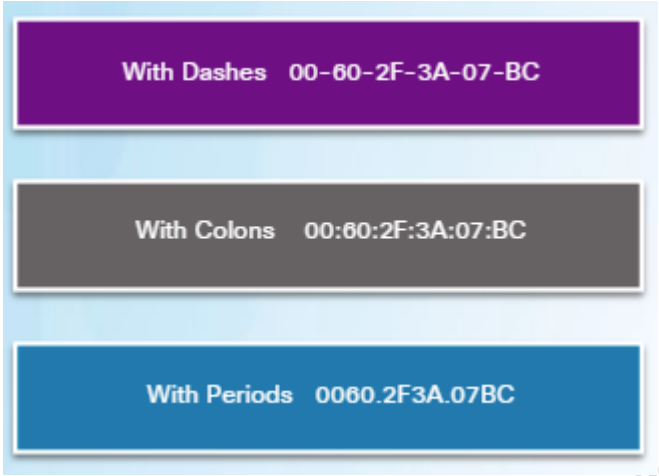
- The header information contains the source and destination MAC address.



MAC Address Representations

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

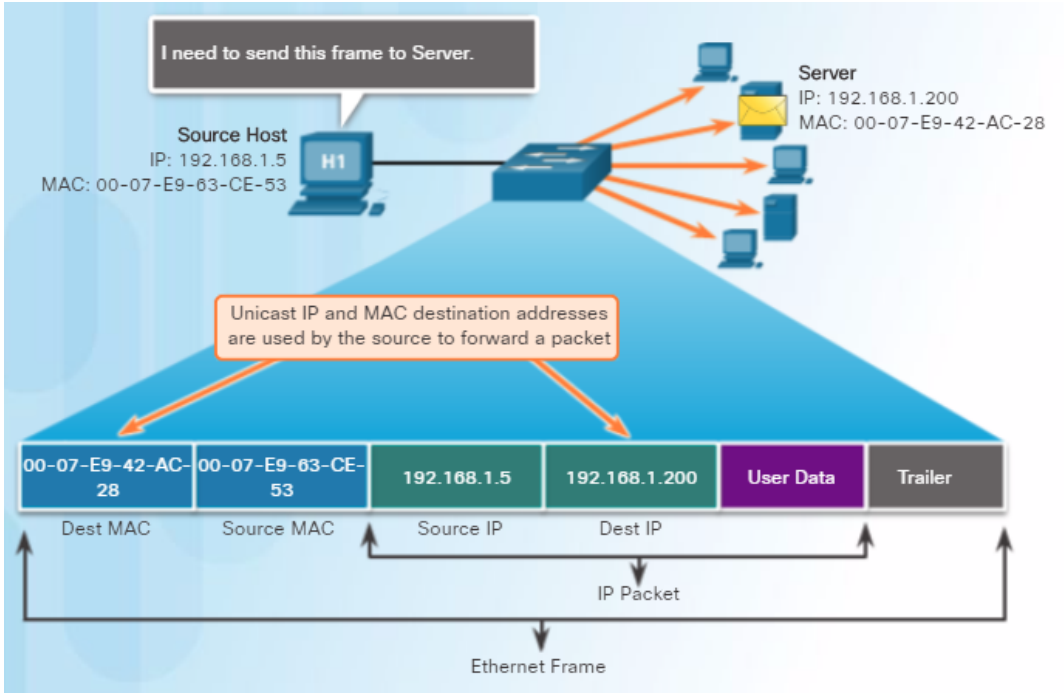
- Depending on the device and the operating system, you will see various representations of MAC addresses.



Unicast MAC Address

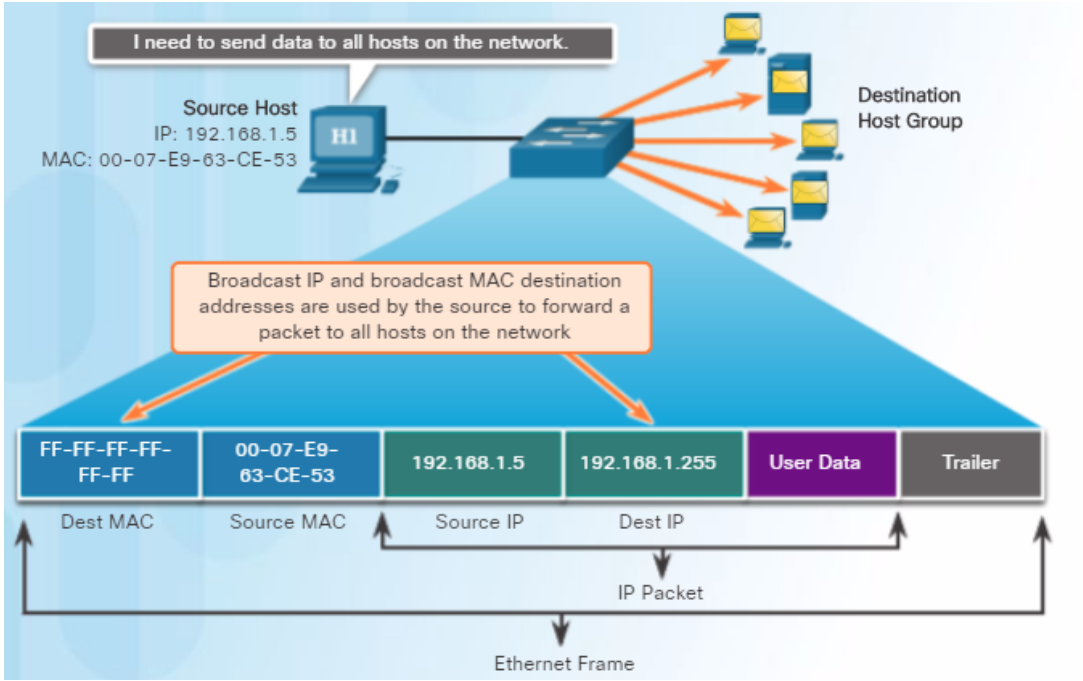
- A unicast MAC address is the unique address used when a frame is sent from a single transmitting device to a single destination device.

- For a unicast packet to be sent and received, a destination IP address must be in the IP packet header and a corresponding destination MAC address must also be present in the Ethernet frame header.



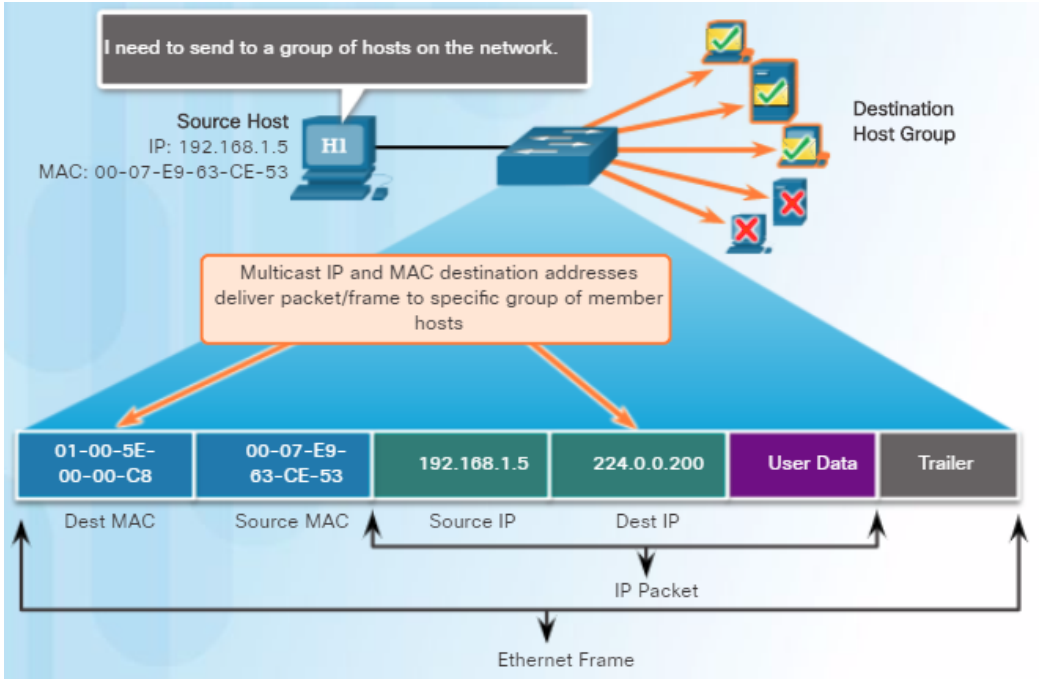
Broadcast MAC Address

- Many network protocols, such as DHCP and ARP, use broadcasts.
- A broadcast packet contains a destination IPv4 address that has all ones (1s) in the host portion indicating that all hosts on that local network will receive and process the packet.
- When the IPv4 broadcast packet is encapsulated in the Ethernet frame, the destination MAC address is the broadcast MAC address of FF-FF-FF-FF-FF-FF in hexadecimal (48 ones in binary).



Multicast MAC Address

- Multicast addresses allow a source device to send a packet to a group of devices.
  - Devices in a multicast group are assigned a multicast group IP address in the range of 224.0.0.0 to 239.255.255.255 (IPv6 multicast addresses begin with FF00::/8).
  - The multicast IP address requires a corresponding multicast MAC address that begins with 01-00-5E in hexadecimal.

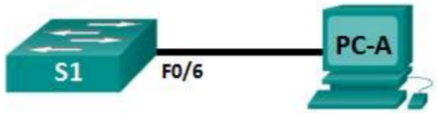


Lab – Viewing Network Device MAC Addresses

Cisco Networking Academy® Mind Wide Open™

Lab – Viewing Network Device MAC Addresses

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.1	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objectives

Part 1: Configure Devices and Verify Connectivity

Part 2: Display, Describe, and Analyze Ethernet MAC Addresses

Background / Scenario

Every device on an Ethernet LAN is identified by a Layer 2 MAC address. This address is assigned by the manufacturer and stored in the firmware of the NIC. This lab will explore and analyze the components that make up a MAC address, and how you can find this information on a switch and a PC.

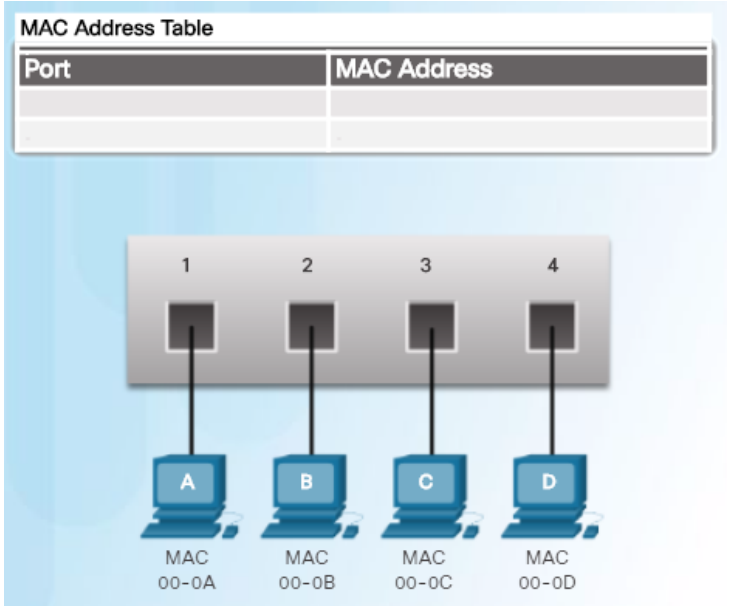
You will cable the equipment as shown in the topology. You will configure the switch and PC to match the addressing table. You will verify your configurations by testing for network connectivity.

After the devices have been configured and network connectivity has been verified, you will use various commands to retrieve information from the devices to answer questions about your network equipment.

5.2 LAN Switches

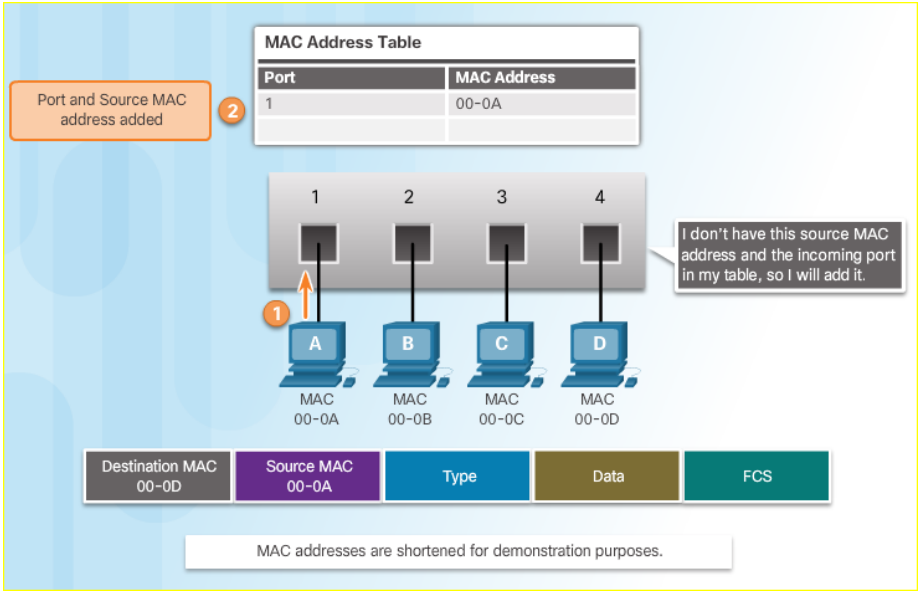
Switch Fundamentals

- A Layer 2 Ethernet switch makes its forwarding decisions based only on the Layer 2 Ethernet MAC addresses.
- A switch that is powered on, will have an empty MAC address table as it has not yet learned the MAC addresses for the four attached PCs.
- Note: The MAC address table is sometimes referred to as a content addressable memory (CAM) table.



Learning MAC Addresses

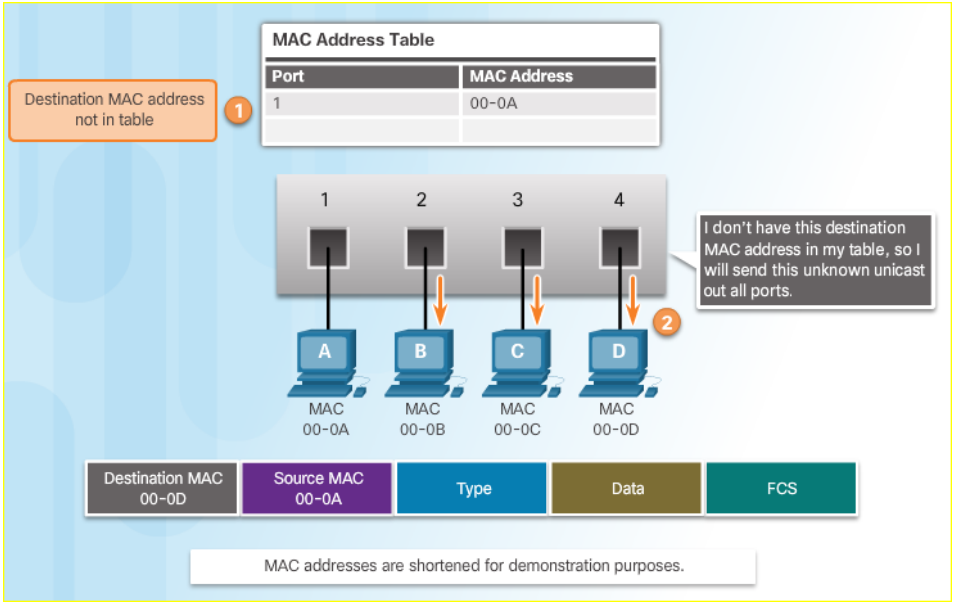
- The switch dynamically builds the MAC address table. The process to learn the Source MAC Address is:
  - Switches examine all incoming frames for new source MAC address information to learn.
  - If the source MAC address is unknown, it is added to the table along with the port number.
  - If the source MAC address does exist, the switch updates the refresh timer for that entry.
  - By default, most Ethernet switches keep an entry in the table for 5 minutes.



Switching Process	Description

Learning MAC Addresses (Cont.)

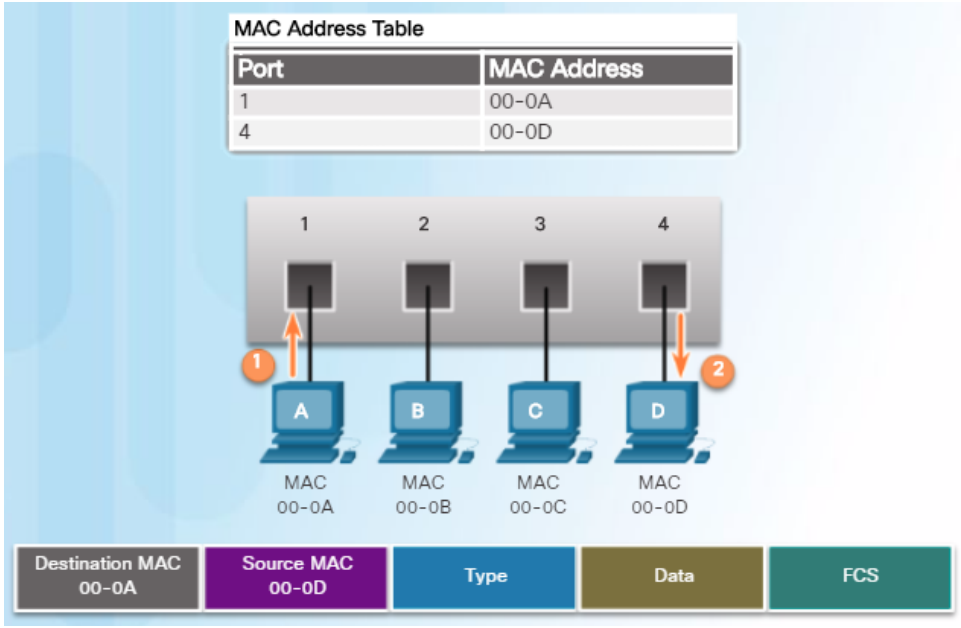
- The process to forward the Destination MAC Address is:
  - If the destination MAC address is a broadcast or a multicast, the frame is also flooded out all ports except the incoming port.
  - If the destination MAC address is a unicast address, the switch will look for a match in its MAC address table.
  - If the destination MAC address is in the table, it will forward the frame out the specified port.
  - If the destination MAC address is not in the table (i.e., an unknown unicast) the switch will forward the frame out all ports except the incoming port.



Filtering Frames

- As a switch receives frames from different devices, it is able to populate its MAC address table by examining the source MAC address of every frame.

- When the switch's MAC address table contains the destination MAC address, it is able to filter the frame and forward out a single port.

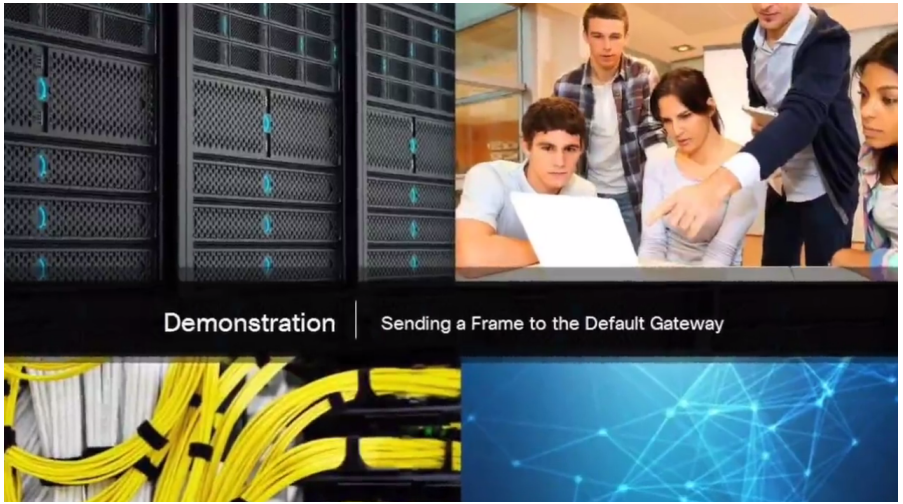


Video Demonstration - MAC Address Tables on Connected Switches

- The switch receives the Ethernet frame, examines the source MAC address and notices that this MAC address is not in its MAC address table, so it adds the MAC address and the incoming port number.
- Next, the switch examines the destination MAC address and notices that this MAC address is not in its table, so it floods it out all ports.
- The computer receives the Ethernet frame, examines the destination MAC address against its own MAC address, and notices that that is a match and receives the rest of the frame.

Video Demonstration - Sending a Frame to the Default Gateway

- The computer is going to send a packet to the Internet, because the destination IP address is in on another network. In this case, the source MAC address is that of the sending computer. The destination MAC address is that of the router of 00-0D.

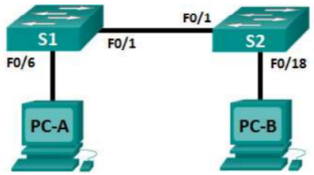


Lab – Viewing the Switch MAC Address Table

Cisco Networking Academy® Mind Wide Open™

Lab – Viewing the Switch MAC Address Table

Topology



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
S1	VLAN 1	192.168.1.11	255.255.255.0	N/A
S2	VLAN 1	192.168.1.12	255.255.255.0	N/A
PC-A	NIC	192.168.1.3	255.255.255.0	N/A
PC-B	NIC	192.168.1.2	255.255.255.0	N/A

Objectives

Part 1: Build and Configure the Network

Part 2: Examine the Switch MAC Address Table

Background / Scenario

The purpose of a Layer 2 LAN switch is to deliver Ethernet frames to host devices on the local network. The switch records host MAC addresses that are visible on the network, and maps those MAC addresses to its own Ethernet switch ports. This process is called building the MAC address table. When a switch receives a frame from a PC, it examines the frame's source and destination MAC addresses. The source MAC address is recorded and mapped to the switch port from which it arrived. Then the destination MAC address is looked up in the MAC address table. If the destination MAC address is a known address, then the frame is forwarded out of the corresponding switch port associated with that MAC address. If the MAC address is unknown, then the frame is broadcasted out of all switch ports, except the one from which it came. It is important to observe and understand the function of a switch and how it delivers data on the network. The way a switch operates has implications for network administrators whose job it is to ensure secure and consistent network communication.

Switches are used to interconnect and deliver information to computers on local area networks. Switches deliver Ethernet frames to host devices identified by network interface card MAC addresses.

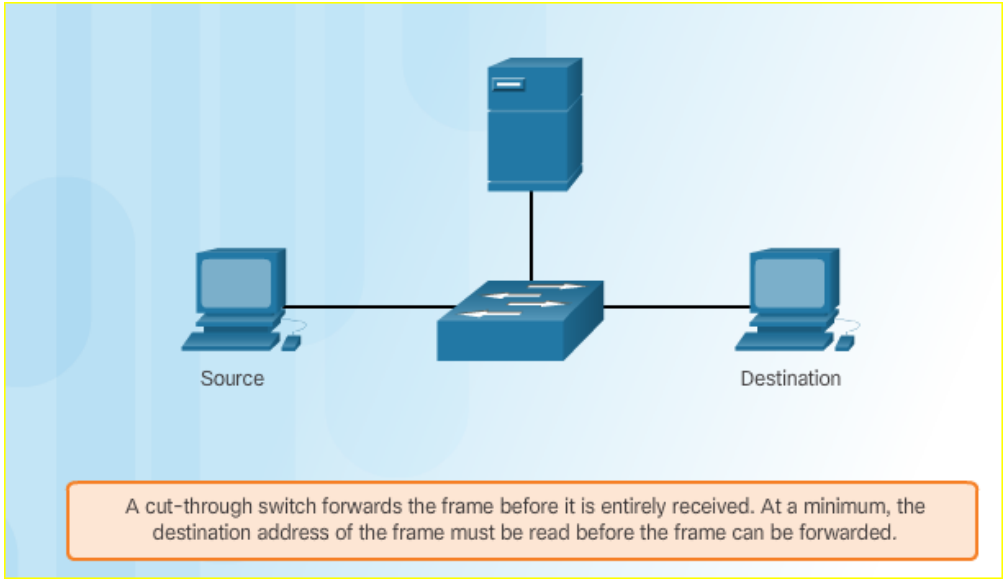
In Part 1, you will build a multi-switch topology with a trunk linking the two switches. In Part 2, you will ping various devices and observe how the two switches build their MAC address tables.

Frame Forwarding Methods on Cisco Switches

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

Cut-Through Switching

- In cut-through switching, 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 switch does not perform any error checking on the frame.
- There are two variants of cut-through switching:
  - Fast-forward switching offers the lowest level of latency. The switch immediately forwards a packet after reading the destination address. This is the most typical form of cut-through switching.
  - Fragment-free switching, in which the switch stores the first 64 bytes of the frame before forwarding. It is a compromise between store-and-forward and fast-forward switching.



Memory Buffering on Switches

- An Ethernet switch may use a memory 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.
- There are two types of memory buffering techniques:

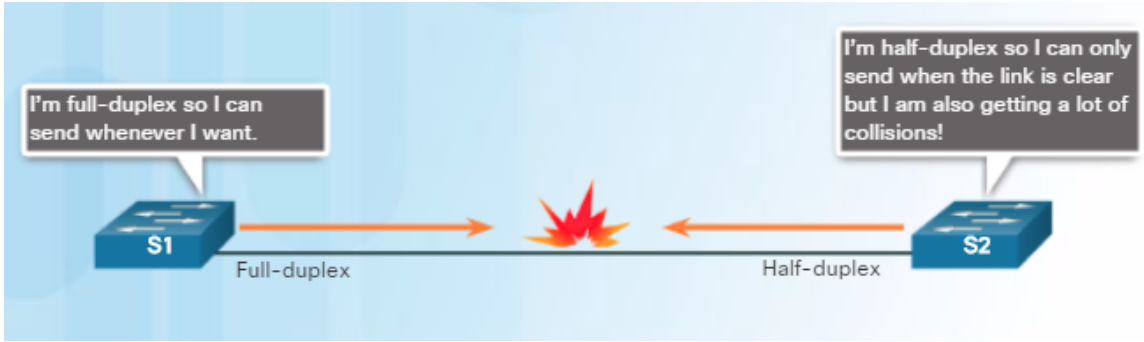
Memory Buffering Method	Description
Port-based memory	• Frames are stored in queues that are linked to specific incoming and outgoing ports. • A frame is transmitted when all the frames ahead of it have been transmitted.
Shared memory	• All frames are deposited into a common buffer which is shared by all ports on the switch.

Duplex and Speed Settings

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

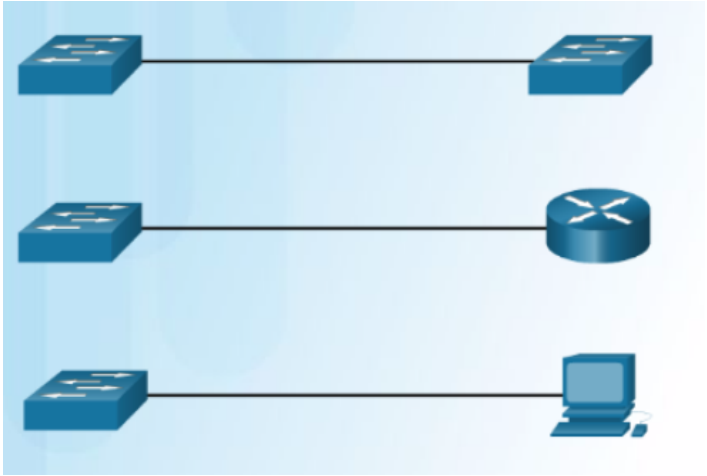
- Most devices use autonegotiation which enables two devices to automatically exchange information about speed and duplex capabilities and choose the highest performance mode.

- **Duplex mismatch** is a common cause of performance issues with Ethernet links. It occurs when one port on the link operates at half-duplex while the other port operates at full-duplex.



Auto-MDIX

- Connections between specific devices such as switch-to-switch, switch-to-router, switch-to-host, and router-to-host devices, once required the use of specific cable types (crossover or straight-through).



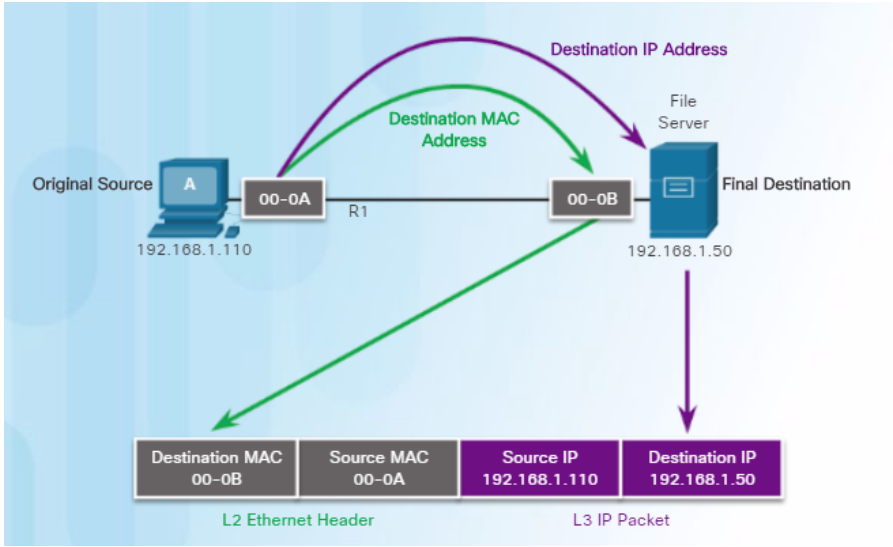
- Most switch devices now support the automatic medium-dependent interface crossover (auto-MDIX) feature. This is enabled by default on switches since IOS 12.2(18)SE.

- When enabled using the **mdix auto** interface configuration command, the switch detects the type of cable attached to the port, and configures the interfaces accordingly.

5.3 Address Resolution Protocol

Destination on Same Network

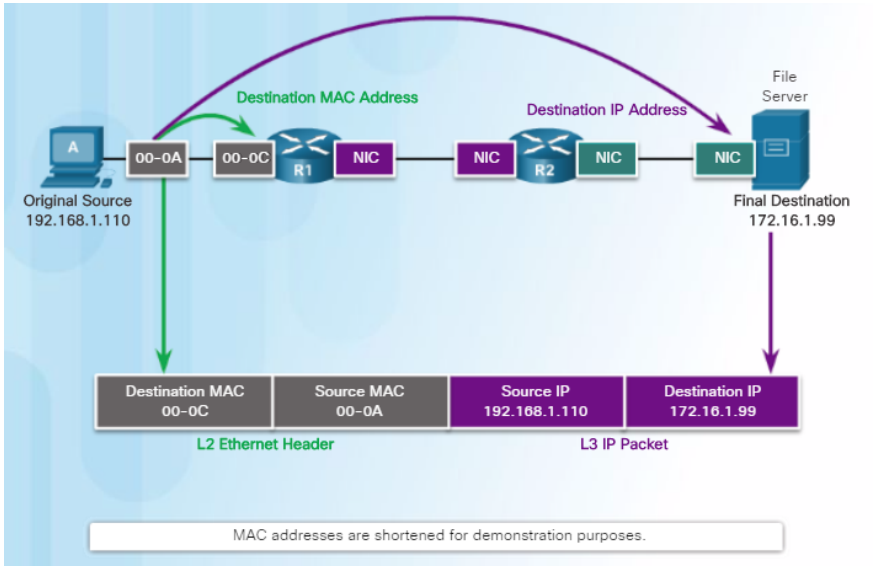
- There are two primary addresses assigned to a device on an Ethernet LAN:
  - Physical address (the Ethernet MAC address)
  - Logical address (the IP address)
- As an example, PC-A sends an IP packet to the file server on the same network. The Layer 2 Ethernet frame contains:
  - Destination MAC address
  - Source MAC address
- The Layer 3 IP packet contains:
  - Source IP address
  - Destination IP address



Destination on Remote Network

- When the destination IP address is on a remote network, the destination MAC address will be the address of the host's default gateway.

- In the figure, PC-A is sending an IP packet to a web server on a remote network.
  - The destination IP address is that of the File Server.
  - The destination MAC address is that of Ethernet interface of R1.

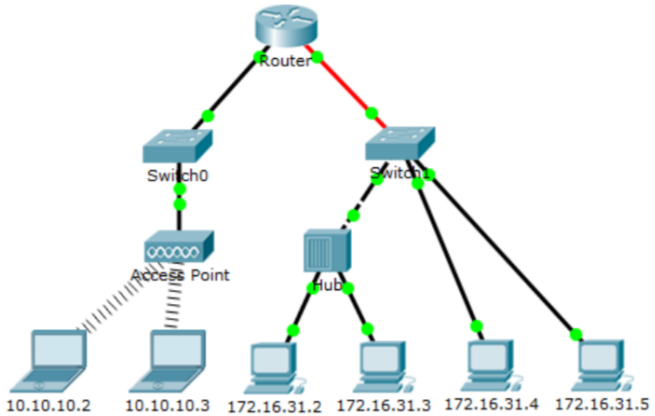


Packet Tracer - Identify MAC and IP Addresses

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Identify MAC and IP Addresses

Topology



Objectives

Part 1: Gather PDU Information

Part 2: Reflection Questions

Background

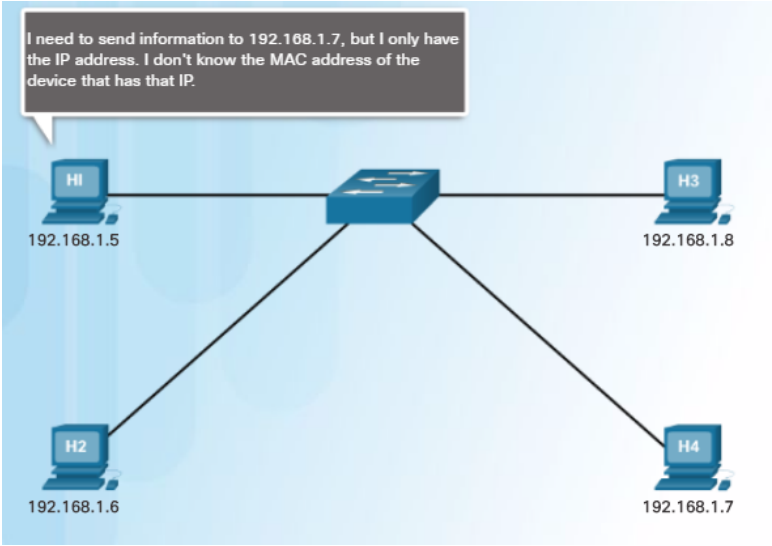
This activity is optimized for viewing PDUs. The devices are already configured. You will gather PDU information in simulation mode and answer a series of questions about the data you collect.

Introduction to ARP

- When a device sends an Ethernet frame, it contains these two addresses:
  - Destination MAC address
  - Source MAC address

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

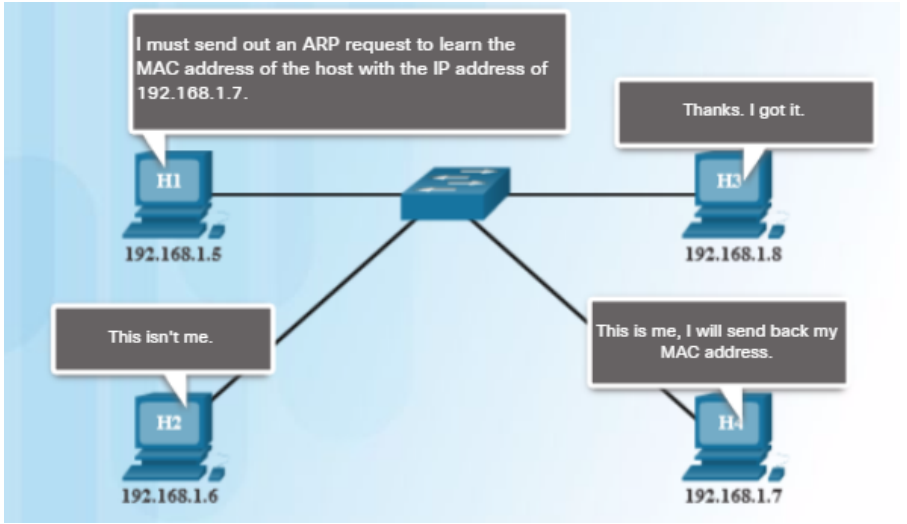
- ARP provides two basic functions:
  - Resolving IPv4 addresses to MAC addresses
  - Maintaining a table of mappings



ARP Functions

- Ethernet devices refer to an ARP table (or the ARP cache) in its memory (i.e., RAM) to find the MAC address that is mapped to the IPv4 address.

- A device will search its ARP table for a destination IPv4 address and a corresponding MAC address.
  - If the packet's destination IPv4 address is on the same network as the source IPv4 address, the device will search the ARP table for the destination IPv4 address.
  - If the destination IPv4 address is on a different network than the source IPv4 address, the device will search the ARP table for the IPv4 address of the default gateway.

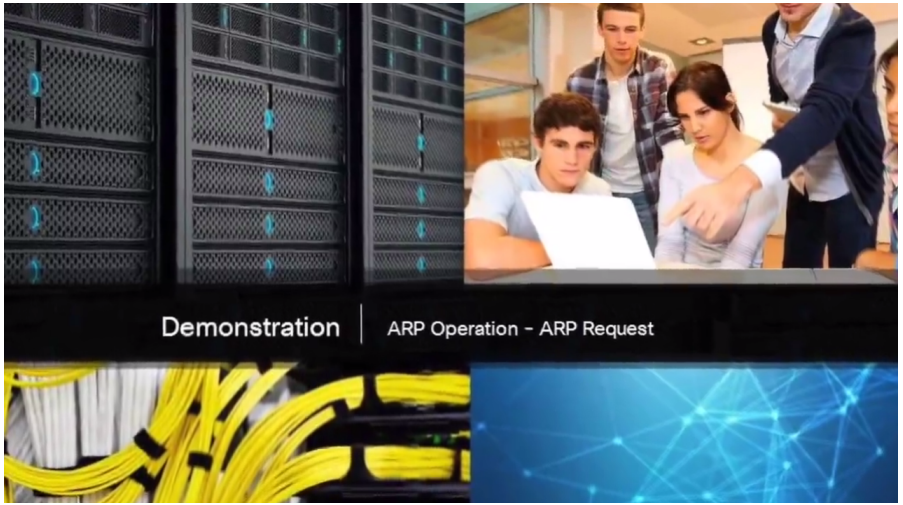


Video Demonstration – ARP Request

- An ARP request is a broadcast frame sent when a device needs a MAC address associated with an IPv4 address, and it does not have an entry for the IPv4 address in its ARP table.

- ARP messages are encapsulated directly within an Ethernet frame. There is no IPv4 header.

- The ARP request message includes:
  - Target IPv4 address
  - Target MAC address

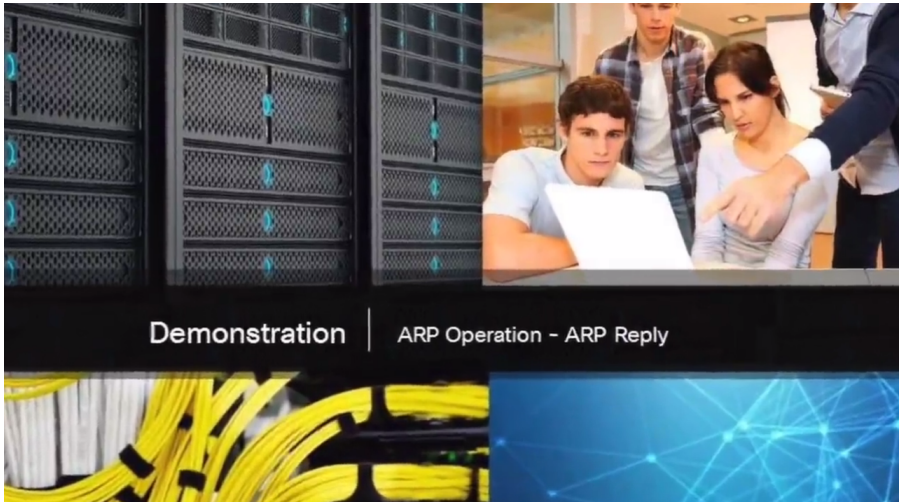


Video Demonstration – ARP Reply

- Only the device with an IPv4 address associated with the target IPv4 address in the ARP request will respond with an ARP reply.

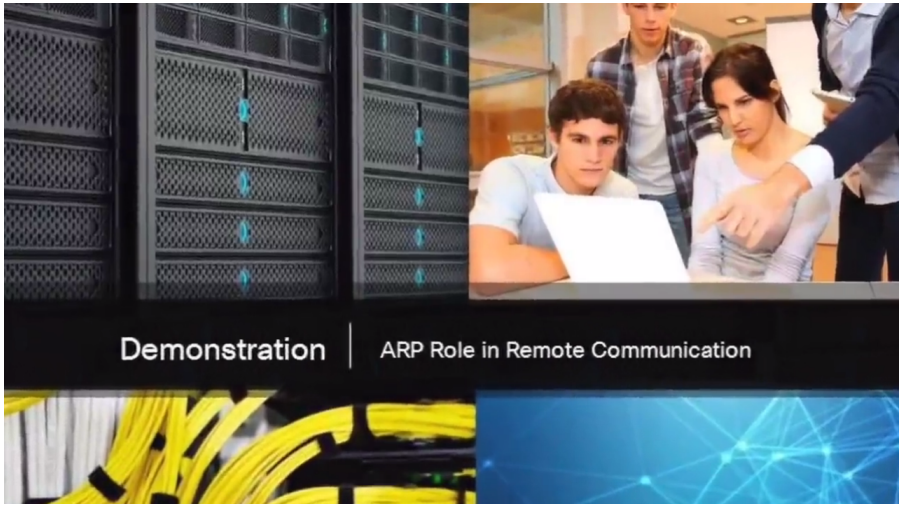
- The ARP reply message includes:
  - Sender's IPv4 address
  - Sender's MAC address

- Entries in the ARP table are time stamped. If a device does not receive a frame from a particular device by the time the timestamp expires, the entry for this device is removed from the ARP table.



Video Demonstration – ARP role in Remote Communications

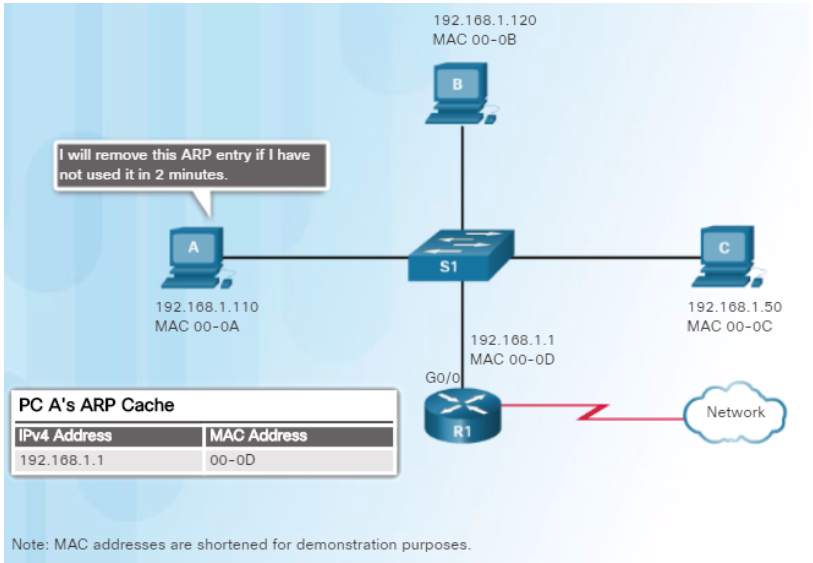
- When a host creates a packet for a destination, it compares the destination IPv4 address and its own IPv4 address to determine if the two IPv4 addresses are located on the same Layer 3 network.
- If the destination host is not on its same network, the source checks its ARP table for an entry with the IPv4 address of the default gateway.
- If there is not an entry, it uses the ARP process to determine a MAC address of the default gateway.



Removing Entries from an ARP Table

- Every device has an ARP cache timer that removes ARP entries that have not been used for a specified period of time.

- The times differ depending on the device's operating system. As shown in the figure, some Windows operating systems store ARP cache entries for 2 minutes.



- You can also manually remove all or some of the entries in the ARP table.

ARP Tables

On a Router

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

```
Router# show ip arp
Protocol  Address          Age (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
Router#
```

On a Windows Host

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

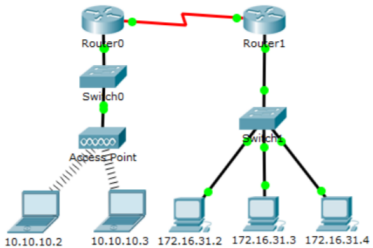
```
C:\> arp -a

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
```

Packet Tracer - Examine the ARP Table

Cisco Networking Academy® Mind Wide Open™

Packet Tracer - Examine the ARP Table

Topology



Addressing Table

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

Objectives

Part 1: Examine an ARP Request

Part 2: Examine a Switch MAC Address Table

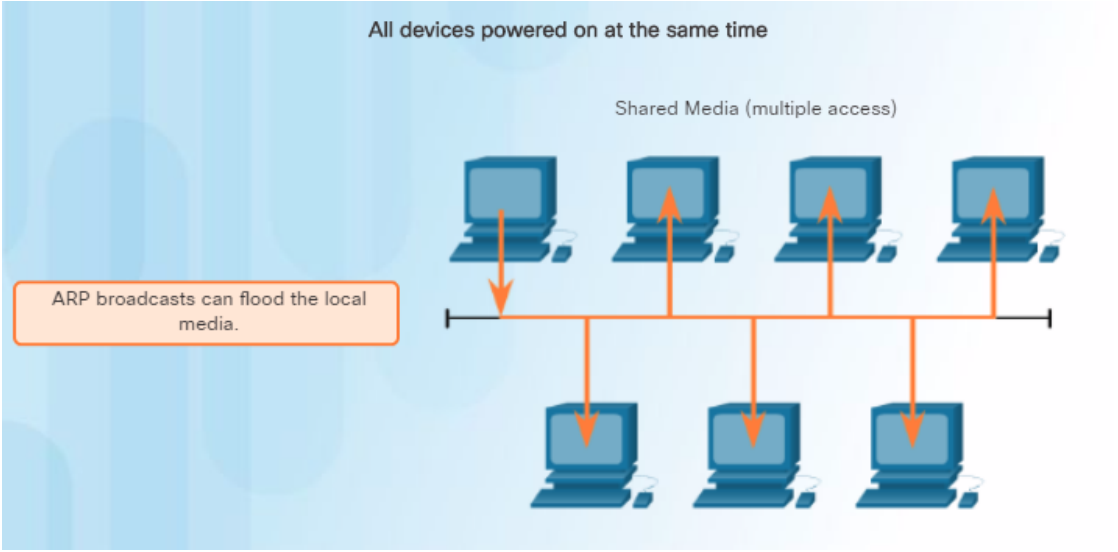
Part 3: Examine the ARP Process in Remote Communications

Background

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.

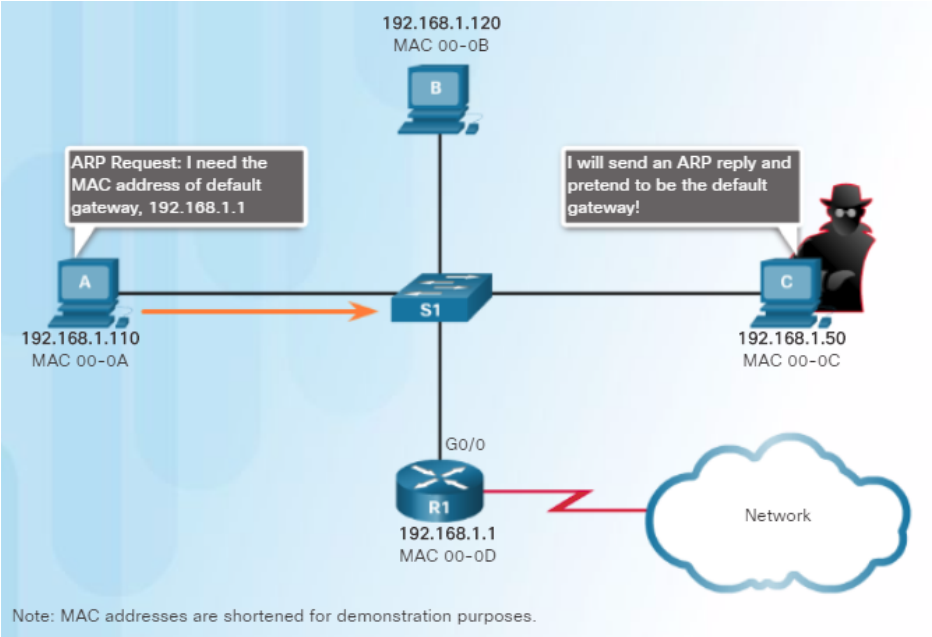
ARP Broadcasts

- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- ARP requests can flood the local segment if a large number of devices were to be powered up and all start accessing network services at the same time.



ARP Spoofing

- Attackers can respond to requests and pretend to be providers of services.
- One type of ARP spoofing attack used by attackers is to reply to an ARP request for the default gateway. In the figure, host A requests the MAC address of the default gateway. Host C replies to the ARP request. Host A receives the reply and updates its ARP table. It now sends packets destined to the default gateway to the attacker host C.
- Enterprise level switches include mitigation techniques known as dynamic ARP inspection (DAI).



5.4 Chapter Summary

Chapter 5: Ethernet

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


CISCO