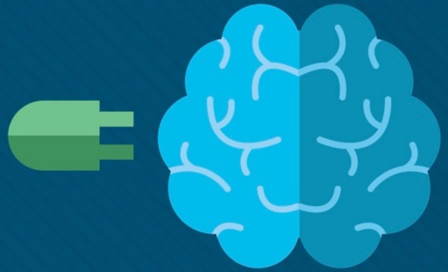


Chapter 3: Network Protocols and Services

Information Security

Dr. Ayman Aljarbouh

3.4 Address Resolution Protocol

Module Objectives

Module Title: Address Resolution Protocol

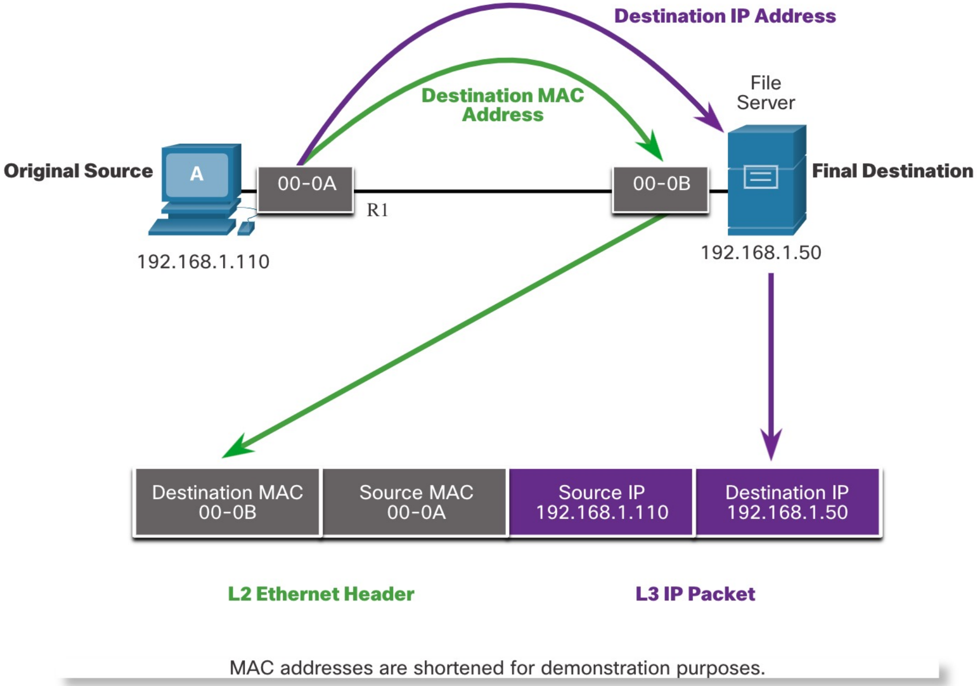
Module Objective: Analyze address resolution protocol PDUs on a network

Topic Title	Topic Objective
MAC and IP	Compare the roles of the MAC address and the IP address.
ARP	Analyze ARP by examining Ethernet frames.
ARP Issues	Explain how ARP requests impact network and host performance as well as potential security risks.

MAC and IP

Destination on Same Network

- Two addresses assigned to an Ethernet device:
  - **MAC address** (Layer 2 physical address) – This is used for Ethernet NIC to Ethernet NIC communications on the same network
  - **IP address** (Layer 3 logical address) – This is used to send the packet from the original source to the final destination
- A device must have both addresses to communicate with another TCP/IP-based device:
  - Uses the source and destination MAC address
  - Uses the source and destination IP address



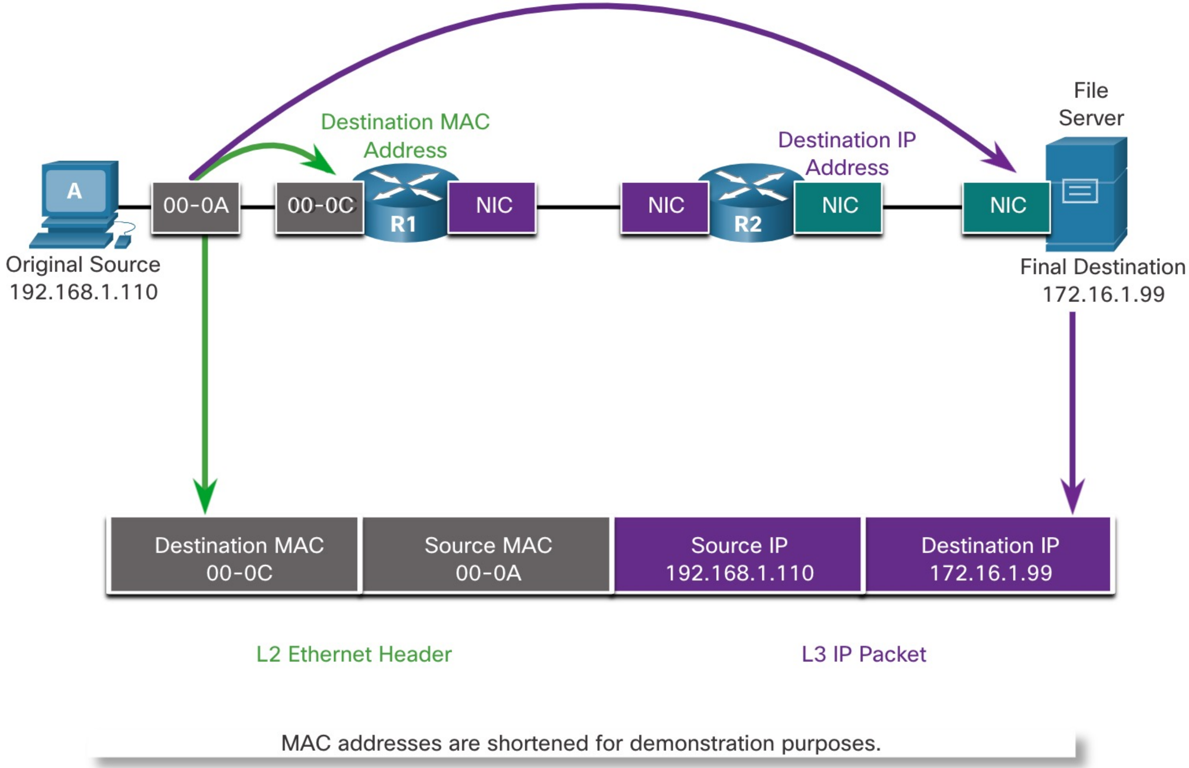
Destination MAC 00-0B	Source MAC 00-0A	Source IP 192.168.1.110	Destination IP 192.168.1.50

MAC addresses are shortened for demonstration purposes.

MAC and IP

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.



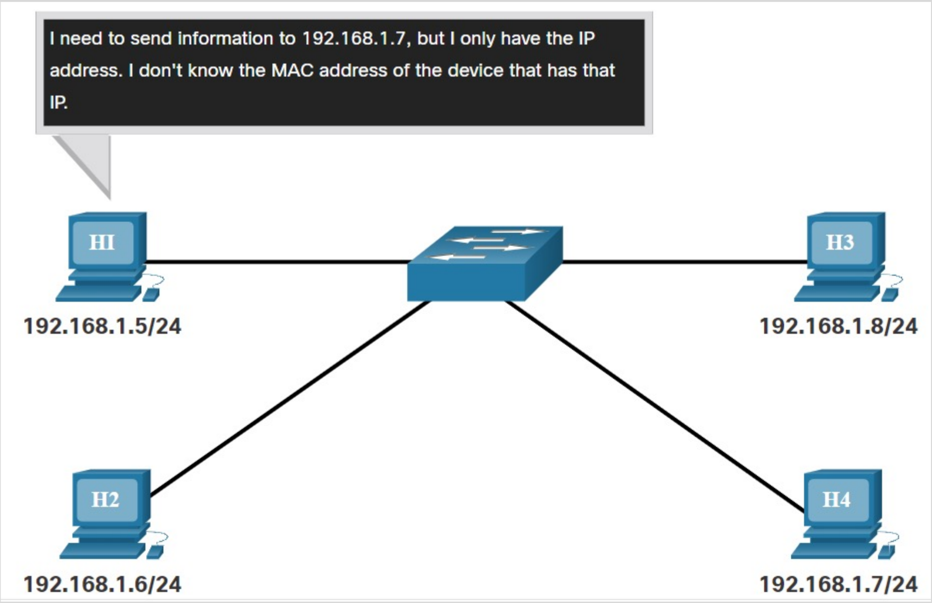
MAC addresses are shortened for demonstration purposes.

This would be similar to a person taking a letter to their local post office. They only need to leave the letter at the post office. It then becomes the responsibility of the post office to forward the letter on towards its final destination.

ARP

ARP Overview

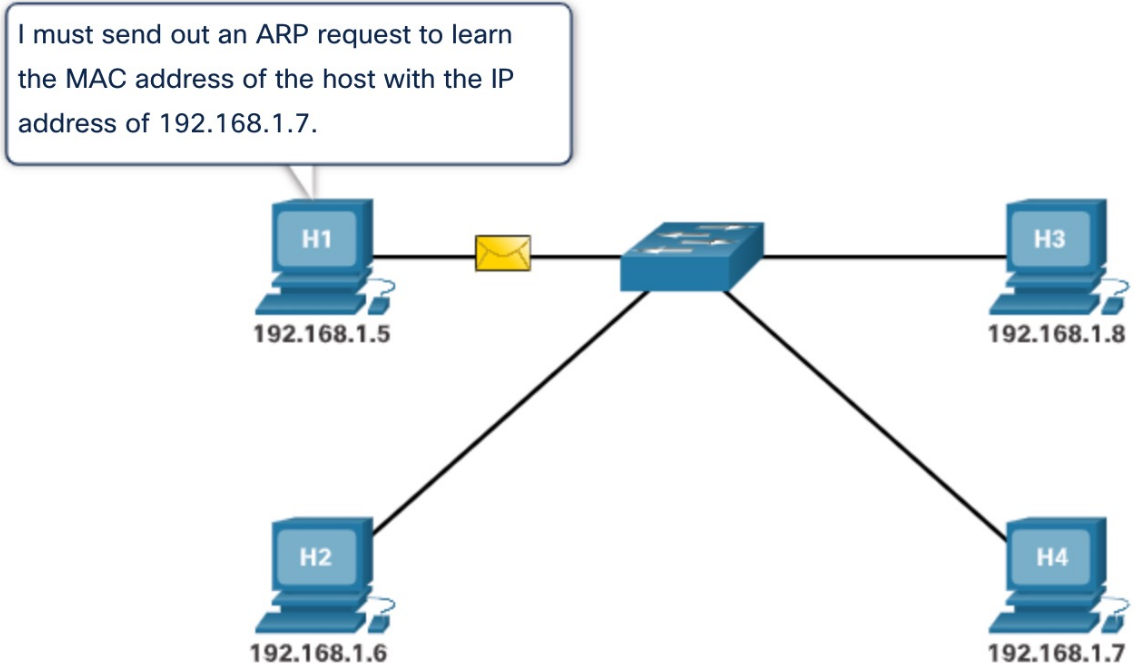
- A device uses Address Resolution Protocol (ARP) to determine the destination MAC address of a local device when it knows its IPv4 address.
- ARP provides two basic functions:
  - Resolving IPv4 addresses to MAC addresses
  - Maintaining a table of IPv4 to MAC address mappings



I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.

ARP Functions

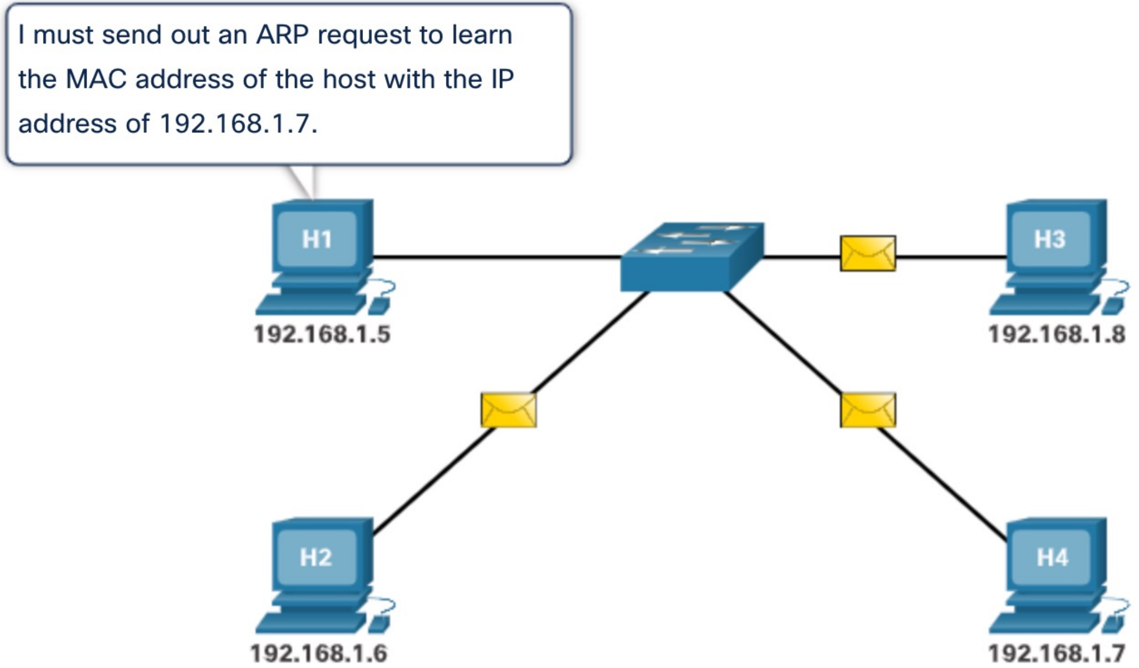
- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.

ARP Functions

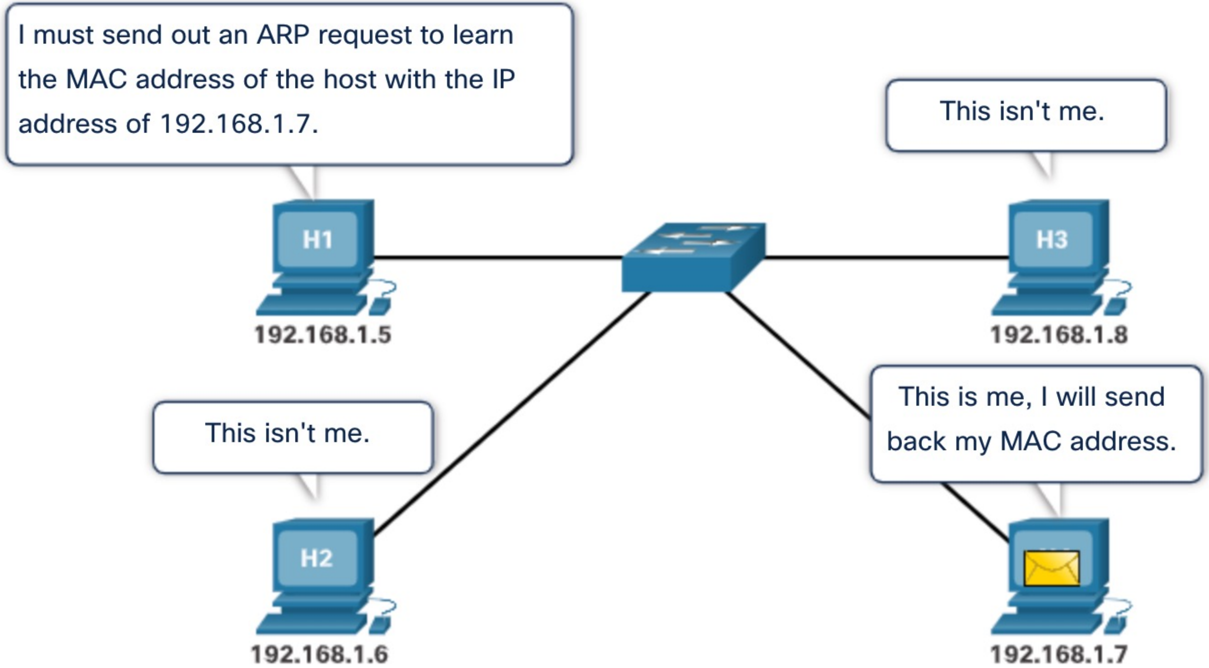
- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.

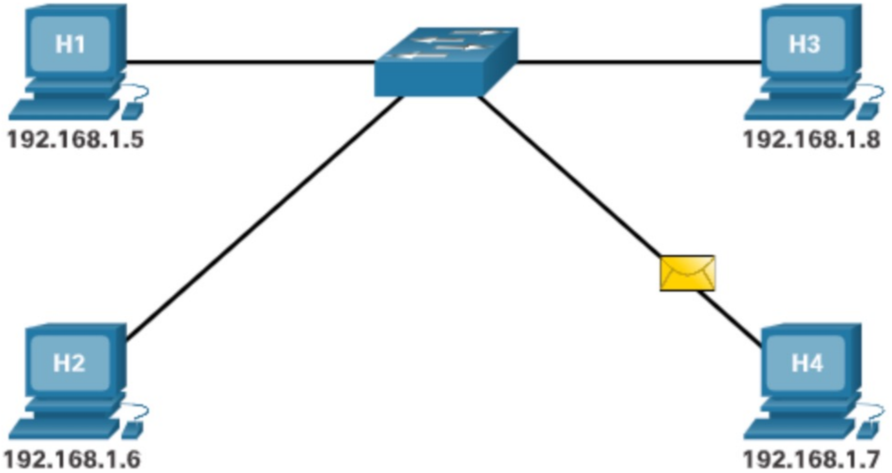
ARP Functions

- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.


I must send out an ARP request to learn the MAC address of the host with the IP address of 192.168.1.7.
This isn't me.
H1
192.168.1.5
H3
192.168.1.8
This isn't me.
This is me, I will send back my MAC address.
H2
192.168.1.6
192.168.1.7

ARP Functions

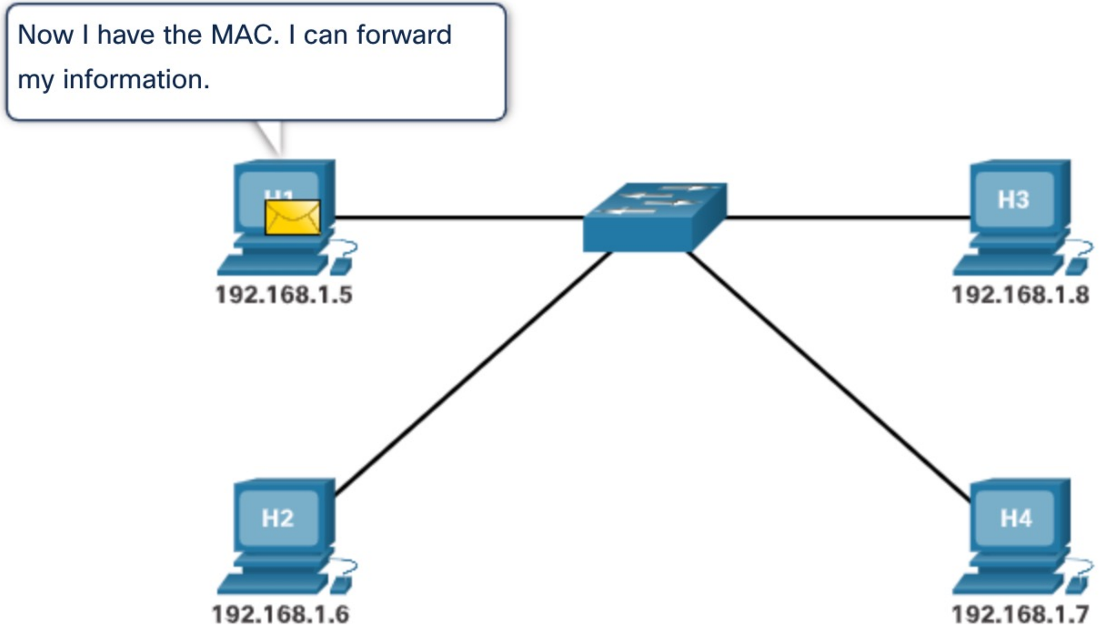
- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



ARP

ARP Functions

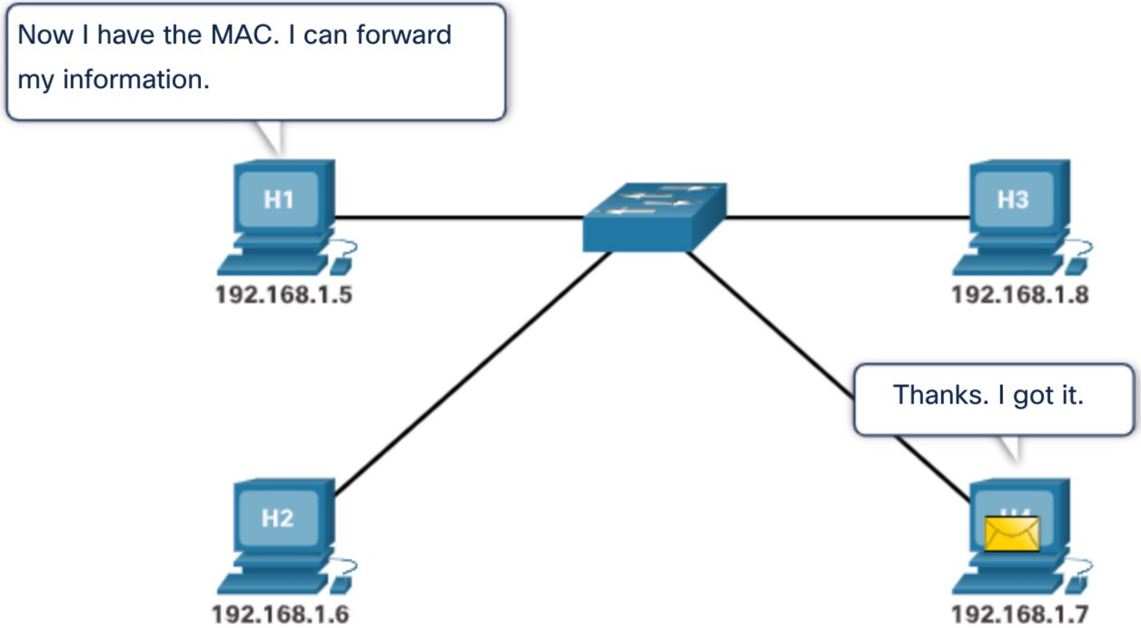
- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



ARP

ARP Functions

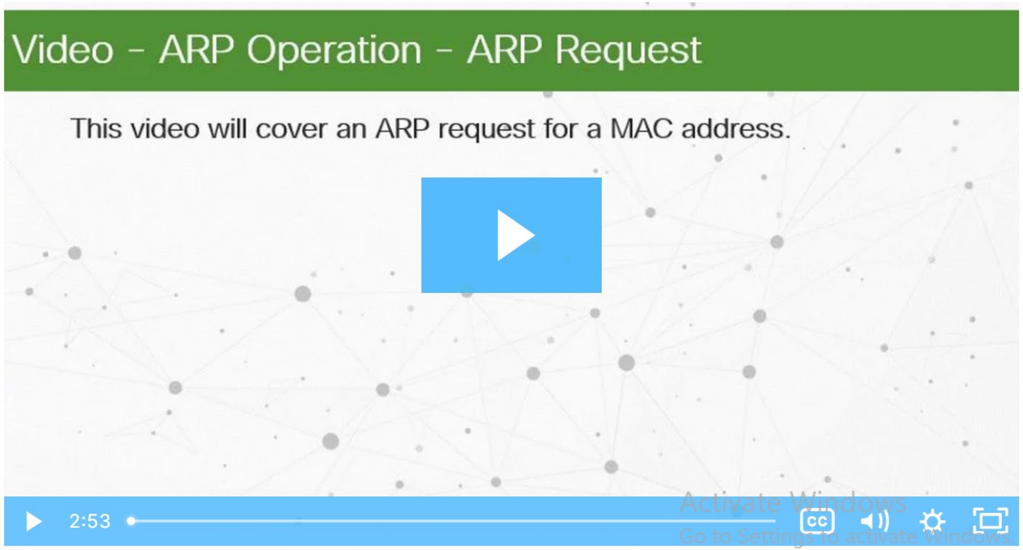
- Used to resolve IPv4 addresses to MAC addresses.
- IPv4 and MAC address mappings kept in an ARP table.



ARP

Video - ARP Operation - ARP Request

- When a device needs to determine the MAC address mapped to the IPv4 address and no entry is found for the IPv4 address in its ARP table, then an ARP request is sent.
- Click Play to view a demonstration of an ARP request for a destination IPv4 address that is on the local network.



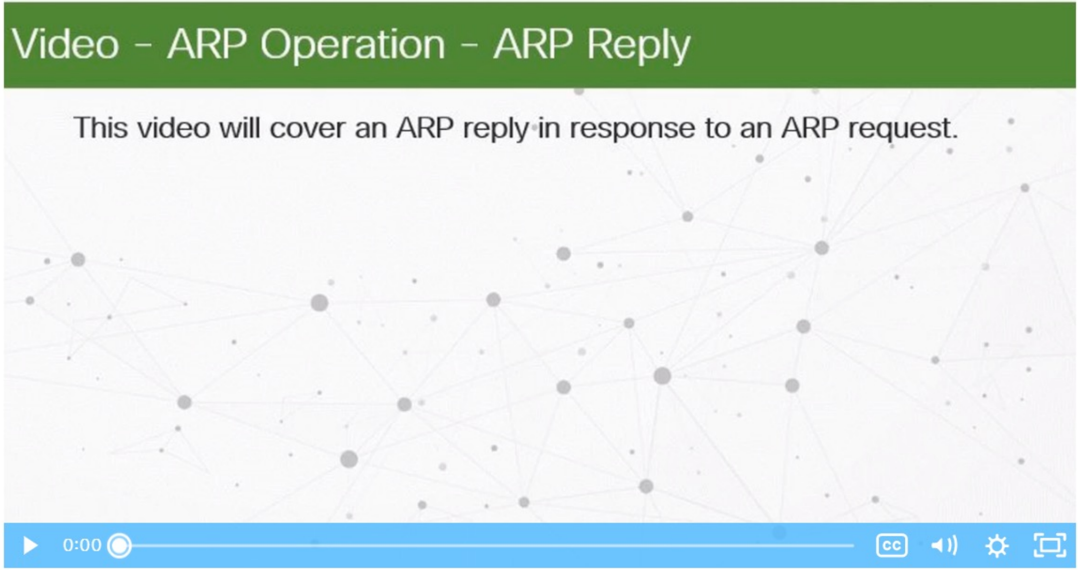
Video – ARP Operation – ARP Request

This video will cover an ARP request for a MAC address.

https://www.youtube.com/watch?v=dGTbwvhoHww

Video - ARP Operation - ARP Reply

- Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply.
- Click Play in the figure to view a demonstration of an ARP reply.



Video – ARP Operation – ARP Reply

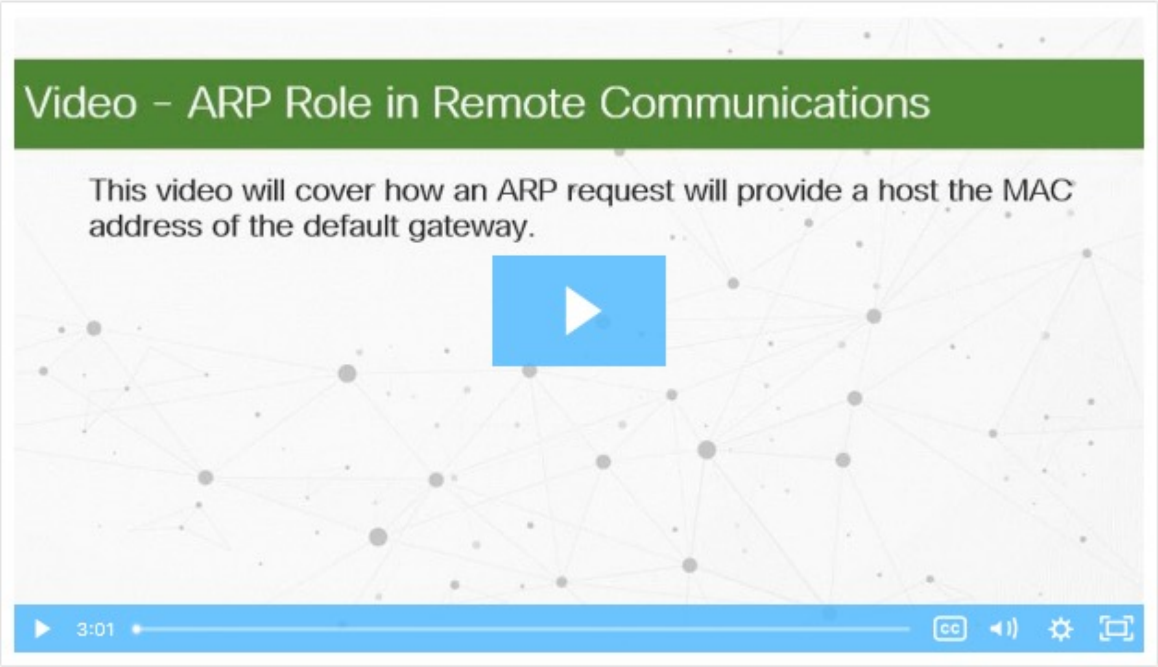
This video will cover an ARP reply in response to an ARP request.

https://www.youtube.com/watch?v=DnbQ6hjBeqI

ARP

Video - ARP Role in Remote Communication

- Click Play to view a demonstration of an ARP request and ARP reply associated with the default gateway.



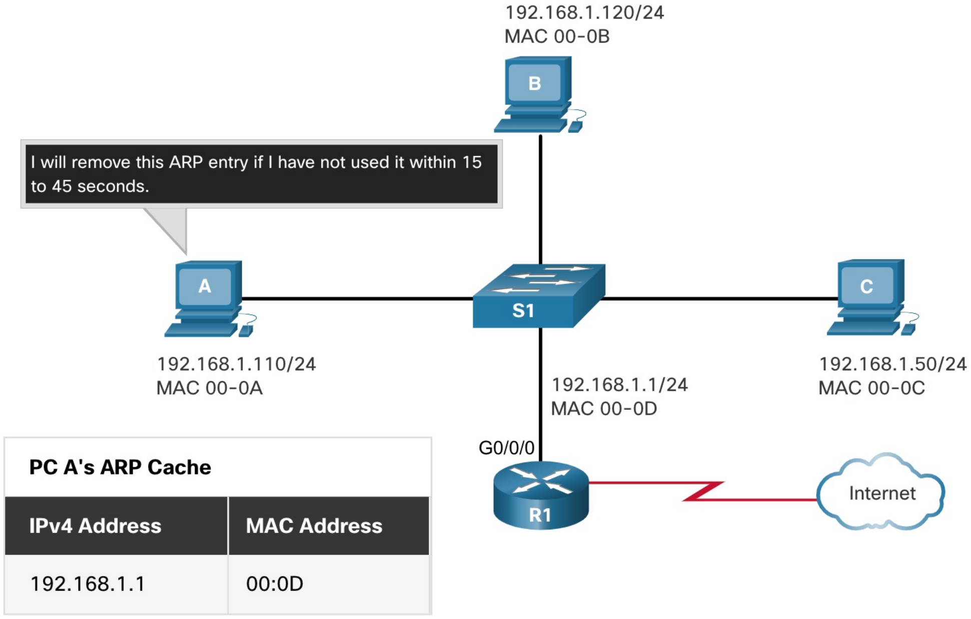
Video – ARP Role in Remote Communications

This video will cover how an ARP request will provide a host the MAC address of the default gateway.

https://www.youtube.com/watch?v=IO31_zPHLNk

Removing Entries from an ARP Table

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



I will remove this ARP entry if I have not used it within 15 to 45 seconds.

PC A's ARP Cache

IPv4 Address	MAC Address
192.168.1.1	00:0D

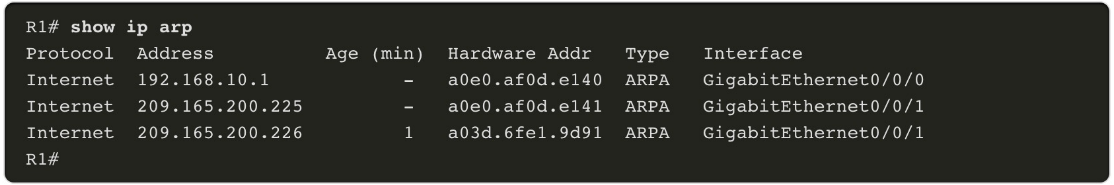
Note: MAC addresses are shortened for demonstration purposes.

ARP

ARP Tables on Networking Devices

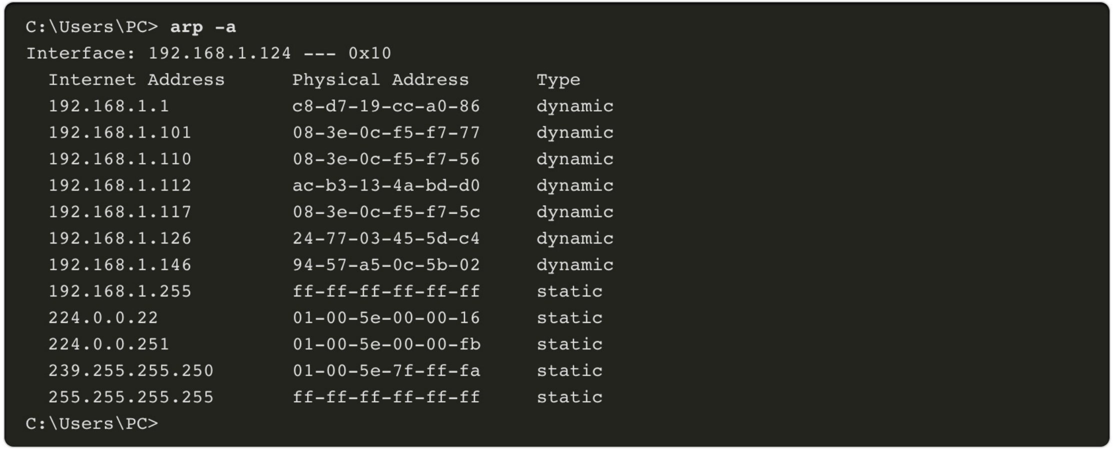
Network hosts and routers keep ARP tables.

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



```
R1# show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.10.1             -  a0e0.af0d.e140  ARPA   GigabitEthernet0/0/0
Internet  209.165.200.225          -  a0e0.af0d.e141  ARPA   GigabitEthernet0/0/1
Internet  209.165.200.226          1  a03d.6fe1.9d91  ARPA   GigabitEthernet0/0/1
R1#
```

On a Windows 10 PC, the **arp –a** command is used to display the ARP table.

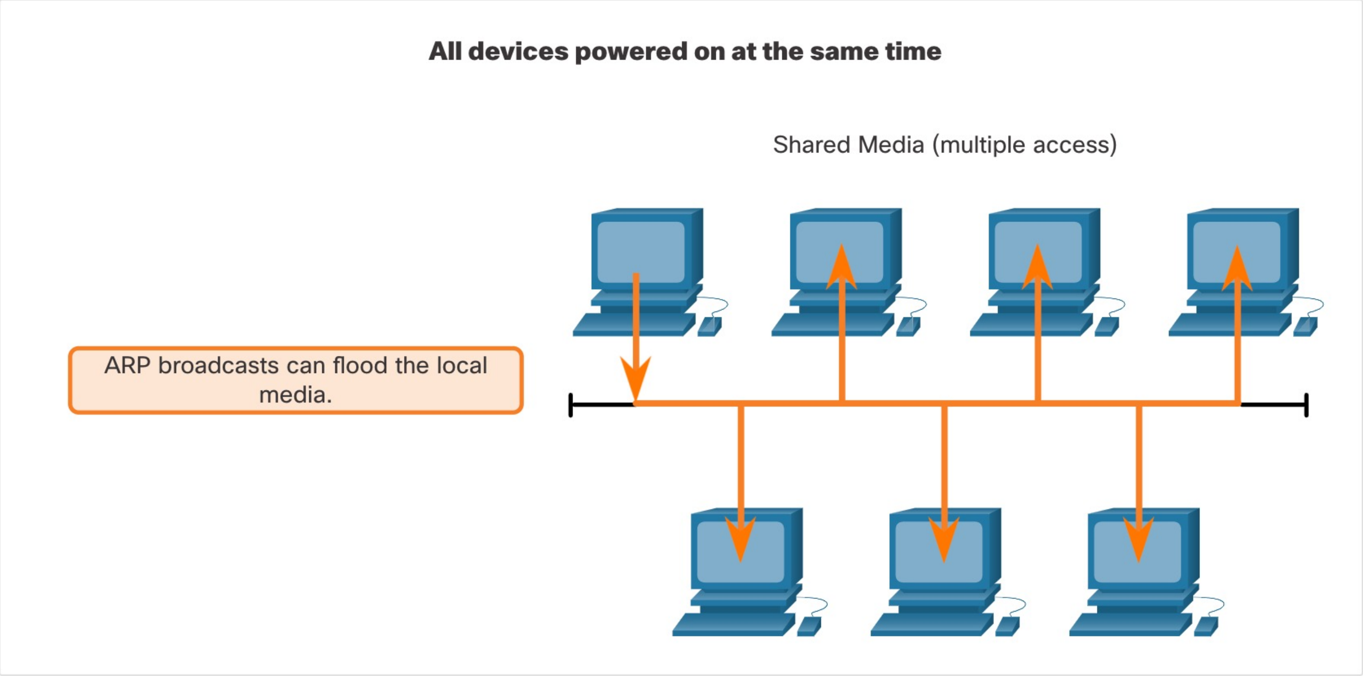


```
C:\Users\PC> arp -a
Interface: 192.168.1.124 --- 0x10
  Internet Address      Physical Address      Type
  192.168.1.1           c8-d7-19-cc-a0-86     dynamic
  192.168.1.101         08-3e-0c-f5-f7-77     dynamic
  192.168.1.110         08-3e-0c-f5-f7-56     dynamic
  192.168.1.112         ac-b3-13-4a-bd-d0     dynamic
  192.168.1.117         08-3e-0c-f5-f7-5c     dynamic
  192.168.1.126         24-77-03-45-5d-c4     dynamic
  192.168.1.146         94-57-a5-0c-5b-02     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
  239.255.255.250       01-00-5e-7f-ff-fa     static
  255.255.255.255       ff-ff-ff-ff-ff-ff     static
C:\Users\PC>
```

ARP Issues - ARP Broadcasts and ARP Spoofing

ARP Broadcasts

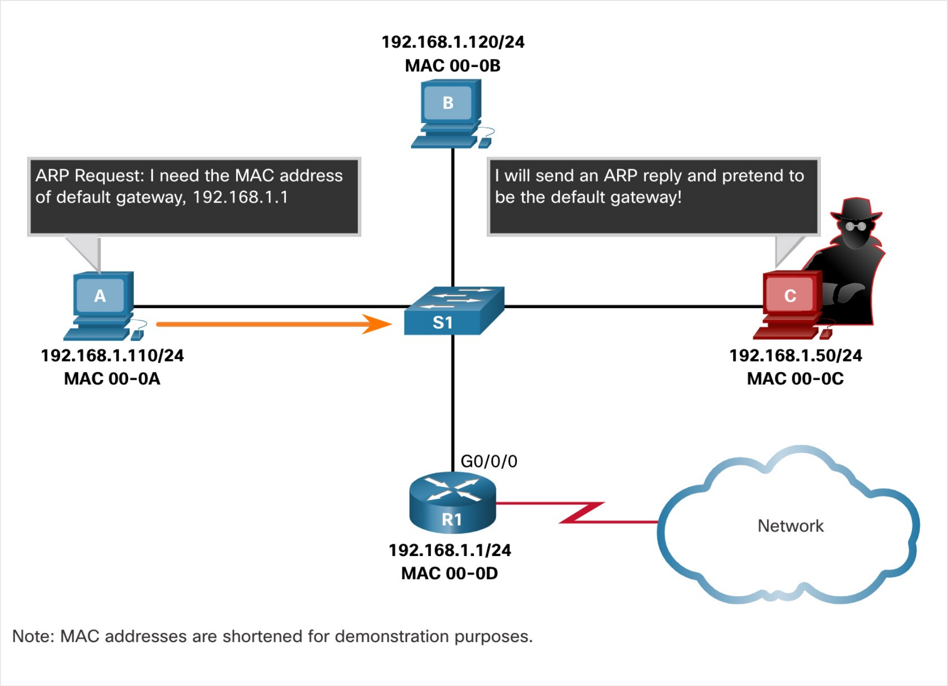
- ARP Broadcasts – could impact large networks. If many devices start accessing network services at the same time, there can be reduction in performance for a short time.


All devices powered on at the same time
Shared Media (multiple access)
ARP broadcasts can flood the local media.

ARP Issues - ARP Broadcasts and ARP Spoofing (Contd.)

ARP Spoofing (ARP poisoning) – security risk

- It is a technique used by a threat actor to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.


192.168.1.120/24
MAC 00-0B
B
ARP Request: I need the MAC address of default gateway, 192.168.1.1
I will send an ARP reply and pretend to be the default gateway!
A
S1
C
192.168.1.110/24
MAC 00-0A
192.168.1.50/24
MAC 00-0C
G0/0/0
R1
192.168.1.1/24
MAC 00-0D
Network

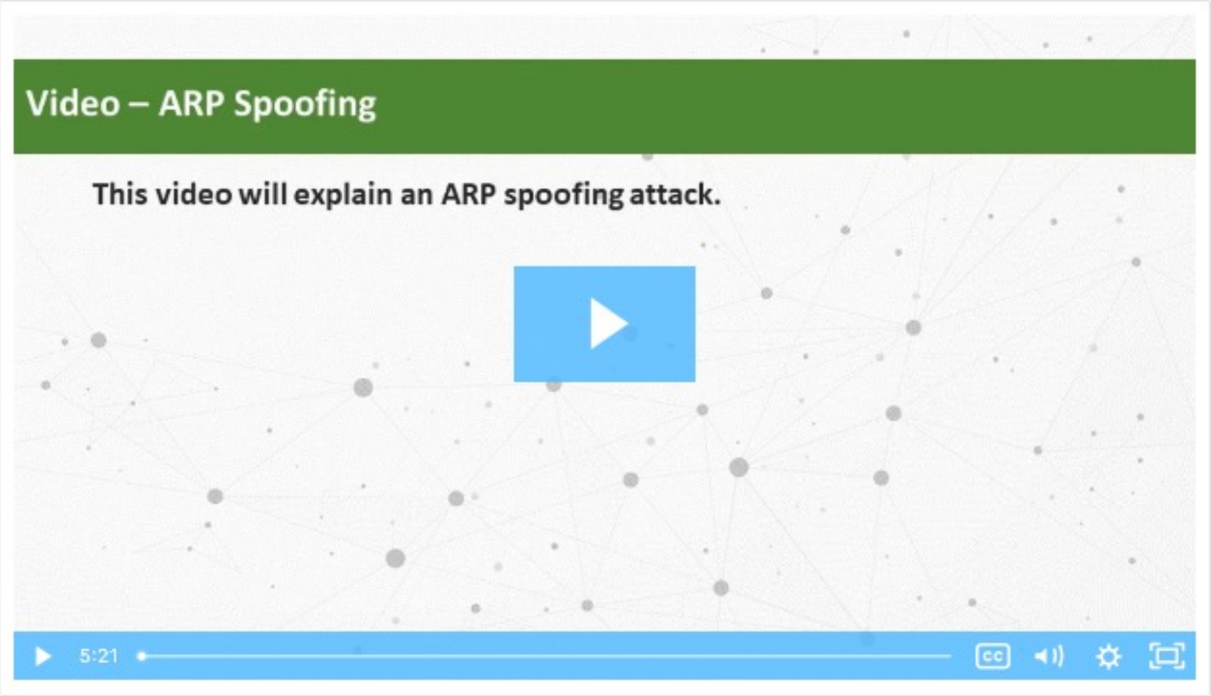
Note: MAC addresses are shortened for demonstration purposes.

The threat actor sends an ARP reply with its own MAC address.
The receiver of the ARP reply will add the wrong MAC address to its ARP table and send these packets to the threat actor.

ARP Issues

Video - ARP Spoofing

- Click Play in the figure to view a video about ARP Spoofing.



Video – ARP Spoofing

This video will explain an ARP spoofing attack.

https://www.youtube.com/watch?v=R_kC-jCEzho

Network Protocols and Services

New Terms and Commands

- IP Address
- MAC Address
- Address Resolution Protocol (ARP)

- ARP Table
- ARP Broadcast
- ARP Spoofing

Lab 12 – Using Wireshark to Examine Ethernet Frames

In this lab, you will do the following:

- Use Wireshark to capture and view Ethernet Frames in order to investigate ARP and IP and MAC addressing.
- Capture and analyze ICMP frames.