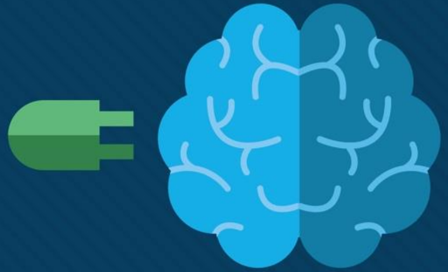


Module 8: Address Resolution Protocol

CyberOps Associate v1.0

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.

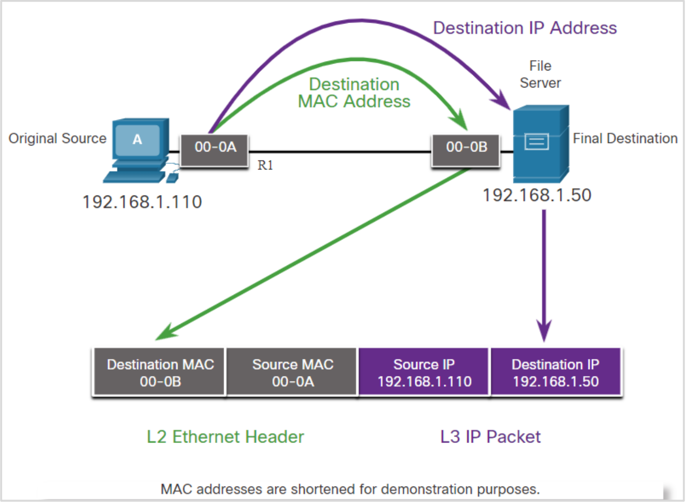
8.1 MAC and IP

Address Resolution Protocol

Destination on Same Network

- The two primary addresses assigned to a device on an Ethernet LAN:

Primary Addresses on Ethernet LAN	Description
Physical Address (The Mac Address)	• Used for Ethernet NIC to Ethernet NIC communications on the same network. • If the destination IP address is on the same network, the destination MAC address will be that of the destination device.
Logical Address (The IP Address)	• Used to send the packet from the original source to the final destination. • The destination IP address may be on the same IP network as the source or may be on a remote network.

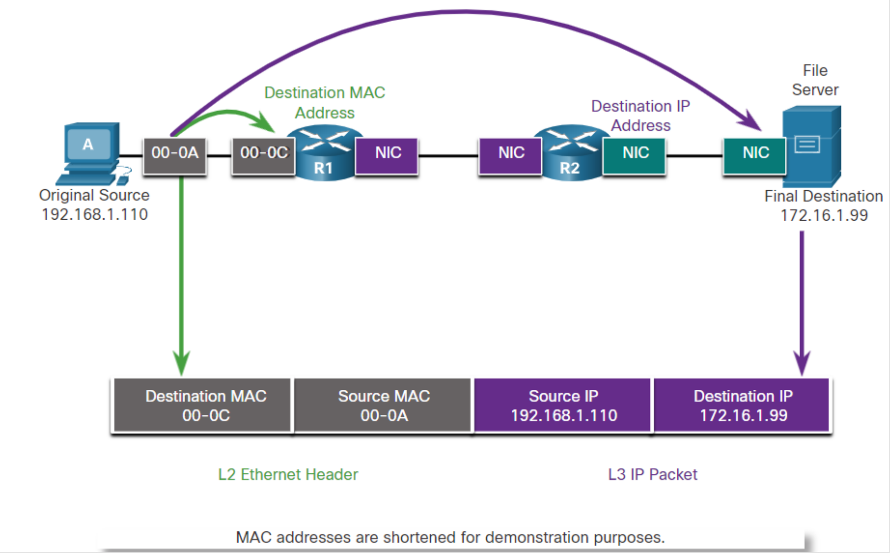


Communicating on a local network

***Note**: Most applications use Domain Name System (DNS) to determine the IP address when given a domain name such as www.cisco.com.*

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. The process in the figure is as below:
  - Routers examine the destination IPv4 address.
  - When the router receives the Ethernet frame, it de-encapsulates the Layer 2 information.
  - Using the destination IP address, the router determines the next-hop device, and then encapsulates the IP packet in a new data link frame for the outgoing interface.
  - If the next-hop device is the final destination, the destination MAC address will be that of the device’s Ethernet NIC.



Destination MAC	Source MAC	Source IP	Destination IP
00-0C	00-0A	192.168.1.110	172.16.1.99

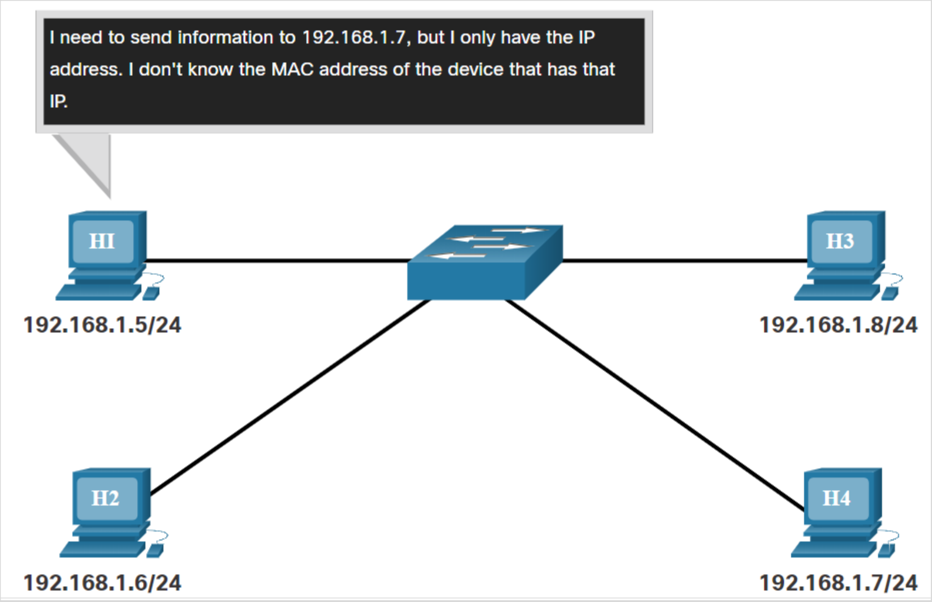
MAC addresses are shortened for demonstration purposes.

Communicating on a remote network

8.2 ARP

ARP Overview

- The figure illustrates a problem while sending a packet to another host on the same local IPv4 network because the IP address is known but the MAC address of the device is unknown.
- 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

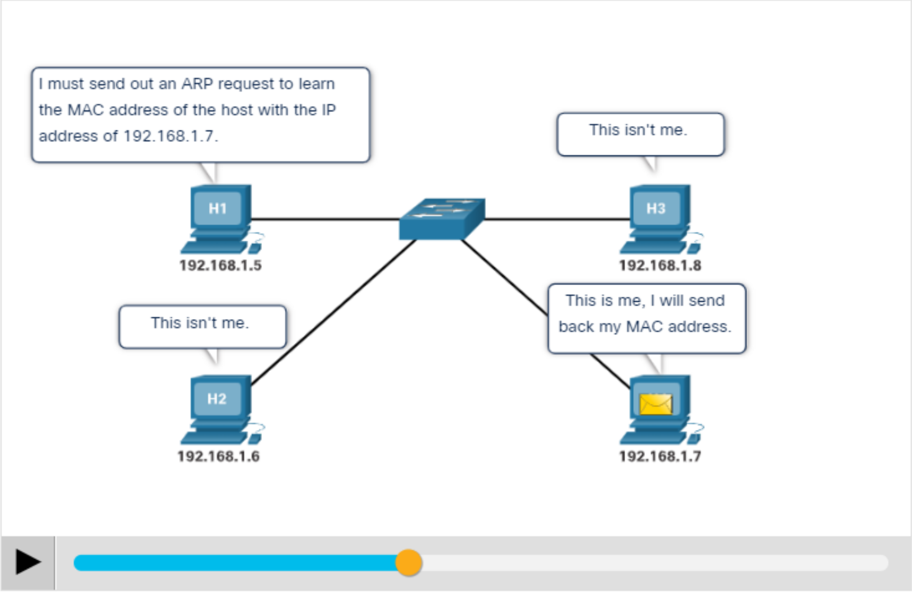


I need to send information to 192.168.1.7, but I only have the IP address. I don't know the MAC address of the device that has that IP.

ARP Functions

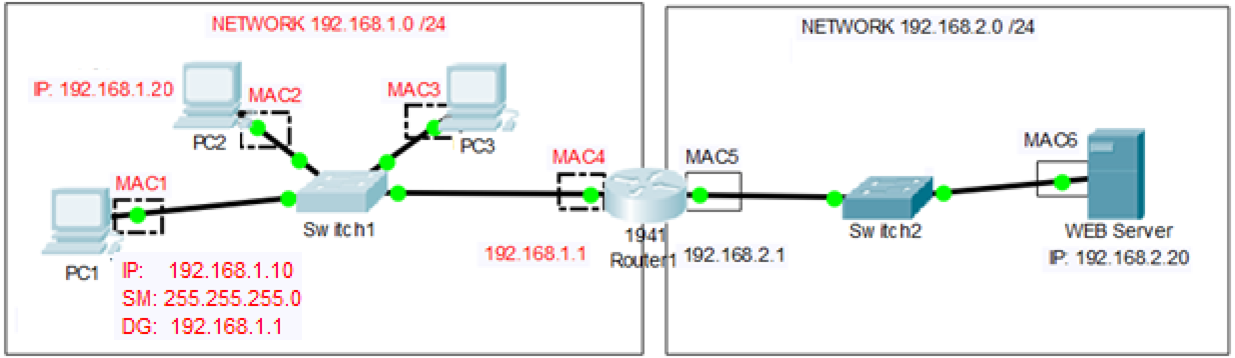
- When a packet is sent to the data link layer to be encapsulated into an Ethernet frame, the device refers to a table called **ARP table** or *ARP cache* in its RAM memory to find the MAC address that is mapped to the IPv4 address.
- The sending device will search its ARP table for a destination IPv4 address and a corresponding MAC address, if the packet's destination IPv4 address is on the same network as the source IPv4 address.
- If the device locates the IPv4 address, its corresponding MAC address is used as the destination MAC address in the frame.

Click play in the figure to see an animation of the ARP function.


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

ARP Operation – (Aynı Networkte iletişim)



IP: 192.168.1.10
SM: 255.255.255.0
DG: 192.168.1.1

```
C:\>arp -a
No ARP Entries Found
```

```
C:\>ping 192.168.1.20
Pinging 192.168.1.20 with 32 bytes of data:
Reply from 192.168.1.20: bytes=32 time=6ms TTL=128
Reply from 192.168.1.20: bytes=32 time=6ms TTL=128
```

S.MAC	D.MAC	S.IP	D.IP	Ping Data
MAC1	??	1.10	1.20	ICMP echo request

1) ARP Request (Broadcast)

MAC1	FF...FF	1.10	1.20	Hey, 192.168.1.20 Bana MAC'ini söyle!

2) ARP Reply (Unicast)

MAC2	MAC1	1.20	1.10	Dostum ben 1.20 MAC Adresim: MAC2

```
C:\>arp -a
  Internet Address      Physical Address      Type
  192.168.1.20         000c.852e.33aa        dynamic
```

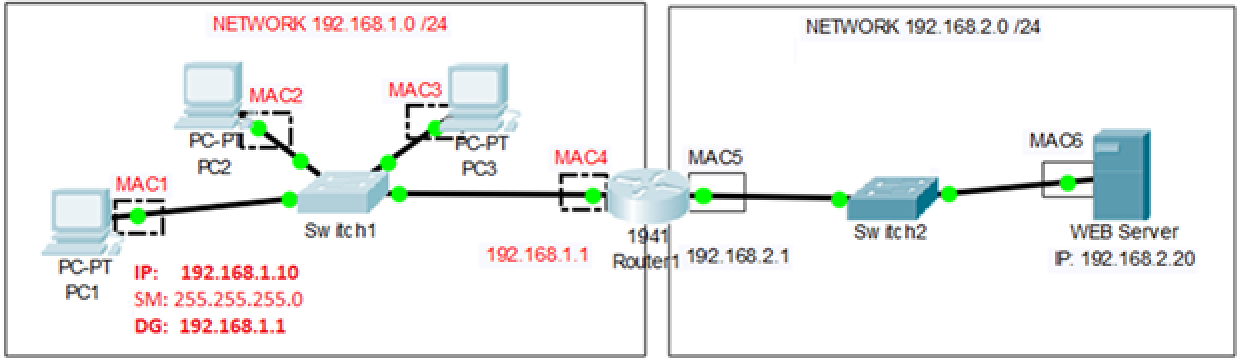
3) ARP Tablosu güncellenir

4) Data paketi hedef MAC Adresi eklenerek iletilir

- ARP tablosunda belirli bir süredir kullanılmayan ARP girişlerini kaldırır

ARP

ARP Operation – (Farklı bir Networkle iletişim) (Remote Network)



```
C:\>arp -a
No ARP Entries Found
```

```
C:\>ping 192.168.2.20
Request timed out.
Reply from 192.168.2.20: bytes=32 time=1ms TTL=127
Reply from 192.168.2.20: bytes=32 time<1ms TTL=127
```

```
C:\>arp -a
 Internet Address     Physical Address     Type
 192.168.1.1          0001.c7ee.eb01       dynamic
```

S.MAC	D.MAC	S.IP	D.IP	Ping Data
MAC1	??	1.10	2.20	ICMP echo request

1) ARP Request (Broadcast)

MAC1	FF...FF	1.10	1.1	Hey Router 192.68.1.1 Bana MAC'ini söyle

2) ARP Reply (Unicast)

MAC4	MAC1	1.1	1.10	Dostum ben 1.1 MAC Adresim: MAC4

3) ARP Tablosu güncellenir

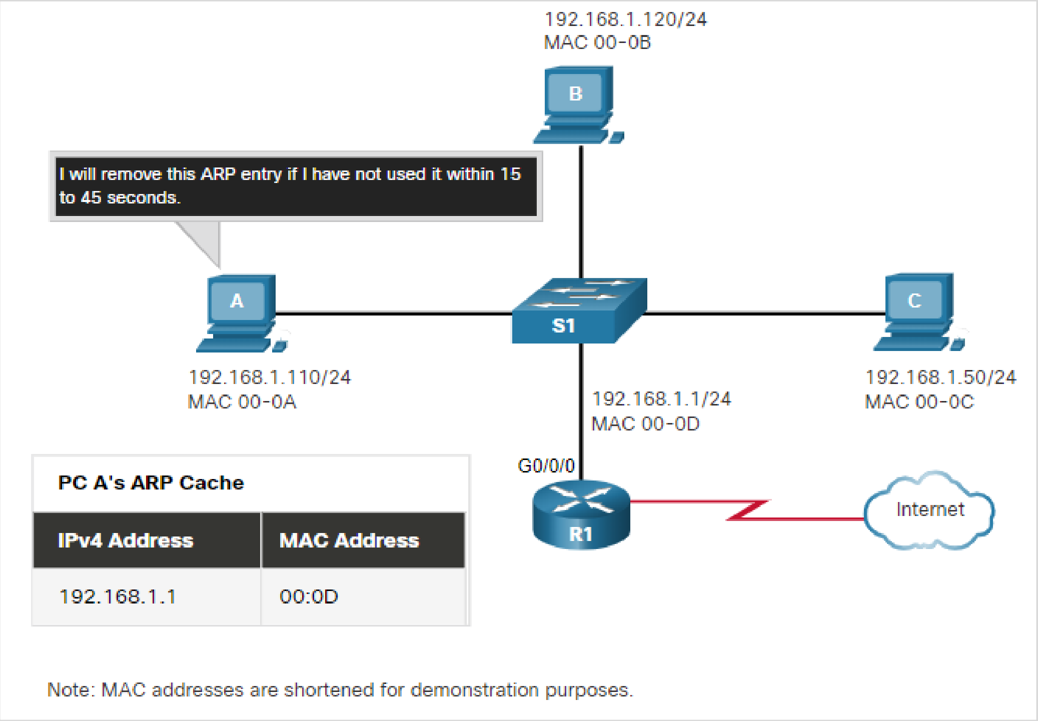
4) Data paketi Default Gateway MAC Adresi eklenerek iletilir

ARP Operation

***Note**: IPv6 uses a similar process to ARP for IPv4, known as **ICMPv6 Neighbor Discovery (ND)**. IPv6 uses **neighbor solicitation** and **neighbor advertisement** messages, similar to IPv4 ARP requests and ARP replies.*

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



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

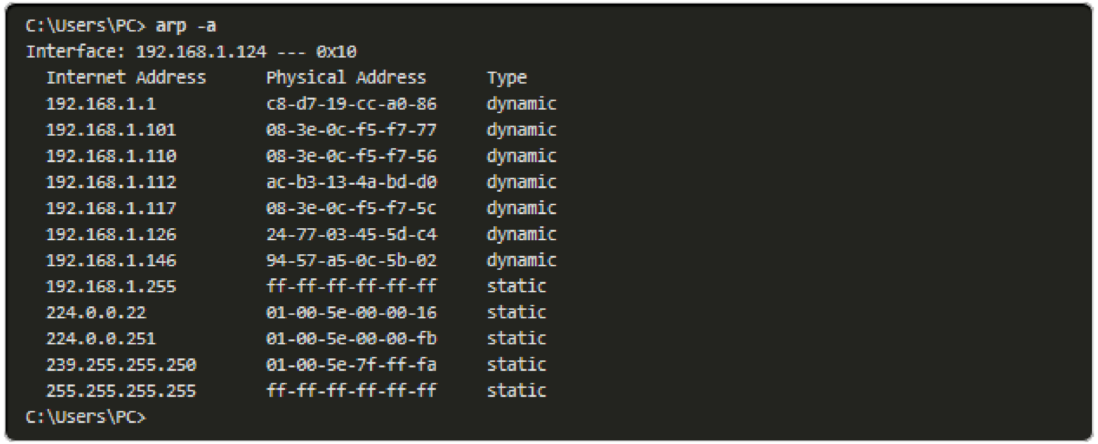
PC A's ARP Cache

IPv4 Address	MAC Address
192.168.1.1	00:0D

Note: MAC addresses are shortened for demonstration purposes.

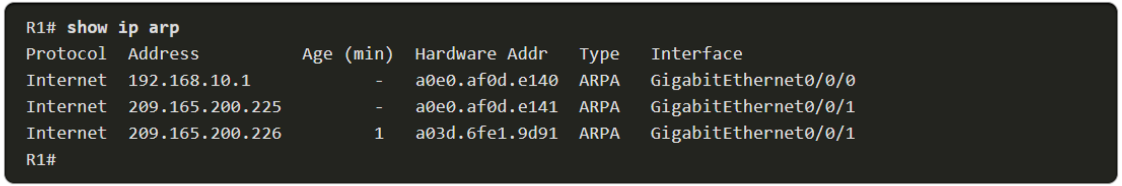
ARP Tables on Networking Devices

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>
```

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#
```

ARP

Lab - Wireshark to Examine Ethernet Frames

In this lab, you will do the following:

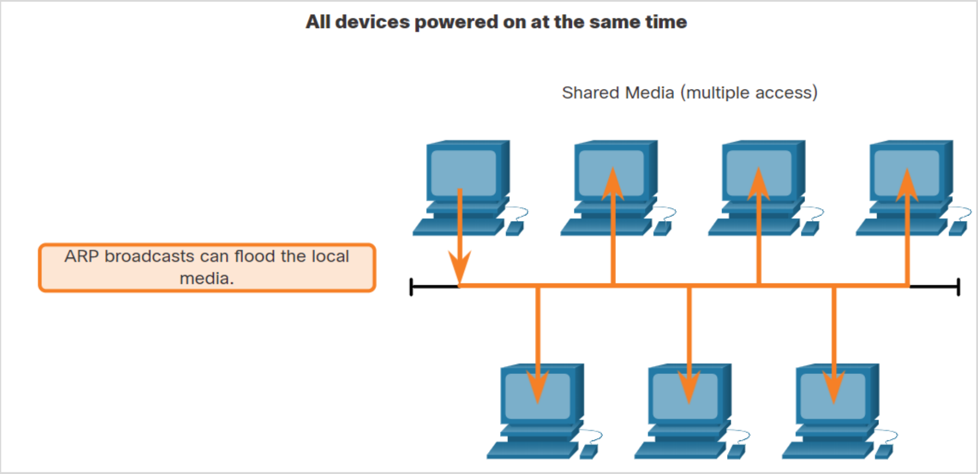
- Use Wireshark to capture and view Ethernet Frames in order to investigate ARP and IP and MAC addressing.
- Capture and analyze ICMP frames.

8.3 ARP Issues

ARP Issues - ARP Broadcasts and ARP Spoofing

ARP Broadcasts

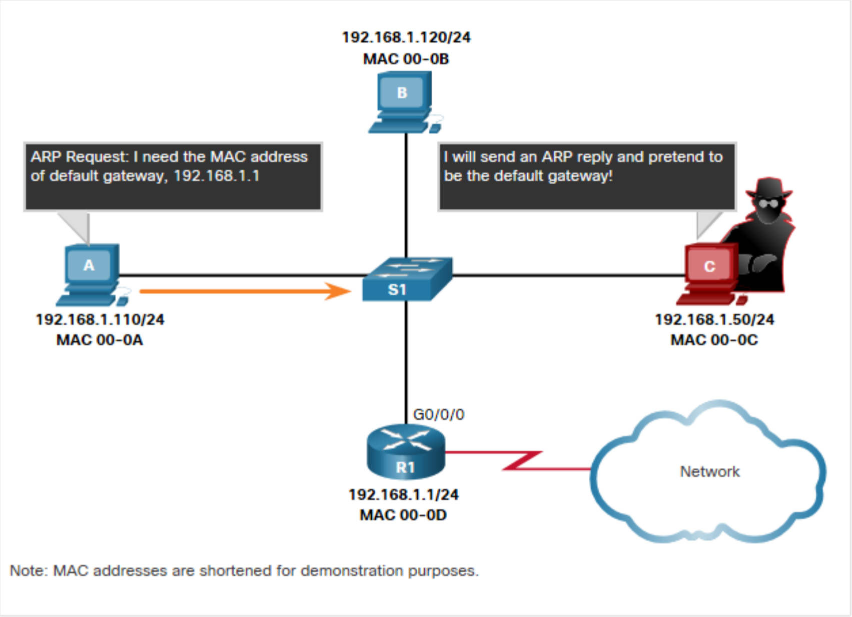
- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- On a typical business network, these broadcasts would have minimal impact on network performance.
- If many devices start accessing network services at the same time, there can be reduction in performance for a short time.
- After the devices send out the initial ARP broadcasts and have learned the necessary MAC addresses, any impact on the network will be minimized.


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

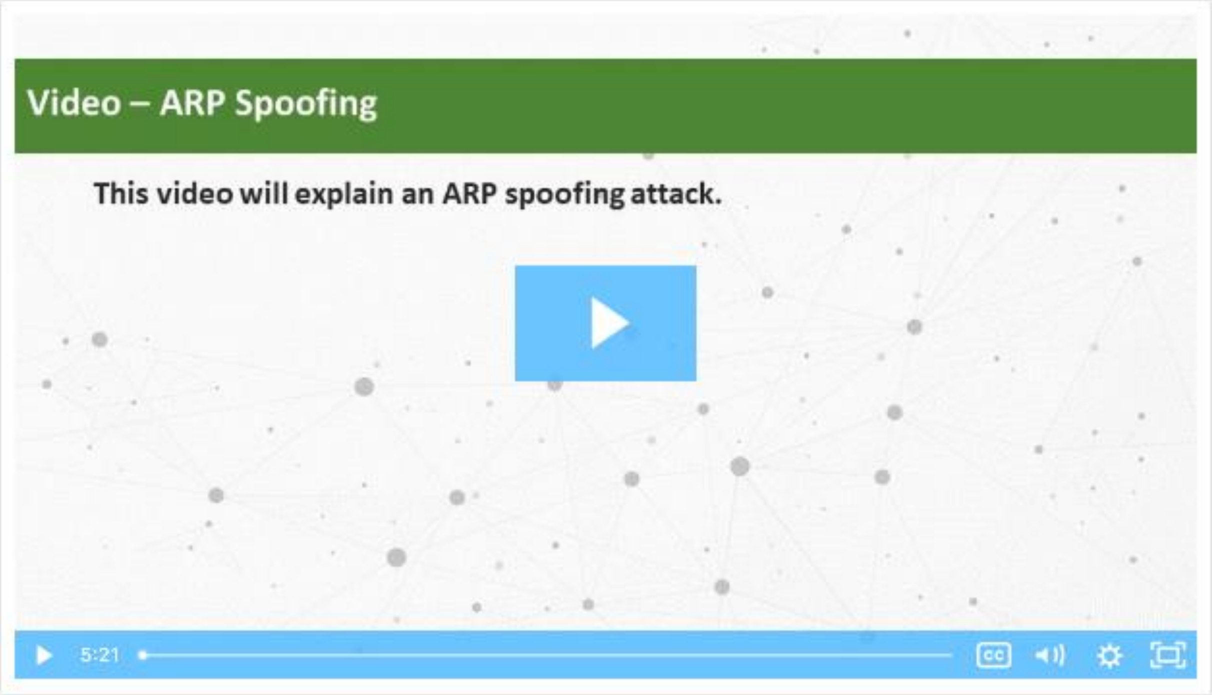
- The use of ARP can lead to a potential security risk in some cases.
- A threat actor uses ARP spoofing to perform an ARP poisoning attack.
  - It is a technique used by a threat actor to reply to an ARP request for an IPv4 address belonging to another device, such as the default gateway.
  - The threat 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.


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.

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.

8.4 Address Resolution Protocol Summary

What Did I Learn in this Module?

- IP addresses are used to identify the address of the original source device and the final destination device.
- MAC addresses are used to deliver the data link frame with the encapsulated IP packet from one NIC to another NIC on the same network.
- ARP is used to map the logical IPv4 address with the Layer 2 MAC address.
- ARP provides two basic functions: resolving IPv4 addresses to MAC addresses and maintaining a table of IPv4 to MAC address mappings.
- When the destination IPv4 address is on the same network as the source, the ARP process sends the IPv4 address to all hosts on the network so that the host with the matching IPv4 address can reply with the 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.

What Did I Learn in this Module? (Contd.)

- If there is no entry for the IPv4 address in its ARP table, the sending device sends out an ARP request to determine the destination MAC address.
- Only the device with the target IPv4 address associated with the ARP request will respond with an ARP reply.
- In IPv6, ICMPv6 Neighbor Discovery (ND) is used.
- As a broadcast frame, an ARP request is received and processed by every device on the local network.
- A threat actor can use ARP spoofing to perform an ARP poisoning attack by replying to an ARP request for an IPv4 address belonging to another device, such as the default gateway.