Chapter 5B

Address Resolution Protocol (ARP)
Introduction to Address Resolution Protocol (ARP)

“address resolution” refers to the process of finding an address of a computer in a network.

When data are sent from one device to another, the OS must have a way to determine the MAC address of the destination device.
ARP
Introduction to Address Resolution Protocol (ARP)

The MAC address is "resolved" using the Address Resolution Protocol (ARP). Information of IP addresses and MAC addresses are stored in the ARP table.
Introduction to Address Resolution Protocol (ARP)

Function of ARP

When data are sent from a node, the IP address and the MAC address of the receiving device are needed.

The ARP protocol provides two basic functions:

- Resolving IPv4 addresses to MAC addresses
- Maintaining a table of mappings (IP address and MAC address of all devices in the network).
ARP
Introduction to Address Resolution Protocol (ARP)

When you try to ping an IP address on your local network, say 192.168.1.1, your system has to turn the IP address 192.168.1.1 into a MAC address. This involves using ARP.

Systems keep an **ARP look-up table** where they store information about what IP addresses are associated with what MAC addresses.

When trying to send a packet to an IP address, the system will first consult this table to see if it already knows the MAC address. If there is a value cached, ARP is not used.

If the IP address is not found in the ARP table, the system will then send a broadcast packet to the network using the ARP protocol to ask "who has 192.168.1.1". Because it is a broadcast packet, it is sent to a special MAC address that causes all machines on the network to receive it.

Any machine with the requested IP address will reply with an ARP packet that says "I am 192.168.1.1", and this includes the MAC address which can receive packets for that IP.
ARP Functions/Operation

ARP Table

- In an Ethernet local area network, a **table**, usually called the **ARP cache**, is used to keep a record of the MAC address and its corresponding IP address of a device.

- It is used by processes to find the data link layer address that is mapped to the destination IPv4 address.

- As a node receives frames from the media, **it records the source IP and MAC address in the ARP table.**

**Note**: Static map entries can be entered in an ARP table, but this is rarely done.
**ARP Functions/Operation**

**ARP Table** – contains IP address and MAC address of a device in a network.

```
C:UsersComputerA>arp -a

Interface: 192.168.1.1 --- 0xb

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Physical Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.2</td>
<td>00-0c-29-63-af-d0</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.1.255</td>
<td>ff-ff-ff-ff-ff-ff</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.22</td>
<td>01-00-5e-00-00-16</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.252</td>
<td>01-00-5e-00-00-fc</td>
<td>static</td>
</tr>
<tr>
<td>239.255.255.250</td>
<td>01-00-5e-7f-ff-fa</td>
<td>static</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>ff-ff-ff-ff-ff-ff</td>
<td>static</td>
</tr>
</tbody>
</table>
```
ARP

ARP Functions/Operation

ARP Request

- When a device sends data to an **IP address**, the ARP wills end out a request to ask for the **MAC address** of the IP address.
- Layer 2 broadcasts to all devices on the Ethernet LAN.
- The node that matches the IP address in the broadcast will reply.
- If no device responds to the ARP request, the packet is dropped because a frame cannot be created.
ARP
ARP Operation 1/5

The whole process using the ARP can be summarized in 5 steps.
Host A sends an ARP request looking for the MAC address associated with IP 10.10.0.3.
ARP

ARP Operation 3/5

Host A — ARP Cache

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host C, with IP address 10.10.0.3, responds with an ARP reply that includes its MAC address.

R1 interface G0/0
10.10.0.254
00-10-7b-e7-fa-ef

G0/0

Network
ARP

ARP Operation 4/5

Adding MAC-to-IP Map in ARP Cache

Host A — ARP Cache
10.10.0.3 00-0d-56-09-fb-d1

Host A
10.10.0.1
00-0d-88-c7-9a-24

Host B
10.10.0.2
00-08-a3-b6-ce-04

Host C
10.10.0.3
00-0d-56-09-fb-d1

Host D
10.10.0.4
00-12-3f-d4-6d-1b

Host A adds the MAC-to-IP address map to its ARP cache.
ARP

ARP Operation 5/5

Forwarding Data with MAC Address Information

Host A — ARP Cache

<table>
<thead>
<tr>
<th>Host A</th>
<th>Host B</th>
<th>Host C</th>
<th>Host D</th>
</tr>
</thead>
<tbody>
<tr>
<td>10.10.0.1</td>
<td>10.10.0.2</td>
<td>10.10.0.3</td>
<td>10.10.0.4</td>
</tr>
<tr>
<td>00-0d-88-c7-9a-24</td>
<td>00-08-a3-b6-ce-04</td>
<td>00-0d-56-09-fb-d1</td>
<td>00-12-3f-d4-6d-1b</td>
</tr>
</tbody>
</table>

Host A forwards data directly to Host C via MAC address.
ARP Role in Remote Communication

- If the destination IPv4 host is on the **local network**, the frame will use the MAC address of this device as the destination MAC address.

- If the destination IPv4 host is **not on the local network**, the source uses the ARP process to determine a MAC address for the router interface serving as the gateway.

- In the event that the gateway entry is not in the table, an ARP request is used to retrieve the MAC address associated with the IP address of the router interface.
ARP

Removing Entries from an ARP Table

- The 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

ARP Tables on Networking Devices

Router#show ip arp

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Address</th>
<th>Age (min)</th>
<th>Hardware Addr</th>
<th>Type</th>
<th>Interface</th>
</tr>
</thead>
<tbody>
<tr>
<td>Internet</td>
<td>172.16.233.229</td>
<td>-</td>
<td>0000.0c59.f892</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.233.218</td>
<td>-</td>
<td>0000.0c07.ac00</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.168.11</td>
<td>-</td>
<td>0000.0c63.1300</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
<tr>
<td>Internet</td>
<td>172.16.168.254</td>
<td>9</td>
<td>0000.0c36.6965</td>
<td>ARPA</td>
<td>Ethernet0/0</td>
</tr>
</tbody>
</table>

C:\>arp -a

Interface: 192.168.1.67 --- 0xa

<table>
<thead>
<tr>
<th>Internet Address</th>
<th>Physical Address</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.254</td>
<td>64-0f-29-0d-36-91</td>
<td>dynamic</td>
</tr>
<tr>
<td>192.168.1.255</td>
<td>ff-ff-ff-ff-ff-ff</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.22</td>
<td>01-00-5e-00-00-16</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.251</td>
<td>01-00-5e-00-00-fb</td>
<td>static</td>
</tr>
<tr>
<td>224.0.0.252</td>
<td>01-00-5e-00-00-fc</td>
<td>static</td>
</tr>
<tr>
<td>255.255.255.255</td>
<td>ff-ff-ff-ff-ff-ff</td>
<td>static</td>
</tr>
</tbody>
</table>
ARP Issues

ARP Problems

When there are too many too frequent ARP requests, the network system will be slowed down and result in other problems.

ARP Security Issues
ARP introduces a security risk resulting from ARP spoofing. For example, a hacker can fool a station by sending from a rogue network device a fictitious ARP response that includes the IP address of a legitimate network device and the MAC address of the rogue device. All legitimate stations automatically update their ARP tables with the false mapping.
Mitigating ARP Problems

To guard against hackers, segmentation is used. Segmentation isolate networks such that only authorized users can gain correct information from the ARP table.
LAN Switches
Switching

Switch Port Fundamentals

Layer 2 LAN Switch

- A LAN switch connects end devices to a central intermediate device on most Ethernet networks
- Performs switching and filtering based only on the MAC address
- Builds a MAC address table that it uses to make forwarding decisions
- Depends on routers to pass data between IP subnetworks
1. The switch receives a broadcast frame from PC 1 on Port 1.
2. The switch enters the source MAC address and the switch port that received the frame into the address table.
3. Because the destination address is a broadcast, the switch floods the frame to all ports, except the port on which it received the frame.
4. The destination device replies to the broadcast with a unicast frame addressed to PC 1.
5. The switch enters the source MAC address of PC 2 and the port number of the switch port that received the frame into the address table. The destination address of the frame and its associated port is found in the MAC address table.

6. The switch can now forward frames between source and destination devices without flooding, because it has entries in the address table that identify the associated ports.
Switching

Duplex Settings

**Half Duplex (CSMA/CD)**
- Unidirectional data flow
- Higher potential for collision
- Hub connectivity

**Full Duplex**
- Point-to-point only
- Attached to dedicated switched port
- Requires full-duplex support on both ends
- Collision-free
- Collision detect circuit disabled
Switching

MDI, MDIX

MDI – Medium Dependent Interface
MDIX – Medium Dependent Interface Crossover

MDI / MDIX IS a type of Ethernet port connection using twisted pair cabling.
Auto-MDIX

Automatic medium-dependent interface crossover (auto-MDIX) is enabled by default. When auto-MDIX is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately.
Frame Forwarding Methods on Cisco Switches

There are 2 methods of forwarding frames used in Cisco Switches:
• Store and Forward
• Cut-Through
  - Fast-forward
  - Fragment-Free
Switching
Frame Forwarding Methods on Cisco Switches

A cyclic redundancy check (CRC) is an error-detecting code.

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.
Switching

Cut-through Switching

Cut-through switching forwards a frame when it receives one, without any error-checking.

The advantage of cut-through switching over store-and-forward switching is, that the amount of time the switch takes to start forwarding the packet (referred to as the switch's latency) is about a few microsecond only, regardless of the packet size.

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

2 Types of Cut-through switching are:

Fast-forward switching:
- Lowest level of latency (fastest). Frames are immediately forwarded after destination address is read. Typical cut-through method of switching.

Fragment-free switching:
- The first 64 bytes of the frame are stored before forwarding is done. As most network errors and collisions occur during the first 64 bytes, this method can avoid errors.
Memory Buffering on Switches

An Ethernet switch may use a buffering technique to store and forward frames. Buffering may also be used when the destination port is busy. The area of memory where the switch stores the data is called the memory buffer.

The memory buffer can use 2 methods of buffering:
1. Port-based Buffering
2. Shared Memory Buffering
## Memory Buffering on Switches

### Port-Based and Shared Memory Buffering

<table>
<thead>
<tr>
<th>Type</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port-based memory</td>
<td>In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.</td>
</tr>
<tr>
<td>Shared memory</td>
<td>Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.</td>
</tr>
</tbody>
</table>
Fixed or Modular

Fixed versus Modular Configuration

Ethernet Switches are categorized into two main types:
- Modular Configuration
- Fixed Configuration.

**Modular switches** allows you to add expansion modules. It allows flexibility to address changing networks.

**Fixed Configuration** switches are switches with a fixed number of ports and are typically not expandable.
Fixed or Modular

Fixed versus Modular Configuration

Power over Ethernet (PoE)

IP Phone receives power through the Ethernet cable

Wireless Access Point receives power through the Ethernet cable
Fixed or Modular

Fixed versus Modular Configuration (cont.)

Types of Ethernet Switches

Fixed Configuration
Switches

Features and options are limited
to those that originally come
with the switch.

Stackable Configuration Switches

Modular Configuration
Switches

The chassis accepts
line cards that
contain the ports.
Fixed or Modular
Module Options for Cisco Switch Slots

**SFP.** (Small Form-factor Pluggable) - A small transceiver that plugs into the SFP port of a network switch and connects to Fibre Channel and Gigabit Ethernet (GbE) optical fiber cables at the other end.
Layer 3 Switching

Layer 2 Switching

Traditional **switching** operates at **layer 2** of the OSI model, where packets are sent to a specific **switch** port based on destination MAC addresses. Routing operates at **layer 3**, where packets are sent to a specific next-hop IP address, based on destination IP address.
Layer 3 Switching

Layer 3 Switching
Layer 3 Switching

Cisco Express Forwarding

Cisco devices which support Layer 3 switching utilize Cisco Express Forwarding (CEF). Two main components of CEF operation are the:

- **Forwarding Information Base (FIB)**
  - Conceptually it is similar to a routing table.
  - A networking device uses this lookup table to make destination-based switching decisions during Cisco Express Forwarding operation.
  - It is updated when changes occur in the network and contains all routes known at the time.

- **Adjacency Tables**
  - Maintain layer 2 next-hop addresses for all FIB entries.
Layer 3 Switching

Types of Layer 3 Interfaces

The major types of Layer 3 interfaces are:

- **Switch Virtual Interface (SVI)** – Logical interface on a switch associated with a virtual local-area network (VLAN).

- **Routed Port** – Physical port on a Layer 3 switch configured to act as a router port. Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command.

- **Layer 3 EtherChannel** – Logical interface on a Cisco device associated with a *bundle* of routed ports.
Layer 3 Switching
Configuring a Routed Port on a Layer 3 Switch

Routed Port Configuration

```
S1(config)#interface f0/6
S1(config-if)#no switchport
S1(config-if)#ip address 192.168.200.1 255.255.255.0
S1(config-if)#no shutdown
S1(config-if)#end
S1#
*Mar  1 00:15:40.115: %SYS-5-CONFIG_I: Configured from console by console
S1#show ip interface brief

Interface       IP-Address          OK? Method Status               Protocol
Vlan1           unassigned          YES unset administratively down down
FastEthernet0/1  unassigned          YES unset down               down
FastEthernet0/2  unassigned          YES unset down               down
FastEthernet0/3  unassigned          YES unset down               down
FastEthernet0/4  unassigned          YES unset down               down
FastEthernet0/5  unassigned          YES unset down               down
FastEthernet0/6  192.168.200.1  YES manual up                   up
FastEthernet0/7  unassigned          YES unset up                 up
FastEthernet0/8  unassigned          YES unset up                 up
<output omitted>
```
Chapter 5

Summary

- Ethernet is the most widely used LAN technology used today.
- Ethernet standards define both the Layer 2 protocols and the Layer 1 technologies.
- The Ethernet frame structure adds headers and trailers around the Layer 3 PDU to encapsulate the message being sent.
- As an implementation of the IEEE 802.2/3 standards, the Ethernet frame provides MAC addressing and error checking.
- Replacing hubs with switches in the local network has reduced the probability of frame collisions in half-duplex links.
- The Layer 2 addressing provided by Ethernet supports unicast, multicast, and broadcast communications.
- Ethernet uses the Address Resolution Protocol to determine the MAC addresses of destinations and map them against known Network layer addresses.
Chapter 5
Summary (cont.)

- Each node on an IP network has both a MAC address and an IP address.
- The ARP protocol resolves IPv4 addresses to MAC addresses and maintains a table of mappings.
- A Layer 2 switch builds a MAC address table that it uses to make forwarding decisions.
- Layer 3 switches are also capable of performing Layer 3 routing functions, reducing the need for dedicated routers on a LAN.
- Layer 3 switches have specialized switching hardware so they can typically route data as quickly as they can switch.
END OF CHAPTER 5B
Review

1. When a device sends information in a network, it only has the ____ address but not the ____ address.
1. When a device sends information in a network, it only has the **IP** address but not the **MAC** address.
2. The MAC address matching an IP address are stored in the _____ table.
Review

2. The MAC address matching an IP address are stored in the ARP table.
Review

3. The ARP protocol provides two basic functions:
   - Resolving IPv4 addresses to ______ addresses
   - Maintaining a table of ________ (IP address and MAC address of all devices in the network).
Review

3. The ARP protocol provides two basic functions:
   - Resolving IPv4 addresses to MAC addresses
   - Maintaining a table of mappings (IP address and MAC address of all devices in the network).
Review

4. In an Ethernet local area network, a **table**, usually called the ____ __________.
Review

4. In an Ethernet local area network, a table, usually called the ARP Cache.
Review

- 5. The ARP cache timer __________ ARP entries that have not been used for a specified period of time.

- Commands may also be used to __________ remove all or some of the entries in the ARP table.
Review

5. The 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.
Review

6. Problems that ARP may create:
   a. Network can slow down if there are too ______ ARP requests.
   b. Network if open to _______ attacks.
Review

6. Problems that ARP may create:
   a. Network can slow down if there are too many ARP requests.
   b. Network if open to hacking attacks.
Review

7. To guard against hackers, ____________ is used.

It ________ networks such that only authorized users can gain correct information from the ARP table.
Review

7. To guard against hackers, segmentation is used.

It isolates networks such that only authorized users can gain correct information from the ARP table.
Switching

Switch Port Fundamentals

Layer 2 LAN Switch

- A LAN switch connects end devices to a central intermediate device on most Ethernet networks
- Performs **switching and filtering** based only on the MAC address
- Builds a **MAC address table** that it uses to make forwarding decisions
- Depends on routers to pass data between IP **subnetworks**
Review

8. In Half-Duplex systems, data travel in _____ direction.

In Full-Duplex systems, data travel in _____ directions.
Review

8. In Half-Duplex systems, data travel in one direction.

In Full-Duplex systems, data travel in both directions.
Review

9. Automatic medium-dependent interface crossover (auto-MDIX) is ________ by default.

When auto-MDIX is enabled on an interface, the interface automatically ________ the required cable connection type (straight through or crossover) and configures the connection appropriately.
Review

9. Automatic medium-dependent interface crossover (auto-MDIX) is enabled by default. When auto-MDIX is enabled on an interface, the interface automatically detects the required cable connection type (straight through or crossover) and configures the connection appropriately.
Review

10. There are 2 methods of forwarding frames used in Cisco Switches:
   • Store and __________
   • Cut-__________
     - Fast-forward
     - Fragment-Free
10. There are 2 methods of forwarding frames used in Cisco Switches:
   • Store and **Forward**
   • **Cut-Through**
     - Fast-forward
     - Fragment-Free
11. A cyclic redundancy check (CRC) is an ________ code.
Review

11. A cyclic redundancy check (CRC) is an error-detecting code.
Review

12. 2 Types of Cut-through switching are:

**Fast-forward switching:**
- Frames are _____________ forwarded after destination address is read. Typical cut-through method of switching

**Fragment-free switching:**
- The first ________of the frame are stored before forwarding is done.

As most network errors and collisions occur during the first 64 bytes, this method can avoid errors.
Review

12. 2 Types of Cut-through switching are:

Fast-forward switching:
- Frames are immediately forwarded after destination address is read. Typical cut-through method of switching

Fragment-free switching:
- The first 64 bytes of the frame are stored before forwarding is done. As most network errors and collisions occur during the first 64 bytes, this method can avoid errors.
Review

13. An Ethernet switch may use a buffering technique to store and forward frames. The area of memory where the switch stores the data is called the ________ ________.

The memory buffer can use 2 methods of buffering:

_____________ Buffering
Shared Memory Buffering
13. An Ethernet switch may use a buffering technique to store and forward frames. The area of memory where the switch stores the data is called the **memory buffer**.

The memory buffer can use 2 **methods** of buffering:

- **Port-based Buffering**
- **Shared Memory Buffering**
Review

14.

Port-based Buffering – frames are stored in ________.

Shared Memory Buffering – frames are stored in a common ________ ________.
Review

14.

Port-based Buffering – frames are stored in queues.

Shared Memory Buffering – frames are stored in a common memory buffer.

<table>
<thead>
<tr>
<th>Port-based memory</th>
<th>In port-based memory buffering, frames are stored in queues that are linked to specific incoming and outgoing ports.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Shared memory</td>
<td>Shared memory buffering deposits all frames into a common memory buffer, which all the ports on the switch share.</td>
</tr>
</tbody>
</table>
Review

15. Ethernet Switches are categorized into two main types:

- __________ Configuration
- __________ Configuration.
15. Ethernet Switches are categorized into two main types:

- Modular Configuration
- Fixed Configuration.
16.

**Modular switches** allows you to add __________ modules. It allows flexibility to address changing networks.

**Fixed Configuration** switches are switches with a ______ number of ports and are typically not expandable.
Review

16.

**Modular switches** allows you to add expansion modules. It allows flexibility to address changing networks.

**Fixed Configuration** switches are switches with a fixed number of ports and are typically not expandable.
Review

17. **SFP.** (Small Form-factor Pluggable) is a small __________ that plugs into the **SFP** port of a network switch and connects to Fibre Channel and Gigabit Ethernet (GbE) optical fiber cables at the other end.
Review

17. **SFP.** (Small Form-factor Pluggable) is a small transciever that plugs into the SFP port of a network switch and connects to Fibre Channel and Gigabit Ethernet (GbE) optical fiber cables at the other end.
Review

18. There are _______ types of SFP Modules
Review

18. There are three types of SFP Modules
19. The major types of Layer 3 interfaces are:

- **SVI** – Logical interface on a switch associated with a virtual local-area network (VLAN).

- Physical port on a Layer 3 switch configured to act as a router port. Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command.

- **Layer 3 EtherChannel** – Logical interface on a Cisco device associated with a *bundle* of routed ports.
19. The major types of Layer 3 interfaces are:

- **Switch Virtual Interface (SVI)** – Logical interface on a switch associated with a virtual local-area network (VLAN).

- **Routed Port** – Physical port on a Layer 3 switch configured to act as a router port. Configure routed ports by putting the interface into Layer 3 mode with the `no switchport` interface configuration command.

- **Layer 3 EtherChannel** – Logical interface on a Cisco device associated with a *bundle* of routed ports.
END OF CHAPTER 5