Week 8 Lab:
ARP & MAC tables, the glue between IP and MAC addresses

Due Date: At the **start** of your next lab period
Submission Requirement: Submit Lab08_AnswerSheet **via Blackboard** for Lab 8
ONLY 1 Lab per pair of lab partners (ie. a team of 2)
RENAME the file as: **Lab08_Surname1Surname2** !!!
Marking Scheme: Normal lab; marks as indicated on Lab08_AnswerSheet

Notes:

1. You will need to MANUALLY assign the IP address of your workstation as: 172.16.1.{station#}

2. You may not be able to complete this lab during lab period; therefore it is important to get screen and wireshark captures for all data before you start answering the questions!

Topology Diagram: Refer to previous labs for the topology diagram.

Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1-ISP	S0/0/0	10.10.10.6	255.255.255.252	N/A
	Fa0/0	192.168.254.253	255.255.255.0	N/A
R2-Central	S0/0/0	10.10.10.5	255.255.255.252	N/A
	Fa0/0	172.16.255.254	255.255.0.0	N/A
Eagle Server	N/A	192.168.254.254	255.255.255.0	192.168.254.253
	N/A	172.31.254.254	255.255.255.0	N/A
host*Pod#***A**	N/A	172.16.*Pod#*.1	255.255.0.0	172.16.255.254
host*Pod#***B**	N/A	172.16.*Pod#*.2	255.255.0.0	172.16.255.254
S1-Central	N/A	172.16.254.1	255.255.0.0	172.16.255.254

Learning Objectives

Upon completion of this lab, you will be able to:

- Use Windows **arp** command.
- Use Wireshark to examine ARP exchanges.

Background

Address Resolution Protocol (ARP) is used by TCP/IP to map a Layer 3 IP address to a Layer 2 MAC address. When a frame is placed on the network, it must have a destination MAC address. To dynamically discover the MAC address to the destination device, an ARP request is broadcast on the LAN. The device that contains the destination IP address responds, and the MAC address is recorded in ARP cache. Every device on the LAN keeps its own ARP cache, or small area in RAM that holds ARP results. An ARP cache timer removes ARP entries that have not been used for a certain period of time. Depending on the device, times differ. **For example, some Windows operating systems store ARP cache entries for 2 minutes. If the entry is used again during that time, the ARP timer for that entry is extended to 10 minutes.**

ARP is an excellent example in performance tradeoff. With no cache, ARP must continually request address translations each time a frame is placed on the network. This adds latency to the communication and could congest the LAN. Conversely, unlimited hold times could cause errors with devices that leave the network or change the Layer 3 address.

A network engineer needs to be aware of ARP but may not interact with the protocol on a regular basis. ARP is a protocol that enables network devices to communicate with the TCP/IP protocol. Without ARP, there is no efficient method to build the datagram Layer 2 destination address. Also, ARP is a potential security risk. ARP spoofing, or ARP poisoning, is a technique used by an attacker to inject the wrong MAC address association in a network. An attacker forges the MAC address of a device, and frames are sent to the wrong destination. Manually configuring static ARP associations is one way to prevent ARP spoofing. Finally, an authorized MAC address list may be configured Cisco devices to restrict network access to only approved devices.

Scenario

With a pod host computer, use the Windows **arp** utility command to examine and change ARP cache entries. In Task 2, Wireshark will be used to capture and analyze ARP exchanges between network devices.

Task 1: Use the Windows arp Command.

Step 1: Access the Windows terminal.

1. Open a Windows terminal by clicking **Start > Run**. Type **cmd**, and click **OK**.
   With no options, the **arp** command will display useful help information.
2. Issue the **arp** command on the pod host computer, and examine the output.

Q1. Answer the following questions about the ARP command.

What command would be used to display all entries in ARP cache?	
What command would be used to delete all ARP cache entries (flush ARP cache)?	
What command would be used to delete the ARP cache entry for 172.16.255.254?	

Step 2: Use the `arp` command to examine local ARP cache.

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

Figure 1. Empty ARP Cache

Without any network communication, the ARP cache would be empty. This is shown in Figure 1.

Delete all the ARP cache entries using an appropriate command from step 1.

Issue the command that displays ARP entries. What are the results?

Step 3: Use the `ping` command to dynamically add entries in the ARP cache.

The **`ping`** command can be used to test network connectivity. By accessing other devices, ARP associations are dynamically added to ARP cache.

```
C:\> ping 172.16.1.2
Pinging 172.16.1.2 with 32 bytes of data:
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Reply from 172.16.1.2: bytes=32 time<1ms TTL=128
Ping statistics for 172.16.1.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms
C:\>
```

Figure 2. `ping` Command to a Pod Host Computer

1. Use the command **`ipconfig /all`** to verify the pod host computer's Layer 2 and Layer 3 information.
2. Issue the **`ping`** command to another pod host computer (your partner device IP address); an example is shown in Figure 2. Figure 3 shows the new ARP cache entry.

```
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
C:\>
```

Figure 3. Display of ARP Cache

Fill in the table with the required information from the output of **arp –a** of your PC; add rows as required.

IP Address	Physical Address	How Discovered?

3. Do not send any traffic to the computer accessed previously. Every few seconds, check the ARP cache again until the entry for your partner's computer disappears.

Q2. How long did it take for the ARP cache entry for your partner's computer to clear?

____

4. Issue the **ping** command to the gateway, R2-Central. Examine the ARP cache entry, and fill in the below table:

IP Address	Physical Address	How Discovered?

5. Issue the **ping** command to Eagle Server, eagle-server.example.com. Examine the ARP cache entry.
6. Document the output of the ARP cache using the command **arp -a**

Q3. What is the physical address **used** for Eagle Server?

____

____

Q4. Why isn't there an ARP table entry for Eagle Server? What devices **never** have an entry in the ARP table?

____

____

Step 4: Manually adjust entries in the ARP cache.

To delete entries in ARP cache, issue the command **arp –d {inet-addr | *}**. Addresses can be deleted individually by specifying the IP address, or all entries can be deleted with the wildcard *****.

Verify that the ARP cache contains two entries: one for the Gateway and one to the partner's pod host computer. It may be easier to ping both devices more than once, which will retain the cache entry for approximately 10 minutes.

```
C:\> arp –a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
  172.16.255.254        00-0c-85-cf-66-40     dynamic
C:\>
C:\>arp -d 172.16.255.254
C:\> arp -a
Interface: 172.16.1.1 --- 0x60004
  Internet Address      Physical Address      Type
  172.16.1.2            00-10-a4-7b-01-5f     dynamic
C:\>
```

Figure 4. Manually Removing an ARP Cache Entry

See Figure 4, which shows how to manually delete an ARP cache entry.

1. On your computer, first verify that the two entries are present. If not, ping the missing entry.

Record the two ARP cache entries:

Device	IP Address	Physical Address	How Discovered?

2. Next, determine what command will delete the entry for your partner's computer. Issue the command on your pod host computer. Record the remaining ARP cache entry:

Device	IP Address	Physical Address	How Discovered?

3. Determine the command that will delete all entries in ARP cache. Issue the command on your pod host computer, and examine the ARP cache with the command **`arp -a`**. All entries should be removed.
4. Consider a secure environment where the Gateway controls access to a web server that contains Top Secret information.

Q5. What is one layer of security that can be applied to ARP cache entries that could aid in countering ARP spoofing?

____

____

5. Determine the command that will add a static ARP entry for the Gateway to ARP cache. Issue the command on your pod host computer.
6. Examine the ARP cache again, and fill in the following table:

Q6. Fill in the following table after you have successfully added the static ARP entry:

IP Address	Physical Address	Type

7. Remove the static entry from the ARP table so that you are ready for the next task.

For the next task, Wireshark will be used to capture and examine an ARP exchange. Do not close the Windows terminal—it will be used to view the ARP cache.

Task 2: Use Wireshark to Examine ARP Exchanges.

Step 1: Configure Wireshark for packet captures.

Prepare Wireshark for captures.

1. Click **Capture > Options**.
2. Select the Interface that corresponds to the LAN.
3. Check the box to Update list of packets in real time.
4. Click **Start**.

This will begin the packet capture.

Step 2: Prepare the pod host computer for ARP captures.

1. If not already completed, open a Windows terminal window by clicking **Start > Run**. Type **`cmd`**, and click **OK**.
2. Flush the ARP cache, which will require ARP to rediscover address maps. Write the command that you used: ______________________________________

Step 3: Capture and evaluate ARP communication.

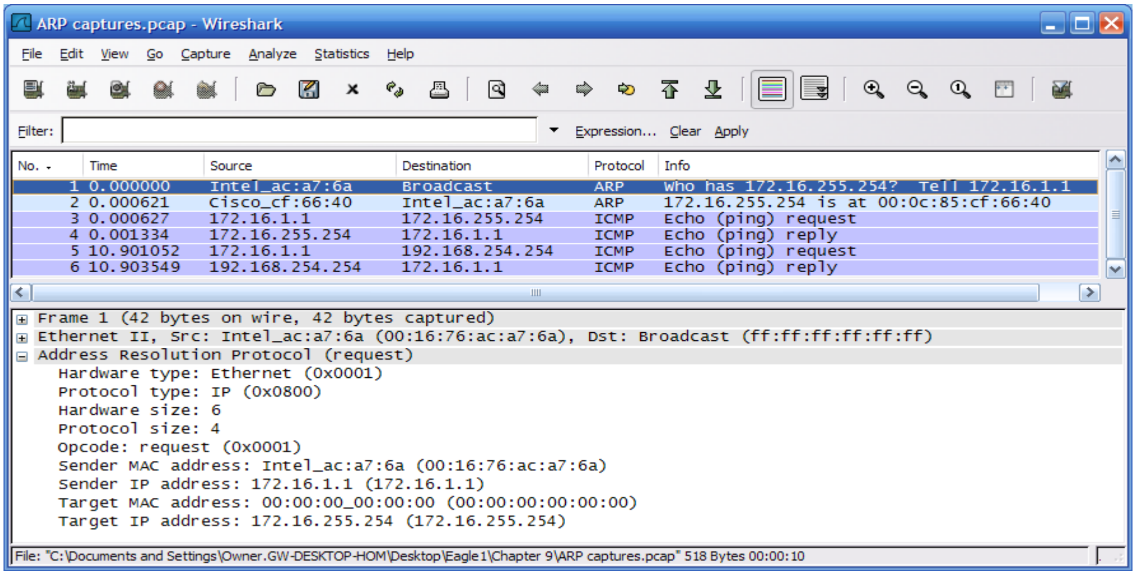
In this step, one ping request will be sent to the Gateway, and one ping request will be sent to Eagle Server. Afterward, Wireshark capture will be stopped and the ARP communication evaluated.

1. Send one ping request to the Gateway, using the command **`ping –n 1 172.16.255.254.`**

Document the output:

2. Send one ping request to Eagle Server, using the command **`ping –n 1 192.168.254.254`**.

Document the output:


ARP captures.pcap - Wireshark
File Edit View Go Capture Analyze Statistics Help
Filter:
Expression... Clear Apply

```
No. .  Time        Source             Destination        Protocol  Info
  1 0.000000    Intel_ac:a7:6a     Broadcast          ARP       Who has 172.16.255.254?  Tell 172.16.1.1
  2 0.000621    Cisco_cf:66:40     Intel_ac:a7:6a     ARP       172.16.255.254 is at 00:0c:85:cf:66:40
  3 0.000627    172.16.1.1         172.16.255.254     ICMP      Echo (ping) request
  4 0.001334    172.16.255.254     172.16.1.1         ICMP      Echo (ping) reply
  5 10.901052   172.16.1.1         192.168.254.254    ICMP      Echo (ping) request
  6 10.903549   192.168.254.254    172.16.1.1         ICMP      Echo (ping) reply
```

```
⊞ Frame 1 (42 bytes on wire, 42 bytes captured)
⊞ Ethernet II, Src: Intel_ac:a7:6a (00:16:76:ac:a7:6a), Dst: Broadcast (ff:ff:ff:ff:ff:ff)
⊟ Address Resolution Protocol (request)
    Hardware type: Ethernet (0x0001)
    Protocol type: IP (0x0800)
    Hardware size: 6
    Protocol size: 4
    Opcode: request (0x0001)
    Sender MAC address: Intel_ac:a7:6a (00:16:76:ac:a7:6a)
    Sender IP address: 172.16.1.1 (172.16.1.1)
    Target MAC address: 00:00:00_00:00:00 (00:00:00:00:00:00)
    Target IP address: 172.16.255.254 (172.16.255.254)
```

File: "C:\Documents and Settings\Owner.GW-DESKTOP-HOM\Desktop\Eagle1\Chapter 9\ARP captures.pcap" 518 Bytes 00:00:10

Figure 5. Wireshark Capture of ARP Communication

3. Stop Wireshark and evaluate the communication. You should see a Wireshark screen similar to the screen shown in Figure 5. The Wireshark Packet list window displays the number of packets captured. The Packet Details Window shows ARP protocol contents.

4. Using your Wireshark capture, answer the following questions:
   What was the first ARP packet?

   ____

   What was the second ARP packet?

   ____

Q7. Fill in the following table with information about the first ARP packet

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

Fill in the following table with information about the second ARP packet:

Field	Value
Sender MAC address	
Sender IP address	
Target MAC address	
Target IP address	

Q8. If the Ethernet II frame for an ARP request is a broadcast, why does the Target MAC address contain all **0**'s?

____

Q9. Why was there no ARP request for the ping to Eagle Server?

____

____

Q10. How long should the gateway mapping be stored in ARP cache on the pod host computer? **Why**?

____

____

Task 3: Reflection

The ARP protocol maps Layer 3 IP addresses to Layer 2 MAC addresses. If a packet must move across networks, the Layer 2 MAC address changes with each hop across a router, but the Layer 3 address never changes.

ARP cache stores ARP address mappings. If the entry was learned dynamically, it will eventually be deleted from cache. If the entry was manually inserted in ARP cache, it is a static entry and will remain until the computer is turned off or the ARP cache is manually flushed.

Lab 9.8.2: Cisco Switch MAC Table Examination

Topology Diagram: One switch per pair of students; no connection to Eagle-server.

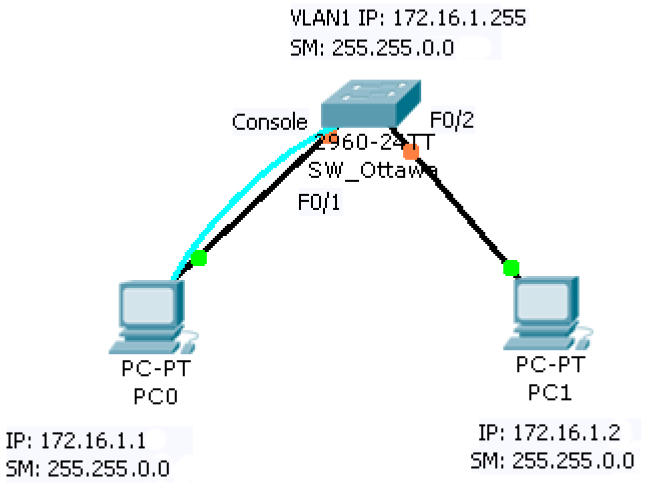


FIG (1)

Learning Objectives

Upon completion of this lab, you will be able to:

- Use the Telnet protocol to log into a Cisco Switch.
- Use the Cisco IOS command **`show mac address-table`** (eg. for switches in T113) to examine MAC address and port associations.

Background

Switches maintain a table of MAC addresses and associated switch port. When a switch receives a frame, the destination MAC address is checked against the table, and the corresponding port is used to route the frame out of the switch. If a switch does not know which port to route the frame, or the frame is a broadcast, then the frame is routed out all ports except the port where it originated.

Access to Cisco devices can be accomplished through several means. A console port can be used if the Cisco router or switch is within the same physical proximity of a computer. Using Windows hyperterm utility, a serial connection can be established. For devices physically distant from the network engineer, network connectivity can be established through two means. If the network is not secure, a modem configured on the AUX port enables telephone access. For secure networks, the Cisco device can be configured for a Telnet session. In this lab, the student will connect to the switch via a Telnet session.

Lab

- Telnet to Sw_Ottawa
- Use the command **`show mac address-table`** to examine the mac addresses and association to ports.

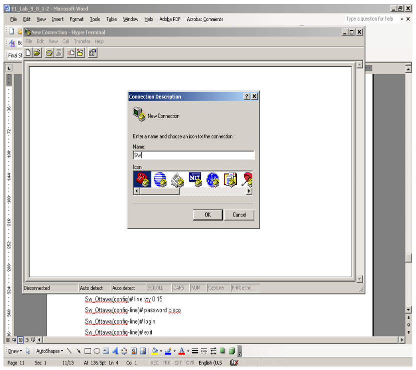
Scenario

Task 1: Configure the switch to allow remote access using Telnet Protocol.

a. Connect the devices as shown in FIG(1)

<u>Note:</u> Configure TCP/IP for PC0 and PC1 as shown in FIG(1)

b. Access the switch through console port from PC0 (using the hyper terminal program)


E1_Lab_9_8_1-2 - Microsoft Word
New Connection - HyperTerminal
OK
Cancel

Connection Description

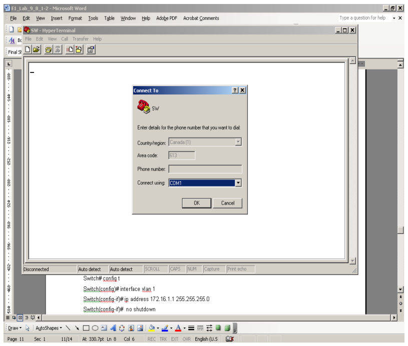
New Connection

Enter a name and choose an icon for the connection:

Name: SW

```
Sw_Ottawa(config)# line vty 0 15
Sw_Ottawa(config-line)# password cisco
Sw_Ottawa(config-line)# login
Sw_Ottawa(config-line)# exit
```

Step1



Connect To

SW

Enter details for the phone number that you want to dial:

Country/region: Canada (1)

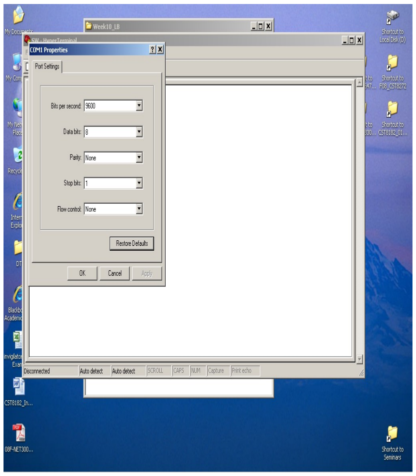
Area code: 613

Phone number:

Connect using: COM1

```
Switch# config t
Switch(config)# interface vlan 1
Switch(config-if)# ip address 172.16.1.1 255.255.255.0
Switch(config-if)#  no shutdown
```

Step2



COM1 Properties

Bits per second: 9600

Data bits: 8

Parity: None

Stop bits: 1

Flow control: None

Step3

c. Configure the switch with an IP address so you could telnet to it. Also configure the switch with a host name (Sw_Ottawa)

Switch> enable

Switch# config t

Switch(config)# interface vlan 1

Switch(config-if)# ip address 172.16.1.255 255.255.0.0

Switch(config-if)# no shutdown

Switch(config-if)# exit

Switch(config)# hostname Sw_Ottawa

Sw_Ottawa(config)#

d. **Configure the telnet password on VTY lines to allow for 16 telnet sessions at the same time to the switch using a password cisco when login:**

```
Sw_Ottawa(config)# line vty 0 15
Sw_Ottawa(config-line)# password cisco
Sw_Ottawa(config-line)# login
Sw_Ottawa(config-line)# exit
Sw_Ottawa(config)#
```

e. **Configure the secret password to access the privilege mode of the switch:**

```
Sw_Ottawa(config)# enable secret cisco
Sw_Ottawa(config)# end
Sw_Ottawa#
```

Task 2: Use the Telnet Protocol to Log in to a Cisco Switch.

Step 1: Access the Windows terminal (from PC1).

Open a Windows terminal by clicking **Start > Run**. Type **cmd**, and click **OK**.

Step 2: Use the Windows Telnet client to access Sw_Ottawa

Issue the Telnet command, **`telnet`** *`destination-ip-address`*:

```
C:/> telnet 172.16.1.255
```

An access prompt will be displayed, similar to the one shown in Figure 1.

```
PC>telnet 172.16.1.255
Trying 172.16.1.255 ...


User Access Verification

Password:
Sw_Ottawa>
```

Figure 1. Telnet Client

1. Now type **enable** to enter the privilege mode (Sw_Ottawa#). When the password prompt appears, type `cisco <ENTER>`.

   The `Sw_Ottawa` # prompt should appear.

Task 3: Use the Cisco IOS command "`show mac address-table`" to Examine MAC Addresses and Port Associations.

Step 1: Examine the switch MAC address table.

1. Issue the command **`show mac address-table? <ENTER>`**. This will output all options for the command.

2. Use the following table to fill in the command options:

Option	Description

Step 2: Examine dynamic MAC address table entries.

1. Issue the command **`show mac address-table`**.
   This command will display static (CPU) and dynamic, or learned entries.

<u>Document the output of the command:</u>

2. List the MAC addresses and corresponding switch ports:

MAC Address	Switch Port

Suppose there was a hub with five active hosts connected to switch port `gi0/0`. How many MAC addresses would be listed for switch port `gi0/0`? __________

Step 3: Examine MAC address table aging time.

1. Issue the command **`show mac address-table aging-time`**.
   This command will display the default time, in seconds, that MAC address entries are stored.

Q11. What is the default aging time for VLAN 1?

____

2. In preparation for the next step, flush the MAC address table of the switch:
   clear mac address-table dynamic
   and check the table again to ensure that it is empty
   show mac address-table

Step4: Examine MAC address table after establishing ping traffic in the network.

Now try to ping from PC0 to PC1 then check the mac address table.

Q12. Document the contents of the mac table.

____

____

Step5: Have your lab professor verify and sign-off that you have completed the lab correctly

To be fill in by Lab Instructor

☺ Console cabling ☺ Switch configuration

☺ Ping successful (PC0 → PC1)

____

Lab Instructor

Task 4: Reflection

Using the Telnet protocol, network engineers can access Cisco devices remotely across secure LANs. This has the benefit of permitting access to remote devices for troubleshooting and monitoring purposes.

A switch contains a MAC address table that lists the MAC address connected to each switch port. When a frame enters the switch, the switch performs a lookup of the frame destination MAC address. If there is a match in the MAC address table, the frame is routed out the corresponding port. Without a MAC address table, the switch would have to flood the frame out each port.

Task 5: Clean Up

Unless directed otherwise by the instructor, turn off power to the host computers. Remove anything that was brought into the lab, and leave the room ready for the next class.