

# Lab 9.3.7 Workstation ARP

# **Objective**

- Introduce Address Resolution Protocol (ARP) and the arp -a workstation command.
- Explore the arp command help feature using the -? option.

# **Background / Preparation**

ARP is used as a tool for confirming that a computer is successfully resolving network Layer 3 addresses to Media Access Control (MAC) Layer 2 addresses. The TCP/IP network protocol relies on IP addresses like 192.168.14.211 to identify individual devices and to assist in navigating data packets between networks. While the IP address is essential to move data from one LAN to another, it cannot deliver the data in the destination LAN by itself. Local network protocols, like Ethernet or Token Ring, use the MAC, or Layer 2, address to identify local devices and deliver all data. A computer MAC address has been seen in prior labs.

This is an example of a MAC address:

#### • 00-02-A5-9A-63-5C

A MAC address is a 48-bit address displayed in Hexadecimal (HEX) format. In this format each hex symbol represents 4 bits. The first half, or 24-bits, **00-02-A5** identifies the network interface card (NIC) manufacturer. In this case it is the manufacturer is Compaq. The good news is that it is not necessary to know this address to deliver data within the network. The only thing needed is an IP address.

ARP maintains a table in the computer of IP and MAC address combinations. In other words, it keeps track of which MAC address is associated with an IP address. If ARP does not know the MAC address of a local device, it issues a broadcast using the IP address. This broadcast searches for the MAC address that corresponds to the IP address. If the IP address is active on the LAN, it will send a reply from which ARP will extract the MAC address. ARP will then add the address combination to the local ARP table of the requesting computer.

MAC addresses and therefore ARP are only used within the LAN. When a computer prepares a packet for transmission, it checks the destination IP address to see if it is part of the local network. It does this by checking to see if the network portion of the IP address is the same as the local network. If it is, the ARP process is consulted to get the MAC address of the destination device using the IP address. The MAC address is then applied to the data packet and used for delivery.

If the destination IP address is not local, the computer will need the MAC address of the default gateway. The default gateway is the router interface that the local network is connected to in order to provide connectivity with other networks. The gateway MAC address is used because the packet will be delivered there and the router will then forward it to the network it is intended for.

If the computer does not receive any packets from an IP address after a few minutes, it will drop the MAC/IP entry from the ARP table assuming the device has logged off. Later attempts to access that IP address will cause ARP to do another broadcast and update the table.

This lab assumes the use of any version of Windows. This is a non-destructive lab and can be performed with a home machine without concern of changing the system configuration. Ideally, this lab will be done in a classroom or other LAN connected to the Internet. It can be done from a single remote connection via a modem or DSL-type connection.

## Step 1 Establish a network connection

If the connection to the Internet is dial-up, connect to the ISP to ensure that the computer has an IP address. In a TCP/IP LAN with a Dynamic Host Configuration Protocol (DHCP) server it should not be necessary to do this step.

### **Step 2 Access a command prompt**

## Windows NT / 2000 / XP users:

Use the Start menu to open the Command Prompt window. This window is similar to the MS-DOS window on older Windows versions:

#### Start > Programs > Accessories > Command Prompt or Start > Programs > Command Prompt

#### Windows 95 / 98 / ME users:

Use the Start menu to open the MS-DOS Prompt window:

#### Start > Programs > Accessories > MS-DOS Prompt or Start > Programs > MS-DOS Prompt

#### Step 3 Display the ARP table

- a. In the window type arp -a and press **Enter**. Do not be surprised if there are no entries. The message displayed will probably be, 'No ARP Entries Found'. Windows computers remove any addresses that are unused after a couple minutes.
- b. Try pinging a couple local addresses and a website URL. Then re-run the command. The figure below shows a possible result of the arp -a command. The MAC address for the website will be listed because it is not local, but that will cause the default gateway to be listed. In the example below 10.36.13.1 is the default gateway while the 10.36.13.92 and 10.36.13.101 are other network computers. Notice that for each IP address there is a Physical Address, or MAC, and type, indicating how the address was learned.

🔤 Command Prompt		
C:\}arp -a		▲
Interface: 10.36.13.223 Internet Address 10.36.13.1 10.36.13.92 10.36.13.101	on Interface 0x1000003 Physical Address Type 00-00-5e-00-01-0a dyna 00-01-02-84-60-85 dyna 00-50-8b-fa-30-05 dyna	mic mic mic
C: \>_		-
•		

#### Step 4 Ping several URLs

a. Ping the following URLs and note the IP address of each. Also select one additional URL to ping and record it below:

www.ci	SCO.CO	m:

www.msn.de:			
	•		
	-		

- b. Now run the arp -a command again and record the MAC addresses for each of the above next to their IP addresses. Can it be done?
- c. Why or why not?
- d. What MAC address was used in delivering each of the pings to the URLs?

\_\_\_\_\_ Why? \_\_\_\_\_

# Step 4 Use the ARP help feature

Try the command arp -? to see the help feature and look over the options.

🖾 Command Prompt				
C:\>arp -?				
Displays and modifies the IP-to-Physical address translation tables used by address resolution protocol (ARP).				
ARP —s inet_add ARP —d inet_add ARP —a [inet_add	r eth_addr [if_addr] r [if_addr] dr] [-N if_addr]			
-a -g inet_addr -N if_addr	Displays current ARP entries by interrogating the current protocol data. If inet_addr is specified, the IP and Physic addresses for only the specified computer are displayed. If more than one network interface uses ARP, entries for each A table are displayed. Same as -a. Specifies an internet address. Displays the ARP entries for the network interface specified	al IRP		
-d	by if_addr. Deletes the host specified by inet_addr. inet_addr may be wildcarded with * to delete all bosts			
-5	Adds the host and associates the Internet address inet_addr with the Physical address eth_addr. The Physical address is given as 6 hexadecimal bytes separated by hyphens. The entry is permanent.			
eth_addr if_addr	Specifies a physical address. If present, this specifies the Internet address of the interface whose address translation table should be modified If not present, the first applicable interface will be used.			
Example:				
> arp -s 157.9 > arp -a	55.85.212    00-aa-00-62-c6-09   Adds a static entry. Displays the arp table.			
C: \>		-		
•		• //		

The purpose of this step is not so much the ARP command options but to demonstrate using the ? to access help, if available. Help is not always implemented uniformly. Some commands use /? instead of -?.

# Step 5 Use help with tracert and ping

Try tracert -? and then ping -? to see the options available for the commands used previously.

🚾 Command Prompt		
C:∖>ping -?		
Usage: ping [-t] [· [-r co [-w ti	-a] [-n count] [-l size] [-f] [-i TTL] [-v TOS] unt] [-s count] [[-j host-list] ¦ [-k host-list]] meout] destination-list	
Ontions:		
-t -t -a -n count -l size -f -i TTL -v TOS -r count -s count -j host-list -k host-list -w timeout	Ping the specified host until stopped. To see statistics and continue - type Control-Break To stop - type Control-C. Resolve addresses to hostnames. Number of echo requests to send. Send buffer size. Set Don't Fragment flag in packet. Time To Live. Type Of Service. Record route for count hops. Timestamp for count hops. Loose source route along host-list. Strict source route along host-list. Timeout in milliseconds to wait for each reply.	;

In looking at the help for ping, notice the –t option, which will send continuous pings, not just four. More importantly, notice the two commands to stop it:

Control-Break

# • Control-C

These two-key commands are common for stopping runaway activities. Try pinging a neighboring computer with the -t option and then try the Control-Break and Control-C features. An example in the above network would be ping 10.36.13.101 -t and then press **Enter**.

Be sure to use the Control-C command to stop the pings.

# Reflection

Based on observations made today, what could be deduced about the following results?

#### Computer 1

IP Address: 192.168.12.113 Subnet Mask: 255.255.255.0 Default Gateway: 192.168.12.1

Pings and tracert to 207.46.28.116 were both successful.

What will be the ARP table entry associated with this address and why?