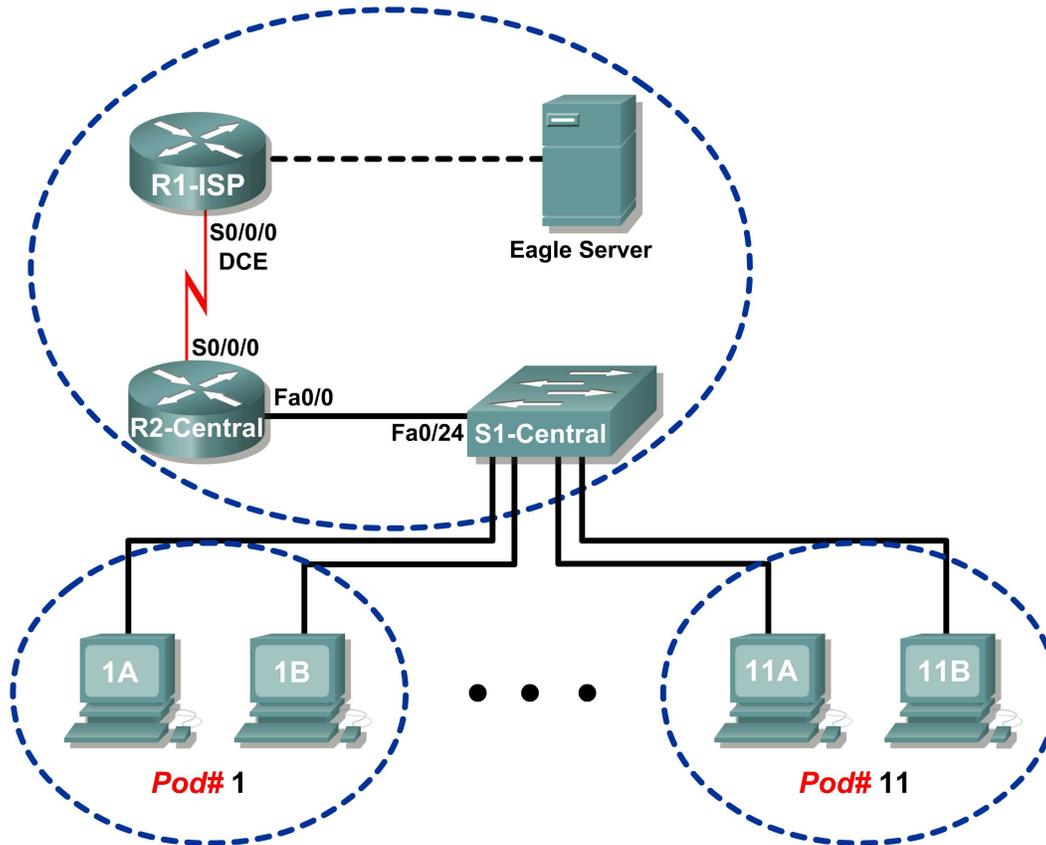


Lab 9.8.1: Address Resolution Protocol (ARP)

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	10.10.10.6
	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	172.31.24.254	255.255.255.0	N/A
hostPod#A	N/A	172.16.Pod#.1	255.255.0.0	172.16.255.254
hostPod#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. If Wireshark has not been loaded on the host pod computer, it can be downloaded from URL ftp://eagle-server.example.com/pub/eagle_labs/eagle1/chapter9/, file `wireshark-setup-0.99.4.exe`.

Task 1: Use the Windows `arp` Command.

Step 1: Access the Windows terminal.

```
C:\> arp
Displays and modifies the IP-to-Physical address translation tables
used by address resolution protocol (ARP).
ARP -s inet_addr eth_addr [if_addr]
ARP -d inet_addr [if_addr]
ARP -a [inet_addr] [-N if_addr]
-a          Displays current ARP entries by interrogating the current
           protocol data. If inet_addr is specified, the IP and
           Physical addresses for only the specified computer are
           displayed. If more than one network interface uses ARP,
           entries for each ARP table are displayed.
-g          Same as -a.
inet_addr  Specifies an internet address.
-N if_addr Displays the ARP entries for the network interface
           specified by if_addr.
-d          Deletes the host specified by inet_addr. inet_addr may be
           wildcarded with * to delete all hosts.
-s          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   Specifies a physical address.
if_addr    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 157.55.85.212 00-aa-00-62-c6-09 .... Adds a static entry.
> arp -a                                     .... Displays the arp table.
C:\>
```

Figure 1. `arp` Command Syntax

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. See Figure 1.
2. Issue the `arp` command on the pod host computer, and examine the output.
3. 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 2. Empty ARP Cache

Without any network communication, the ARP cache should be empty. This is shown in Figure 2. 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
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 3. `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, shown in Figure 3. Figure 4 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 4. Display of ARP Cache

How was the ARP entry added to the ARP cache? Hint: review the Type column.

What is the physical address of the destination pod host computer?

What is the physical address of the destination pod host computer?

IP Address	Physical Address	How Discovered?

3. Do not send any traffic to the computer accessed previously. Wait between 2 and 3 minutes, and check ARP cache again. Was the ARP cache entry cleared? _____
4. Issue the **ping** command to the Gateway, R2-Central. Examine ARP cache entry. What is the physical address of the Gateway? _____

IP Address	Physical Address	How Discovered?

5. Issue the **ping** command to Eagle Server, eagle-server.example.com. Examine ARP cache entry. What is the physical address of Eagle Server? _____

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 destination 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 5. Manually Removing an ARP Cache Entry

See Figure 5, 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.
2. Next, delete the entry for the pod host computer.
3. Finally, verify your change.
4. Record the two ARP cache entries:

Device	IP Address	Physical Address	How Discovered?

5. Write the command that will delete the entry for the pod host computer:

6. Issue the command on your pod host computer. Record the remaining ARP cache entry:

Device	IP Address	Physical Address	How Discovered?

7. Simulate removing all entries. Write the command that will delete all entries in ARP cache:
- _____

8. Issue the command on your pod host computer, and examine the ARP cache with the command **arp -a**. All entries should be removed. _____

9. Consider a secure environment where the Gateway controls access to a web server that contains Top Secret information. What is one layer of security that can be applied to ARP cache entries that could aid in countering ARP spoofing? _____

10. Write the command that will add a static ARP entry for the Gateway to ARP cache:
- _____

11. Examine the ARP cache again, and fill in the following table:

IP Address	Physical Address	Type

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

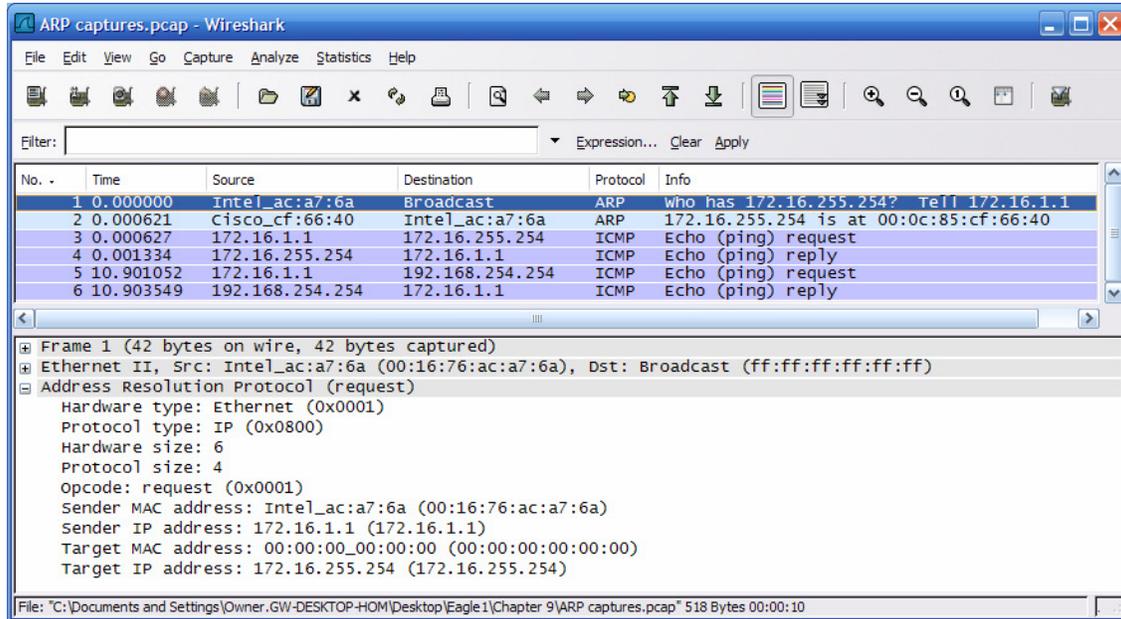


Figure 6. Wireshark Capture of ARP Communication

- Stop Wireshark and evaluate the communication. You should see a Wireshark screen similar to the screen shown in Figure 6. The Wireshark Packet list window displays the number of packets captured. The Packet Details Window shows ARP protocol contents.
- Using your Wireshark capture, answer the following questions:

What was the first ARP packet? _____

What was the second ARP packet? _____

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	

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

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

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.

Task 4: Challenge

Using outside resources, perform a search on ARP spoofing. Discuss several techniques used to counter this type of attack.

Most wireless routers support wireless network access. Using this technique, MAC addresses that are permitted access to the wireless network are manually added to the wireless router. Using outside resources, discuss the advantages of configuring wireless network access. Discuss ways that attackers can circumvent this security.

Task 5: Clean Up

Wireshark was installed on the pod host computer. If Wireshark needs to be uninstalled, click **Start > Control Panel**. Open **Add or Remove Programs**. Highlight Wireshark, and click **Remove**.

Remove any files created on the pod host computer during the lab.

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.