Lab 4 ARP

ARP (Address Resolution Protocol) is an essential glue protocol that is used to join Ethernet and IP. It is covered in Chapter 5.7.4 of the textbook. Review the text section before doing this lab.

Objective

- Know ARP packet format;
- Understand the operation of ARP cache table;
- Understand how ARP works (including both ARP request and reply messages).

Requirements

You need to install following tools on your computer beforehand:

- **Wireshark:** This lab uses the Wireshark software tool to capture and examine a packet trace. Refer to previous labs for details.
- **ifconfig/ipconfig:** This lab uses the "*ipconfig*" (Windows) or "*ifconfig*" (Mac/Linux) command-line utility to inspect the state of your computer's network interface. *ifconfig/ipconfig* is installed as part of the operating system on Windows, Linux, and Mac computers.
- **route/netstat:** "*route*" or "*netstat*" command-line utility are used to inspect the routes on your computer. A key route is the *default route* (or route to prefix 0.0.0.0) that uses the default gateway to reach remote parts of the Internet. Both "*route*" and "*netstat*" are installed as part of the operating system across Windows and Mac/Linux, but there are many variations on the command-line parameters that must be used.
- **arp:** This lab uses the "*arp*" command-line utility to inspect and clear the cache used by the ARP protocol on your computer. *arp* is installed as part of the operating system on Windows, Linux, and Mac computers, but uses different arguments. It requires administrator privileges to clear the cache.

Exercise

We assume the following network setup (Figure 1), which should be very common in most home LANs. The network between your computer and the default gateway is an Ethernet.

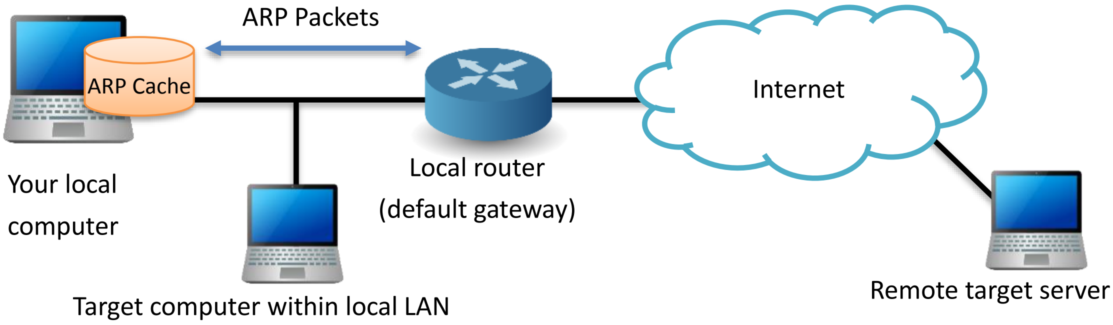


Figure 1: Network topology (IP and MAC addr. may be varied)

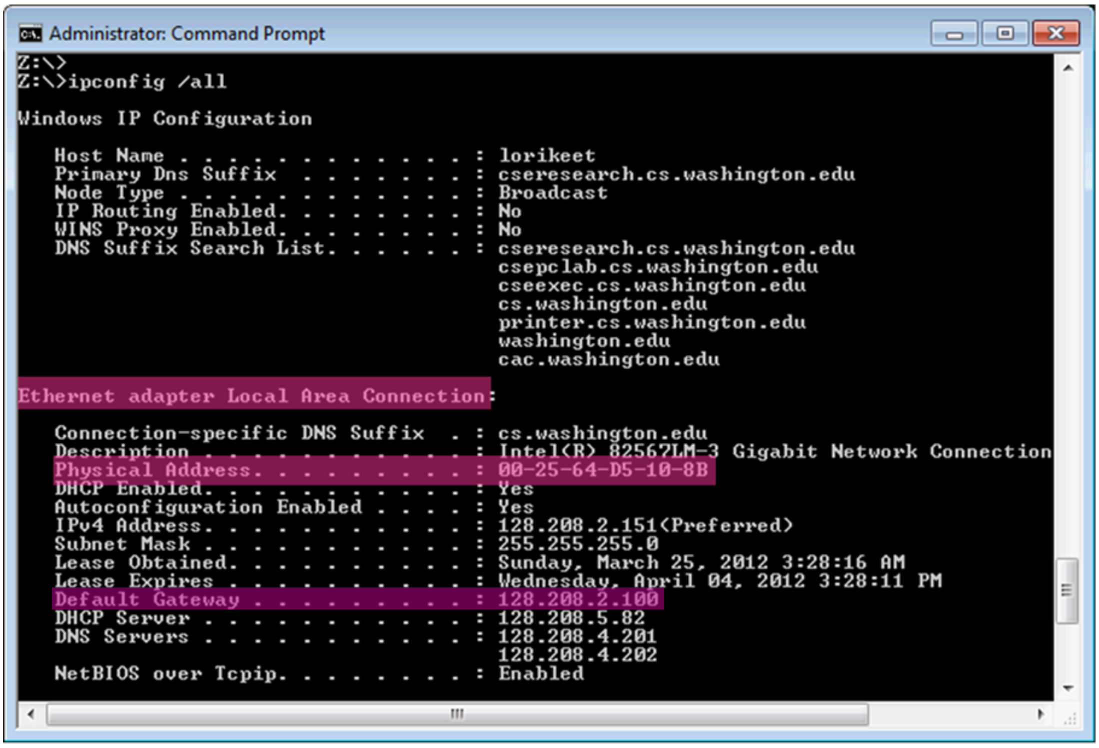
Task 1: First try to capture a trace of ARP (You can bypass this task on the lab report)

To gather ARP packets, we will cause your computer to send traffic to the local router when it does not know the router's Ethernet address – your computer will then use ARP to discover the Ethernet address.

1. Find the *Ethernet address* of the main network interface of your computer with the *ifconfig* / *ipconfig* command. On Windows, execute command "*ipconfig /all*". On Mac/Linux, execute command "*ifconfig*".

   Tips:

   - Among the output will be a section for the main interface of the computer (likely an Ethernet interface) and its Ethernet address. Common names for the interface are "eth0", "en0", or "Ethernet adapter".
   - On Windows, you can also obtain the MAC address through the graphic interface.



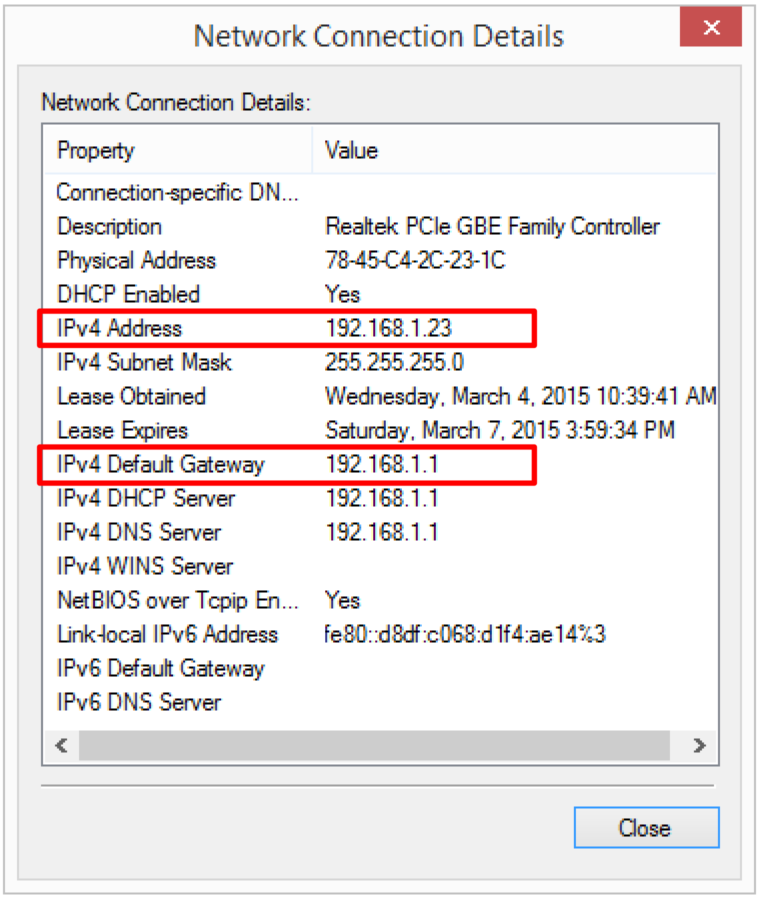
```
Z:\>
Z:\>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : lorikeet
   Primary Dns Suffix  . . . . . . . : cseresearch.cs.washington.edu
   Node Type . . . . . . . . . . . . : Broadcast
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No
   DNS Suffix Search List. . . . . . : cseresearch.cs.washington.edu
                                       csepclab.cs.washington.edu
                                       cseexec.cs.washington.edu
                                       cs.washington.edu
                                       printer.cs.washington.edu
                                       washington.edu
                                       cac.washington.edu

Ethernet adapter Local Area Connection:

   Connection-specific DNS Suffix  . : cs.washington.edu
   Description . . . . . . . . . . . : Intel(R) 82567LM-3 Gigabit Network Connection
   Physical Address. . . . . . . . . : 00-25-64-D5-10-8B
   DHCP Enabled. . . . . . . . . . . : Yes
   Autoconfiguration Enabled . . . . : Yes
   IPv4 Address. . . . . . . . . . . : 128.208.2.151(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Lease Obtained. . . . . . . . . . : Sunday, March 25, 2012 3:28:16 AM
   Lease Expires . . . . . . . . . . : Wednesday, April 04, 2012 3:28:11 PM
   Default Gateway . . . . . . . . . : 128.208.2.100
   DHCP Server . . . . . . . . . . . : 128.208.5.82
   DNS Servers . . . . . . . . . . . : 128.208.4.201
                                       128.208.4.202
   NetBIOS over Tcpip. . . . . . . . : Enabled
```



Network Connection Details

Network Connection Details:

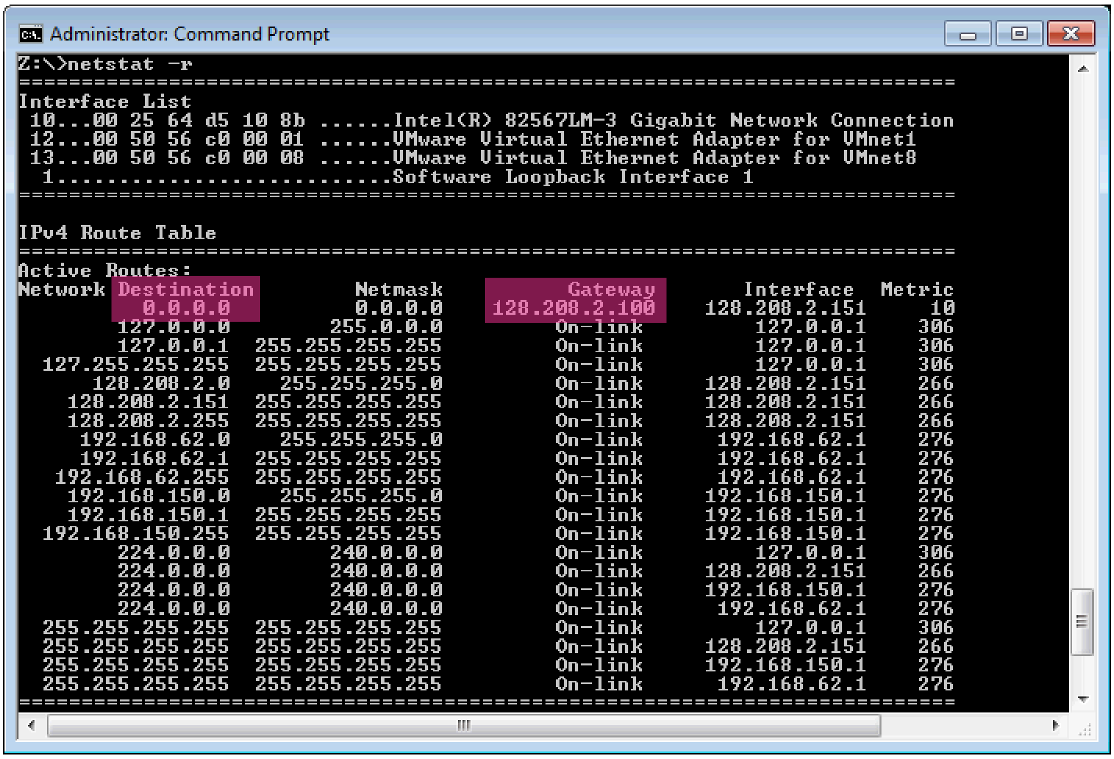
Property	Value
Connection-specific DN...	
Description	Realtek PCIe GBE Family Controller
Physical Address	78-45-C4-2C-23-1C
DHCP Enabled	Yes
IPv4 Address	192.168.1.23
IPv4 Subnet Mask	255.255.255.0
Lease Obtained	Wednesday, March 4, 2015 10:39:41 AM
Lease Expires	Saturday, March 7, 2015 3:59:34 PM
IPv4 Default Gateway	192.168.1.1
IPv4 DHCP Server	192.168.1.1
IPv4 DNS Server	192.168.1.1
IPv4 WINS Server	
NetBIOS over Tcpip En...	Yes
Link-local IPv6 Address	fe80::d8df:c068:d1f4:ae14%3
IPv6 Default Gateway	
IPv6 DNS Server	

Figure 2: Finding the computer's Ethernet address (Windows)

2. Find the *IP address* of the *local router* or *default gateway* that your computer uses to reach the rest of the Internet.

   Tips:

   - You can locate the IP address of default gateway in results of last step (See Figure 2).
   - Or you can use the *netstat* / *route* command: You should be able to use the *netstat* command ("*netstat -r*" on Windows, Mac and Linux, may require Ctrl-C to stop). Alternatively, you can use the *route* command ("*route print*" on Windows, "*route*" on Linux, "*route –n get default*" on Mac). In either case you are looking for the *gateway* IP address that corresponds to the destination of "default" or "0.0.0.0". See following figure.



```
Z:\>netstat -r
===========================================================================
Interface List
 10...00 25 64 d5 10 8b ......Intel(R) 82567LM-3 Gigabit Network Connection
 12...00 50 56 c0 00 01 ......VMware Virtual Ethernet Adapter for VMnet1
 13...00 50 56 c0 00 08 ......VMware Virtual Ethernet Adapter for VMnet8
  1...........................Software Loopback Interface 1
===========================================================================

IPv4 Route Table
===========================================================================
Active Routes:
Network Destination        Netmask          Gateway       Interface  Metric
          0.0.0.0          0.0.0.0    128.208.2.100    128.208.2.151     10
        127.0.0.0        255.0.0.0         On-link         127.0.0.1    306
        127.0.0.1  255.255.255.255         On-link         127.0.0.1    306
  127.255.255.255  255.255.255.255         On-link         127.0.0.1    306
      128.208.2.0    255.255.255.0         On-link     128.208.2.151    266
    128.208.2.151  255.255.255.255         On-link     128.208.2.151    266
    128.208.2.255  255.255.255.255         On-link     128.208.2.151    266
     192.168.62.0    255.255.255.0         On-link      192.168.62.1    276
     192.168.62.1  255.255.255.255         On-link      192.168.62.1    276
   192.168.62.255  255.255.255.255         On-link      192.168.62.1    276
    192.168.150.0    255.255.255.0         On-link     192.168.150.1    276
    192.168.150.1  255.255.255.255         On-link     192.168.150.1    276
  192.168.150.255  255.255.255.255         On-link     192.168.150.1    276
        224.0.0.0        240.0.0.0         On-link         127.0.0.1    306
        224.0.0.0        240.0.0.0         On-link     128.208.2.151    266
        224.0.0.0        240.0.0.0         On-link     192.168.150.1    276
        224.0.0.0        240.0.0.0         On-link      192.168.62.1    276
  255.255.255.255  255.255.255.255         On-link         127.0.0.1    306
  255.255.255.255  255.255.255.255         On-link     128.208.2.151    266
  255.255.255.255  255.255.255.255         On-link     192.168.150.1    276
  255.255.255.255  255.255.255.255         On-link      192.168.62.1    276
===========================================================================
```

Figure 4: Finding the default gateway IP address

3. Launch Wireshark and start a capture with a filter of "*arp*".
   Tips:
   - Remember to choose correct interface.
   - We only want to record packets sent to/from your computer. So, the "promiscuous mode" of should be disabled (Normally, this is a default setting of Wireshark).
4. When the capture is started, use the "*arp -d*" command to clear the *default gateway* from the ARP cache.
   Tips:
   - Using the command "*arp -a*" will show you the contents of the ARP cache. You should see an entry for the IP address of the default gateway.
   - To clear this entry, use the *arp* command with different arguments ("*arp -d* xx.xx.xx.xx", where xx.xx.xx.xx is the IP address of the default gateway on Linux).
   - This usage of *arp* command may need administrator privileges to run. If so, you may run as a privileged user on Windows or issue "*sudo arp -d* xx.xx.xx.xx" on Linux/Mac.
   - Note that the command should run without error but the ARP entry may not appear to be cleared if you check with "*arp -a*". This is because your computer will send ARP packets to repopulate this entry as soon as you need to send a packet to a remote IP address, and that can happen very quickly due to background activity on the computer.
5. Now that you have cleared your ARP cache, fetch a remote page with your Web

browser. This will cause ARP to find the Ethernet address of the default gateway so that ARP packets can be sent. These ARP packets will be captured by Wireshark.

Tips:

- You might clear the ARP cache and fetch a webpage a couple of times.
- Hopefully there will also be other ARP packets sent by other computers on the local network that will be captured. These packets are likely to be present if there are other computers on your local network. In fact, if you have a busy computer and extensive local network, you may capture many ARP packets.
- The ARP traffic of other computers will be captured when the ARP packets are sent to the broadcast address, since in this case they are destined for all computers including the one on which you are running Wireshark.
- Because ARP activity happens slowly, you may need to wait up to 30 seconds to observe some of this background ARP traffic.

6. Once you have captured some ARP traffic, stop the capture. You will need the trace, plus the Ethernet address of your computer and the IP address of the default gateway for the next steps.

Tips:

- If there are many ARP packets in your trace, you can narrow our view to only the ARP packets that are sent directly from or to your computer.
- You can set a filter for packets with the Ethernet address of your computer. For example, if your Ethernet address is 01:02:03:04:05:06 then enter a filter expression of "*eth.addr == 01:02:03:04:05:06*".

Task 2: ARP for hosts within the same LAN

This task needs two students to collaborate with each other, using two computers connected to the same local LAN (say Host A and Host B), to investigate the operations of ARP.

- You are suggested to **use computers in the lab room**.
- Otherwise, you should ensure that the two computers in your experiments connect to the same LAN (You can prove this using the IP address, subnet mask and default gateway of both Host A and Host B).

1. On both Host A and Host B, start Wireshark to capture both ARP and ICMP packets, and use *arp -d* to clear ARP cache.
2. Host A *ping* Host B.
3. Stop the capture in Wireshark, and inspect the captured ARP trace.
   There are two kinds of ARP packets, ARP request and reply (also called response). You need to inspect them in turn.
   (a) Find an *ARP request* for the default gateway and examine each field.

Tips:

- The Info line for the request will start with "Who has …".

- You can look for one of these packets that asks for the MAC address of the default gateway, e.g., "Who has xx.xx.xx.xx …" where xx.xx.xx.xx is your default gateway.
- You need to examine each fields of both *Ethernet frame header* and *ARP packets*.
- Refer to the *Reading material* on course website for detailed format of ARP packets.

(b) Select an *ARP reply* and examine its fields.

Tips:

- The reply will answer a request and have an Info line of the form "xx.xx.xx.xx is at yy:yy:yy:yy:yy:yy".
- You need to examine each fields of both *Ethernet frame header* and *ARP packets*.

4. Draw a figure that shows the *ARP request/reply* and *ICMP request/response* packets sent between Host A and Host B.

Tips:

- Label one packet the request and the other the reply.
- Give the sender and target MAC & IP addresses for each ARP packet.
- **Please indict the time sequence of these packets on the figure**.

Questions:

1. What columns are included in the high-speed ARP cache table?
2. What *opcode* is used to indicate a request? What about a reply?
3. How large is the ARP header for a request? What about for a reply?
4. What value is carried on a request for the unknown target MAC address?
5. What Ethernet Type value indicates that ARP is the higher layer protocol?
6. Is the ARP reply broadcast (like the ARP request) or not?

Task 3: ARP for a remote server

In this task, you will investigate the ARP process for a remote server. For example, your setup can be:

- A local computer within a LAN and a remote server on the Internet, e.g., *www.baidu.com*.
- Or, two computers in the JNU campus LAN but connected to different default gateway, e.g., one computer in the lab room and the other one connects to the campus WiFi.

  (In this case, if possible, I suggest you to capture traffic on the remote target computers).

  (You should the IP address, subnet mask and default gateway of both computers.)

1. On your local computer, start Wireshark to capture both ARP and ICMP packets.
2. Execute the following commands in a *batch* file (Windows) or a *shell script*

(Linux and MacOS):

```
                arp      -d
                ping     www.baidu.com
```

Tips:

- Consider why we prefer to use a batch file. Are there any risks if not using batch processing?

3. Stop the capture in Wireshark, and inspect the captured ARP as in **Task 2**.
4. Similar to **Task 2**, draw a figure that shows process of the ARP request/reply and ICMP probe/response packets, which are exchanged among **your computer, the default gateway and the remote server**.

Task 4: Explore on Your Own (Not required in the lab report. But please try if possible.)

I encourage you to explore ARP on your own once you have completed above tasks. One suggestion is to look at other ARP packets that may have been recorded in your trace. We only examined an ARP request by your computer.

To see if there is other ARP activity, make sure to clear any Ethernet address filter that is set in Wireshark. Other ARP packets may exhibit any of the following kinds of behavior for you to explore:

- ARP requests broadcast by other computers. The other computers on the local network are also using ARP. Since requests are broadcast, your computer will receive their requests.
- ARP replies sent by your computer. If another computer happens to ARP for the IP address of your computer, your computer will send an ARP reply to tell it the answer.
- Gratuitous ARPs in which your computer sends a request or reply about itself. This is helpful when a computer or link comes up to make sure that no-one else is using the same IP address. Gratuitous ARPs have the same sender and target IP address, and they have an Info field in Wireshark that identified them as gratuitous.

Questions:

1. The command "*arp -s InetAddr EtherAddr*" allows you to manually add an entry to the ARP cache that resolves the IP address *InetAddr* to the physical address *EtherAddr*. What would happen if, when you manually added an entry, you entered the correct IP address, but the wrong Ethernet address for that remote interface?

   Tips: Check ARP Poison/Spoofing on the course website or Google.
2. What is the default amount of time that an entry remains in your ARP cache before being removed?

   Tips: You can determine this empirically (by monitoring the cache contents) or by looking this up in your operation system documentation. Please indicate how/where you determined this value.

3. Continue to Question 2, there is a timer for each entry in ARP cache. What happened if the timer is set too long or too short?
4. For ARP protocol, what’s the difference between finding the MAC address of a host within the same subnet and a host within another subnet connected by router?
5. Is the length of ARP packet fixed? Explain why.
6. Suppose a computer needs to send an IP packet. List at least two cases that the computer does not need to send ARP request.

   Tips: One case is a special destination address for the packet.