Networking Lab 2, ARP

Do this lab using your Windows workstation. This lab assumes computers are back on the school network if you disconnected them in Lab 1.

Remember, computers talk to each other at Data Link layer 2, using MAC addresses. However, applications are designed to work across the Internet, and use the IP addresses from Network layer 3. Therefore, computers need a way to find the MAC addresses of local computers and routers (default gateway) when they know the IP address of the other computer/router.

This lab is about the Address Resolution Protocol (ARP), which is used by IP version 4. IPv6 uses a different method, which we will discuss later in the course.

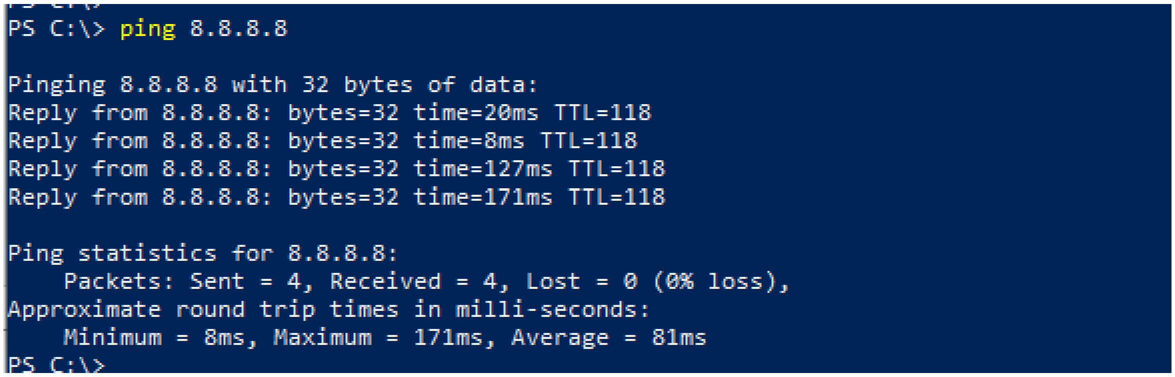
Procedure

Overview

We are going to delete the arp cache from our computer, and then watch the computer send arp requests to rebuild its cache. If you are using Windows, it may rebuild the cache so quickly that you do not have time to open Wireshark after the cache is deleted. So, we need to have Wireshark running when we delete the cache. Also, we can build a display filter so that it only shows arp traffic that is to or from our computer to remove noise.

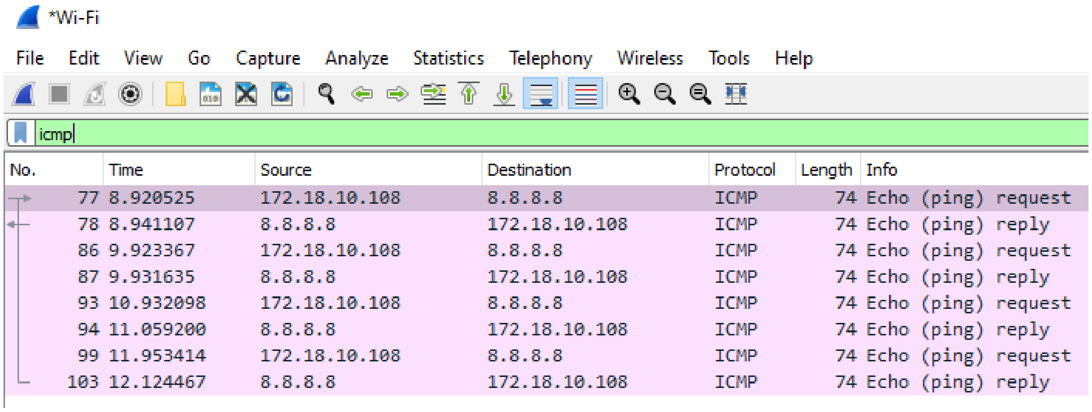
Find our MAC address using Wireshark

1) Open Wireshark and start a packet capture.
   The first thing we need to do is find the MAC address of our adapter so we can filter out traffic that doesn't involve our adapter. You can find the MAC address from the command prompt or terminal by running `ipconfig /all` (Windows) or `ip link` (Linux). For practice, let's generate some traffic and examine it in Wireshark. (If you do not need Wireshark practice, you can just use he command prompt or terminal.)
2) From a terminal or command prompt, enter
   ping 8.8.8.8
   This is a Google address that they kindly make available for pings and DNS lookups.



```
PS C:\> ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=20ms TTL=118
Reply from 8.8.8.8: bytes=32 time=8ms TTL=118
Reply from 8.8.8.8: bytes=32 time=127ms TTL=118
Reply from 8.8.8.8: bytes=32 time=171ms TTL=118

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 8ms, Maximum = 171ms, Average = 81ms
PS C:\>
```

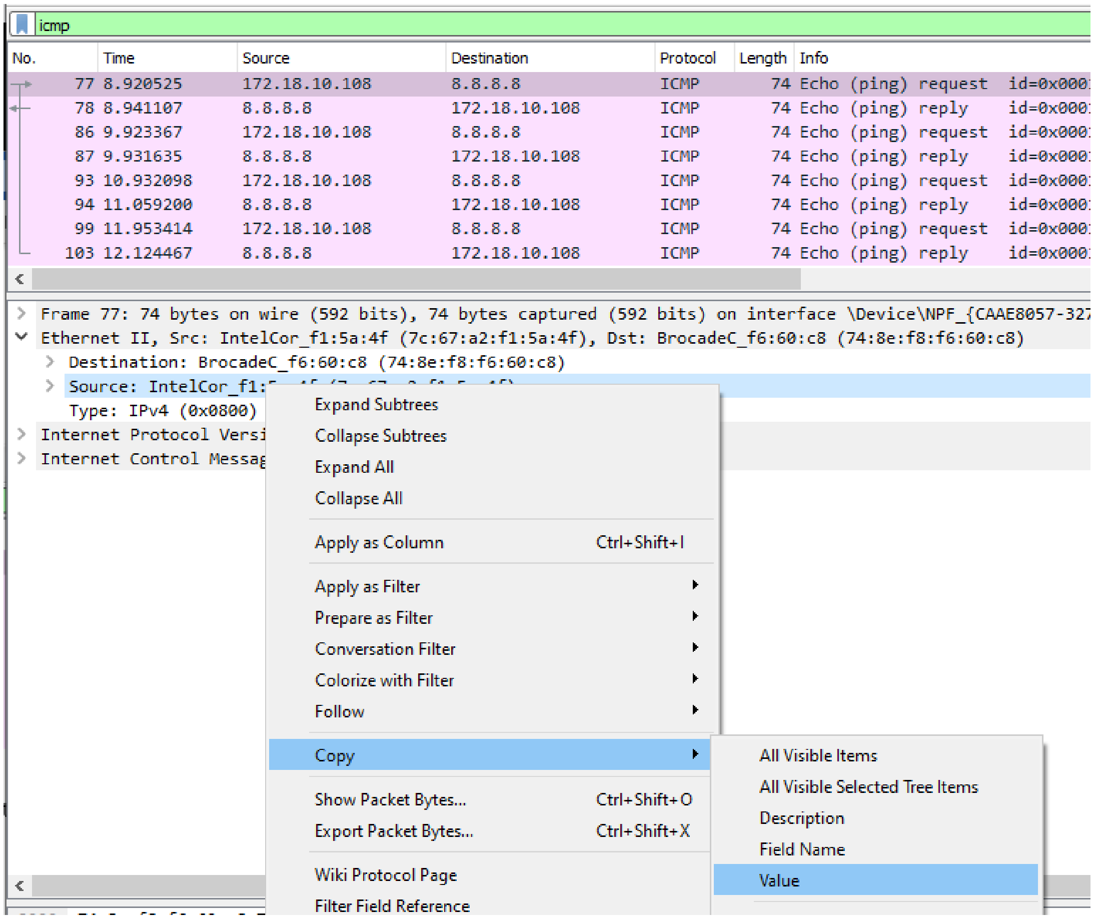
3) In Wireshark, stop the capture and enter a display filter of `icmp`.


*Wi-Fi
File Edit View Go Capture Analyze Statistics Telephony Wireless Tools Help

icmp

No.	Time	Source	Destination	Protocol	Length	Info
77	8.920525	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request
78	8.941107	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply
86	9.923367	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request
87	9.931635	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply
93	10.932098	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request
94	11.059200	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply
99	11.953414	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request
103	12.124467	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply

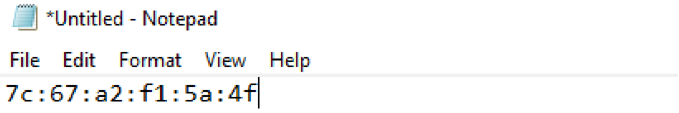
4) Select a packet where the source address is your IP address (i.e., not 8.8.8.8). In the packet details section, select the Ethernet Source. Right-click and select copy -> value. Paste this into notepad (or gedit or a convenient editor) so you can remember it.



icmp

No.	Time	Source	Destination	Protocol	Length	Info
77	8.920525	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request id=0x000
78	8.941107	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply id=0x000
86	9.923367	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request id=0x000
87	9.931635	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply id=0x000
93	10.932098	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request id=0x000
94	11.059200	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply id=0x000
99	11.953414	172.18.10.108	8.8.8.8	ICMP	74	Echo (ping) request id=0x000
103	12.124467	8.8.8.8	172.18.10.108	ICMP	74	Echo (ping) reply id=0x000

```
> Frame 77: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface \Device\NPF_{CAAE8057-327
v Ethernet II, Src: IntelCor_f1:5a:4f (7c:67:a2:f1:5a:4f), Dst: BrocadeC_f6:60:c8 (74:8e:f8:f6:60:c8)
  > Destination: BrocadeC_f6:60:c8 (74:8e:f8:f6:60:c8)
  > Source: IntelCor_f1:
    Type: IPv4 (0x0800)
> Internet Protocol Versi
> Internet Control Messag
```

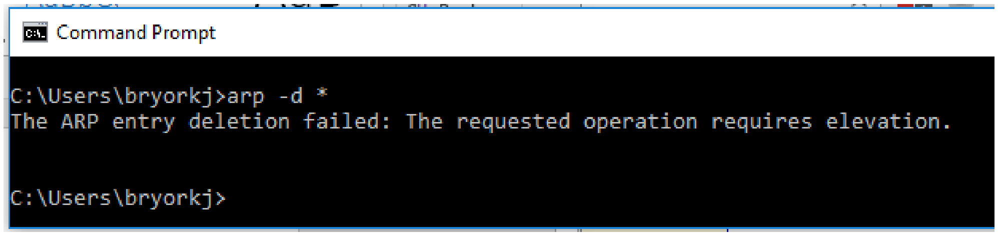


```
7c:67:a2:f1:5a:4f
```

This is my MAC address!!

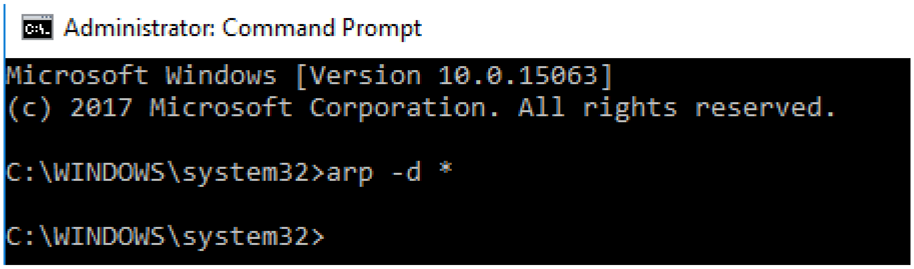
Watch the ARP traffic

1) Open an "elevated" command or PowerShell prompt. "Elevated" means the prompt has administrative rights. To open an elevated command prompt, type cmd in the search window. Instead of clicking the icon that appears, right-click it and select Run as administrator. A command prompt with normal user rights looks like this.
   (if you are using Linux, just use sudo.)

   ```
   C:\Users\bryorkj>arp -d *
   The ARP entry deletion failed: The requested operation requires elevation.

   C:\Users\bryorkj>
   ```

   A command prompt with elevated or administrator rights looks like this.

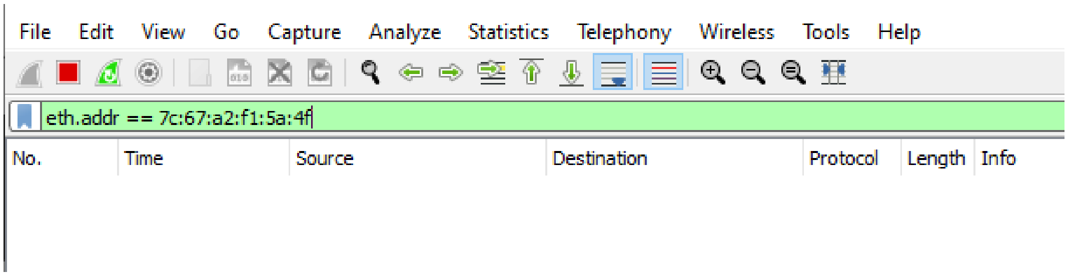
   

   ```
   Microsoft Windows [Version 10.0.15063]
   (c) 2017 Microsoft Corporation. All rights reserved.

   C:\WINDOWS\system32>arp -d *

   C:\WINDOWS\system32>
   ```

2) Run the command *arp -a* (This command also works in Linux, but you don't need the -a.) This will show you the contents of the ARP cache, a table of IP and MAC addresses of hosts the computer has talked to recently. You should see several entries. A MAC address that is ff-ff-ff-ff-ff-ff is a broadcast address, as is an IP address of 255.255.255.255. Broadcasts are sent to all hosts on the local network. MAC addresses starting with 01-00-5e and IP addresses starting with 224 to 239 are multicast addresses. Multicast is similar to broadcast, except that computers announce that they want to hear multicast traffic. Your computer talks to the Internet a lot, so you will probably see the IP and MAC address of your default gateway, the router that connects you to the Internet. If your computer has recently talked with other computers on the local network, their IP and MAC addresses will appear as well.
3) Run the command *ipconfig /all* (the command for Linux is *ip address*.) This will show the IP and MAC addresses of your computer, and much other information. Write down the IP and MAC (shown as Physical Address) of your main Ethernet interface (the IP should start with 172.18.), as well as your default gateway (the IP address of the router that connects you to the Internet.)
4) Start Wireshark, and enter a display filter that will look for ARP traffic to our from your MAC address

   ```
   arp && eth.addr == 7c:67:a2:f1:5a:4f
   ```

   Note: your MAC address will be different from mine.

5) 

```
eth.addr == 7c:67:a2:f1:5a:4f
```

6) Run the command _arp -d *_ to remove all the entries from your ARP cache. It will only work if you are at an elevated command prompt.
7) Run _arp -a_ to see your ARP cache. The broadcast and multicast entries will probably come back quickly. The default gateway may come back as well.
8) Look at your packet capture (that should already be running) on Wireshark. If nothing has appeared, use a browser to visit a web site and force your computer to send an ARP request for the default gateway. After it loads, stop the packet capture, and run _arp -a_ again to see if there were any changes. The default gateway should be there now if it was not there before. In Wireshark, look for ARP traffic--did your computer use ARP to find the MAC address of the default gateway? If you do not see anything, it is possible the MAC address in your display filter is wrong, or that you are monitoring the wrong interface.

The first step your traffic takes on the way to the distant web server is the default gateway. That router connects you to the rest of the school network, and eventually to the Internet.

9) Ask your neighbors to tell you the IP addresses of their computers. Start a packet capture, ping one of your neighbors, and stop the capture. Examine your ARP cache--the IP and MAC address of your neighbor should now be in your cache. Examine the packet capture to see if you can find the ARP request and reply frames to and from your neighbor, as well as the ping packets.
10) Repeat the procedure with another neighbor. Take screenshots of the ARP and ping traffic from Wireshark, and of your ARP cache for hand-in.

Later on, we'll show how ARP can be abused to force traffic to pass through an attacker's computer. This allows an attacker to eavesdrop on a switched network. The attack is called ARP cache spoofing.

Hand in

1) Turn in your screenshots from Wireshark and the command prompt showing your ARP cache. Which addresses are those of your neighbors?
2) Explain why you don't see the MAC or IP addresses of the distant web site in your ARP cache. What do you see in the cache instead?