Networking Lab 2, ARP

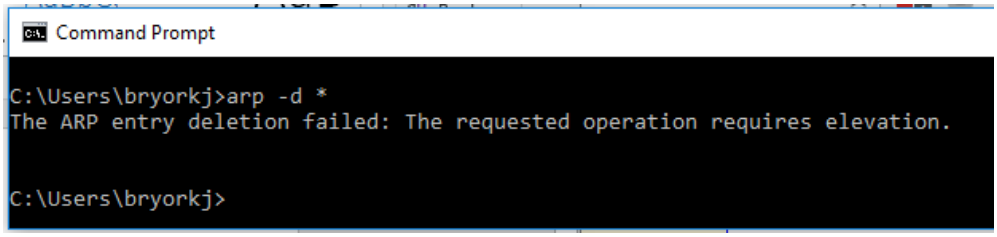
Do this lab using your Windows workstation. This lab assumes computers are back on the school network, if you disconnected them in Lab 1.

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.

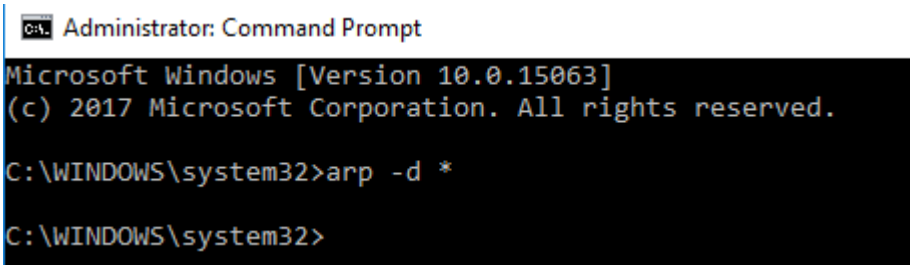
This lab is about the Address Resolution Protocol (ARP), which is used by IP version 4. IPv6 uses a different method, which we will discuss later in the course.

Procedure

1) Open an "elevated" command 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.



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



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 will be different.) 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) 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.
5) 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.
6) Start a packet capture with Wireshark. Then, use a browser to visit a web site. 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?

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.

7) 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.
8) 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?