IT2400 - ARP Lab

Objectives

- Use different network utilities to obtain information about your computer and network
- This should be done on your Windows virtual machine

Update your network settings

- Make sure your vm has the correct settings for:
  - ip address
  - default gateway
  - subnet mask
  - dns servers

Here is the process, but note that your numbers will be different:
Network Connections

Ethernet Properties

Networking

Connect using:
- Realtek RTL8139C+ Fast Ethernet NIC

This connection uses the following item:
- \Device\Network\XXXXX

Description:

OK Cancel
How did I get the numbers above? First, look at the ip allotment that is checked out to you:

The first address, 64, is my network id (cannot assign to hosts). The second address, 65, is usually my default gateway (cannot assign to hosts). The last address, 95, is usually the broadcast address (cannot assign to hosts). Choose something else in your range to assign to your host. Your subnet mask is probably going to be 255.255.255.248.

Dns servers should be the same as mine.

Test network connectivity

Open the command prompt (cmd).
See if you can ping your gateway address. I would, for example, do the following:

```
ping 144.38.220.65
```

If connection times out, you have a problem. You should be able to determine it succeeds.

Let’s also test that dns is working by pinging a domain name.

```
ping cit.dixie.edu
```

Create a new word document and paste a screenshot of your successful pings. If you weren’t successful, go back and fix things.

**More pings**

Using the ping command, record the answers to the following in your document:

- What is the ip address of cit.dixie.edu?
- What is the ip address of www.dixie.edu?
- What is the ip address of www.nfl.com?

**Mac address**

On your word document, record the mac address of your virtual machine. Also record how you found this out.

**Switches**

Switches store mac addresses too. Look at the following file and answer the following questions. Note that you really only care about the first and last columns in the table. The file represents the output of a certain command
on a switch that shows the mac address table of mac addresses that a switch knows about.

- How many mac addresses does the switch know about? (you may have to count them)
- What port should the switch forward frames out of if it is tagged with the following mac address: 000d.ed8e.a780? Hypothesize why you think that mac address listed more than once in the table?
- Why are so many different mac addresses listed out port FastEthernet0/1? What do you suppose is plugged in at the other end of that port?
- What is the maximum number of MAC addresses that the switch can store?(it is given in that file) What do you think the switch does if it learns about mac addresses after it has maxed out? (Hypothesize and then go to google and see if you can find an answer)

**View your ARP cache**

- Open the windows command line and issue the following command: `arp -a`. This command should display the entries in your ARP cache. You might not have any entries. (Print screen to your document)
- If you do have entries issue a `arp -d *` to clear out all the arp entries. (This may require higher permissions. To gain administrative permissions, close the command prompt and re-open it by right clicking on it and ‘run as administrator’)
- Visit a website or two in your browser, then re-issue the command. ARP messages are those messages that are sent within a single network to query for the MAC address of a recipient machine. Now issue the `arp -a` command again and record the information you found(screenshot). Why do you suppose that address is given. Does it ever change if you repeat steps 2 and 3? Write your answer on your document.

**Wireshark**

Open wireshark and let’s look at a frame. You can visit a website after you have started capturing packets to generate some network traffic. It doesn’t really matter which website. Stop the capture. Anyways, since we are ignoring all other high level traffic and only want to see frames, disable the higher-level frames by clicking on Analyze->Enabled Protocols and uncheck IPv4. This will make it so that the IP layer (along with all layers above it) are not shown. Now we can just focus on the Data Link layer and information associated with it.

Choose any packet and answer the following questions:

- What is the 48 bit address of your computer? (in hexadecimal)
- What is the 48 bit address of the destination? (hex)
- Capture again and visit a different website, does the answer to the above question ever change? Why?
- Find the response from the above frame and identify the source mac and destination mac. (screenshot)

Before you close wireshark, start a capture again and type ‘arp’ in the filter box. Now wireshark will only show you arp traffic. If you on your windows VM you should readily see some arp traffic. If you do not, issue the `arp -d *` command again, to delete all your arp entries and then visit a website again to generate some network traffic.

- What is in the ‘Info’ section of any arp frame?
- Record (screenshot) any arp request along with its’ corresponding reply.

**To pass off**

Upload your document on Canvas.