NSSA 290 Network Essentials for Developers
Lab Exercise 01 – Network Settings, Testing, Monitoring and Encapsulation

Name Ellie Parobek

Lab Exercise Overview

We've talked about standards, protocols, network sizes, network topologies, network hardware and the OSI and TCP/IP Models. We have also specifically discussed how each of these relates to you as developers. In this lab, we will walk through several exercises to explore these concepts. We will examine network settings, testing, monitoring and encapsulation. Throughout your experience, be sure to continue to keep in mind the relevance to you as developers.

What to Submit

Please submit answers to all the questions in this document to the MyCourses dropbox.

Working Together

Please work with a partner for this lab. Be sure to reference the guidelines for working together in groups that we previously discussed during class to help you.

Lab Exercise Setup and Nomenclature

Note that a pod consists of two benches. On one bench, the PCs are numbered 1, 2, and 3. On the other bench the PCs are numbered 4, 5, and 6. In the instructions, when you see a PC indicated with 1/4 or 2/5 or 3/6 it means to use the PCs on the side of the pod where you are working. (For example, 1 or 4).

Let's take a few minutes to walk through how things are physically setup and wired in the lab, especially the bench machines to the racks and then to the front of the room.

Getting Started

Before beginning this exercise, reboot Windows on all three PCs. This will reset the machines in case anyone was using them before us.

- You can do this by clicking on the Windows icon  and then the restart button.

Activity 1: Network Settings

Let's begin by exploring the network settings on the machines. We will bring up a command line window and then examine the specific network settings. Although some specific questions follow, I encourage you to look up anything that is of interest to you in addition to what we will examine during this period.

How to find the MAC address in Windows

1. Go to the DOS prompt
    - Click the search button
    - Type ***cmd*** and press ENTER
2. In the DOS command window prompt, type ***ipconfig /all*** and press ENTER
   Ipconfig is a console application that displays all of the TCP/IP information configured on the computer. You can find more information about this application at

https://en.wikipedia.org/wiki/Ipconfig.
You should see several network cards listed along with specific details for each.

3. Look for the MAC address in this format 00:00:00:00:00:00

What is a MAC address? What is an OUI?

A MAC address is a unique identifier for network interfaces. They can be written in either of these hexadecimal formats:

- **MM:MM:MM:SS:SS:SS**
- **MM-MM-MM-SS-SS-SS**

An OUI {Organizationally Unique Identifier} is a 24-bit number that uniquely identifies a vendor or manufacturer. They are purchased and assigned by the IEEE. The OUI is the first three octets or 24 bits of a MAC address. For example, these are examples of an OUI:

- **00:00:0A** -- this is owned by Omron
- **00-0D-4B** -- this is owned by Roku, LLC
- Open up this website https://www.adminsub.net/?sc0=3

Using the website above, determine who is the manufacturer of this Ethernet network card.

Activity 1: Questions

1. What does the OUI website do?

   You can figure out your MAC address and vendor

2. What is the MAC address for the Ethernet 2 adapter in your machine?

   00-50-56-C0-00-08

3. Who is the manufacturer?

   VMware Inc.

4. What organization manages the OUIs?

   IEEE

5. Find any two other network card manufacturers (not necessarily physical cards on your bench, just out there in the world) and list them here along with the 24 bits of hexadecimal code that correspond.

F832E4 - ASUSTek COMPUTER INC.
AC44F2 - YAMAHA CORPORATION

6. How and where did you find these addresses and manufacturers?

   https://www.adminsub.net/?sc0=3 : searched for “ASUS” and “Yamaha”

What is an IP address and a subnet mask?

Continue to look through the settings from ipconfig /all, specifically for the Ethernet 2 adapter. An IPv4 address is a unique identifier for your machine that exists at layer 3 of the OSI model. It is formatted in what is known as dotted quad notation. Find the IPv4 address for the Ethernet 2 adapter on the computer.

Changing the IP Address Settings

4. Go to Windows -> Settings -> Network and Internet - > Change Adapter Options
5. Double click on Ethernet 2

Right now, you see that the IPv4 connectivity is identified as Internet. This means that the IP address is coming from the network, specifically from a DHCP server as opposed to being statically entered on the machine. We'll talk more about this throughout the semester.

Make a note of the speed for the network connection. Again, we will talk more about this next week in regards to bandwidth, latency and implications for development.

6. Click on details

Take a moment to look through everything that is listed. We will be talking about several of these details throughout the semester. You should also see the same IP and MAC address as you previously saw through the command line.

7. Close this dialog box to go back to the Ethernet 2 status window.
8. Next click on the properties button.
9. In the list of connection items, find and select Internet Protocol Version 4 (TCP/IPv4)
10. click properties.

You will also see that the IP address is set to be obtained automatically. Change this to use a different and static IP address. This will make it so that the IP address is set by us at the machine rather than through the DHCP protocol (again we will discuss this more throughout the semester).

11. Set the IP address to: 20.20.20.P1/4 (where P is your pod number).
12. Set the subnet mask to 255.255.255.0.
13. Click OK and close out of all the dialog boxes.
14. Go back to the command window and rerun the ipconfig command to confirm that your settings changed.

15. Complete this for a total of two of the three PCs on your bench except change the IP addresses to be 20.20.20.P2/5 with the mask of 255.255.255.0

Activity 1: More Questions

7. What is the IP address for the machine where you are working?

   20.20.20.83

8. What is the subnet mask?

   255.255.255.0

9. How many bits are in an IPv4 address?

   32

10. Where did you find this information? (Provide the resource you used.)

    RIPE.net

11. What is the network portion of the address?

    192.168

12. What is the node portion of the address? (If we have not yet covered this, go ahead and do some internet sleuthing.)

    179.1

13. What organization manages the global allocation of IP addresses? (Please also provide the resource where you found this.)

    IANA - in class

14. Explain the difference between a dynamic and a static IP address.

    static- address does not change

    dynamic- addresses are assigned by the network and connect and change over time

15. What is the RFC number for the IPv4 Address Space Registry? (Provide the resource for where you found this.)

RFC1466

16. What is a RFC? (Provide the resource for where you found this.)

    contains protocols and procedures from the Internet Engineering Task Force

17. What is the RFC number and official title for the carrier pigeon RFC?

    RFC1149

Activity 2: Network Testing

Now let's test that the two nodes can talk to each other. We are going to use something called ping. Ping is a utility to test network connectivity and it uses ICMP echo request and ICMP echo reply as we discussed in class. You can learn more about ping here https://www.websitepulse.com/blog/what-is-ping-test. Take a moment to read about its purpose and all that it can do.

The command to ping another device from the command line window is:
Ping <destination IP address>

Test that all of your bench machines can ping each other and make a note of what you see.

16. Ping from each computer on your bench to every other computer on your bench using the ping command: Ping <destination IP address>

You can also find more options for ping by using the help command use **`ping /?`** Take another moment to experiment with some of the options. For example, by default you see that when you send a ping, four replies come back. Can you send a ping that goes on continuously, forever, until you stop it (with ctrl-C)?

17. Try another ping:
    ping -l 6000 IP addr
    - -l is a 'send buffer size' switch - what is this actually doing?
    - What happens when you send this ping?

18. Try some more pings:

ping -l 9000
ping -f -l 6000
ping - n 8
ping -a
ping -s

- For each of these, take a look at the help page for ping at ping /? and consider what each switch is doing.
- What do you see as a result when you attempt these pings?
- Why would you want to do each of these switches?

Activity 2: Questions

18. Explain what you are seeing after you execute each ping. You will need to do some internet sleuthing for this. Be sure to explain each field.

    For example, what does bytes = 32 mean? What does time<1ms mean? What does TTL mean? (Be sure to do more than simply spell out the acronym – explain to me what this is actually reporting to someone who is testing the network using the ping utility).

    bytes is the size of the ping, time is how fast it was received, and TTL is "time to live"- tells the router whether the router has been in the network too long and should be discarded
19. What is a send buffer size switch?
    -l which sends the buffer size which is the temporary storage in memory that stores information while processing other information
20. Explain the -f -l switches and what you saw as a result of that ping.

    -f : don't fragment flag in the packet
    -l : send buffer size
21. Explain the -n switch and what you saw as a result of that ping.
    -n: count number of echo requests to send
22. Explain the -s ping and what you saw as a result of that ping.
    -s: timestamp for count hops

Just for fun on your own time …
Different operating systems will report different data from ping. On your own time, try pinging something more global like cnn.com from one of your own devices or another device (different operating systems, etc.). Look at what is reported. What is different? What is the same? Why do you think that they are different or the same?

Activity 3: Network Monitoring and Encapsulation

Assuming your pings were successful, you saw the echo reply messages being reported on the command line to that effect. Now let's dig a little deeper and look at what is actually going across the physical network wires. We'll do this by using a network packet analyzer called Wireshark.

A packet analyzer is a computer program or piece of computer hardware that can intercept and log traffic passing over a digital network. There are many packet analyzers available, but you can learn more about Wireshark at https://www.wireshark.org/.

Be careful about monitoring network traffic on networks that you do not own or lease. In the past few years, wiretapping laws have been reevaluated in the light of sniffing packets on wired and wireless networks. While there is still some debate around what is legal, you should also consider any policies in place for the networks that you are accessing. Although your actions may not be illegal, they may violate a policy and lead to unexpected consequences. I encourage you to look into this further for yourself.

19. Launch Wireshark and select the Network Interface Card (NIC) where you want to capture network traffic. Be sure to continue working with the Ethernet adapter 2. Double clicking on the Ethernet 2 adapter should automatically launch Wireshark.

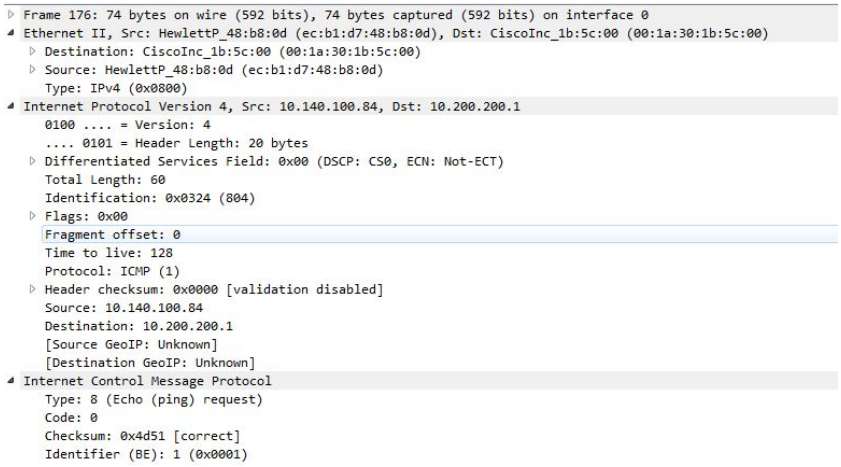
Alternatively, you can select **Capture** from the text toolbar and then **Options** from the drop-down menu**.** From the window presented select the Ethernet Adapter and make sure the Enable Promiscuous Mode is checked, since this is what allows the NIC to capture all the network traffic and display it. Click the Start button. The capture window will open and frames may or may not appear in the window. To generate the traffic needed for this exercise you will execute some pings. The capture operation can be controlled from the icon toolbar. The red square will stop a capture, the leftmost icon will start a new capture, and the icon to the right of the stop button will restart a current capture. Take some time to mouse over the other icons and see what they do.

20. Ping between all of your machines again while running Wireshark to capture the messages.

21. After your ping is complete, stop the Wireshark capture. The capture window is divided into three segments. The top segment contains one summary line for each frame captured. Select one of the summary lines and the details of that frame will be displayed in the center segment in a text format and in hexadecimal in the bottom section. Let's focus on the top and middle windows for now.

22. We are specifically looking for echo request and echo reply messages (they should be highlighted lavender). Find one of these and select the summary frame in the top segment so that the details are displayed in the middle segment. Then further expand the message layers using the caret symbols on the left side.

23. We are looking to identify the different TCP/IP layers as discussed during class. The image below shows a frame that has been expanded. Note that you can save the data from the packet captures if you want to look at them later. You can also take screen captures.



24. Expand each section of the frame to examine the data. You should recognize the IP addresses that you just entered as the source and destination addresses. The protocol is ICMP and the length is 74 and the Info is Echo (ping) request or reply. Make particular note of the encapsulation type, arrival time, frame number and frame length when you expand the Frame 23 section. You will need to Google for each of these and make a table to explain them.

25. Next expand the Ethernet II level. Again, make a table to explain what you see.

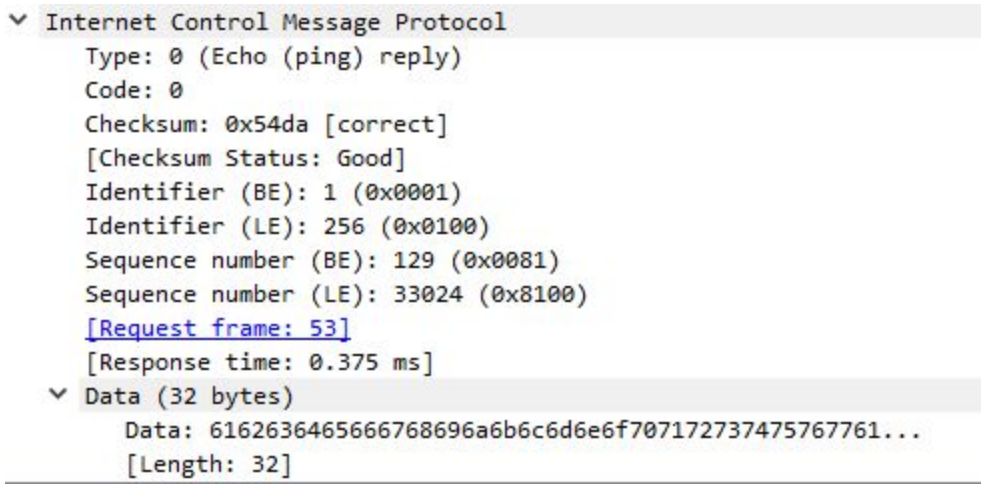
26. Then expand the Internet Protocol Version 4 level and explain the src, dst, and fragment offset.

27. Finally, expand the Internet Control Message Protocol level and explain the type field.

Activity 3: Questions

23. Explain what you saw in Wireshark in regards to the echo request message and the echo reply. Be sure to describe the encapsulation in regards to the layers in the OSI model.

```
Frame 54: 74 bytes on wire (592 bits), 74 bytes captured (592 bits) on interface 0
  Interface id: 0 (\Device\NPF_{4ECD0482-634A-4EC5-ACD7-DF72A7F68180})
      Interface name: \Device\NPF_{4ECD0482-634A-4EC5-ACD7-DF72A7F68180}
    Encapsulation type: Ethernet (1)
    Arrival Time: Feb 21, 2019 09:05:24.069407000 Eastern Standard Time
    [Time shift for this packet: 0.000000000 seconds]
    Epoch Time: 1550757924.069407000 seconds
    [Time delta from previous captured frame: 0.000375000 seconds]
    [Time delta from previous displayed frame: 0.000375000 seconds]
    [Time since reference or first frame: 22.848933000 seconds]
    Frame Number: 54
    Frame Length: 74 bytes (592 bits)
    Capture Length: 74 bytes (592 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ethertype:ip:icmp:data]
    [Coloring Rule Name: ICMP]
    [Coloring Rule String: icmp || icmpv6]
Ethernet II, Src: HewlettP_45:11:26 (ec:b1:d7:45:11:26), Dst: HewlettP_40:d9:fb (ec:b1:d7:40:d9:fb)
  Destination: HewlettP_40:d9:fb (ec:b1:d7:40:d9:fb)
      Address: HewlettP_40:d9:fb (ec:b1:d7:40:d9:fb)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
  Source: HewlettP_45:11:26 (ec:b1:d7:45:11:26)
      Address: HewlettP_45:11:26 (ec:b1:d7:45:11:26)
      .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
      .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
    Type: IPv4 (0x0800)
Internet Protocol Version 4, Src: 20.20.20.81, Dst: 20.20.20.83
    0100 .... = Version: 4
    .... 0101 = Header Length: 20 bytes (5)
  Differentiated Services Field: 0x00 (DSCP: CS0, ECN: Not-ECT)
      0000 00.. = Differentiated Services Codepoint: Default (0)
      .... ..00 = Explicit Congestion Notification: Not ECN-Capable Transport (0)
    Total Length: 60
    Identification: 0x69d7 (27095)
  Flags: 0x00
      0... .... = Reserved bit: Not set
      .0.. .... = Don't fragment: Not set
      ..0. .... = More fragments: Not set
    Fragment offset: 0
    Time to live: 128
    Protocol: ICMP (1)
    Header checksum: 0x801e [validation disabled]
    [Header checksum status: Unverified]
    Source: 20.20.20.81
    Destination: 20.20.20.83
    [Source GeoIP: Unknown]
    [Destination GeoIP: Unknown]
```



encapsulation type- ethernet: the method which data is transferred
arrival time- Feb 21, 2019 9:05.24: the time the message arrived
frame number- 54: container for the network packet
frame length- 74 bytes: max length of a payload field

We saw all the information of the frame, ethernet, protocol used, and message protocol used during the transfer.

Final Lab Questions

24. What went well during this lab experience and why?

Seeing information in the command line was easy to understand.

25. What could have gone better and why?

Understanding what's going on in wireshark because it is a lot of information at once.

26. Reflect on how each of the three activities in this lab experience relate to you as a developer. For example:

How do network settings and configurations impact you as a developer?

Everyone has different configurations and settings so we have to accomodate for everyone.

Why would you as a developer be concerned with network testing?

We want to be sure everything works to the best of its ability.

How does network monitoring and/or encapsulation affect development work?

Different protocols are accounted for along with network changes to make sure everything is working correctly.

Just for fun on your own time …
It is very easy for there to be a tremendous amount of network traffic visible in Wireshark. There are filters available to make it easier to examine the messages that are of particular interest. For example, we could set up a filter to only show me traffic from a particular MAC address, or a particular IP address or a particular protocol. I encourage you to take a few minutes to experiment with some filtering. If you do set up a filter please be sure to show me what you've done!

BONUS – Looking for some more networking fun????
then complete this anytime during the semester before the drop box closed in week 13:
******
Next week in class we will continue to discuss the messages traversing a networking. In particular, we will discuss bandwidth, throughput and latency as they relate to packet sizes. To see the effect of packet sizes, consider how you might send larger or smaller packets on a small network like the one you used today.

For example, use the MS DOS Help command to determine how to vary the layer 3 packet size. Can you send a ping that is larger than the default and observe and differences in the captures? Specifically, you will be looking for how the message is fragmented and reassembled on the other end. Capture packets to note the behavior of the network, including average response time with varying packet sizes. Try sending packets with sizes that will "fit" in a single layer-2 frame (less than 1500 bytes) followed by sizes much larger than can be accommodated by a single packet (maximum of 65, 500 bytes). Record results of the different tests you run along with an explanation of why you are seeing those results.

Or for some more fun, change your IP network setting back to DHCP (automatic serving of IP addresses) and
1. Ping domain names instead of IP addresses:
ping google.com
facebook.com
cnn.com
Amazon.com
rit.edu
ur.edu

- What happens for each?
- What do you see that is different for each?
- Why do you think that some results are different?
- Why is this important?

2. Try to trace the route to the domains you previously pinged:
tracert google.com
facebook.com
cnn.com

Amazon.com
rit.edu
ur.edu