CPE 464 Lab 1 **Worksheet**

Name: Bryce Melander

This lab worksheet needs to be typed. Each student must type in their own answers. You cannot have a "group" version. You will upload your worksheet to Canvas. This worksheet is due on the Friday after lab at 11:59 pm.

In this lab we are going to look at some basic networking concepts and tools. The steps in this lab are:

A. Introductions
B. Program #1 questions
C. Ping
D. Traceroute (tracert on windows)
E. Wireshark for packet analysis

This lab assumes you have already installed Wireshark. (https://www.wireshark.org/#download)

1) **Introduce yourself to your group and fill in the table:**

Have each person introduce themselves to the group (fill in table below).

a. Name
b. Major, Year
c. Where they are from
d. Something about themselves

First name	Major	Where they are from (City)
Bryce	CPE, 2024	Yreka, Ca.
Jacqueline	CPE, 2023	San Jose, Ca.
Joey	CPE, 2023	Los Angeles, Ca.
Thomas	CS, 2024	Davis, Ca.

2) **Ping**

The ping command allows you to query another computer to see if that computer is correctly connected to a network.

The format for the ping command is: **ping <*hostname*>**
You can execute this command in a Linux terminal or in the windows command window. On a Linux/Mac us: ping -c 5 <hostname>. This will limit the ping command to 5 requests/replies.

a. ping a University. e.g. ping www.msu.edu. (DO NOT use www.msu.edu... Pick some other university in the US and try them. If the entire class goes to the same university, they may lock us out. Keep trying until you get all successful pings for a site.)

   What is the average time it takes for this ping to be successful? (note – a ping is measured by sending and then receiving a ping packet – so it's a round trip. We can refer to this time as RTT or round trip time.)

   Avg: 47.686 ms

b. ping www.imperial.ac.uk. What is the average time (RTT) it takes for this ping to be successful?

   Avg: 155.904 ms

c. We talked about latency (RTT or round trip time) in lecture. Can you speculate why it takes longer to ping www.imperial.ac.uk than the US based university?

   - The US-based domain has a shorter distance to travel, as in the wires themselves are shorter and therefore the travel time is lower. A longer travel path likely also means more points in the path that the information needs to stop and wait for redirection.

We will look at the ping command again as part of our use of wireshark later in this lab.

3) **Traceroute** (on windows its **tracert** or **tracepath** on newer Linux boxes)

The traceroute (tracert, tracepath) command allows you to see the path taken across the Internet. It returns the IP address or name of the routers that the packet traverses. Let’s look at the path between your location and Oxford and UCSB.

a. In a terminal/command window type: traceroute www.imperial.ac.uk (or on windows: tracert www.imperial.ac.uk or on some Linux boxes: tracepath www.imperial.ac.uk)

i. How many hops (routers) are between you and www.imperial.ac.uk?
15 hops, 14 when omitting unresponsive routers.

ii. Speculate which hop takes you from the US to England, which hop is it?

The hop to the U.K. is likely either hop 10 or 11:

```
 9  lag-47.ear3.sanjose1.level3.net (4.68.74.221)
10  * ae1.3108.ear3.london2.level3.net (4.69.143.198)
11  janet.ear3.london2.level3.net (212.187.216.238)
```

iii. For the router that you think is the first one in England, look it up using Google. Go to Google and search for the name of the router. (For me the router is *ldn-bb3-link.telia.net,* so I typed ‘who has ldn-bb3-link.telia.net’ in Google.)

For your traceroute, what is the router name?
Level 3 Communications

In what country (and city) is this router located?
London, U.K.

b. Traceroute to www.umich.edu (traceroute www.umich.edu)

i. How many hops are between you and www.umich.edu?
19 hops, 18 when omitting unresponsive routers.

ii. How many routers are the same in the traceroute results for www.imperial.ac.uk and www.umich.edu?
6 routers

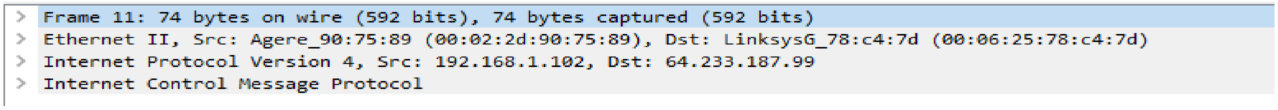
4) **Wireshark**.

In this part of the lab you need Wireshark (www.wireshark.org) on your computer. Wireshark allows you to analyze packet traces. These packets may be captured on a live network (this is called packet sniffing) or wireshark can analyze packet traces previously captures and stored in a file with the extension '.pcap' or '.pcapng.' In this lab (and in program 1) you will analyze packet trace files that I captured on my network.

Note…Your first program, called trace, is to write a simple version of a packet analyzer. You will be given packet trace files (.pcap) and are required to output information on each packet.

a. Download and install wireshark (www.wireshark.org) on your computer
b. Download the ping.pcap file from canvas
c. Open the ping.pcap file in wireshark

First, you are going to look at the headers for ping packets. For the first part of the lab, there are three headers that we are interested in. These are the Ethernet header, IP header and ICMP (ping) header.



```
> Frame 11: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Agere_90:75:89 (00:02:2d:90:75:89), Dst: LinksysG_78:c4:7d (00:06:25:78:c4:7d)
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 64.233.187.99
> Internet Control Message Protocol
```

Using Wireshark, you will expand each of these headers and look at the values in these headers.

5) **Ethernet Overview (using the ping.pcap file)**

a. Based on the lecture, draw (or list the fields in) a standard ethernet header, including the length of each field. (If you don't remember google ethernet header).

Ethernet Type II Frame:

Source MAC Address	: 6 Bytes
Dest MAC Address	: 6 Bytes
Type	: 2 Bytes
Payload	: 46 - 1500 Bytes
Checksum	: 4 Bytes

Looking at the Ethernet header in the 4th packet from the ping.pcap file via wireshark. Expand the Ethernet PDU so you can see all of the fields.

b. What is the source Ethernet MAC address in the colon notation (e.g. 05:03:…)?
`00:06:25:78:c4:7d`

c. What is the destination Ethernet MAC address?
`00:02:2d:90:75:89`

d. This Ethernet frame carries an IP payload, what is the Ethernet **Type** value that specifies this?
IPv4 - 0x0800

What is the hex value for the **type** field for the following payloads that may be carried by Ethernet (see https://en.wikipedia.org/wiki/EtherType):

e. **Type** field value for Internet Protocol version 4 (IPv4)? **0x0800**
f. **Type** field value for Internet Protocol version 6 (IPv6)? **0x86dd**
g. **Type** field value for Address Resolution Protocol (ARP)? **0x8006**

h. Explain how you could determine that an Ethernet Frame carries a TCP segment (talk about it with your group)?
That info would be contained in the IP Header protocol field.

6) Internet Protocol Overview (using the ping.pcap file)

Go to the 1st packet in the file. The ping protocol is called ICMP. Expand the packet in the middle window (right click then "Expand All").

a. What is the **source** IP address for the 1st ping request?
   Source Address: 192.168.1.102

b. What is the **destination** IP address for the 1st ping request packet?
   Destination Address: 66.94.230.35

Compare the packet in the ping.pcap file and the IP header figure from Wikipedia:
https://en.wikipedia.org/wiki/IPv4#/media/File:IPv4_Packet-en.svg

c. What Version of IP is this in binary and decimal?
   0b0100 / 0x4

d. What is the header length (IHL) value in binary and decimal?
   0b0101 / 0x5

e. What is the total length value?
   60

f. What is the Time to Live (TTL) value?
   128

g. What is the Protocol value?
   1 (ICMP)

Go to Wikipedia for a list of protocol numbers:
https://en.wikipedia.org/wiki/List_of_IP_protocol_numbers

h. What is the protocol number for TCP? **6**

i. What is the protocol number for UDP? **17**

j. What is the protocol number for ICMP? **1**

7) **Ping** – officially called Internet Control Message Protocol (ICMP)

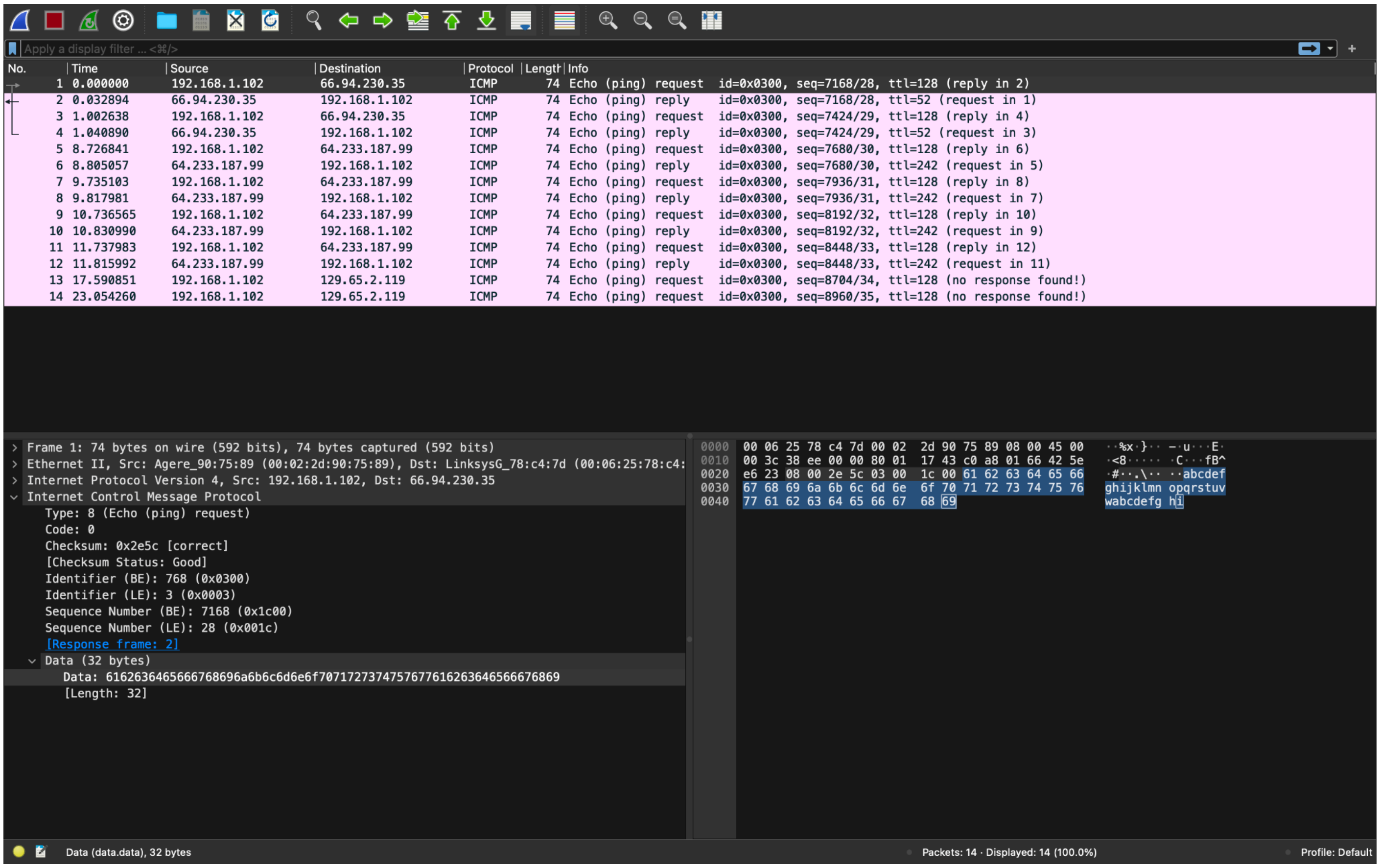
Looking at the "Internet Control Message Protocol" section of packet #1.

a. What is the ICMP **type** value for the ICMP Echo request packet (packet 1)?
   Type: 8 (Echo (ping) request)

b. Look at packet 2, what is the **type** value for the ICMP Echo reply packet?
   Type: 0 (Echo (ping) reply)

c. Back to packet 1, what is the data that was sent in the ping request packets (in ASCII – select the data in the middle window and look at what is highlighted in the bottom window)?
   Data: abcdefghijklmnopqrstuvwabcdefghi

d. When you turn in this lab, include a screenshot of wireshark running on your computer with the ping.pcap packets.



Apply a display filter ... <⌘/>

No.	Time	Source	Destination	Protocol	Length	Info
1	0.000000	192.168.1.102	66.94.230.35	ICMP	74	Echo (ping) request id=0x0300, seq=7168/28, ttl=128 (reply in 2)
2	0.032894	66.94.230.35	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=7168/28, ttl=52 (request in 1)
3	1.002638	192.168.1.102	66.94.230.35	ICMP	74	Echo (ping) request id=0x0300, seq=7424/29, ttl=128 (reply in 4)
4	1.040890	66.94.230.35	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=7424/29, ttl=52 (request in 3)
5	8.726841	192.168.1.102	64.233.187.99	ICMP	74	Echo (ping) request id=0x0300, seq=7680/30, ttl=128 (reply in 6)
6	8.805057	64.233.187.99	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=7680/30, ttl=242 (request in 5)
7	9.735103	192.168.1.102	64.233.187.99	ICMP	74	Echo (ping) request id=0x0300, seq=7936/31, ttl=128 (reply in 8)
8	9.817981	64.233.187.99	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=7936/31, ttl=242 (request in 7)
9	10.736565	192.168.1.102	64.233.187.99	ICMP	74	Echo (ping) request id=0x0300, seq=8192/32, ttl=128 (reply in 10)
10	10.830990	64.233.187.99	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=8192/32, ttl=242 (request in 9)
11	11.737983	192.168.1.102	64.233.187.99	ICMP	74	Echo (ping) request id=0x0300, seq=8448/33, ttl=128 (reply in 12)
12	11.815992	64.233.187.99	192.168.1.102	ICMP	74	Echo (ping) reply id=0x0300, seq=8448/33, ttl=242 (request in 11)
13	17.590851	192.168.1.102	129.65.2.119	ICMP	74	Echo (ping) request id=0x0300, seq=8704/34, ttl=128 (no response found!)
14	23.054260	192.168.1.102	129.65.2.119	ICMP	74	Echo (ping) request id=0x0300, seq=8960/35, ttl=128 (no response found!)

```
> Frame 1: 74 bytes on wire (592 bits), 74 bytes captured (592 bits)
> Ethernet II, Src: Agere_90:75:89 (00:02:2d:90:75:89), Dst: LinksysG_78:c4:7d (00:06:25:78:c4:
> Internet Protocol Version 4, Src: 192.168.1.102, Dst: 66.94.230.35
v Internet Control Message Protocol
    Type: 8 (Echo (ping) request)
    Code: 0
    Checksum: 0x2e5c [correct]
    [Checksum Status: Good]
    Identifier (BE): 768 (0x0300)
    Identifier (LE): 3 (0x0003)
    Sequence Number (BE): 7168 (0x1c00)
    Sequence Number (LE): 28 (0x001c)
    [Response frame: 2]
  v Data (32 bytes)
      Data: 6162636465666768696a6b6c6d6e6f7071727374757677616263646566676869
      [Length: 32]
```

```
0000  00 06 25 78 c4 7d 00 02  2d 90 75 89 08 00 45 00   ··%x·}·· –·u···E·
0010  00 3c 38 ee 00 00 80 01  17 43 c0 a8 01 66 42 5e   ·<8····· ·C···fB^
0020  e6 23 08 00 2e 5c 03 00  1c 00 61 62 63 64 65 66   ·#···.\·· ··abcdef
0030  67 68 69 6a 6b 6c 6d 6e  6f 70 71 72 73 74 75 76   ghijklmn opqrstuv
0040  77 61 62 63 64 65 66 67  68 69                     wabcdefg hi
```

Data (data.data), 32 bytes   Packets: 14 · Displayed: 14 (100.0%)   Profile: Default

8) **DHCP (still using wireshark)**

Now we are going to study one of the network protocols we use every day. This protocol is called DHCP. Using Google, answer the questions below.

a) What does DHCP stand for?
Dynamic Host Configuration Protocol

b) What is the purpose of DHCP?
It manages a record of all the IP addresses it allocates to network nodes.

c) Name and explain the four basic packets used in DHCP
- **Discover** - Locate the DHCP server
- **Offer** - The server offers an IP address
- **Request** - Client asks for an offered address
- **Ack** - The server grants the address lease

d) Draw a packet flow diagram of the packets that flow between your computer and the DHCP server.

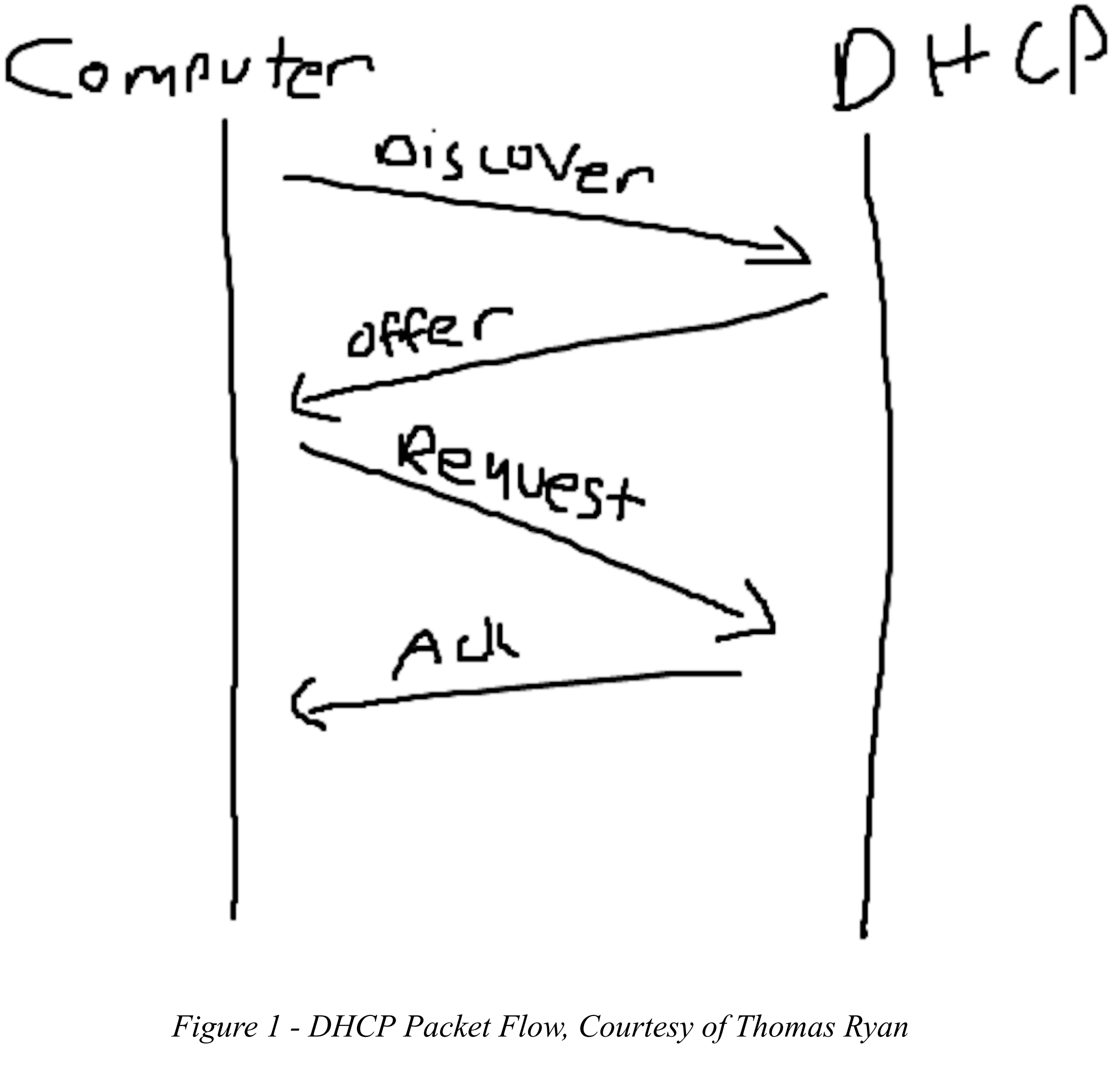


Figure 1 - DHCP Packet Flow, Courtesy of Thomas Ryan

e) Looking at the DHCP packet trace file (found on canvas, dhcp_trace.pcapng) using wireshark, answer the following questions:

i. Looking at the first packet, expand the Ethernet II header:

a. What is the source (src) MAC address?
Source: (98:5f:d3:4e:bc:13)

b. In the same packet, what is the destination (dst) MAC Address?
Destination: (ff:ff:ff:ff:ff:ff)

c. The destination MAC address is a broadcast address, explain why.
The host does not yet have an IP address, so they can only accept broadcasts.

ii. Looking at the DHCP Offer packet (expand this header) answer the following questions:

a. What is the IP address of the DHCP server?
DHCP Server Identifier (192.168.86.1)

b. How long is the lease for this DHCP offer?
1 Day

c. What is the client **offered** (your) IP Address?
Domain Name Server: 192.168.86.221

d. What is the Router's IP address (this is also called a default gateway)?
Domain Name Server: 192.168.86.1

f) Describe two different types of DHCP Vulnerabilities. (google DHCP security issues)

1. **Spoofing:** Pretending to be a DHCP server and handing out bad information to legitimate end users, sending them to a fake site.
2. **Starvation:** An attack that exhausts all available IP addresses that can be allocated by the DHCP server.

9) **A quick look at TCP**

The goal of this section is to walk you through the calculation of the TCP segment length and to look at the endianness of the numbers. (It's suggested that you ask for help as you work through this. It is not obvious.)

a. Download the largeMix2.pcap file from Canvas[1]

b. Using Wireshark, answer the following question about the IP and TCP headers based on **packet 36**:

i. Regarding the IP header length

a. Looking at packet 36, what is the value for the IP Header Length in hex and in decimal (so what is the header length in words… so the value in the actual packet header)?

- **0x5 / 5 Words**

b. Now, calculate the actual number of bytes in the IP Header (show your calculation) based on this IP's header length field.

- **5 * 4 Bytes = 20 Bytes**

ii. Looking at packet 36, what is the total length of the entire IP PDU in hex and decimal?[2]

- **0x010E / 270 Bytes**

iii. In hex, what would be the total length of the entire IP PDU in **little endian**?

- **0x0E01**

iv. Calculate the length of the TCP PDU (so the TCP segment). Note, the "TCP Segment Len: 230" displayed by wireshark is **incorrect**. Show your work.

- **250 Bytes**

Note – to use this calculated TCP segment length in your pseudo header you would need to put it into network order (htons()).

When you are done, I recommend you begin working on program #1 called trace.

[1] Both pcap files used in this lab are part of program #1 (trace), so you should already have them. They are also on Canvas for this lab.

[2] If you select the field (e.g. "Total Length" field in the IP header), it will highlight at the bottom of the screen the value in hex.