CPE 464 Lab 2
Ethernet

Name: Nick Bell

This lab worksheet needs to be typed. You will upload your worksheet to PolyLearn. This worksheet is due on Friday, April 17 by 11:59 pm.

In this lab we are going to look at some basic tools for networking. These are:

1) Introduction to the group
2) A quick look at TCP
3) ARP
4) Address Learning
5) Spanning Tree Protocol (STP)

1) Since it's a new group Introduce yourself to your group (make note of your zoom group number)

Please turn your cameras on during the group work part of the lab.

Have each person introduce themselves to the group.

a. Name
b. Current Location
c. Major, Year
d. Something about themselves

2) A quick look at TCP

The goal of this section is to walk you through the calculation of the TCP segment and to look at the endianness of the numbers.

a. Download the largeMix2.pcap file from PolyLearn[1]
b. Answer the following question about the IP and TCP headers based on **packet 36**:

i. Looking at packet 36, what is the total length of the entire IP PDU in hex and decimal (see IP header)?[2]

270 bytes or 0x010e

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

0x0e, 0x01 or 3585 in decimal

iii. Calculate the length of the IP Header (show your work).

Header length: 20 bytes

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

iv. Calculate the length of the TCP PDU (so the TCP segment). Note, the “TCP Segment Len: 301” displayed by wireshark is incorrect. Show your work.

    TCP Segment length + TCP Header = 230 + 20 = 250 bytes

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

3) Address Resolution Protocol (ARP)

a. What is the purpose of the ARP protocol?

   To translate IP addresses to MAC addresses

b. Describe the ARP process.

   ARP request is sent – broadcast message asking who has IP address ____

   ARP reply is sent back – unicast message from machine that owns the requested IP, sends their MAC address

c. Download the arpTest.pcap packet trace from PolyLearn

d. Open this file using Wireshark

e. Google how to look at your ARP cache (also called ARP table) for your Operating system (e.g. Windows, iOS, Linux).

   i. Using the ARP command for your OS:

      a. How many dynamic (see type field) entries are there?

         5 dynamic entries

      b. What is one of the entries?

         192.168.0.149 20-df-b9-97-90-d9 dynamic

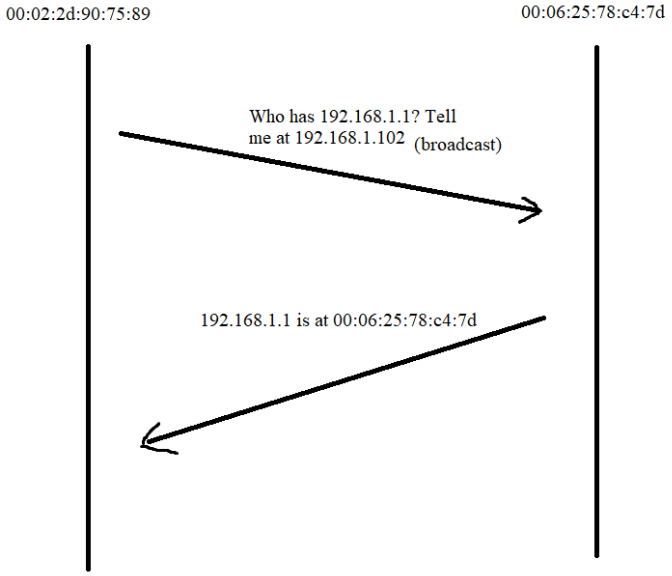
f. Looking at the first two packets in arpTest.pcap:

   ARP requires a request and a reply. In the first two frames, what is the request question and what is the reply to this question?

   Request – Who has 192.168.1.1? Tell me at 192.168.1.102

   Reply – 192.168.1.1 is at 00:06:25:78:c4:7d

g. Draw a packet flow diagram for the request/reply exchange found in frames 1 and 2. Include in the flow the source and destination MAC addresses for each transmission.


00:02:2d:90:75:89
00:06:25:78:c4:7d
Who has 192.168.1.1? Tell me at 192.168.1.102
(broadcast)
192.168.1.1 is at 00:06:25:78:c4:7d

h. Based on the first 2 frames in arpTest.pcap, fill in the data below:

Packet 1 (request)

Ethernet II Header	Destination Address:	ff:ff:ff:ff:ff:ff
	Source Address:	00:02:2d:90:75:89
	Type (in hex):	0x0806
ARP PDU	Hardware Type (in hex):	***0x0001***
	Protocol Type (in hex):	0x0800
	Hardware Address size:	6
	Protocol Address size:	4
	OPCODE (in hex):	0x0001
	Sender’s Hardware Address:	00:02:2d:90:75:89
	Sender’s IP Address:	192.168.1.102
	Target Hardware Address:	00:00:00:00:00:00
	Target IP Address:	192.168.1.1

Packet 2 (reply)

Ethernet II Header	Destination Address:	00:02:2d:90:75:89
	Source Address:	00:06:25:78:c4:7d
	Type (in hex):	0x0806
ARP PDU	Hardware Type (in hex):	**0x0001**
	Protocol Type (in hex):	0x0800
	Hardware Address size:	6
	Protocol Address size:	4
	OPCODE (in hex):	0x0002
	Sender's Hardware Address:	00:06:25:78:c4:7d
	Sender's IP Address:	192.168.1.1
	Target Hardware Address:	00:02:2d:90:75:89
	Target IP Address:	192.168.1.102

i. **Answer the following questions on ARP:**

   i. How does Wireshark (or your computer's networking functionality) know that these two Ethernet frames contain an ARP PDU?

      The type field in the ethernet header specifies it as an ARP PDU.

   ii. Why does the ARP request packet need to be sent to a broadcast address?

      It doesn't know where its destination is located, that's the whole purpose of the protocol. I has to send it to everyone and have the owner of the IP reply.

4) **Regarding the switch's <u>address learning</u> functionality**

   a. What is the purpose of the address learning functionality (how does it make an Ethernet switch better than a Ethernet hub)?

      A switch that knows which addresses are on which interfaces can send frames exclusively on that interface and not broadcast every packet.

   b. What is the name of the table that is created? Also, draw the table with column labels.

      MAC address table – column labels are Vlan, Mac Address, Type, and Ports.

c. Describe the process of Ethernet address learning that is used by a switch.

Every time it receives a new frame, it updates the table with the source of the frame and the interface it came in on.

d. As part of the address learning functionality, does a switch modify the frame as it passes through the switch?

No, it doesn't.

e. There are (at least) two different situations where a switch will broadcast a frame. Name and explain these two situations:

i. If the address is not already saved in the table, the frame will be broadcast to every interface.

ii. If the frame has a destination of ff:ff:ff:ff:ff:ff (broadcast), it will also send it on all interfaces.

f. What is the difference between a Switch and a router (think about the layers)?

A router understands IP addresses and determines IP destinations for the connected devices while a switch only communicates to MAC addresses.

5) Spanning Tree Protocol (STP)

Using Wikipedia… look up the spanning tree protocol

a. What is the purpose of STP?

It removes loops from the network.

b. How is the root node chosen?

The root node is the bridge with the lowest bridge ID, which is a concatenation of the bridge priority and the MAC address.

c. How is the shortest path chosen?

It chooses the path back to the root with the lowest cost, defined as 20 Tbit/s / bandwidth.

d. What is a BPDU (Briefly explain)?

A BDPU is a bridge protocol frame used by STP. A switch sends them as multicast packets to the other switches, with two different kinds. A Configuration BPDU is sent by a root bridge to provide STP info to the others, and a Topology Change Notification (TCN) is sent by other bridges towards the port bridge to notify them of topology changes.

e. How are links chosen if there is a tie in the least cost path back to the root?

It uses the lowest bridge ID as a first tiebreaker, then the lowest port ID as a second tiebreaker.