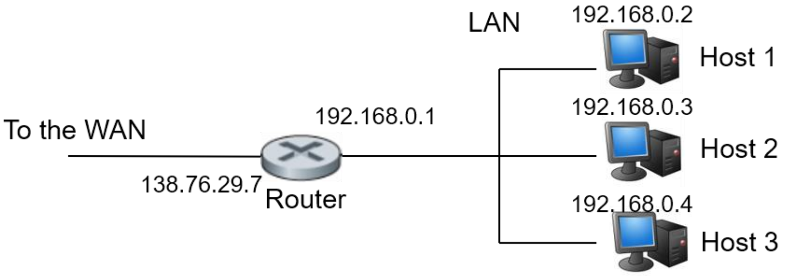
University of Pittsburgh, ECE 1150

ASSIGNMENT 7

<u>Show all steps in answering the following questions. Make sure to put units of measurements (if applicable) in your answers.</u>

Question 1: Consider a NAT router is used to connect a LAN with 3 hosts to the WAN. The network structure and NAT table is given as follows:



WAN side	LAN side
138.76.29.7:8001	192.168.0.2:2202
138.76.29.7:8002	192.168.0.3:2489
138.76.29.7:8003	192.168.0.4:1533

a) If two packets from the LAN side have following source and destination IP / port, what are their source and destination IP / port after the NAT translation?

Source	Destination
192.168.0.2:2202	136.142.34.104:80
192.168.0.4:1533	52.25.108.148:443

b) If two packets from the WAN side have following source and destination IP / port, which hosts are their destination?

Source	Destination
136.142.34.104:80	138.76.29.7:8002
52.25.108.148:443	138.76.29.7:8001

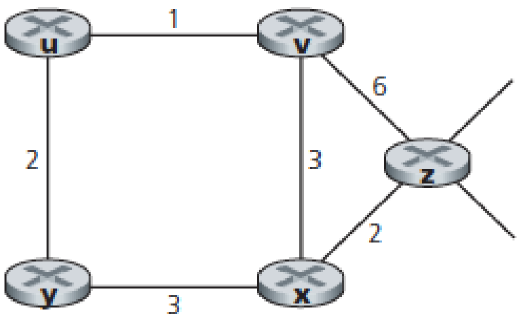
Question 2: Consider a datagram network using 32-bit host address. Suppose a router has four links, numbered 0 through 3. Packets are forwarded to the link interface as follows:

Destination Address Range	Link Interface
11100000 00000000 00000000 00000000 through 11100000 00111111 11111111 11111111	0
11100000 01000000 00000000 00000000 through 11100000 01000000 11111111 11111111	1
11100000 01000001 00000000 00000000 through 11100001 01111111 11111111 11111111	2
otherwise	3

Provide a forwarding table (at least one entry for each interface). The table uses the largest prefix matching and forwards packets to the correct interface.

Question 3: Consider the below network shown. Assume that each node <u>initially</u> knows the costs to each of its neighbors. Nodes keep exchanging information about their connections. Consider the distance-vector algorithm and show the distance table entries at node z.

(Represent your answer in a table with 3 rows; being z and its neighbors (v,x) and 5 columns corresponding to all nodes in the network (u, v, x, y, z). Each entry at (row i, column j) in the table corresponds to cost of path/link from node in row i to node in column j. Show how table at node z progresses as nodes exchange their routing information)



Three steps showing progressing in time are sufficient for this question.

Question 4: Wireshark Mini-Lab: Follow the following steps to answer the questions

ARP - Make sure you downloaded the Wireshark (instructions in separate file in the Network Layer folder of your course documents).

Close all browsers and Internet applications Open a terminal. Use "arp – a" to view contents of ARP cache.

a) **Describe what is displayed.**

Open Wireshark, and start capturing packets (click on the interface you will capture form). In the terminal, delete ARP cache: use "sudo arp –a –d". Start a browser and go to my.pitt.edu. Stop capturing packets. From the Wireshark captured packets, find ARP packets (you can arrange packet captured by protocol by clicking on the protocol column)

b) **Note the destination address in the ARP request (destination column). Is it broadcast or unicast? Note that "broadcast" means it is transmitted to all devices in same network, "unicast" means that it is addressed to a single device.**
c) **From the ARP response message: is it broadcast or unicast?**
d) **What is the purpose of these ARP messages?**

Question 5:

a) **Mention the main difference between TCP and UDP.**
b) **Check your one computer network application you use and search the web to figure out whether it uses TCP or UDP at the transport layer.**

Question 6: Wireshark Mini-Lab: TCP/IP

In this exercise, you need to use MATLAB to establish a client-server connection and transfer data. You will also need to use Wireshark to capture the TCP/IP packets to see how the protocol works. Please follow the instructions below and answer the corresponding questions.

- Open two instances of MATLAB.
- Each MATLAB instance should have a command window.
- One will act as your server and the other one acts as your client (name them using comments %server, %client).
- Open Wireshark. Select the interface used for local loopback (i.e., double-click on the option with "loopback").
- First, both MATLAB windows should create a variable using the *tcpip* function.
    - To use the *tcpip* function, *Instrument Control Toolbox* need to be installed (check MATLAB Add-Ons)
    - *tcpip* has 4 inputs arguments (check MATLAB help/documentation).

    - For the server, use "0.0.0.0" for the first input argument. This means the server will accept the first machine to connect.
    - For the client, use "localhost" or "127.0.0.1" for the first input argument.
    - Advice use port 30000.
- Open the server, then the client (check *fopen* MATLAB command).
- Using *fscanf* and *fprintf,* transmit "ECE1150" from the client to the server.

a) Show the result in the server side. Take a screenshot of both command windows (or script if you use).

- Use *fclose* to terminate the connection.
- Stop capturing in Wireshark

b) Find the packets correspond to this TCP/IP link and take a screenshot. (You can use the filter by typing "tcp.port == (the port you use)").

c) What is the purpose of first 3 TCP packets?

d) What are the sequence and acknowledgement numbers of these three TCP packets?

Note that you may get relative numbers (sequence number 0, 1, 2…). For exact raw numbers, you need to go to Edit → Preferences → Protocols → TCP, and uncheck "Relative sequence numbers and window scaling."

e) Find the packet that contains the word "ECE1150" (or 45 43 45 31 31 35 30 0a in hex) and take a screenshot. (You can click on the packets and see detailed information in below)

Question 7: Wireshark Mini-Lab: DNS

In this exercise, you should be able to know messages exchanged to get IP address of the server you want to connect to. The protocol that enables us to get IP address of a destination is called DNS. DNS (Domain Name System) is a naming system used for identifying the computers and servers that are connected over internet, and allows us from a URL to get the IP address of the destination. After we get IP address of the server on pitt.edu, we should see the TCP messages exchanged for establishing the connections. Please follow the instructions below and answer the corresponding questions.

- Close all Internet applications (all browsers)
- Open Wireshark, select the interface used for Internet connection by double-clicking on it (e.g., double-click on "Wi-Fi: en0" if you use Wi-Fi), and start capturing packet (which starts automatically at first)
- Start a terminal, and clear the DNS cache
    - For Windows, open Command Prompt. Type in "ipconfig/flushdns" and hit Enter
    - For MacOS, open Terminal. type in "sudo killall -HUP mDNSResponder" and hit Enter.
- Type in "ping www.pitt.edu" and hit Enter
- Stop capturing packet in Wireshark (by clicking on the stop button [red square button])

- In Wireshark, locate and examine the DNS query & response by searching the “Protocol” column for “DNS”, or type DNS in filter bar. Then, in the “info” column look for: “standard query” for “A www.pitt.edu”. Then right click on the query and select follow --> UDP stream. You should be able to see the “standard query response”.

a) **Take a screenshot of the query and response packet**

b) **Click on the DNS query response and look into the details of the message (middle portion in Wireshark). Click on the arrows to expand different fields. Are they sent over UDP or TCP?**

Hint: You can find this information next to source port (Src Port) and destination port numbers (Dst Port). This information is also in the IP header (next header field)

c) **What is the destination port number for the DNS query message? What is the source port number of DNS response message?**

d) **Examine the DNS response message. What is the IP address of the URL you typed in your terminal (www.pitt.edu)?**

Hint: expand “Domain Name System (response), then expand “Answers”, the IP address should be in the “Address field”.