

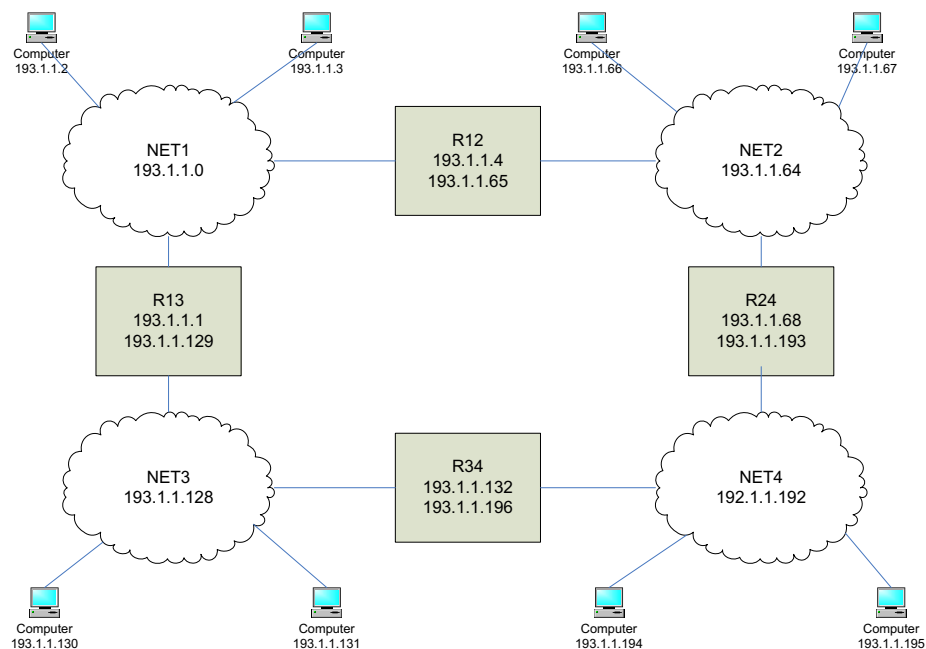
Part One: Short Answer Questions

1. What are the pros and cons of limiting reassembly to the endpoint as compared to allowing en route reassembly?

To solve the problem of reassembling the fragments that arrive out of order a unique identification number is placed in the IDENTIFICATION field of each outgoing datagram. When a router fragments a datagram, the router copies the identification number into each segment. A receiver uses the identification number and IP source address in an incoming fragment to determine the datagram to which the fragment belongs. In addition, the fragment OFFSET field tells a receiver how to order fragments within a given datagram.

2. A company gets a Class C address, 193.1.1.0. Please help the company partition the network into 4 sub-networks, by identifying the subnet mask, assigning addresses to each of the four sub-networks, assigning needed IP addresses to routers and computers. Suppose there are two computers on each sub-network.

The subnet mask is 255.255.255.192



3. A router has the following (CIDR) entries in its routing table:

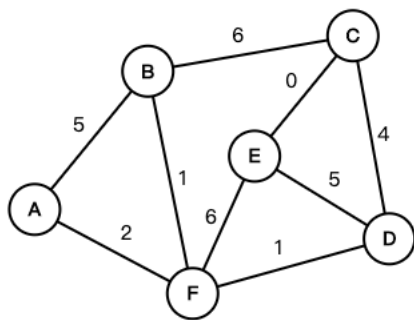
<u>Address/Mask</u>	<u>Next Hop</u>
135.46.56.0/22	Interface 0
135.46.60.0/22	Interface 1
192.53.40.0/23	Router 1
default	Router 2

For each of the following IP addresses, what does the router do of a packet with that address arrives?

- a) 135.46.63.10 **Interface 1**
- b) 135.46.57.14 **Interface 0**
- c) 135.46.52.2 **Router 2**
- d) 192.53.40.7 **Router 1**
- e) 192.53.56.7 **Router 2**

Part Two: Routing Question

Given the graph below, where weights are assigned on the edges, simulate the first two updates which will be carried out on the routing table information for node A according to each of the distributed route computation algorithms provided with this assignment. Give your answers as parts (a) and (b) below. (Assume all other node's routing tables are up to date)



- a) Distance Vector Routing (Explain all your answers)
 - 1) Give the initial Routing Table for node A in the graph.
 - 2) Show what happens when A receives the first Distance Vector from B.
 - 3) Show what happens when A receives the second Distance Vector from F.

- b) Link-State Routing (SPF) from Dijkstra's algorithm (Explain all your answers)

- 1) Give the initial Routing Table for node A in the graph.
- 2) Show the first iteration of the algorithm and the resulting routing table for A.
- 3) Show the second iteration of the algorithm and the resulting routing table for A.

(Solution)

(a) Distance Vector Routing (Explain all your answers)

- 1) Give the initial Routing Table for node A in the graph.

Destination	Next Hop	Distance
A	-	0

- 2) Show what happens when A receives the first Distance Vector from B.

A receives the following Distance Vector: [(C,6), (F,1), (A,5), (B,0)]

Looking at (C,6) from B: No route exists to C.

Looking at (F,1) from B: No route exists to F.

Looking at (A,5) from B: A route to 'A' exists, but none with next hop equal to B.
but none with distance greater than 10.

Looking at (B,0) from B: No route exists to B.

Updated routing table:

Destination	Next Hop	Distance
A	-	0
C	B	11
F	B	6
B	B	5

- 3) Show what happens when A receives the second Distance Vector from F.

A receives the following Distance Vector: [(E,6), (D,1), (B,1), (A,2), (F,0)]

Looking at (E,6) from F: No route exists to E.

Looking at (D,1) from F: No route exists to D.

Looking at (B,1) from F: A route to B exists, but none with next hop equal to F.
with distance greater than 3.

Looking at (A,2) from F: A route to A exists, but none with next hop equal to F.
but none with distance greater than 4.

Looking at (F,0) from F: A route to F exists, but none with next hop equal to F.
with distance greater than 2.

Updated routing table:

Destination	Next Hop	Distance
A	-	0
C	B	11**
F	F	2
B	F	3
E	F	8
D	F	3

**Note: The alg. given for the assignment appears to be somewhat incomplete, since this entry should be recalculated to 9.

(b) Link-State Routing (SPF) from Dijkstra's algorithm (Explain all your answers)

1) Give the initial Routing Table for node A in the graph.

D(v): DISTANCE TABLE

Distance	5	∞	∞	∞	2
Destination	B	C	D	E	F

R(v): NEXT-HOP TABLE

N.H	B	0	0	0	F
Destination	B	C	D	E	F

S -> B,C,D,E,F

2) Show the first iteration of the algorithm and the resulting routing table for A.

Choose F, $D(F) = 2$.

Looking at edge(F,A): A is not in S.

Looking at edge(F,B): B is still in S.

$$c = 2 + 1 = 3, D(B) = 5.$$

$$3 < 5,$$

$$R(B) = R(F)$$

$$D(B) = 3.$$

Looking at edge(F,D): D is still in S.

$$c = 2 + 1 = 3, D(D) = \infty.$$

$$3 < \infty,$$

$$R(D) = R(F),$$

$$D(D) = 3.$$

Looking at edge(F,E): E is still in S.

$$c = 2+6 = 8, D(E) = \infty.$$

$$8 < \infty,$$

$$R(E) = R(F),$$

$$D(E) = 8.$$

Updated routing table:

D(v): DISTANCE TABLE

Distance	3	∞	3	8	2
Destination	B	C	D	E	F

R(v): NEXT-HOP TABLE

N.H	F	0	F	F	F
Destination	B	C	D	E	F

S -> B,C,D,E

3) Show the second iteration of the algorithm and the resulting routing table for A.
Choose B, $D(B) = 3$.

Looking at edge(B,A): A is not in S.

Looking at edge(B,F): F is not in S.

Looking at edge(B,C): C is still in S.

$$c = 3+6 = 9, D(C) = \infty.$$

$$9 < \infty,$$

$$R(C) = R(B).$$

Updated routing table:

D(v): DISTANCE TABLE

Distance	3	9	3	8	2
Destination	B	C	D	E	F

R(v): NEXT-HOP TABLE

N.H	F	F	F	F	F
Destination	B	C	D	E	F

S -> C, D, E

Part Three: Wireshark (Network Packet Analyzer) Application Question

This section covers questions which are based on packet capture and analysis performed using Wireshark.

Wireshark is one of the widely used free open source network packet analyzer (packet sniffer) today. Packet sniffer is a tool for observing and analyzing packets that get exchanged in a network and has two components - one is the packet capture (pcap) library and the other is the packet analyzer. **pcap library** provides the functionalities to passively capture all the link-layer frames that are being send out and received by the computer on a network. Since the network messages/packets being originated by applications, protocols running on the computer ultimately get encapsulated in the link-layer frame, capturing all link-layer frames essentially gives access to all the network messages/packets that are being sent/received by the applications/protocols running on the computer. **Packet analyzer** incorporates the functionalities to store, decipher, analyze and display the contents of the frames being captured. Technically speaking, Wireshark is a packet analyzer that uses a packet capture library in your computer.

Download and install Wireshark in your computer from the link
<https://www.wireshark.org/download.html>.

In windows machines you might need to install WinPcap; if it is not already installed. For Linux and Mac OSX, libpcap will be installed along with Wireshark installation.

Wireshark documentation is available at:

http://www.wireshark.org/docs/wsug_html_chunked/

<https://www.wireshark.org/download/docs/user-guide-a4.pdf>.

Familiarize with Wireshark by going through either one of the links mentioned above.

Essentials details for getting through the questionnaire are listed below:

1. Start up the Wireshark application.
2. List the available network interfaces via the *Capture* pull down menu by selecting *Interfaces*. This will list the set of interfaces available on the computer. Identify the interface which is used to connect to the network/internet and select *start* to commence packet capture on the interface.
3. In the window that was opened as a result of step 2; set the **filter** to display only dns, icmp packets by typing in 'dns||icmp' **filter** toolbar field (without the single quotes).
4. Issue the following command in the shell or command prompt: ping www.bing.com .
5. Stop the capture after receiving 3 ping replies.
6. Answer the following questions by analyzing the packets captured: **Paste the packet capture that was used to answer the question along with the answer.** To print a packet, use File -> Print, choose **selected packet only**, and select the minimum amount of packet details that you need to answer the question. **Annotate the packet capture to explain your answer. Answering this question without capture packets will not be marked and**

receive an automatic 0. (Hint: If you have not captured any DNS message, try a different domain name in your mind and specify it in your answer.)

- Q1. Based on the DNS query message that was captured, identify the IP address of the DNS server and the MAC address which was contacted to lookup the IP address corresponding to domain name www.bing.com.
- Q2. List the two types of ICMP messages that were exchanged and explain what caused those messages to be exchanged.
- Q3. Based on the DNS response message that was captured, identify the IP address related to the domain name.
- Q4. Identify the packet captured in UDP segment, and explain the benefit of using UDP in that types of packets.