1. a) Describe why an application developer might choose to run an application over UDP rather than TCP.

The reasons why an application developer chooses to run an application over UDP rather than TCP are as follows:

- At the time of congestion, the TCP's congestion control suffocates the application's sending rate. Thus, many application developers don't want their applications to use TCP's congestion control.

- When application runs over UDP, many more active clients can be supported by the server which is devoted to a particular application.

- Even though data transfer by TCP is reliable, some applications do not need reliable TCP data transfer. Therefore, application developers prefer UDP.

- Generally, designers of IP (internet protocol) video conference applications and IP telephony run their applications over UDP to avoid TCP congestion control.

b) Is it possible for an application to enjoy reliable data transfer even when the application runs over UDP? If so, how?

Yes. **The application developer can put reliable data transfer into the application layer protocol**.

2. a) Why is it that voice and video traffic is often sent over TCP rather than UDP in today's Internet?

- Data transfer by TCP is reliable compare with UDP.

- The most firewalls are configured to block UDP traffic. Using TCP for voice and video traffic allows the traffic go through the firewalls.

- Connections that use voice/video are quite fast and hence prefer TCP as delays due to lost packets would be fewer.

- UDP (user datagram protocol) provides a best deal since voice applications in the case of most interactive part.

- TCP's advantages over UDP include the fact that it has congestion control, reliable transport, and in-order receipt of segments.

- TCP's congestion control and reliability mechanisms lead to 100% delivery.

b) Assume Host A is streaming a video from Server B using UDP. Also assume that the network suddenly becomes very congested while Host A is seeing the video. Is there any way to handle this situation with UDP? What about with TCP? Is there any other option?

3. a) Suppose a process in Host C has a UDP socket with port number 6789. Suppose both Host A and Host B each send a UDP segment to Host C with destination port number 6789. Will both of these segments be directed to the same socket at Host C? If so, how will the process at Host C know that these two segments originated from two different hosts?

Yes, both the segments that are sent by Host A and Host B will be directed to the same socket at Host C because:

• Host C has a UDP socket with port number 6789.

• Host A as well as Host B will sent UDP segment to Host C with destination port number as 6789.

• Both the hosts A and B use the same destination port number.

The process at Host C can know the origins of the UDP segment. This is because:

• For each received segment, at the socket interface, the IP addresses are provided by the operating system.

• These IP addresses provided by the operating system determine the origins of the individual segments.

• Host C can identify the sockets which contains values non-identical source addresses.

• Host C checks its datagram for its fields , it contains the four fields which gives the data and finds which socket is send those data.

b) Suppose that a Web server runs in Host C on port 80. Suppose this Web server uses persistent connections, and is currently receiving requests from two different Hosts, A and B. Are all of the requests being sent through the same socket at Host C? If they are being passed through different sockets, do both of the sockets have port 80? Discuss and explain.

Yes, even though the requests pass through different sockets, both sockets have the same port number 80. This is because, the web server runs in Host C on port 80. Thus, the Web server receives the requests from the Host A and Host B through port 80 i.e., the destination port number for both sockets is 80.

4. In our rdt protocols,

a) why did we need to introduce sequence numbers?

The reason for the need to introduce sequence numbers in rdt (reliable data transfer) protocols is to make the receiver know whether the arriving packet contains new data or retransmitted data.

• Sometimes the packet may be lost during transmission.

• Sometimes the packet that is received at the receiver may contain errors.

• In order to avoid loss in the channel, such packets are retransmitted again.

- Specifying sequence numbers will make receiver know whether the arriving packet is a retransmitted packet or a new packet.

b) why did we need to introduce timers?

To handle losses in the channel. If the ACK for a transmitted packet is not received within the duration of the timer for the packet, the packet (or its ACK or NACK) is assumed to have been lost. Hence, the packet is retransmitted.

c) Suppose that the roundtrip delay between sender and receiver is constant and known to the sender. Would a timer still be necessary in protocol rdt 3.0, assuming that packets can be lost? Explain,

Yes, even when the round trip delay time between the sender and the receiver is constant and known to the sender, yet a timer would still be necessary in the protocol rdt 3.0.

- The round trip delay time will make the sender know whether the packet or the ACK for the packet is lost or not.

- The timers are used to keep track of time the packet is to be transmitted.

- A timer of constant duration is necessary at the sender to detect the loss for each packet.

5. Suppose Host A sends two TCP segments back to back to Host B over a TCP connection. The first segment has sequence number 90; the second has sequence number 110.

a) How much data is in the first segment?

20

b) Suppose that the first segment is lost but the second segment arrives at B. In the acknowledgment that Host B sends to Host A, what will be the acknowledgment number?

90

6. a) Why sender TCP reduces its transmission speed? Assume application is generating data at a steady rate.

TCP increases sending rate exponentially until a loss or timeout event occurs, after which it enters congestion avoidance by reducing transmission speed or sending rate.

b) In protocol rdt3.0, the ACK packets flowing from the receiver to the sender do not have sequence numbers (although they do have an ACK field that contains the sequence number of the packet they are acknowledging). Why is it that our ACK packets do not require sequence numbers?

To best answer this question, consider why we needed sequence numbers in the first place. We
saw that the sender needs sequence numbers so that the receiver can tell if a data packet is a
duplicate of an already received data packet. In the case of ACKs, the sender does not need

this info (i.e., a sequence number on an ACK) to tell detect a duplicate ACK. A duplicate ACK is
obvious to the rdt3.0 receiver, since when it has received the original ACK it transitioned to the
next state. The duplicate ACK is not the ACK that the sender needs and hence is ignored by the
rdt3.0 sender

7. Answer true or false to the following questions and briefly justify your answer.

a) With the SR protocol, it is possible for the sender to receive an ACK for a packet that falls outside of its current window.

True. Suppose the sender has a window size of 3 and sends packets 1, 2, 3 at t 0 . At t1 (t1 >
t 0) the receiver ACKS 1, 2, 3. At t 2 (t 2 > t1) the sender times out and resends 1, 2, 3. At t 3 the receiver receives the duplicates and re-acknowledges 1, 2, 3. At t 4 the sender receives the ACKs that the receiver sent at t1 and advances its window to 4, 5, 6. At t 5 the sender receives the ACKs 1, 2, 3 the receiver sent at t 2 . These ACKs are outside its window.

b) With GBN, it is possible for the sender to receive an ACK for a packet that falls outside of its current window.

True. By essentially the same scenario as in (a)

8. a) Assume a TCP sender transmits 5 TCP segments with respective sequence numbers 1200, 2000, 2800, 3600, 4400. The sender receives five acknowledgements with the following sequence numbers, 2400, 2800, 2800, 2800, 2800. Complete the Figure #1 to show what TCP segments are exchanged between sender and receiver.

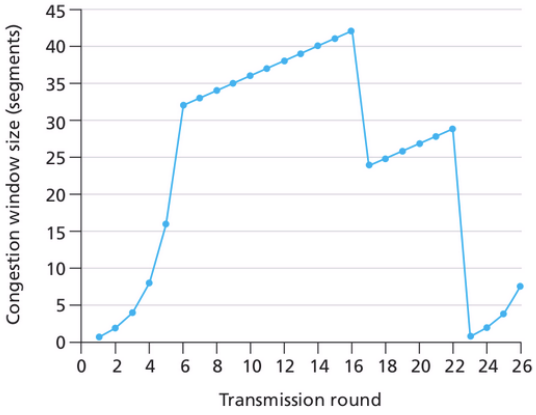
b) Assume a TCP sender transmits 5 TCP segments with respective sequence numbers 200, 1000, 1800, 2600, 3400. The sender receives five acknowledgements with the following sequence numbers, 1000, 1800, 2600, 2600, 2600. Draw the window diagram to show what TCP segments are exchanged between sender and receiver.

9. a) TCP connection has currently estimated RTT of 15 ms with a deviation of 1.9 ms. What is the value of the retransmission timer after the next acknowledgement coming in after 20 ms?

b) TCP connection has currently estimated RTT of 25 ms with a deviation of 2.8 ms. What is the value of the retransmission timer after the next acknowledgement coming in after 30 ms?

DevRTT is calculated with the following equation: (1-beta)*DevRTT + beta * |estimatedRTT - sampleRTT|
estimatedRTT is calculated with the following equation: (1-alpha)*estimatedRTT + alpha*sampleRTT
TCP timeout is calculated with the following equation: estimatedRTT + (4*DevRTT)

10. Assuming TCP Reno is the protocol experiencing the behavior shown in Figure # 2, answer the following questions. In all cases, you should provide a short discussion justifying your answer.



a) If TCP slow start is operating, then the intervals of time **1 to 6 and 23 to 26**.

b) If TCP congestion avoidance is operating, then the intervals of time **6 to 23**.

c) After the 16th transmission round, then the segment loss detected by **a triple duplicate ACK**.

d) After the 22nd transmission round, then the segment loss detected by **timeout**.

e) The initial value of ssthresh at the first transmission round **32**.

f) The value of ssthresh at the 18th transmission round **21**.

g) The value of ssthresh at the 24th transmission round **13**.

h) The transmission round is the 70th segment sent is **7**.

i) If a packet loss is detected after the 26th round by the receipt of a triple duplicate ACK, then the value is **4**.

j) Suppose TCP Tahoe is used (instead of TCP Reno), and assume that triple duplicate ACKs are received at the 16th round. Then the ssthresh and the congestion window size at the 19th round is 1 and transmission round is 21.

k) Again suppose TCP Tahoe is used, and there is a timeout event at 22nd round, then the packets have been sent out from 17th round till 22nd round(inclusive) is **52**.

Consider sending a 3000 byte datagram into a link that has an MTU of 500 bytes. How many fragments are generated? What are their characteristics (i.e. what are the flags and offset values for each

Assume that the DF flag was not set :)
Assume that no optional fields of the IP header are in use (i.e. IP header is 20 bytes)
The original datagram was 3000 bytes, subtracting 20 bytes for header, that leaves 2980 bytes of data.

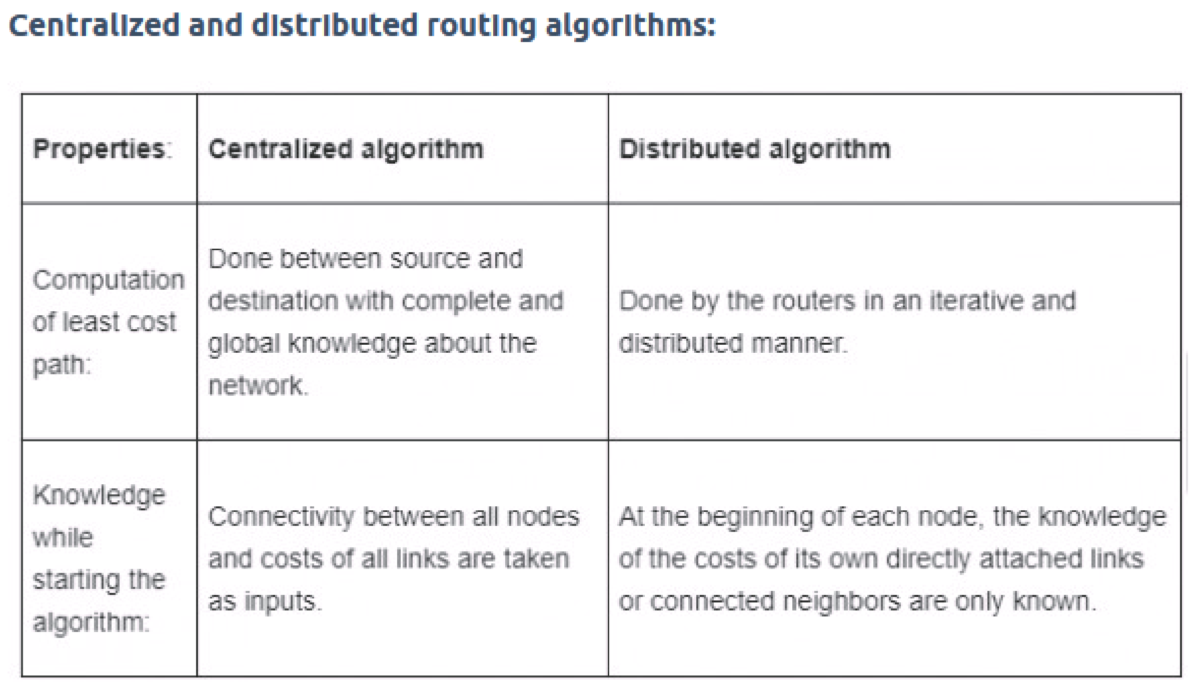
Assume the ID of the original packet is 'x'
With an MTU of 500 bytes, 500 - 20 = 480 bytes of data may be transmitted in each packet
Therefore, ceiling(2980 / 480) = 7 packets are needed to carry the data.
The packets will have the following characteristics (NOTE: offset is measured in 8 byte blocks, you don't need to specify Total_len)

Packet 1: ID=x, Total_len=500, MF=1, Frag_offset=0
Packet 2: ID=x, Total_len=500, MF=1, Frag_offset=60
Packet 3: ID=x, Total_len=500, MF=1, Frag_offset=120
Packet 4: ID=x, Total_len=500, MF=1, Frag_offset=180
Packet 5: ID=x, Total_len=500, MF=1, Frag_offset=240
Packet 6: ID=x, Total_len=500, MF=1, Frag_offset=300
Packet 7: ID=x, Total_len=120, MF=0, Frag_offset=360

1. What is meant by a control plane that is based on logically centralized control? In such cases, are the data plane and the control plane implemented within the same device or in separate devices? Explain.

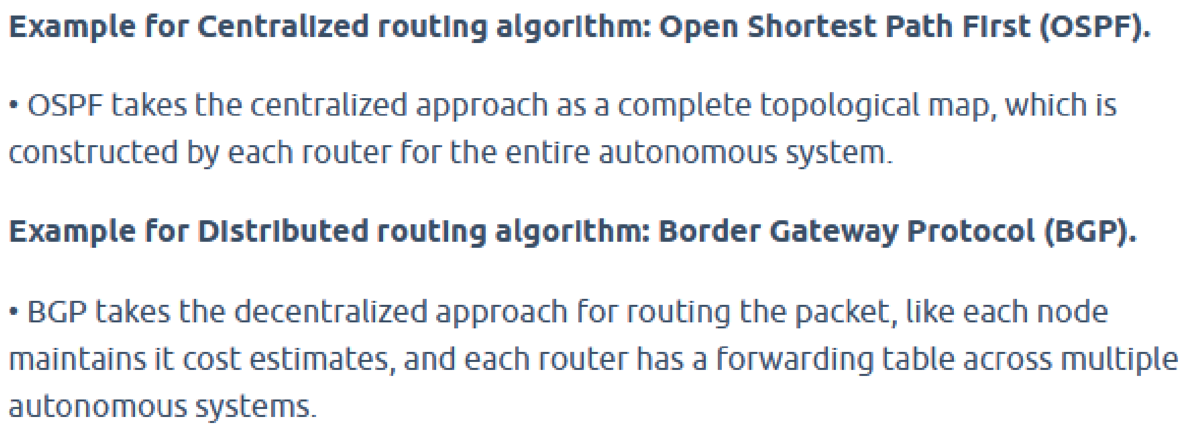
Control plane:
Control plane on a logically centralized control represents that, it knows all the routing tables and forwarding tables in the routers of the network.
The Data plane consists of different network switches which are very simple and fast devices. These devices can execute “match plus action” rules in the flow tables.
The control plane consists of different servers and software which are determined and managed by the switch’s flow tables.
Therefore, the data plane and control plane are implemented in separate devices.

2. Compare and contrast link-state and distance-vector routing algorithms. Give an example of a routing protocol thattakes a centralized and a decentralized approach.



Centralized and distributed routing algorithms:

Properties:	Centralized algorithm	Distributed algorithm
Computation of least cost path:	Done between source and destination with complete and global knowledge about the network.	Done by the routers in an iterative and distributed manner.
Knowledge while starting the algorithm:	Connectivity between all nodes and costs of all links are taken as inputs.	At the beginning of each node, the knowledge of the costs of its own directly attached links or connected neighbors are only known.



Example for Centralized routing algorithm: Open Shortest Path First (OSPF).

• OSPF takes the centralized approach as a complete topological map, which is constructed by each router for the entire autonomous system.

Example for Distributed routing algorithm: Border Gateway Protocol (BGP).

• BGP takes the decentralized approach for routing the packet, like each node maintains it cost estimates, and each router has a forwarding table across multiple autonomous systems.

3. What is the “count to infinity” problem in distance vector routing? Will the count-to-infinity problem occur if wedecrease the cost of a link? Why? How about if we connect two nodes which do not have a link?

Count to infinity problem:

1. One of the important issue in Distance Vector Routing is County of Infinity Problem.
2. Counting to infinity is just another name for a routing loop.
3. In distance vector routing, routing loops usually occur when an interface goes down.
4. It can also occur when two routers send updates to each other at the same time.

4. Why are different inter-AS and intra-AS protocols used in the Internet? Is it necessary that every autonomous systemuse the same intra-AS routing algorithm? Why or why not?

Reasons for the different inter-AS and intra-AS protocol used in the Internet:
1. Policy:
- The policy issues of the inter-AS and the intra-AS leads to the usage of the different inter-AS and intra-AS in the Internet.
- In inter-AS, the traffic originating in each Autonomous System (AS) cannot pass through another specific AS.
- The BGP (Border Gateway Protocol) carries the path attributes and provides for the controlled distribution of routing information leading to the policy-based routing decisions.
- In the Intra-AS routing protocol, the Autonomous System (AS) is under the same administrative control. So, the policy issues play a less important role in choosing routes.

2. Scalability:
- The Scalability is one of the reasons for the usage of the different inter-AS and intra-AS in the Internet.
- The ability to scale and handle the routing among a large number of networks is difficult in the inter-AS routing protocol.
- The ability to scale the routing is less in Intra-AS routing. if there is a large single administrative domain, then it can be divided into smaller AS’s.

3. Performance:
- The inter-AS is the policy-oriented protocol. The policy of the inter-AS dominates the quality and the performance associated with the routes among the AS’s.
- The intra-AS focuses on the performance of the routing on a router because of a single AS.

5. True or false: When an OSPF route sends its link state information, it is sent only to those nodes directly attachedneighbors. Explain.

- OSPF routing constructs complete topology map by each router for the entire autonomous system.
- A router broadcasts the routing information to all the routers in the autonomous system not only to the neighboring routers using OSPF.

Hence, it is false that OSPF sends its link state information to only those directly attached neighbors.

6. What is meant by an area in an OSPF autonomous system? Why was the concept of an area introduced?

Open Shortest Path First (OSPF):
- In an OSPF autonomous system, the system is divided hierarchically into areas.
- Each area consists of the routers, which helps in broadcasting the link state to all other routers present in the area by running its own OSPF link-state routing algorithm.
- An area in an autonomous system is the set of networks and hosts that are grouped together. The area should be a collection of contiguous IP sub netted networks.

Introducing area in an autonomous system:

- In every autonomous system, one OSPF area is configured as the backbone area which is responsible for routing traffic between other areas in the autonomous system.
- OSPF area helps in knowing the link state of the routers.

Hence, concept of area is introduced for routing the traffic to route the packets in an autonomous system.

7. True or false: When a BGP router receives an advertised path from its neighbor, it must add its own identity to thereceived path and then send that new path on to all of its neighbors. Explain.

Border Gateway Protocol (BGP):

- An inter-autonomous system routing protocol, which is used while routing a packet across multiple autonomous system is said to be known as Border gateway protocol.
- It is a routing protocol used to transfer data and information between different host gateways, the internet or autonomous system.
- The management of how packets are routed across the internet through the exchange of routing and reachability information between edge routers are done by the Border Gateway Protocol.
- It directs the packets of information between autonomous systems managed by a service provider.
- The two main responsibilities of the BGP protocol are as follows:
- Obtain the prefix reachability information from the neighbour autonomous systems.
- To find the best route by sending the prefix information.

In Border Gateway Protocol:

- Between BGP protocols, the protocol establishes before sending the new path to neighbors, it must advertise the path from its neighbors underlying connection.
- By adding the identity to the received path, while sending the new path to its neighbors, it will help the neighbors not only to know the existence of the routers but to know the path of the autonomous system that leads to the destination.

Therefore, the statement “When a BGP router receives an advertised path from its neighbor, it must add its own identity to the received path and then send that new path on to all of its neighbors” is true.

8. How does BGP use the NEXT-HOP attribute? How does it use the AS-PATH attribute?

BGP protocol: BGP (Border Gateway Protocol) is an Inter-AS routing protocol.

- It obtains the subnet reachability information from neighboring AS.
- It also propagates the reachability information to all routers within an AS.
- The peers determine the routes to each other AS system.

The BGP uses the attributes for routing the paths between the Autonomous Systems (AS’s). The two most important attributes are AS-PATH and NEXT-HOP.

1. AS-PATH:

- The advertisement passed for the prefix values contains the AS’s in the AS-PATH.
- When the value of prefix is passed into an AS, it adds the ASN (Autonomous System Number) to the AS-PATH attribute.

The following are the ways for determining the use of AS-PATH in BGP:

- The routers use the AS-PATH attribute for detecting and preventing the looping advertisements. When the router finds the AS is already present in the list, the advertisement is rejected by the router.
- The routers also uses the AS-PATH attribute in order to choose among the multiple paths with the same prefix.

2. NEXT-HOP:

- The NEXT-HOP is the router interface that initiates the AS-PATH.
- The attribute is necessary in providing the critical link between the Inter-AS routing and Intra-AS routing protocols.

The following are the ways for determining the use of NEXT-HOP in BGP:

- The NEXT-HOP attribute indicates the IP address of the first router along the advertised path that is the advertisement received by the external AS to a given prefix.
- When the forwarding table for the first router is configured, the router uses the NEXT-HOP attribute.

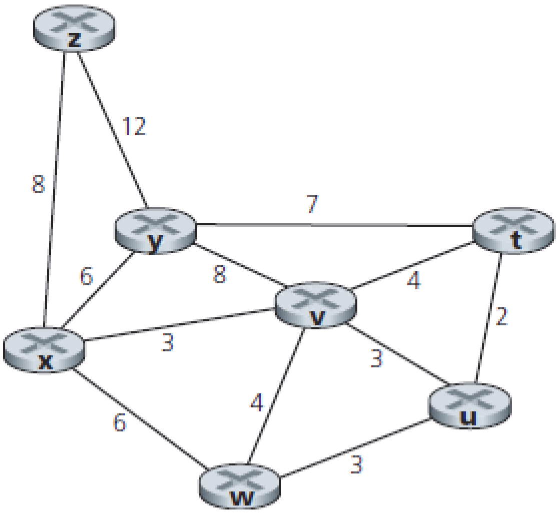
9. Suppose you wanted to implement a new routing protocol in the SDN control plane. At which layer would youimplement that protocol? Explain.

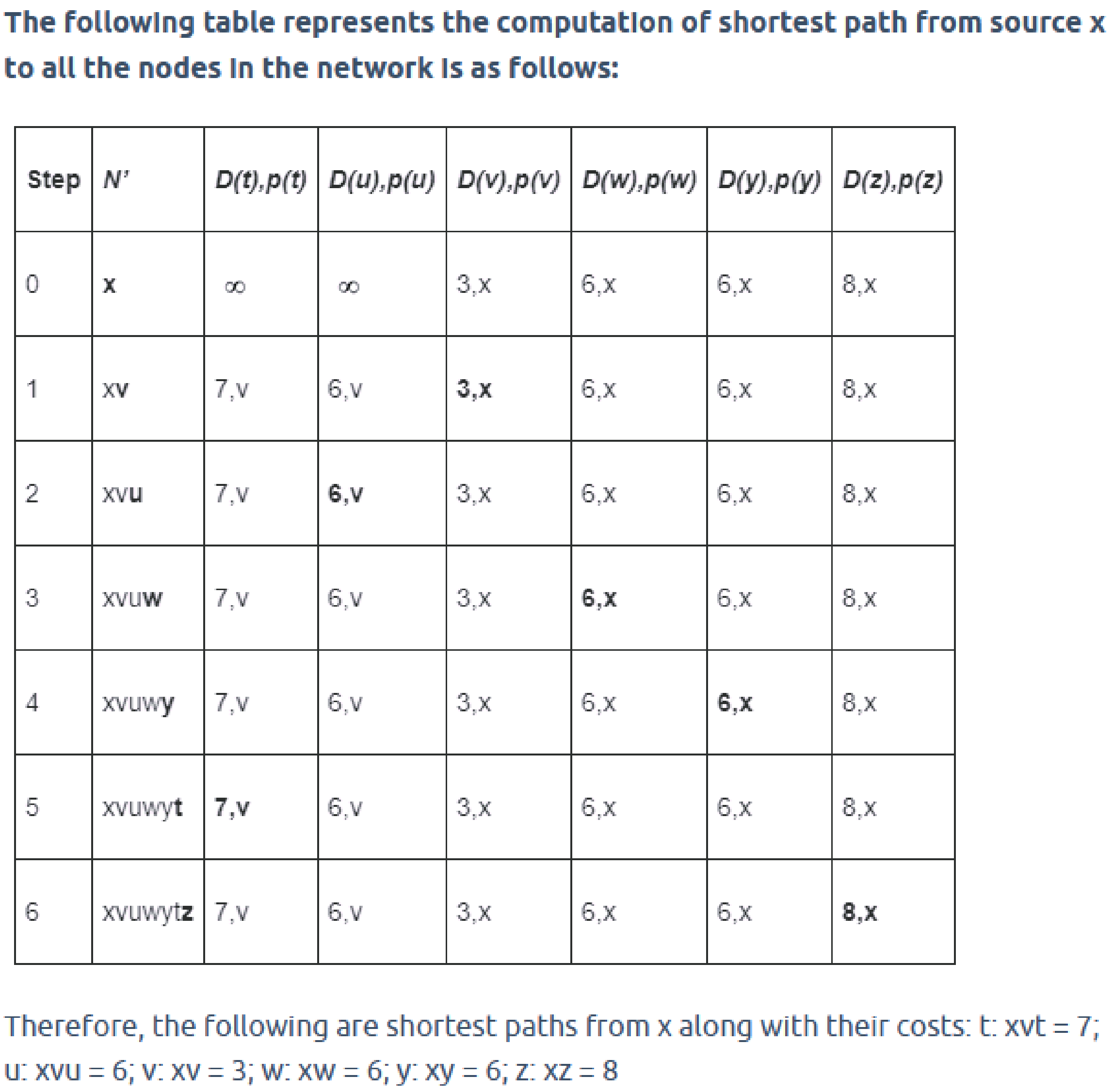
Routing is the procedure of stirring packets transversely to a network from one host to another host. The answer would be routing would happen in the management layer. This is because the management layer is the one that interrelates with SNMP, Telnet, SSH, and TFTP.

10. Consider the following network. With the indicated link costs, use Dijkstra’s shortest-path algorithm to compute theshortest path from x to all network nodes.

step	*N′*	*D(v),p(v)*	*D(w),p(w)*	*D(x),p(x)*	*D(y),p(y)*	*D(z),p(z)*
0	u	2,u	5,u	1,u	∞	∞
1	ux	2,u	4,x		2,x	∞
2	uxy	2,u	3,y			4,y
3	uxyv		3,y			4,y
4	uxyvw					4,y
5	uxyvwz					

Table 4.3 ♦ Running the link-state algorithm on the network in Figure 4.27





The following table represents the computation of shortest path from source x to all the nodes in the network is as follows:

Step	*N'*	*D(t),p(t)*	*D(u),p(u)*	*D(v),p(v)*	*D(w),p(w)*	*D(y),p(y)*	*D(z),p(z)*
0	**x**	∞	∞	3,x	6,x	6,x	8,x
1	x**v**	7,v	6,v	**3,x**	6,x	6,x	8,x
2	xv**u**	7,v	**6,v**	3,x	6,x	6,x	8,x
3	xvu**w**	7,v	6,v	3,x	**6,x**	6,x	8,x
4	xvuw**y**	7,v	6,v	3,x	6,x	**6,x**	8,x
5	xvuwy**t**	**7,v**	6,v	3,x	6,x	6,x	8,x
6	xvuwyt**z**	7,v	6,v	3,x	6,x	6,x	**8,x**

Therefore, the following are shortest paths from x along with their costs: t: xvt = 7; u: xvu = 6; v: xv = 3; w: xw = 6; y: xy = 6; z: xz = 8

11. Consider the network shown below. Suppose AS3 and AS2 are running OSPF for their intra-AS routing protocol.

Suppose AS1 and AS4 are running RIP for their intra-AS routing protocol. Suppose eBGP and iBGP are used for the inter-AS routing protocol. Initially suppose there is no physical link between AS2 and AS4.

a. Router 3c learns about prefix x from which routing protocol: OSPF, RIP, eBGP, or iBGP?

b. Router 3a learns about x from which routing protocol?

c. Router 1c learns about x from which routing protocol?

d. Router 1d learns about x from which routing protocol?

EBGP: external BGP runs between routers in different ASs
IBGP: internal BGP runs between routers in the same AS
a. eBGP: Router 3c learns about x from eBGP
b. iBGP: Router 3a learns about x from iBGP

c. eBGP: Router 1c learns about x from eBGP
d. iBGP: Router 1d learns about x from iBGP

12. What are some of the possible services that a link-layer protocol can offer to the network layer? Which of these link-layer services have corresponding services in IP? In TCP? The below are some of the possible services that a link-layer protocol that offer to the network:

- Link access
- Reliable delivery
- Framing
- Error detection and correction

The above 4 link-layer services(Link access, Reliable delivery, Framing, and Error dection and correction) have corresponding services in TCP(Transfer control protocol).
The below 3 link layer services that have corresponding to the services of IP are as follows:

- Link access
- Framing
- Error detection and correction

13. How big is the MAC address space? The IPv4 address space? The IPv6 address space?

2^48 MAC addresses; 2^32 IPv4 addresses; 2^128 IPv6 addresses.

14. Suppose nodes A, B, and C each attach to the same broadcast LAN (through their adapters). If A sends thousands of IP datagrams to B with each encapsulating frame addressed to the MAC address of B, will C's adapter process these frames? If so, will C's adapter pass the IP datagrams in these frames to the network layer C? How would your answers change if A sends frames with the MAC broadcast address?

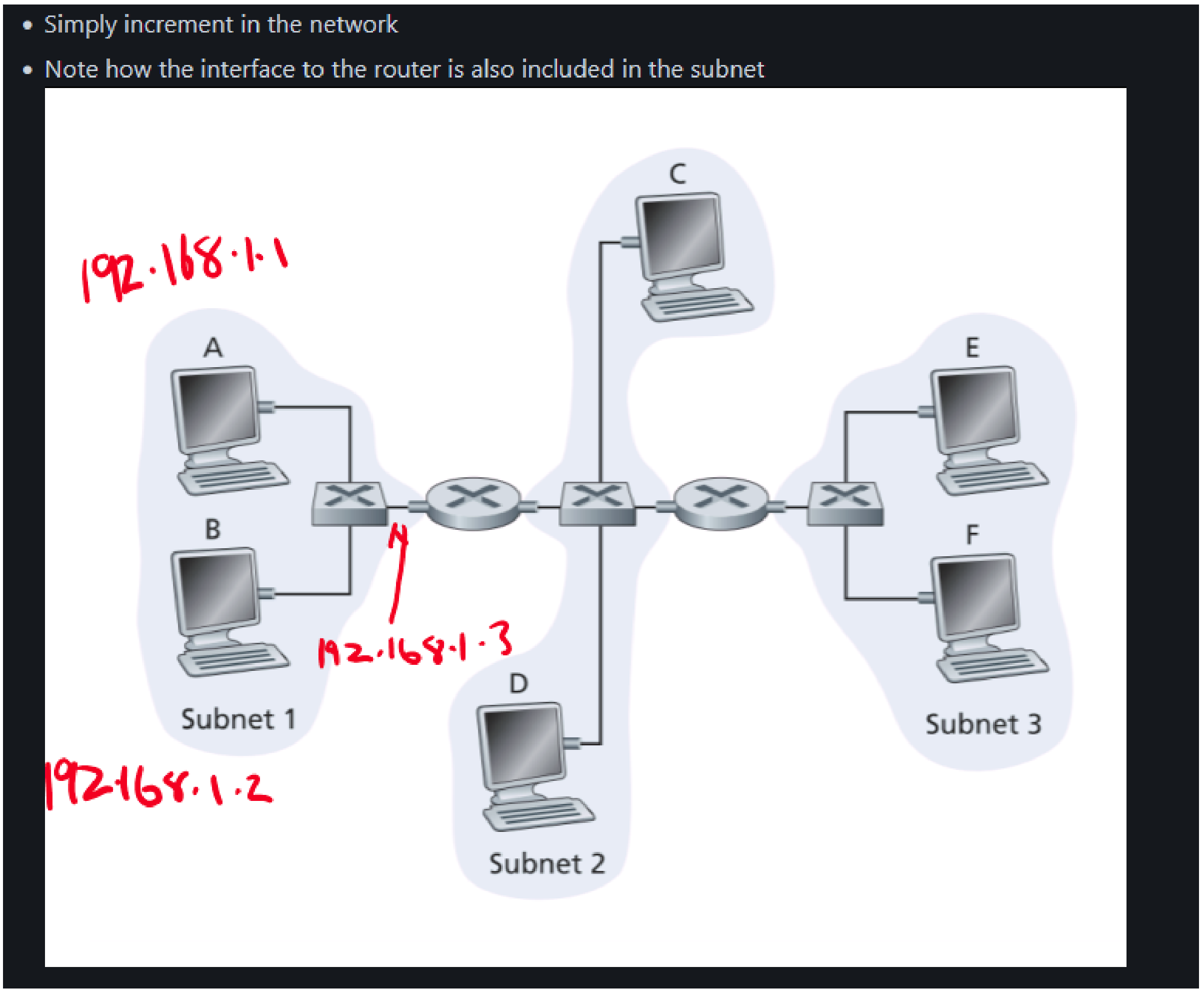
C's adapter will process the frames, but the adapter will not pass the datagrams up the protocol stack. If the LAN broadcast address is used, then C's adapter will both process the frames and pass the datagrams up the protocol stack..

15. Why is an ARP query sent within a broadcast frame? Why is an ARP response sent within a frame with a specificdestination MAC address?

The following is the reason for ARP request to be sent as broadcast message:
• For a datagram to be sent to the destination node, the source node should know the IP (Internet protocol) address and MAC (Media Access Control) address of the destination node.
• Source node with IP address of destination node will send ARP query as broadcast message across the LAN to know the MAC address of the destination node.
• All nodes will receive this ARP query message. ARP module present at each node will check whether the IP address in ARP query matches with its IP address.
• If the IP address matches then the node will send the ARP response with MAC address of the node.
• Then the source node will know the MAC address of the destination node.

Hence, ARP query is sent as broadcast message by the source node to get the unknown MAC address of destination node.
The ARP response is sent within a frame with specified destination MAC address because the node that sends the ARP response knows the MAC address of source node (which has sent the ARP query).

(a) Assign IP addresses to all of the interfaces. For Subnet 1 use addresses of the form 192.168.1.xxx; for Subnet 2 uses addresses of the form 192.168.2.xxx; and for Subnet 3 use addresses of the form 192.168.3.xxx.



- Simply increment in the network
- Note how the interface to the router is also included in the subnet

(b) Assign MAC addresses to all of the adapters.

- 16 bit hexadecimal
- Just pretend these MAC addresses were made in the factory lol
- You can actually change your MAC address
- Won't check if your MAC address is valid

(c) Consider sending an IP datagram from Host E to Host B. Suppose all of the ARP tables are up to date. Explain the process of sending the datagram, including details of source and destination IP and MAC addresses of the datagrams sent.

- The prefix of the IP is different
- If the prefix is not the same then it'll go through a different router
- E sends it's source IP and source MAC address

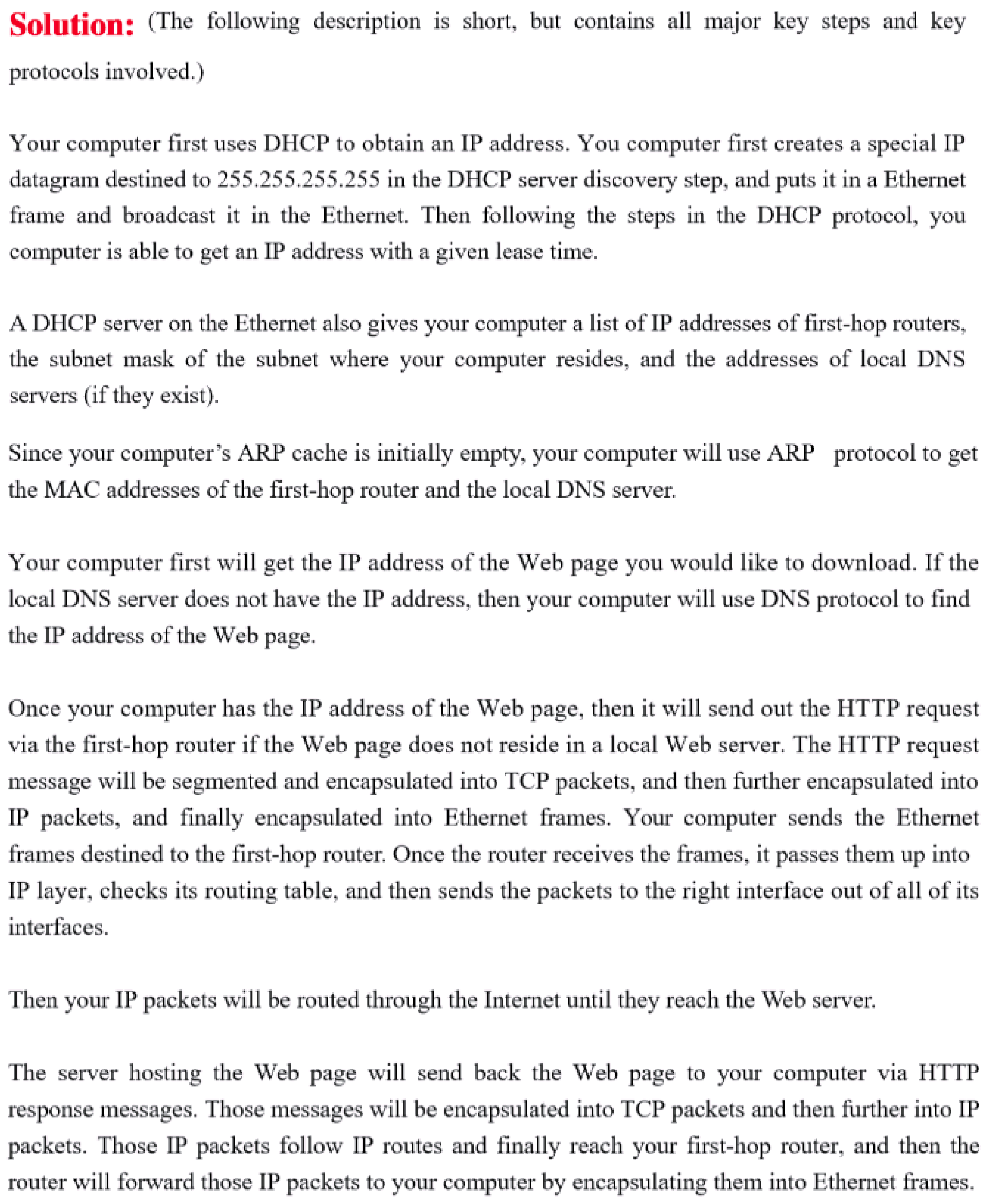
- Send a packet to destination 192.168.1.3 router 2
- Ask router to do the rest
- Router 2 then extracts the data gram and determines it has to send it to Router 1
    - Source MAC of the router 2's sending interface is used and desintation MAC of router's 1 interface used
    - IPs of E and B are still used and sent to router 1
    - Router 1 sends it to B

(d) Repeat (c), now assuming that the ARP table in the sending host is empty (and the other tables are up to date).

- E knows R2 IP
- Broadcast ARP from E, then the R2 receives this and transmits back it's MAC address
- E now knows the IP and MAC address of R2
- Repeated across the whole network

17. In this problem, you will put together much of what you have learned about Internet protocols. Suppose you walk into a room, connect to Ethernet, and want to download a Web page. What are all the protocol steps that take place, starting from powering on your PC to getting the Web page? Assume there is nothing in our DNS or browser caches when you power on your PC.

(Hint: The steps include the use of Ethernet, DHCP, ARP, DNS, TCP, and HTTP protocols.) Explicitly indicate in your steps how you obtain the IP and MAC addresses of a gateway router.



Solution: (The following description is short, but contains all major key steps and key protocols involved.)

Your computer first uses DHCP to obtain an IP address. You computer first creates a special IP datagram destined to 255.255.255.255 in the DHCP server discovery step, and puts it in a Ethernet frame and broadcast it in the Ethernet. Then following the steps in the DHCP protocol, you computer is able to get an IP address with a given lease time.

A DHCP server on the Ethernet also gives your computer a list of IP addresses of first-hop routers, the subnet mask of the subnet where your computer resides, and the addresses of local DNS servers (if they exist).

Since your computer's ARP cache is initially empty, your computer will use ARP protocol to get the MAC addresses of the first-hop router and the local DNS server.

Your computer first will get the IP address of the Web page you would like to download. If the local DNS server does not have the IP address, then your computer will use DNS protocol to find the IP address of the Web page.

Once your computer has the IP address of the Web page, then it will send out the HTTP request via the first-hop router if the Web page does not reside in a local Web server. The HTTP request message will be segmented and encapsulated into TCP packets, and then further encapsulated into IP packets, and finally encapsulated into Ethernet frames. Your computer sends the Ethernet frames destined to the first-hop router. Once the router receives the frames, it passes them up into IP layer, checks its routing table, and then sends the packets to the right interface out of all of its interfaces.

Then your IP packets will be routed through the Internet until they reach the Web server.

The server hosting the Web page will send back the Web page to your computer via HTTP response messages. Those messages will be encapsulated into TCP packets and then further into IP packets. Those IP packets follow IP routes and finally reach your first-hop router, and then the router will forward those IP packets to your computer by encapsulating them into Ethernet frames.