Take-Home Quiz II

Due Monday Nov 27 11:55pm

Csci4211: Introduction to Computer Networks
Fall 2017
Prof. Zhi-Li Zhang

Last Name: **First Name:**

Student Id.

Instructions:

1. This is a **open-book** and **open-note** quiz.
2. There are **five** questions in total, each of which has several sub-questions with a total of 125 points. You have about **a week** to work on the quiz.
3. Please make sure to write down your name and student id. on your answer sheets.
4. Partial credit is possible for an answer; please include intermediate steps as appropriate. Please try to be as concise and make your exam as neat as possible. We *must* be able to read your handwriting in order to be able to grade your exam.
5. **Please work on the quiz *individually, by yourself only!* No discussion among the students in the class, or with others, is allowed. If you find your answers from the Internet, please cite your sources. Any violation of the University's *Student Conduct Code* will be reported to both the department and the University, and you may be suspended or expelled! Please note that if you let another student to copy your answers, you are also in violation of the University's *Student Conduct Code.***
6. Good luck. Enjoy! And *Happy Thanksgivings!*

---

1. Short Questions and Answers: (15 points total. Approx. 20 minutes)
(*Two or three sentences would generally suffice.*)

a. (3 points) Given an IP address 128.101.34.35 and a network mask 255.255.192.0, what is its *network prefix*?

Answer

The network prefix is 128.101.0.0/18.
Note that to figure this out, you need to find the subnet and the netmask length.
To calculate the netmask length, expand the "dot notation" of the network mask into its binary representation. Then, count the number of contiguous 1 bits, starting at the most significant bit (i.e., the left-hand-side of the binary number).
255 = 11111111 (=$2^7 + 2^6 + ... + 2^1 + 2^0$) in binary, and 192 = 128 +64 (=$2^7 + 2^6$), which is 11000000 in binary.
Thus, 255.255.192.0 = 11111111 11111111 11000000 00000000.
The netmask length = 18
To find the subnet, you need to expand the "dot notation" of the IP address into its binary representation. Then, use the bitwise "and" operation of the the binary representation of the IP address and the network mask.
128 = 10000000 (=2^7) in binary, 35 = 32+2+1 = (=$2^5+2^1+2^0$) which is 00100011 in binary.
128.101.34.35: 10000000 01100101 00100010 00100011
255.255.192.0: 11111111 11111111 11000000 00000000
& ____
Subnet: 10000000 01100101 00000000 00000000 : 128.101.0.0

b. (3 points) In DHCP, how does a client machine requesting an IP address know whether a DHCP offer message from a DHCP server is meant for it or not, since it does not have an IP address yet?

Answer

Before a client broadcasts a DHCP discover message, it generates a (random) transaction id, which is included in the message. The transaction id is used to identify whether a message is meant for the client or not. DHCP messages are broadcast (note that dst IP are always 255.255.255.255, which yields the broadcast MAC address FF:FF:FF:FF:FF:FF as the dst MAC.

c. (2 points) Suppose that the MAC addresses of two stations are `6A:78:BF:01:99:33` and `6A:78:BF:01:88:55` (in hexadecimal representation, where ":" delimits the 6 bytes in the 48-bit MAC address). Do we know whether they reside on the same LAN? Briefly explain your answer.

Answer

No. Unlike IP addresses, MAC addresses are "flat" and ("*physically*") tied to each network interface of a machine. In other words, when a machine moves from one IP network to another IP network, the MAC addresses of its interfaces do not change.

d. (3 points) What is MTU?

Answer

MTU is the maximum size (i.e., total number of bytes) that can be carried in a single layer 2 frame that can be transmitted along a link. In other words, it is the maximum size of an IP datagram that can be transmitted along a link without the need for IP datagram fragmentation. (Note that MTU stands for *maximum transmission unit.*)

e. (4 points) Given two IP datagrams D_1 and D_2, where the "length" field, "offset" field and "more fragment" flag in their respective IP headers are given as follows: in datagram D_1, `length`= 1500, `offset` =0, `more fragments flag`=1; and in datagram D_2, `length`= 120, `offset` =185, `more fragments flag`=0. How can you tell whether these datagrams are *fragments* of the *same* original IP datagram? *Suppose* that they are fragments of the same original IP datagram, what is the payload size of the original IP datagram?

Answer

There is a unique (datagram) identifier for each datagram and it will be the same of each of the datagrams fragments and using the identifier we can check whether the fragments are from the same original datagram or not. If the two packets are of the same original IP datagram then the length will be Length = 1480 + 100 = 1580. (Note that the length field in the IP header includes 20 bytes of the IP header; and the offset field is measured in multiples of 8: 185x8 =1480 bytes).

2. TCP Flow and Congestion Control (24 points total. Approx. 20 minutes)

a. (6 points) Briefly describe how TCP flow control works.

Answer

TCP flow control is a mechanism for keeping the sender to send data at a rate that the receiver can process because the rates on both ends can vary. It uses a sliding window to keep the sending rate in check and the window size is determined by the receiver which advertises the size along with the acknowledgments.

b. (6 points) Suppose that the congestion window, `CongWin`, of a TCP connection is currently at 9 KB, and `threshold` = 20 KB. The sender sends **6** TCP data segments, each of size 1500 bytes. (Here we assume that 1KB = 1000 bytes; and the TCP maximum segment size is 1500 bytes.) The last data segment of the 6 data segments sent carries a sequence number 2003000 (in decimal representation, not binary representation). The sender then receives three acknowledgments from the receiver, each acknowledging the receipt of two consecutive data segments. In particular, the last acknowledgment from the receiver carries the acknowledgment number 2004500. What will the sender set `CongWin` to at the end?

Answer

Here the sender is in slow start mode as CongWin < Threshold. Thus, each round the CongWin is doubled.
Maximum Segment Size (MSS) = 1.5 KB
CongWin = 9 KB, Threshold = 20 KB
Since the sender's sends 6 TCP segments
1 segment = 1.5 KB
6 segments = 9 KB
So CongWin = Initial + 6*MSS = 18 KB

c. (6 points) Suppose that during the next round of data transmission after **b.**, a *time-out* event occurs at the sender side. What will be the value (in bytes) of `CongWin` after this event? What will be the value (in bytes) of `threshold`?

Answer

Since the timeout occurs Threshold= $\frac{CongWin}{2}$
Threshold = 9 KB
CongWin = 1 MSS = 1.5 KB
It goes back to the slow start mode.

d. (6 points) Now consider a *new* scenario where the congestion window, `CongWin`, at the sender side is currently set to 15 KB, and `threshold` = 15 KB. The sender then sends 10 data segments of 1500 bytes each (thus a total of 15 KB data is sent), where the *last* data segment carries a sequence number 2011500 (in decimal representation, not binary representation). After having sent these 10 data segments, the sender receives **5** acknowledgments from the receiver, each acknowledging the receipt of two consecutive data segments. In particular, the *last* acknowledgment from the receiver carries the acknowledgment number 2013000. What will the sender set `CongWin` to at the end? What will be the value (in bytes) of `threshold`?

Answer

Here the sender is in congestion avoidance mode as CongWin $\geq$ Threshold.
Upon ACK receipt for previously unacked data, the CongWin is modified as following:
CongWin = CongWin+(num of segments ACKed) * MSS * (MSS/CongWin)
Which results in increasing the CongWin by 1 MSS every RTT.
Maximum Segment Size (MSS) = 1.5 KB
Hence, CongWin = 15 KB + 10 * $\frac{1.5KB}{15KB}$ * 1.5 KB = 16.5 KB
Threshold = 15 KB

3. Virtual Circuit and IP Datagram Forwarding (25 points total. Approx. 25 minutes)

In the following the first two questions are related to virtual circuits, and the last question is related to IP datagram forwarding.

a. (5 points) Consider the network shown in Figure 1, where the numbers beside the links connecting hosts and routers represents the port numbers of the routers. The table beside the routers represent the VCI translation table at the routers. When a packet carrying VCI no. 2 arrives at port 3 of router 3, what will be the VCI no. it carries after it passes through router 3? Trace and write down the VCI no.'s the packet carries as it goes through each router until it reaches its destination. Which host is its destination?

Answer

Let $[i, j]$ *router* k $[m, n]$ denote that a virtual circuit connection (or a "flow") will enter router k at port i with (input) VCI j and leave the router at port m with (output) VCI n. The VC connection in question would traverse as follows (*green* VC in Fig. 1):
host C $\rightarrow [3, 2]$ *router* 3 $[2, 2] \rightarrow [3, 2]$ *router* 4 $[2, 2] \rightarrow$ *host D*. [The destination is host D.]

In Fig. 1, we also show the other two VC connections, the *red* VC connection:
host A $\rightarrow [0, 3]$ *router* 1 $[3, 2] \rightarrow [0, 2]$ *router* 3 $[2, 1] \rightarrow [3, 1]$ *router* 4 $[2, 3] \rightarrow$ *host D*.
And the *blue* VC connection:
host A $\rightarrow [0, 4]$ *router* 1 $[1, 2] \rightarrow [0, 2]$ *router* 2 $[1, 1] \rightarrow$ *host B*.

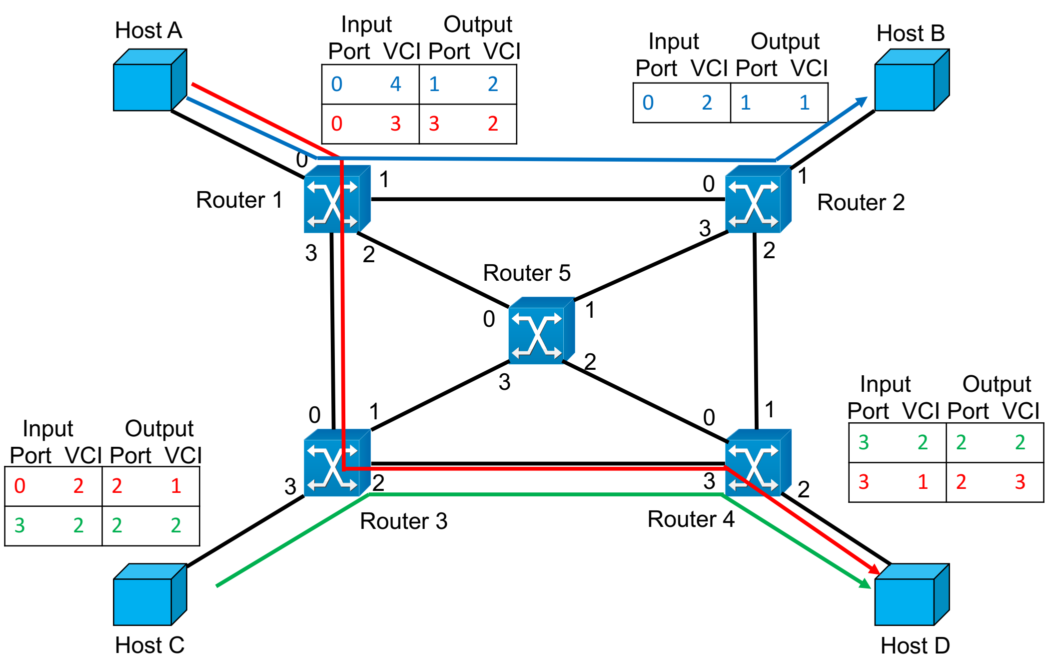


Figure 1: Figure for Solution for Question 3.

b. (10 points) Using the network shown in Figure 1, please write down the virtual circuit translation tables for *all the routers* after the following three **new** connections are established in the order given below.

(1) Host A connects to host D via router 1, router 2 and router 4.

(2) Host B connects to host C via router 2, router 5 and router 3.

(3) Host D connects to host C via router 4, router 5 and router 3.

Answer

Note that, depending on how your assign the VCIs, there could be many correct solutions (remember that you need to ensure that you pick VCIs that will not cause conflict, namely, *if there is another VC connection that leaves at the same outport m and is assigned VCI n, you cannot pick n as the VCI of the* new *VC connection.*).

In Fig. 2, we present and illustrate one solution:

The VC connection for (1) is illustrated as the *purple* VC connection:
$host\ A \rightarrow [0,2]\ router\ 1\ [1,1] \rightarrow [0,1]\ router\ 2\ [2,3] \rightarrow [1,3]\ router\ 4\ [2,4] \rightarrow hostD.$

The VC connection for (2) is illustrated as the *orange* VC connection:
$host\ B \rightarrow [1,2]\ router\ 2\ [3,3] \rightarrow [1,3]\ router\ 5\ [3,3] \rightarrow [1,3]\ router\ 3\ [3,3] \rightarrow hostC.$

The VC connection for (3) is illustrated as the *cyan* VC connection:
$host\ D \rightarrow [2,4]\ router\ 4\ [0,4] \rightarrow [2,4]\ router\ 5\ [3,4] \rightarrow [1,4]\ router\ 3\ [3,4] \rightarrow hostC.$

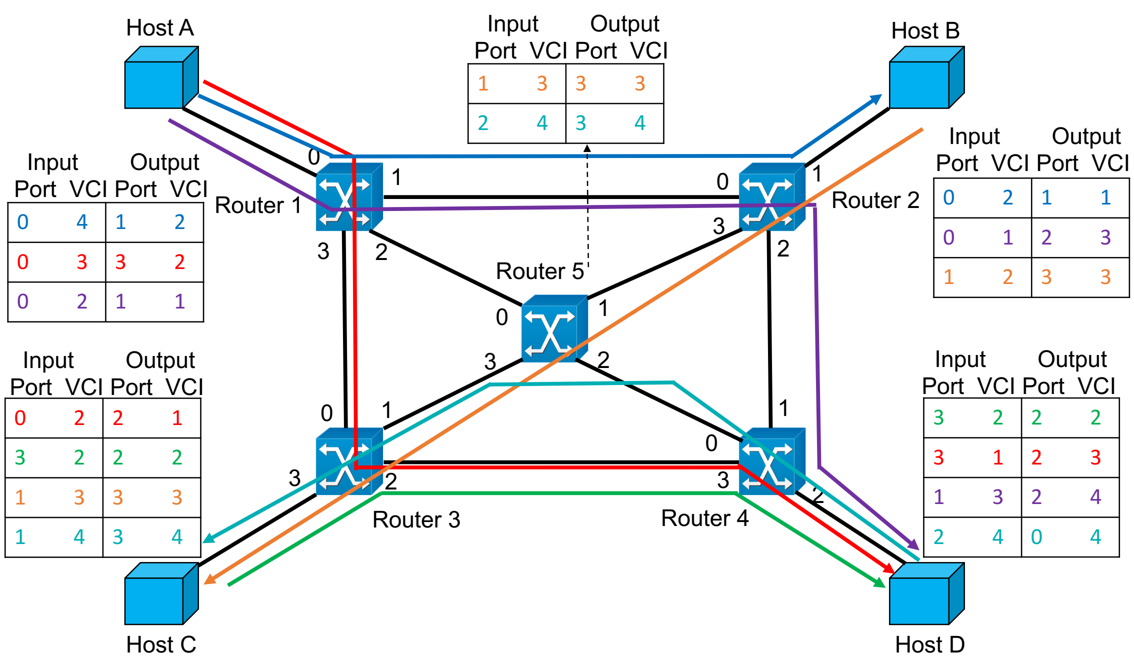


Figure 2: Figure for Solution for Question 3.

c. (10 points) Suppose a router has built up the following routing table as shown in Table 1.

Table 1: Routing Table.

id	Network Prefix	Network Mask	Next-Hop (Interface)
1	162.11.128.0	255.255.128.0	ppp
2	162.11.128.0	255.255.192.0	eth0
3	94.25.80.0	255.255.255.0	eth1
4	94.25.0.0	255.255.0.0	wifi
5	0.0.0.0	0.0.0.0	ppp

Where will the router send packets addressed to each of the following destinations? Please, specify the rule used for matching and the next-hop.

i. 162.11.97.1

ii. 162.11.231.98

iii. 94.25.80.10

iv. 94.25.80.100

v. 162.11.135.47

Answer

By expnading the IP addresses as in Q1-a, and using the longest prefix match.

i. 162.11.97.1 is matched to rule 5 (the default rule) and the next-hop is ppp.

ii. 162.11.231.98 is matched to rule 1 and the next-hop is ppp.

iii. 94.25.80.10 is matched to rule 3 and the next-hop is eth1.

iv. 94.25.80.100 is matched to rule 3 and the next-hop is eth1.

v. 162.11.135.47 is matched to rule 2 and the next-hop is eth0.

4. MAC Addresses, ARP, Switches and Routers (36 points total. Approx. 35 minutes)

Consider a campus network as shown in Figure 3, where there are two IP routers $R1$ (the border gateway router) and $R2$ and four Ethernet switches, $S1$, $S2$, $S3$ and $S4$. The numbers (1, 2, 3 or 4) beside the routers/switches indicate their interface numbers. As you can see from the figure, the campus network is segmented into three IP *subnets*: IP subnet 1 with the IP address block 128.101.0.0/18, IP subnet 2 with the IP address block 128.101.164.0/22, and IP subnet 3 with the IP address block 128.101.100.0/20. (For your convenience, we have shaded the links and switch(es) belonging to each IP subnet in Figure 3: IP subnet 1 with light blue color, IP subnet 2 with light orange, and IP subnet 3 with light green, when viewed in color print or on screen.) Note that host H is *multi-homed*, with its interface 1 connected to IP subnet 1, and its interface 2 connected to IP subnet 3. As a result, host H is assigned two IP addresses: 128.101.0.15 and 128.101.100.21.

The forwarding tables at routers $R1$ and $R2$ as well as their ARP caches at *the current moment* are given in Figure 4; a snapshot of the forwarding (or switch) table of the switch $S3$ at the *current moment* is also shown in the figure. Answer the following questions *briefly*. (A few sentences would be sufficient!)

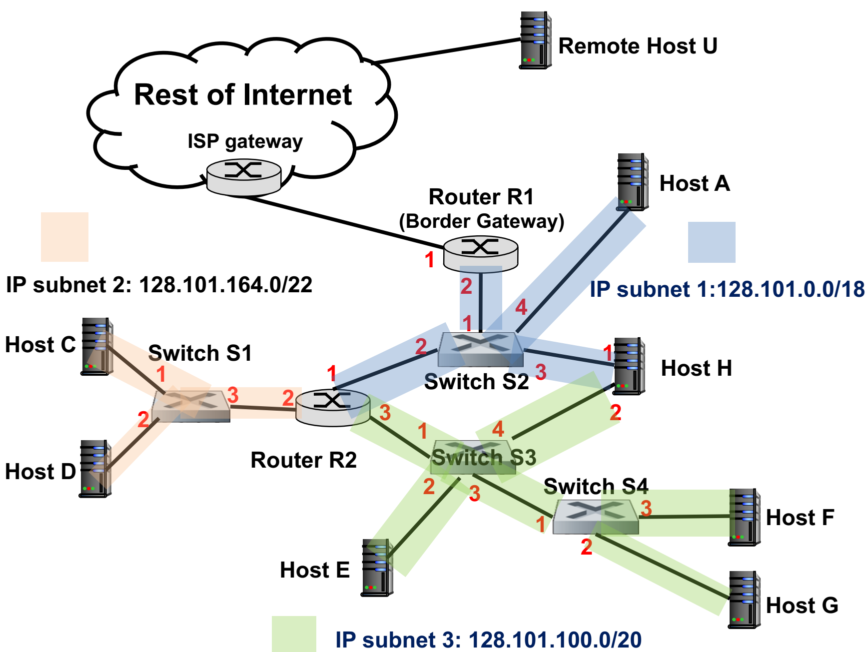


Figure 3: Figure for Question 4.: a Campus Network with three IP subnets

Router R1's Forwarding Table

Destination network	Next-hop	Interface
128.101.0.0/18	Direct	2
128.101.100.0/20	R2	2
128.101.164.0/22	R2	2
0.0.0.0/0	ISP's gateway	1

Router R1's ARP Cache

IP address	MAC address
R2's IP address	R2's MAC address
A's IP address	A's MAC address

Router R2's ARP Cache

IP address	MAC address
R1's IP address	R1's MAC address
C's IP address	C's MAC address
128.101.0.15	H's MAC address1
128.101.100.21	H's MAC address2

Router R2's Forwarding Table

Destination network	Next-hop	Interface
128.101.0.0/18	R1	1
128.101.100.0/20	Direct	3
128.101.164.0/22	Direct	2
0.0.0.0/0	R1	1

Switch S3's Forwarding Table

MAC address	Interface
R2's MAC address	1
F's MAC address	3
H's MAC address	4

Host C's ARP Cache

IP address	MAC address
R2's IP address	R2's MAC address
D's IP address	D's MAC address

Figure 4: Figure for Question 4.: Routing Tables at $R1$ and $R2$, Snapshots of $S3$'s Switch Forwarding Table and ARP Caches at $R1$, $R2$ and Host C

a. (12 points) Consider a scenario where host G wants to send an IP datagram packet to host F. Suppose host G's ARP cache is empty, so it *broadcasts* an *ARP request* message with F's IP address as the target address, and encapsulates the ARP message into an Ethernet frame with its own MAC address and the MAC broadcast address `FF:FF:FF:FF:FF:FF` as the source and destination MAC addresses, respectively.

i) (3 points) Will Switch $S3$ receive this broadcast frame from host G? If yes, what will it do when it receives this broadcast frame, and what will its forwarding table look like afterward?

Answer

Since the destination MAC address is a broadcast MAC address, $S4$ will first receive the ARP request, and will broadcast it on all its ports except port 2 (because the request came from port 2). Using the source MAC address, S4 will also add the entry of G's MAC address to its forwarding table. Thus, $S3$ will receive this ARP request, and it will broadcast it on all of its ports except port 3 (because the request came from port 3); Using the source MAC address, $S3$ will add the entry of G's MAC address to its forwarding table.

S3's Forwarding Table:

MAC Address	Interface
R2's MAC address	1
F's MAC address	3
H's MAC address	4
G's MAC address	3

ii) (3 points) Will router $R2$ also receive this ARP request message? If yes, will it forward to IP subnet 1 (via its interface 1) and IP subnet 2 (via its interface 2)? Why or Why not?

Answer

Router $R2$ will also receive the ARP request, since the destination MAC address is a broadcast address. But it will not forward it, because ARP requests are not forwarded across IP subnets and is a layer 2 functionality.
(Incidentally, all layer-2 broadcast frames will not be forwarded across IP subnets; a layer-2 broadcast frame is meant to all hosts residing on the same IP subnet.)

iii) (3 points) When host F receives this *ARP request* message, it will reply back with an *ARP response* message to host G, encapsulating this ARP response message in a *unicast* Ethernet frame with its own MAC address and host G's MAC address as the source and destination MAC addresses, respectively. Does host F need to perform an ARP query in order to find out host G's MAC address? Why or why not?

Answer

Host F does not need to perform an ARP query for G's MAC address as the Ethernet frame encapsulating the ARP message for F contains G's MAC address as the source MAC address.

iv) (3 points) When Switch $S4$ receives this Ethernet frame containing the ARP response message from host F, what will it do with this frame?

Answer

When Switch $S4$ receives the ARP response from host F, it will forward the response message to the interface 2 on which host G resides. (Note that there should be a forwarding entry for G in $S4$'s forwarding table, added, for example, when it received the ARP request message from G earlier, cf. the answer to 4.a.i) earlier). In addition, if there is no forwarding entry for host F in $S4$'s forwarding table, it will be added also.

b. (4 points) Consider another scenario where host C wants to send an IP datagram packet to host D. How does host C know that it can directly forward the packet to host D instead of asking for its default router $R2$ to help deliver it? Given the current ARP cache of host C as shown in Figure 4, what source and destination IP addresses and MAC addresses will be used in the corresponding IP datagram and Ethernet frame headers for delivering this packet to host D?

Answer

Host C can find out that both host C and D are on the same IP subnet and hence it does not have to ask its default router ($R2$) to forward the IP datagram packet. Since the ARP table of C already has the IP to MAC mapping for host D, they will be used for the constructing the datagram using both C and D's IP addresses and MAC addresses as the source and destination IP addresses and MAC addresses, respectively, in the corresponding IP datagram and Ethernet frame.

c. (12 points) Now suppose host C wants to send an IP datagram packet to host H using H's IP address, 128.101.0.15 (one of host H's two IP addresses).

i) (2 points) Since H's MAC address is currently *not* in its ARP cache, would it perform an ARP query to find out H's MAC address? Why or why not?

Answer

Based on the IP address of H, host C knows that host H is not on the same IP subnet, it will therefore ask its default Router $R2$ to forward the IP datagram. Hence, it will not issue an ARP request for host H's MAC address.

ii) (4 points) If host C would forward the packet to its default router $R2$ to have it delivered to host H, what source and destination IP addresses should be used in the IP datagram header *and* what source and destination MAC addresses should be used in the encapsulating Ethernet frame in order to deliver this packet to router $R2$?

Answer

The Ethernet frame and IP datagram will have the following source and destination addresses:

Source MAC	Destination MAC	Source IP	Destination IP
C's MAC Address	$R2$'s MAC Address	C's IP Address	128.101.0.15

iii) (2 points) When router $R2$ receives this IP datagram from host C, can it use any of the two outgoing interfaces (1 or 3) to deliver the IP datagram from host C to host H? Why or why not? If your answer is negative, which outgoing interface (1 or 3) should $R2$ use to forward the packet?

Answer

Upon receiving the IP datagram from host C, the router $R2$ will look up its routing table using the destination IP address 128.101.0.15 and perform a longest prefix matching. It matches the first routing entry in its routing table, and hence it will forward it using interface 1.
In other words, even though host H can also be reached via Switch $S3$ by using the interface 3, which interface $R2$ will use to forward an IP datagram is completely determined by the destination IP address and its routing table.

iv) (4 points) In order to deliver the IP datagram from host C to host H, $R2$ will encapsulate it in a new Ethernet frame. What source and destination MAC addresses will $R2$ use in this Ethernet frame?

Answer

The Ethernet frame will have the following source and destination MAC addresses (note that there is a mapping between H's IP address 128.101.0.15 and its MAC address 1 in $R2$'s ARP cache):

Source MAC	Destination MAC
$R2$'s MAC Address	H's MAC Address 1

d. (2 points) Consider a scenario where host H wants to send an IP datagram to the remote host U, and router $R1$ is its default router. Will switch $S3$ receive the Ethernet frame containing the IP datagram sent by host H to the remote host U? Briefly explain your answer.

Answer

Since hosts H's default router $R1$ is on the blue IP subnet (128.101.0.0/18), it will only send the IP datagram encapsulated in an Ethernet frame to switch $S2$ (via its interface 1). Hence, $S3$ will not receive this Ethernet frame.

e. (6 points) Consider yet another scenario where host G is sending an IP datagram packet to host H, where the *destination* IP address in the IP datagram is 128.101.0.15 (one of host H's two IP addresses). This datagram is encapsulated in an Ethernet frame with $R2$'s MAC address as the *destination* MAC address.

i) (2 points) When Switch $S3$ receives this Ethernet frame, which outgoing interface (1 or 4) will it use to forward this Ethernet frame?

Answer

The packet will be forwarded using interface 1.

ii) (4 points) When host H eventually receives the IP datagram from host G, it sends an IP datagram back to G. Which interface will host H likely use to deliver this IP datagram to host G? What determines which interface host H will be using to deliver this IP datagram to host G?

Answer

The answer here is more detailed than necessary to help you better understand how routing is done by a multi-homed host.
It depends on how many routing entries H has in its routing. Since, we have assumed $R1$ is H's default router, it will have at least two routing entries of the form:

Destination Prefix	Next Hop	Interface
128.101.0.0/18	direct	Interface 1
0.0.0.0/0	$R1$	Interface 1

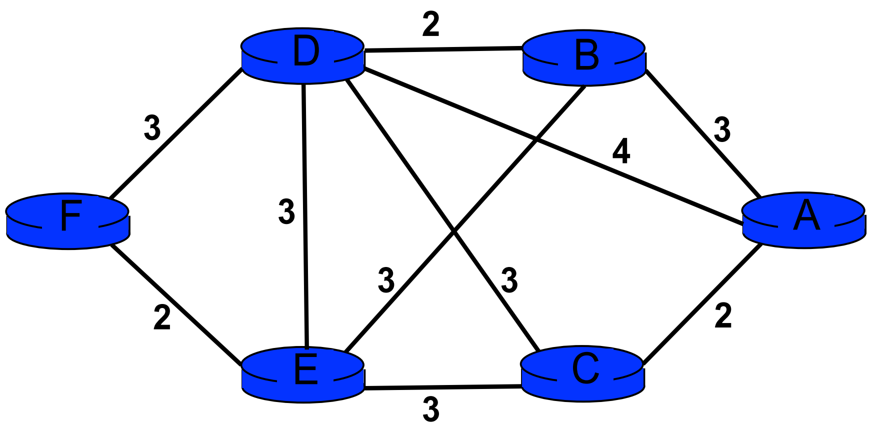
In this case, H will send its reply IP datagram back to host G via interface 1.
However, since H also has a second interface that is assigned an IP address 128.101.100.21, it will likely have an additional routing entry (in particular, if the second IP address 128.101.100.21 is assigned via DHCP, not simply statistically configured without manually adding a new routing entry) in this routing table (check this out yourself by connecting your laptop to a Wi-Fi network and an Ethernet switch on two different IP subnets):

Destination Prefix	Next Hop	Interface
128.101.0.0/18	direct	Interface 1
128.101.100.0/20	direct	Interface 2
0.0.0.0/0	$R1$	Interface 1

Hence, H will likely send the IP datagram via its interface 2: using G's IP address as the destination IP address to look up its routing table, it will match the second routing entry and hence forward it to interface 2.

5. Distributed Routing Algorithms and Centralized Control Plane (25 points) (Approx. 25 minutes)

Consider the network shown in Figure 5, where the number on a link between two nodes are the distance (i.e., link cost) between them.



step	*N*	*D(B),p(B)*	*D(C),p(C)*	*D(D),p(D)*	*D(E),p(E)*	*D(F),p(F)*
0	*A*	*3, A*	*2, A*	*4, A*	*∞, -*	*∞, -*
1						
2						
3						
4						
5						

Figure 5: Figure for Question 5.

The questions from **a.** to **d.** assume that the conventional *distributed* control plane is used, namely, each router needs to exchange routing information with its neighbors and compute its own routing table.

a. (8 points) Use Dijkstra's shortest path algorithm to find the shortest path from A to all other network nodes. Show how the algorithm works by completing the table below the figure shown in Figure 5. (The first row is already completed for you.)

Answer

step	N	D(B),p(B)	D(C),p(C)	D(D),p(D)	D(E),p(E)	D(F),p(F)
0	A	3, A	***2, A***	4, A	∞, -	∞, -
1	AC	***3, A***		4, A	5, C	∞, -
2	ACB			***4, A***	5, C	∞, -
3	ACBD				***5, C***	7, D
4	ACBDE					***7, D***
5	ACBDEF					

Note that using node E at step 4, there is another equivalent path to reach destination F from node A with the same cost: $A \rightarrow C \rightarrow E \rightarrow F$. Thus, both answers are correct and accepted.

b. (4 points) Draw the *shortest path spanning tree* rooted at node A formed by the shortest paths from A to all other network nodes you have derived from **a.**

Answer

Based on the two possible paths for destination F, here are their equivalent shortest path spanning trees. The spanning tree is highlighted in red color.

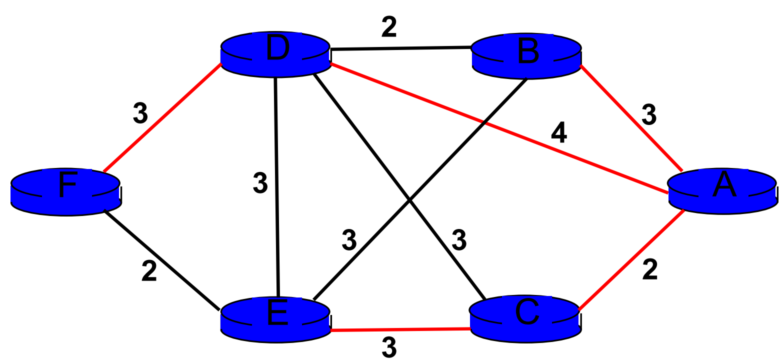


Figure 6: Shortest Path Spanning Tree Question 5.

The spanning tree equivalent to reach destination F using the path: $A \rightarrow C \rightarrow E \rightarrow F$.

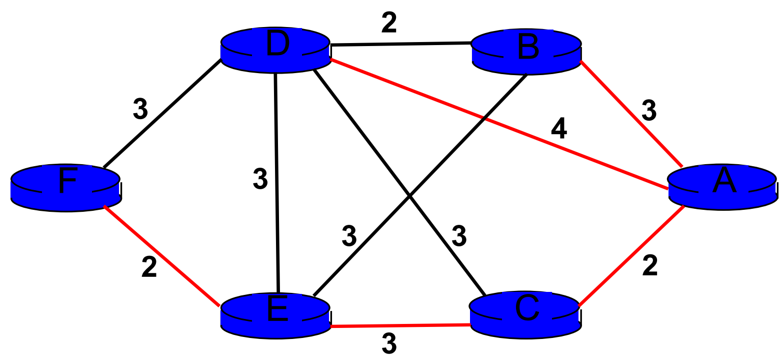


Figure 7: Shortest Path Spanning Tree Question 5.

c. (4 points) Suppose the datagram network service model is used for packet forwarding. Construct the *routing table* at node A from the shortest path spanning tree in **b.**

Answer

A's routing table is the following:

Destination	Next Hop
B	B
C	C
D	D
E	C
F	D

A's routing table using the path: $A \rightarrow C \rightarrow E \rightarrow F$ to reach destination F:

Destination	Next Hop
B	B
C	C
D	D
E	C
F	C

You can also mantain some information to choose between the two next hops for destination F in one table.

d. (5 points) Recall that in the virtual circuit network service model, before a virtual circuit is set up, the source router needs to specify a path (e.g., the shortest path) from the source to the destination. What additional information do we need to maintain in the routing table to support this function? Write down the resulting routing table.

Answer

Note that VCI translation tables are used for packet forwarding, NOT for routing. Here we are asking you if a source (say, router A) needs to specify a shortest path from A to a destination F, say, $A \rightarrow B \rightarrow D \rightarrow F$, for setting a VC (e.g., a MPLS tunnel), what additional information it needs to install in the routing table? A simple answer is that for each destination, router A would maintain a complete (shortest) path as following:

Destination	Route
B	$A \rightarrow B$
C	$A \rightarrow C$
D	$A \rightarrow D$
E	$A \rightarrow C \rightarrow E$
F	$A \rightarrow D \rightarrow F$

Note this table contains some redundant info (e.g., for destinations C, E, & D, F). A more "clever" way is to maintain the previous-hop info (namely, p(.) in part (a) when computing the shortest paths) for each destination: now we have the following table — basically adding one additional column to the routing table in part (c):

Destination	Previous Hop	Next Hop
B	A	B
C	A	C
D	A	D
E	C	C
F	D	D

In other words, we are basically storing the shortest path tree computed in part (b) in a table format. From the above table, we can re-construct the shortest path info for each destination by starting with the entry corresponding to the destination, using the prev-hop information to piece together the shortest path. [We are essentially trading-off space with time: it may take more time to construct the path but less space to store it.

***** A General Pedagogical Note ***

Please note that there is a difference between forwarding and routing functions, and there are forwarding tables (and routing tables from which forwarding tables are derived). Routing tables are the results of routing computations (i.e., executing some routing algorithms) — it often contains more information than forwarding tables.

In destination-based IP datagram service model, for intra-domain routing, the routing tables are often the same/very similar to forwarding tables (but for inter-domain routing, BGP maintains its own routing tables; the IP forwarding tables are in fact derived from both intra-domain routing tables and BGP routing tables).

In other forms of service models, e.g., virtual circuit, or in centralized routing paradigm such as SDN, the routers or SDN controllers need to maintain information for path selection (with resort to performing path computation for each path set-up).

e. (4 points) Now assume that a *centralized* control plane is used, where a SDN controller would monitor and collect the network topology information, select paths and install the routing table at each router for packet forwarding. Suppose that the SDN controller wants to set up a path from router A to router F using the paths $A \rightarrow B \rightarrow D \rightarrow F$. Write down the routing entries (or "match-action" rules) that the SDN controller will be installing at the routers along the path. (As an example, the routing entry (the "match-action" rule) in router A is given to you as follows: `[destination IP address == F` $\Longrightarrow$ `forward to router B]`, where the expression before $\Longrightarrow$ represents the match pattern, and the expression afterward $\Longrightarrow$ represents the action.)

Answer

The match action rules are the following:

Router	Match	Action
A	Src.IP == A, Dst.IP == F	Forward (B)
B	Src.IP == A, Dst.IP == F	Forward (D)
D	Src.IP == A, Dst.IP == F	Forward (F)

Using SDN, you can also choose one of the two shortest paths to reach the destination F as well. If you want all packets destined to node F to follow the same path, you do not need to include the source IP in the match field. However, if you want to specify a specifc path from each source to the destination F, then you need to include the source node in the match field.