UNIVERSITÉ YORK UNIVERSITY

Department of Electrical Engineering and Computer Science

EECS 3214: Computer Network Protocols and Applications

Instructor: N. Vlajic
Date: Feb 25

Midterm Examination

Instructions:

- Examination time: 75 min.
- Print your name and CSE student number in the space provided below.
- This examination is closed book and closed notes.
- There are 6 questions. The points for each question are given in square brackets, next to the question title. The overall maximum score is 100.
- Answer each question in the space provided. If you need to continue an answer onto the last page, clearly indicate that and label the continuation with the question number.

FIRST NAME: ____________________________

LAST NAME: ____________________________

STUDENT #: ____________________________

Question	Points
1	/ 20
2	/ 12
3	/ 25
4	/ 15
5	/ 16
6	/ 12
Total	/ 100

1. Multiple Choice [20 points]

Circle the correct answer(s) for the following statements. For each statement, you will obtain 0 marks if the number of circled answers is more/less than appropriate.

(1.1) The key advantage(s) of bus topology (in LAN networks) – compared to the other three LAN topologies - include:

(a) robustness to link failure
(b) no need to manage collisions
(c) guaranteed QoS for all users/machines
(d) none of the above

(1.2) The key advantage(s) of circuit-switching – relative to packet-switching – include:

(a) better utilization of bandwidth
(b) potentially a larger overall number of serviced users
(c) better QoS provided to the serviced users
(d) none of the above

(1.3) In the layered OSI architecture, a '**communication protocol**' is used to facilitate:

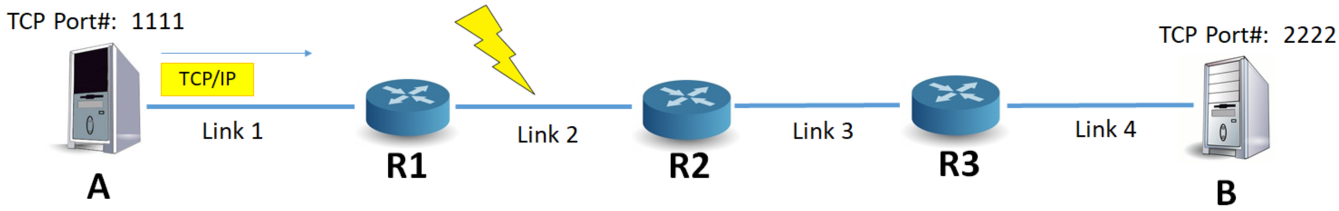
(a) horizontal communication between peers of the same layer
(b) vertical communication between adjacent layers
(c) communication between lower layers of the sending machine and upper layers of the receiving machine
(d) none of the above

(1.4) Bob and Alice are both claiming that there is an application running on TCP port number 55555 on each of their machines.

(a) This is impossible as transport-layer port numbers are globally unique, and this would crate a conflict.
(b) This is possible only if the two applications are communicating with each other over the same port.
(c) This is possible only if Bob's and Alice's machine are situated on different LANs.
(d) This is generally possible and may suggest that they both are running the same type of client application.

(1.5) A TCP packet encapsulated inside an IP packet is being transmitted between machine A (TCP Port# 1111) and machine B (TCP Port# 2222), as illustrated in the below figure. During the transmission over Link 2 a bit error corrupts the value of the destination port number in the given packet – so instead of 2222 now it reads 2238. (This is the only bit error affecting the given packet. Assume no data-link layer error control on ether of the links.) As a result of this:

(a) router R2 will detect this error by validating IP checksum and drop the packet
(b) router R2 will detect this error by validating TCP checksum and drop the packet
(c) the given packet will reach B, but will be delivered to a wrong application
(d) none of the above



(1.6) The below QoS requirements correspond to which of the following applications? (Note: '**Low Latency/Jitter/Loss Tolerance**' means that the application requires latency/jitter/loss to be low, otherwise the QoS will degrade.)

(a) videoconferencing
(b) video on demand
(c) Web browsing
(d) file transfer

Throughput Demand	Latency Tolerance	Jitter Tolerance	Loss Tolerance
Medium - High	Low	Low	Low

(1.7) A router uses WFQ to schedule/place packets on its outgoing link. This link has a bandwidth of 100 Mbps. The router has 2 incoming links/buffers - A and B. The weight for incoming link/buffer A is 4, and the weight for incoming link/buffer B is 1. The effective outgoing rate allocated to link A is:

(a) 80 Mbps
(b) 50 Mbps
(c) 40 Mbps
(d) 10 Mbps

(1.8) What can you say about the following IP address: **169.254.1.255** ?

(a) A computer with such an IP address belongs to a class B network.
(b) A computer with such an IP address belongs to a class C network.
(c) This is a broadcast address of a class C network.
(d) A computer with such an IP address has a limited communication reach.

(1.9) What can you say about the following IP address: **255.255.255.255** ?

(a) Such an IP address is never used.
(b) Packets with this IP address as their destination will be sent to the entire Internet.
(c) This IP address can only be used as a 'source IP address' and not as a 'destination IP address'.
(d) Packets with this IP address as their destination are dropped by routers.

(1.10) The link-state routing algorithm (Dijkstra) should be the algorithm 'of choice' in networks where:

(a) each node is not expected/required to know the entire network topology

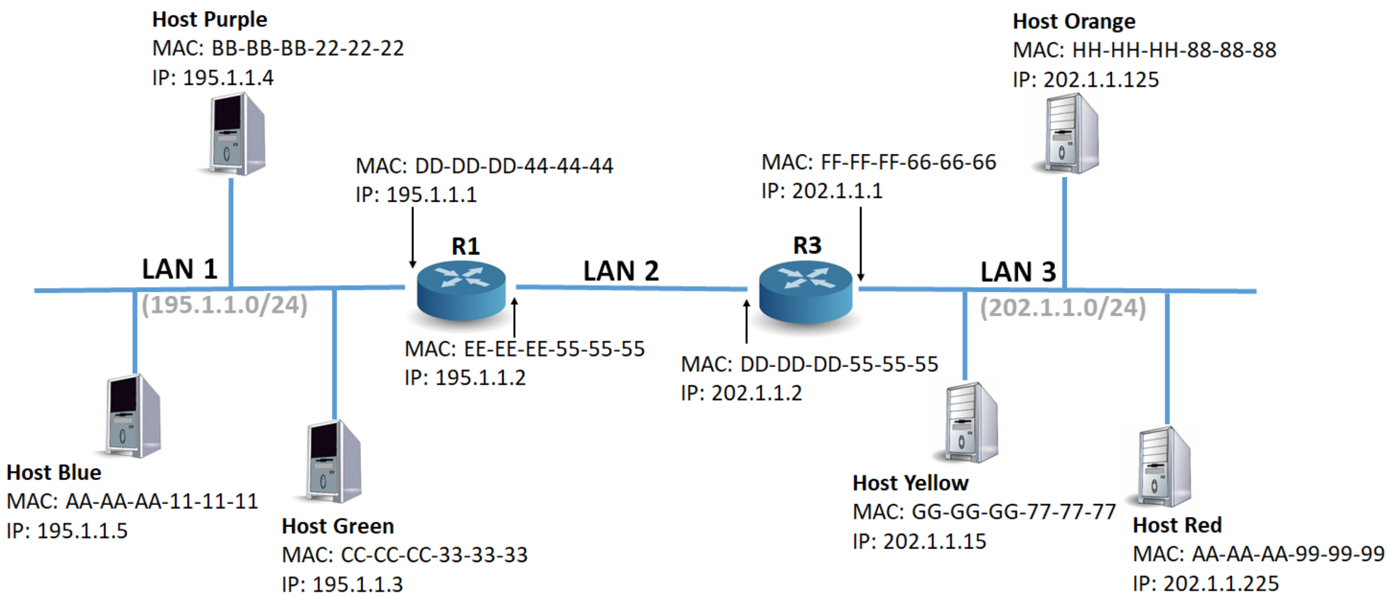
(b) packet broadcast is generally discouraged

(c) routing paths should be quickly adjusted in case of link-failure(s)

(d) none of the above

2. Networking Basics Potpourri [12 points]

Consider a simple network topology, comprising 3 LANs, as shown in the below figure. In the given topology, packets traveling between LAN 1 and LAN 3 have to pass through LAN 2 (i.e., have to pass through routers R1 and R3). The MAC and IP addresses associate with (assigned to) various network interfaces on all 3 LANs are provided.



2.1) [3 points]

Based on the provided information, is it possible to conclude whether any of the involved network interface cards have been manufactured by the same vendor? Briefly justify your answer.

Solution

The first 3 bytes (24 bits) of a NIC's MAC address are called Organizational Unique Identifier (OUI) and they uniquely identify the actual vendor of this NIC.
Based on the provided MAC addresses:

- **the left NICs of R1 and R3 are produced by the same vendor;**
- **the NICs of Host Blue and Host Red also appear to be produced by the same vendor.**

2.2) [3 points]

Inspect the IP addresses assigned to various network interfaces closely. Is there anything obviously problematic with the way some of the IP addresses have been assigned? Briefly justify your answer.

Solution

One obvious issue is the fact that the IP addresses on LAN 2 are very different from each other and seem to actually belong to different networks. In particular, the IP address of R1's right interface belongs to LAN 1 while the IP address of R3's left interface belongs to LAN 3.

2.3) [2 points]
Assume **Host Blue** needs to be moved to **LAN 3**. How will the move impact the values of Host Blue's MAC and IP addresses?

Solution
MAC address will remain the same.
IP address will have to change – Host Blue will have to be given an unoccupied IP addresses of LAN 3.

2.4) [4 points]
Assume that **Host Orange** runs a Web server. **Host Purple** has sent an HTTP (Web-page) request to this server. The given request has been sniffed while passing over **LAN 2**. Fill out the missing fields in the sniffed packet. For the fields whose value cannot be determined, leave a blank line.

Data-link Header of the Sniffed Packet:

MAC Source: ______________________

MAC Destination: ______________________

IP Header of the Sniffed Packet:

IP Source: ______________________

IP Destination: ______________________

TCP Header of the Sniffed Packet:

Port Source: ______________________

Port Destination: ______________________

Solution

Data-link Header of the Sniffed Packet:

MAC Source:	EE-EE-EE-55-55-55
MAC Destination:	DD-DD-DD-55-55-55

IP Header of the Sniffed Packet:

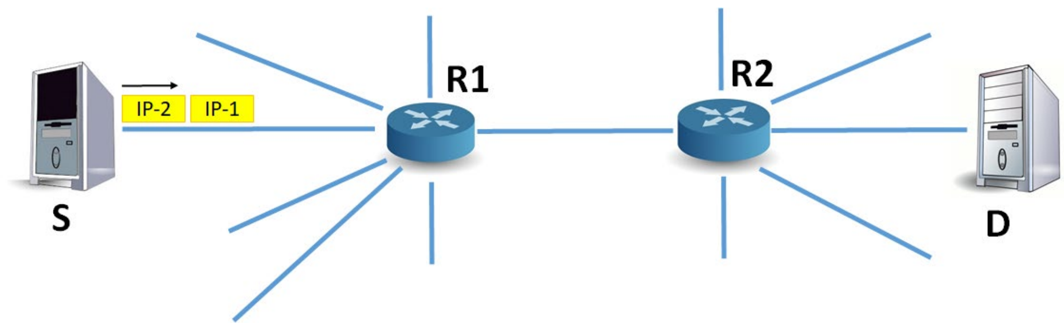
IP Source:	195.1.1.4
IP Destination:	202.1.1.125

TCP Header of the Sniffed Packet:

Port Source:	
Port Destination:	80

3. IP Packets & IP Fragmentation [25 points]

3.1) [5 points]
Assume the below scenario, where the source computer (S) is sending two back-to-back IP packets to the destination computer (D) through 2 intermediate routers. The entire network is currently experiencing congestion. The probability of an/any IP packet being dropped at router R1 is 0.2, and the probability of an/any IP packet being dropped at R2 is 0.1. What is the probability that both packets sent from S to D successfully arrive at their destination?

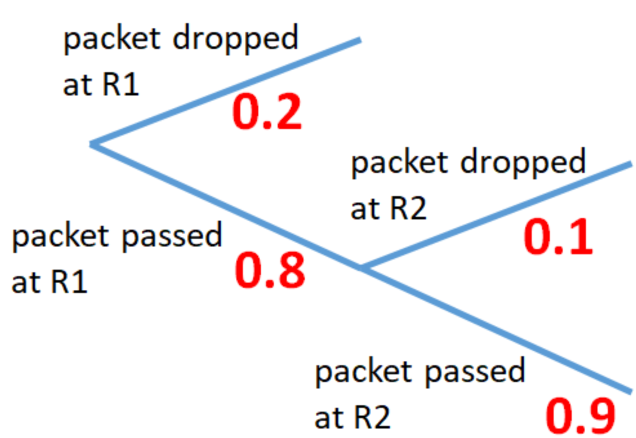


<u>Solution</u>
One single packet will arrive successfully from S to D if it is **<u>not</u>** dropped at R1 **AND** it is **<u>not</u>** dropped at R2. Hence:

$$\mathbf{P_{success}(single\ packet) = (1-P_{R1\text{-}drop}) \times (1-P_{R2\text{-}drop}) = (1-0.2) \times (1-0.1) = 0.8 \times 0.9 =}$$
$$\mathbf{= 0.72}$$

The probability of both packets arriving successfully at D corresponds to the probability of one packet arriving successfully at D AND the other packet arriving successfully at D:

$$\mathbf{P_{success}(two\ packets) = P_{success}(single\ packet) \times P_{success}(single\ packet) =}$$
$$\mathbf{= 0.72 \times 0.72 =}$$
$$\mathbf{= 0.5184}$$

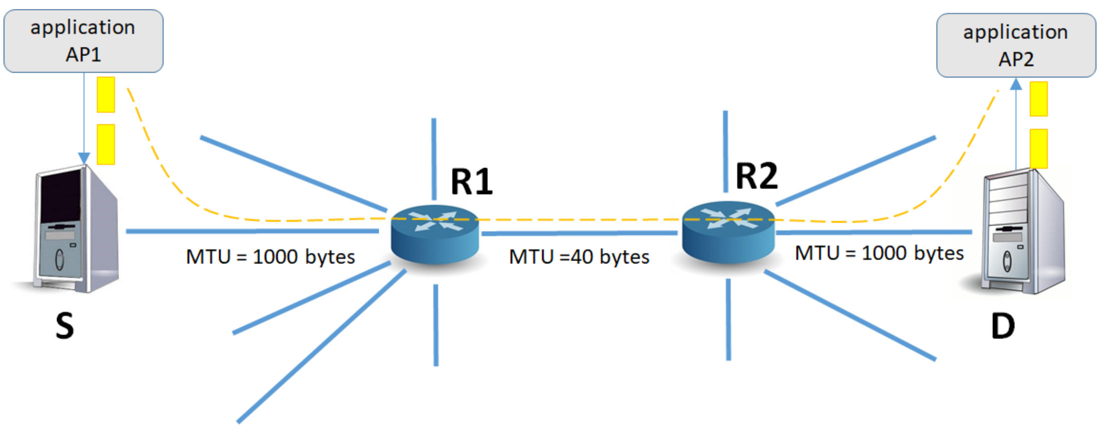


3.2) [8 points]
Assume the same topology as in 3.1). Moreover, the value of MTU on each of the three links is as shown in the below figure.

In this question also assume that application program (AP1) on computer S is sending 20 bytes of data every second to a peer application (AP2) on computer D. AP1 and AP2 are supported by UDP protocol in the transport layer.

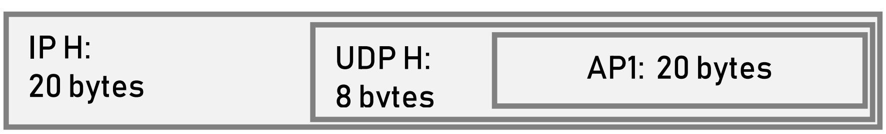
Finally, in this question, the probability of a packet being drop at R1 is zero, while R2 is heavily congested and as a result every 2nd IP packet that arrives to R2 and carries D's IP address as its destination ends up being dropped. (D is currently receiving only packets from S.)

How many bytes of AP1's data arrive to AP2 every second?



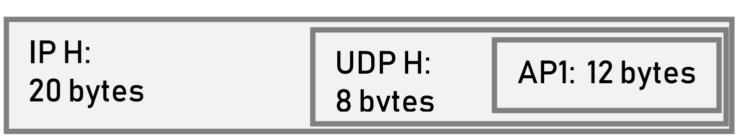
Solution

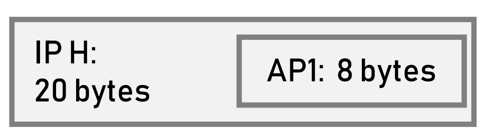
In this question it is first important to observe that (every) 20 bytes of AP1's data will be first encapsulated by UDP (adds an 8-byte header) and then IP (adds a 20-byte header). Thus, the overall size of each IP packet sent from S to D while carrying 20 bytes of AP1's data will be 48 bytes.



Unfortunately, due to the value of MTU of only 40 bytes between R1 and R2, R1 will have to fragment each of these IP packets into 2 IP packets/fragments:

- 1st fragment will have its own IP header (20 bytes) and will carry the 8-byte UDP header plus the first 12 bytes of AP1's data from the original IP packet;
- 2nd fragment will have its own IP header (20 bytes) and will carry the remaining 8 bytes of AP1's data form the original IP packet.





Since every second packet that arrives to R2 and carries D's IP as its destination ends up being dropped – which, in fact, implies that the second fragment of every original IP packet sent from

S/AP1 to D/AP2 is dropped – we conclude that no complete IP packet will ever arrive from S/AP1 to D/AP2. **In other words, the rate of data arrival from AP1 to AP2 will be zero!**

3.3) [3 points]
Give 2 reasons why, in general, intermediate routers do not engage in re-assembly of fragmented IP packets?

Solution
Any two of the following:
1. Fragments of an IP packet may not all arrive at the same router.
2. There is no point of re-assembling a packet as the packet may be fragmented again.
3. The re-assembly would additionally and unnecessarily use up the processing resources of intermediate routers.

3.4) [3 points]
How can IP packet fragmentation be exploited by an adversary in order to cause the target/destination host to start dropping legitimate packets?

Solution
Receiving hosts are responsible for collecting/buffering IP fragments in order to re-assemble the respective eoriginal IP packets
The adversary could send a very large number of fragmented IP packets to the target/destination host, with one fragment missing from each packet so that the reassembly is impossible. Thus, this attack causes resource exhaustion on the destination node, possibly denying reassembly services to other flows, and possibly dropping legitimate fragments/packets.

3.5) [6 points]
Suppose that instead of using variable size IP packets, all IP packets were required to be of the same size. Name 2 disadvantages for each of the following scenarios:

a. We fixed the packet size to be very small (e.g., 50 bytes). The disadvantages would be:

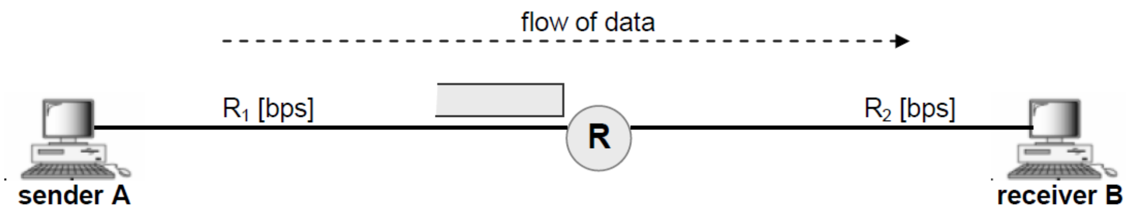
Solution
1. Larger overall communication overhead – since every small packet would still have to have a 20-byte header.
2. Increased overall processing overhead on routers, as they would have to process an overall larger number of headers (determine route, calculate checksum, reduce TTL, ...)

b. We fixed the packet size to be very large (e.g., 5,000 bytes). The disadvantages would be:

Solution
1. Longer overall end-to-end delays, since larger packets imply larger 'store-and-forward' delays on each hop (even if there are no other packets in the queue).
2. Possible problems with (real-time) applications that may require periodic transmission of smaller amounts of data.

4. Packet Delay [15 points]

Suppose we have two hosts connected via an intermediate router, as shown in the figure below.



The datarate on link A-R is R_1 = 2 [Mbps], and the datarate on link R-B is R_2= 1 [Mbps]. Router R has a limited buffer of size B = 800 [packets]. Each packet comprises P = 5,000 [bits]. The propagation delay on both links is negligible.

a) [9 points]

Suppose A starts sending a continuous stream of back-to-back packets. Clearly, after a certain interval of time, this will saturate the A-R link and R's input buffer.
At what time, exactly, will the first packet loss occur?

Solution

Packets arrive into R at the rate (in bits) of λ = R_1 [bps] = 2 [Mbps].
Departure rate (in bits) from R is η = R_2 [bps] = 1 [Mbps].

Since $\lambda > \eta$, or specifically $\lambda = 2 * \eta$, the system is unstable, and the buffer will grow until it gets full, and then it will start dropping packets

.

Based on the above, we also conclude: for every packet sent out (i.e., taken out of the queue), two new packets will arrive into the queue.
Hence, the 'effective arrival rate' into the queue is ½ of the actual arrival rate.
That is: **R_1-effective = 1 [Mbps].**

Buffer_size [bits] = B[packets]*P[bit/packet] = 800 * 5,000 = 4,000,000 [bits] = 4 [Mbits]

With such a data-rate, it will take
Buffer_size [bits] / R_1-effective = 4 [Mbits] / 1 [Mbps] = 4 [seconds] to fill out (i.e., saturate) R's buffer.

So, T = 4 [seconds].

b) [4 points]
Assume A has enumerated the transmitted packets in order/sequence: 1, 2, 3, … What is the sequence number of the packet that gets dropped first from R's buffer?

Solution
We have concluded from part a) that it takes 4 seconds to fill R's buffer. The packet that gets generated right after the 4^{th} second is the one that will get dropped from R.

In other words, if we determine how many packets have been successfully generated and received by R within the first 4 seconds – e.g., M packets, then the sequence number of the packet that gets dropped is M+1. (Recall, we assume the propagation delay from A to R is negligible.)

The number of packets that get transmitted by A and received by R within 4 seconds is:
R_1 * T / P = 2 [Mbps] * 4 [sec] / 5,000 [bits] = 8 000 000 [bits] / 5,000 [bits] = 1600 [packets]

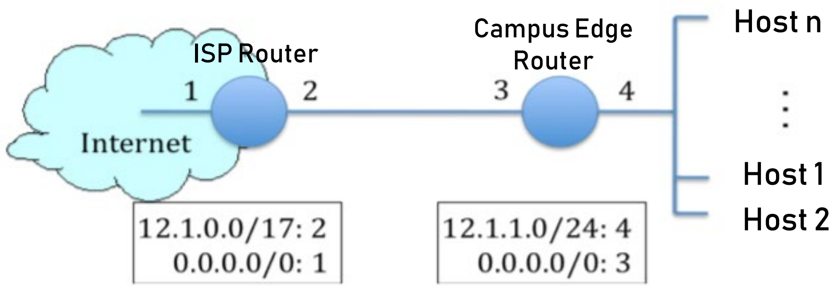
Hence, the sequence number of the packet that gets dropped first is 1601.

c) [2 points]
What is the impact of packet loss on link A-R on the utilization of link R-B?

Solution
None. Link R-B remains 100% utilized.

5. IP Addressing and Subnetting [16 points]

A small university campus uses a single Internet Service Provider (ISP) to reach the rest of the Internet. The ISP assigns a large address block 12.1.0.0/17 to the campus, but the campus is using only a portion of these addresses (12.1.1.0/24) to number its computers - as illustrated in the below figure.



The figure also shows the forwarding tables on the ISP's router (on the left) and the forwarding tables on the campus edge router (on the right). The two tables imply the following:

- The ISP router forwards all packets with destination address 12.1.0.0/17 out over interface #2 towards the campus edge router.
- The campus edge router forwards all packets with destination 12.1.1.0/24 out over interface #4 towards its internal network.
- Both routers include a default forwarding entry 0.0.0.0/0 that can match any (other) destination IP address.

a) [2 points]
How many IP addresses does the campus theoretically 'own' in its originally assigned block 12.1.0.0/17?

Solution
The 17-bit mask leaves 32-17 = 15 bits to identify individual hosts. Hence, theoretically, the number of individual IP addresses in this block is:

$$2^{15} = 32{,}768$$

b) [2 points]
How many IP addresses does the campus actually deploy by using only the sub-block 12.1.1.0/24?

Solution
The 24-bit sub-mask leaves 32-24 = 8 bits to identify the actual hosts on the campus network. Hence, practically, the number of utilized IP addresses is:

$$2^{8} = 256$$

c) [3 points]
What are the first and the last IP address from the 12.1.1.0/24 sub-block assigned to an actual host on the campus network?

Solution
The 1st IP assigned to an actual host: 12.1.1.1
The last IP assigned to an actual host: 12.1.1.254

d) [4 points]
Suppose the ISP router receives a packet with destination IP address 12.1.1.1? What path does this packet follow? (Name all the interfaces that the packet goes through – incoming and outgoing!)

Solution
On the ISP router, this packet will 'match' the first entry of the forwarding tables and thus be sent over interface # 2 and ultimately reach the campus edge router over interface # 3.
On the campus edge router, the packet will again match the fist entry of the forwarding tables and thus be forwarded over interface #4 towards the campus' internal network.
Overall the path followed is:

2 -> 3 -> 4

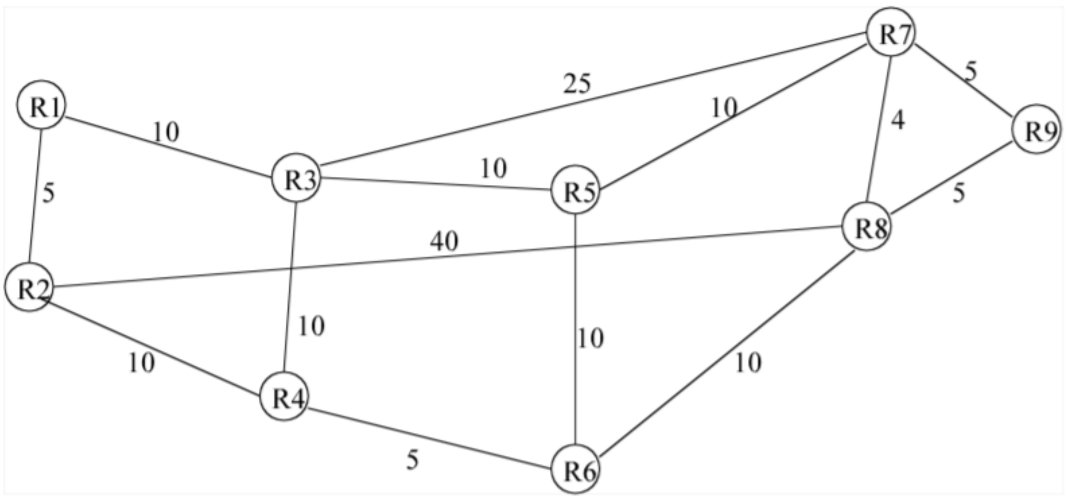
e) [5 points]
Suppose the ISP router receives a packet with destination IP address 12.1.20.1? What path does this packet follow? (Name all the interfaces that the packet goes through – incoming and outgoing!)

Solution
On the ISP router, this packet will 'match' the first entry of the forwarding tables and thus be sent over interface # 2 and ultimately reach the campus edge router over interface # 3.
However, on the campus edge router, the packet will NOT match the fist entry (i.e., it will match the 2nd entry), and as a result will be forwarded over interface #3 back to the ISP router ...
Overall the path followed is:

2 -> 3 -> 2 -> 3 -> …

6. Unicast Routing [12 points]

In the following topology, assume all the links are bidirectional and the cost is the same for both directions. **Use Bellman-Ford algorithm to <u>find the lowest-cost paths to R1</u> from every other node/router in the given network**. In order to find these lowest-cost paths to R1, calculate the current lowest-cost to reach R1 (and the respective next hop router to get there) for each of the other nodes/routers during each iteration of Bellman-Ford algorithm until convergence.



Note: You should not build the entire table for all other nodes, but only show the entry that is related to R1. Those entries and their respective vales at the end of the 1st iteration of Bellman-Ford algorithm are provided below. You need to complete the rest.

Entries of routers R2 – R9 related to R1:

	1st iteration		2nd iteration		3rd iteration		4th iteration		5th iteration	
Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R2	R1	5								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R3	R1	10								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R4	-	∞								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R5	-	∞								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R6	-	∞								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R7	-	∞								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R8	-	∞								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R9	-	∞								

Solution

	1st iteration		2nd iteration		3rd iteration		4th iteration		5th iteration	
Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R2	R1	5								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R3	R1	10								

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R4	-	∞	R2	15						

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R5	-	∞	R3	20						

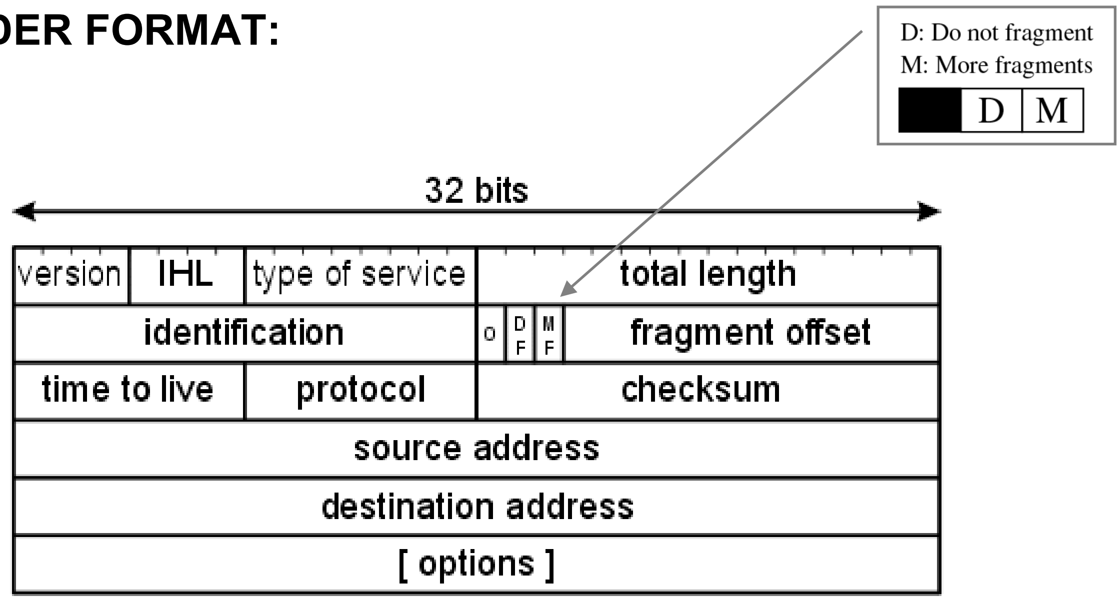
Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R6	-	∞	-	∞	R4	20				

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R7	-	∞	R3	35	R5	30				

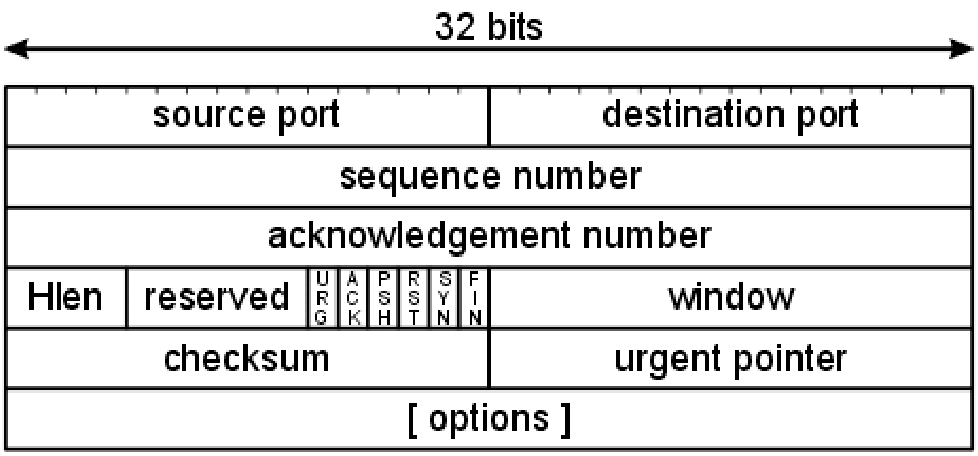
Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R8	-	∞	R2	45	R7	39	R6	30		

Router	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist	Hop	Dist
R9	-	∞	-	∞	R7	40	R7	35		

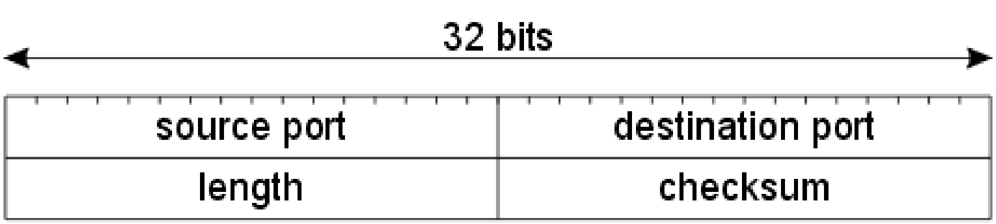
IPv4 HEADER FORMAT:



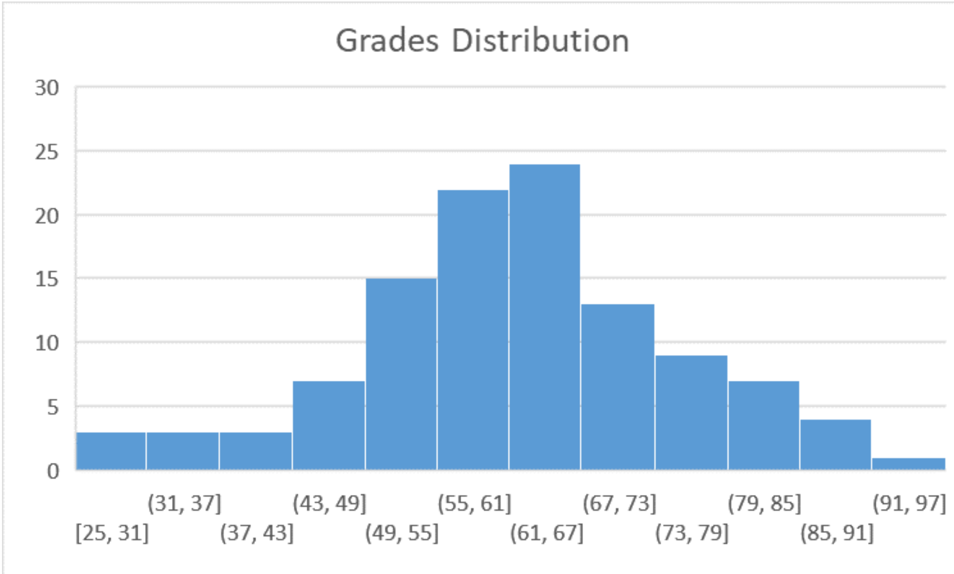
TCP HEADER FORMAT:

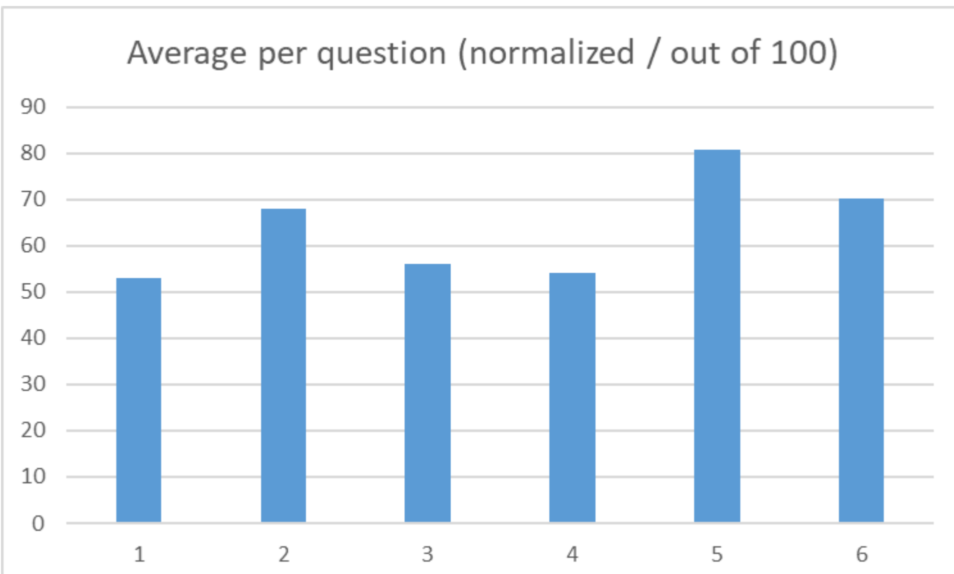


UDP HEADER FORMAT:



Grade Statistics:





	Midterm	Final	Assignments	
% weight	35	40	25	
Grade	45	45	80	53.75
	Midterm	Final	Assignments	
% weight	35	40	25	
Grade	68	68	100	76