

Tutorial 2 (Week 10)

Note: Some questions are from past exams. We are providing questions to prepare you for the final exam which will have mostly short questions.

Q1. Host A uses TCP Reno to transfer a file to host B. The file contains 32 MSS of data. During the first transmission round, the congestion window is equal to 1 MSS. During the fourth round when the connection is still in the slow-start mode all the transmitted packets are lost (and, therefore, host A transmits less during the fifth round). There is no packet loss during any other round. During what round does host B receive the complete file?

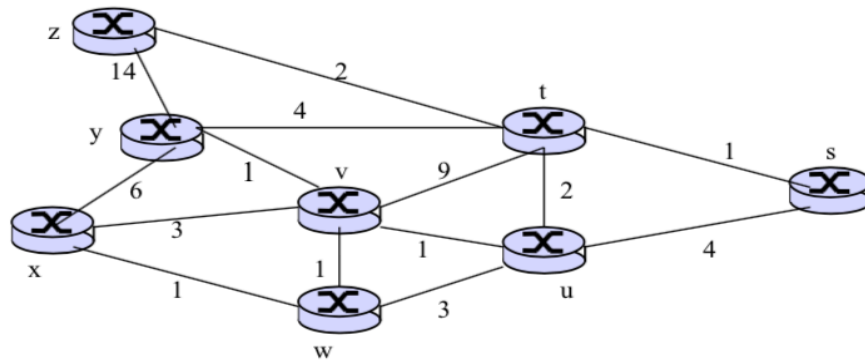
Q2. Consider the following forwarding table for a router R.

Destination	Interface
128.8.16.0/20	Port 1
128.8.24.0/21	Port 2
128.8.128.0/24	Port 3
128.8.128.0/28	Port 4
Default	Port 5

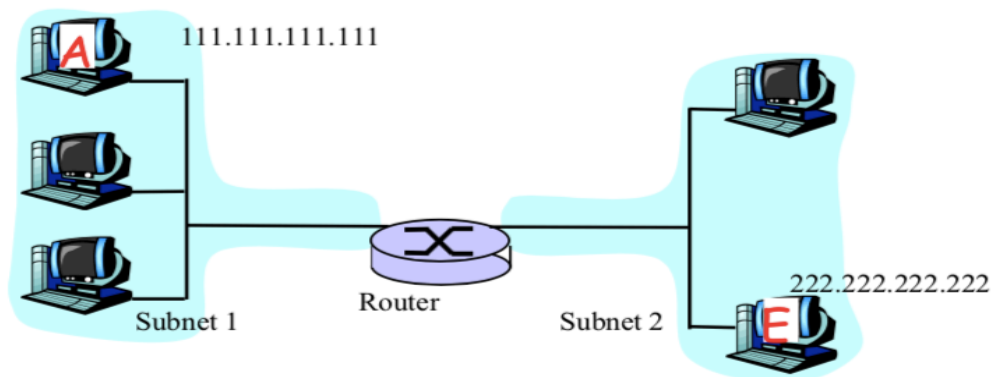
For each of the following destination IP addresses, indicate which port the packet is sent out on:

- (a) 128.8.128.252
- (b) 128.8.128.5
- (c) 128.8.25.223
- (d) 155.128.45.21

Q3. Consider the following network with the indicated link costs. Use Dijkstra's shortest path algorithm to compute the shortest path from node x to all network nodes. Show the forwarding table at node x.



Q4. Consider the network topology shown in the figure below.



- (a) Write down an IP address for all interfaces at all hosts and routers in the network. The IP addresses for A and E are as given. Both Subnet1 and Subnet2 make use of 24 bit network prefixes. You should assign IP addresses so that interfaces on the same sub-network have the same network-part of their IP address.
- (b) Choose physical addresses (LAN addresses) for only those interfaces on the path from A to E. Can these addresses be the same as in part (a)? Why?
- (c) Now focus on the actions taken at both the network and the data link layers at Sender A, the Router and the destination E in moving an IP datagram from A to E:
 - 1) What, specifically, are the source and destination addresses in the IP datagram that flows from A to the Router. What specifically are the source and destination addresses in the IP datagram that flows from the Router to node E?
 - 2) Name any three other fields found in an IP datagram?
 - 3) How do A, E and the Router determine the physical (LAN) addresses required for the data link layer frame?

(d) Suppose that the router in figure above is replaced by a layer 2 switch.

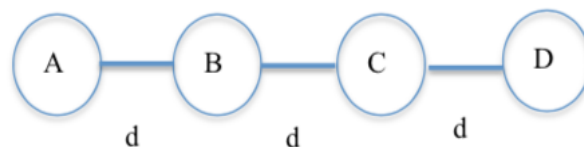
- 1) How would the IP addresses of the hosts change in this scenario? (simply provide an explanation without specifying the changed IP addresses).
- 2) How would the physical (LAN) addresses change in this case?
- 3) How does the switch learn the physical addresses of the attached hosts?

Q5. Suppose that nodes A and B are attached to the opposite ends of a shared 900m Ethernet cable and that they each have one 1000 bit frame (including all headers and preambles) to send to each other. Suppose that there are four repeaters between A and B, each inserting a 20-bit delay (this is the time taken to transmit 20 bits on the Ethernet cable) and that the transmission rate is 10 Mbps. Assume that CSMA/CD with back-off intervals of multiples of 512 bit time (i.e. each backoff interval is a multiple of the time taken to transmit 512 bits on the Ethernet cable) is used. Assume that both A and B transmit their packets simultaneously at time $t = 0$ sec resulting in a collision. After the collision, A draws $K=0$ whereas B draws $K=1$ in the exponential back-off protocol. Ignore the jam signal and the 96-bit time delay.

a. What is the one-way propagation delay (including the repeater delays) between A and B in seconds? Assume that the signal propagation speed is 2×10^8 m/sec.

b. At what time (in seconds) is A's packet completely delivered at B?

Q6. Consider a wireless network consisting of four nodes A, B, C, D where each node has a radio range of distance d . In the figure, two nodes are in each other's range, if there is an edge between them.



Consider two collision resolution schemes:

CS: This is a pure carrier sense scheme in which a node does not send when it hears someone else transmitting, but otherwise can send whenever it wants.

802.11: This uses carrier sensing as in CS. In addition, nodes wishing to communicate use an RTS-CTS-Data-ACK exchange. Nodes overhearing an RTS wait to allow the CTS to be sent. If no CTS is heard, the node can transmit. If a CTS is heard (even if no earlier RTS is heard), the node is quiet for the entire duration of the data transmission.

Assume that A and B are in the midst of a communication and C has been listening to their exchange so far (and so has heard whatever RTS or CTS packets that B may have sent if any). While A and B are in the “sending data” part of their exchange, C decides that it wants to communicate with D. Consider the following cases: (explain all answers)

(a) A is sending data to B.

(i) If scheme CS is used, would C be allowed to send a message to D?

(ii) If scheme 802.11 is used, would C be allowed to send a message to D?

(b) B is sending data to A.

(i) If scheme CS is used, would C be allowed to send a message to D?

(ii) If scheme 802.11 is used, would C be allowed to send a message to D?

Q7. Suppose Alice wants to visit the Web site `activist.com` using a TOR-like service. This service uses two non-colluding proxy servers, Proxy1 and Proxy2. Alice first obtains the certificates (each containing a public key) for Proxy1 and Proxy2 from some central server. Denote $K1^+(\cdot)$, $K2^+(\cdot)$, $K1^-(\cdot)$, and $K2^-(\cdot)$ for the encryption/decryption with public and private RSA keys.

- a. Using a timing diagram, provide a protocol (as simple as possible) that enables Alice to establish a shared session key S_1 with Proxy1. Denote $S_1(m)$ for encryption / decryption of data m with the shared key S_1 .
- b. Assuming S_1 is in place, using a timing diagram, provide a protocol (as simple as possible) that allows Alice to establish a shared session key S_2 with Proxy2 *without revealing her IP address to Proxy2*.
- c. Assume now that shared keys S_1 and S_2 are now established. Using a timing diagram, provide a protocol (as simple as possible and **not using public-key cryptography**) that allows Alice to request an html page from `activist.com` *without revealing her IP address to Proxy2 and without revealing to Proxy1 which site she is visiting*.