Instructions to Candidates

Answer question 1 and two others

Exam Duration: 2 hours

A scientific calculator is allowed

QUESTIONS

|  |  |
| --- | --- |
| QUESTION 1 |  |
| Suppose there is exactly one packet switch between a sending host and a receiving host. The transmission rates between the sending host and the switch and between the switch and the receiving host are R1 and R2, respectively. Assuming that the switch uses store-and-forward packet switching, what is the total end-to-end delay to send a packet of length L? (Ignore queuing, propagation delay, and processing delay.) | [8 marks] |
| A Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates R1 = 500 kbps, R2 = 2 Mbps, and R3 = 1 Mbps. Assuming no other traffic in the network, what is the throughput for the file transfer? Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to Host B? Repeat (a) and (b), but now with R2 reduced to 100 kbps. | [4 marks] |
| A Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates R1 = 500 kbps, R2 = 2 Mbps, and R3 = 1 Mbps. Assuming no other traffic in the network, what is the throughput for the file transfer? Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to Host B? Repeat (a) and (b), but now with R2 reduced to 100 kbps. | [4 marks] |
| A Suppose Host A wants to send a large file to Host B. The path from Host A to Host B has three links, of rates R1 = 500 kbps, R2 = 2 Mbps, and R3 = 1 Mbps. Assuming no other traffic in the network, what is the throughput for the file transfer? Suppose the file is 4 million bytes. Dividing the file size by the throughput, roughly how long will it take to transfer the file to Host B? Repeat (a) and (b), but now with R2 reduced to 100 kbps. | [6 marks] |
| What are the five layers in the Internet protocol stack? What are the principal responsibilities of each of these layers? | [8 marks] |
| QUESTION 2 |  |
| The process of HTTP asking TCP to send some data and making sure that it is received correctly is an example of what? (choose one answer) Same-layer interaction. Adjacent-layer interaction. OSI model. All of the above. | [5 marks] |
| The process of a web server adding a TCP header to the contents of a web page, followed by adding an IP header and then adding a data-link header and trailer, is an example of what? (choose one answer) Data encapsulation. Same-layer interaction. Adjacent-layer interaction. All of the above. | [5 marks] |
| Which of the following answers lists the prefix (CIDR) format equivalent of 255.255.254.0? (choose one answer) /19 /20 /23 /24 | [8 marks] |
| Working at the help desk, you receive a call and learn a user’s PC IP address and mask (10.55.66.77, mask 255.255.255.0). When thinking about this using classful logic, you determine the number of network (N), subnet (S), and host (H) bits. Which of the following is true in this case? (choose one answer) N = 12 S = 12 H = 64 H = 8 | [8 marks] |
| Consider a router that interconnects three subnets: Subnet 1, Subnet 2, and Subnet 3. Suppose all of the interfaces in each of these three subnets are required to have the prefix 223.1.17/24. Also suppose that Subnet 1 is required to support at least 60 interfaces, Subnet 2 is to support at least 90 interfaces, and Subnet 3 is to support at least 12 interfaces. Provide three network addresses (of the form a.b.c.d/x) that satisfy these constraints. | [9 marks] |
| QUESTION 3 |  |
| Consider the following network.     With the indicated link costs, use Dijkstra’s shortest-path algorithm to compute the shortest path from u to all network nodes. Show how the algorithm works by computing the routing table. | [10 marks] |
| What advantage does a circuit‐switched network have over a packet‐switched network? | [8 marks] |
| What are the differences between message confidentiality and message integrity? Can you have confidentiality without integrity? Can you have integrity without confidentiality? Explain your answer. | [9 marks] |
| Can you “decrypt” a hash of a message to get the original message? Explain your answer. | [8 marks] |
| QUESTION 4 |  |
| From a service perspective, what is an important difference between a symmetric-key system and a public-key system? | [7 marks] |
| Suppose Alice wants to send an e-mail to Bob. Bob has a public-private key pair (KB+, KB-), and Alice has Bob’s certificate. But Alice does not have a public, private key pair. Alice and Bob (and the entire world) share the same hash function H(.). In this situation, is it possible to design a scheme so that Bob can verify that Alice created the message?  Is it possible to design a scheme that provides confidentiality for sending the message from Alice to Bob? | [8 marks] |
| Consider sending a stream of packets from Host A to Host B using IPsec. Typically, a new security association (SA) will be established for each packet sent in the stream. True or false? | [8 marks] |
| Consider RSA with p=5 and q=11. What are n and z? Let e be 3. Why is this an acceptable choice for e? Find d such that de=1 (mod z) and d<160. | [12 marks] |