Practice Exercises for the Final

1. The purpose of both distance-vector and link-state protocols is to construct routing tables. What is the difference in their mechanisms?

2. The sequence number field in the TCP header is 32 bits long, which is big enough to cover over 4 billion bytes of data. Even if these many bytes were never transferred over a single connection, why might the sequence number still wrap around from $2^{32} - 1$ to 0?

3. Packet loss and packet jitter can significantly degrade the quality of multimedia streams (at the receiver end). Forward-error correction schemes address these problems by adding redundancy to the original packet stream, thus allowing the receiver to reconstruct approximations of the original packet stream in the presence of packet loss and packet jitter. Describe one forward error correction scheme for multimedia streaming.

4. Recall that the Address Resolution Protocol (ARP) is a protocol for translating IP addresses into hardware addresses (also referred to as Ethernet or MAC addresses). The ARP entries at a node in a local area network usually time out after 10-15 minutes. Describe the problems that can occur if the timeout value is too small or too large.

5. Consider our symmetric-key based authentication protocol in which Alice authenticates herself to Bob as follows: (i) Alice sends an "I am Alice" message to Bob; (ii) Bob chooses a nonce R and sends it to Alice; (iii) Alice encrypts the nonce using the shared key K_{A-B} and sends the cipher text to Bob; and (iv) Bob decrypts the received message and compares with the nonce.

Suppose that while Alice is authenticating herself with Bob, Bob must authenticate himself with Alice. Describe a scenario in which Trudy, pretending to be Alice, can now authenticate herself to Bob as Alice.

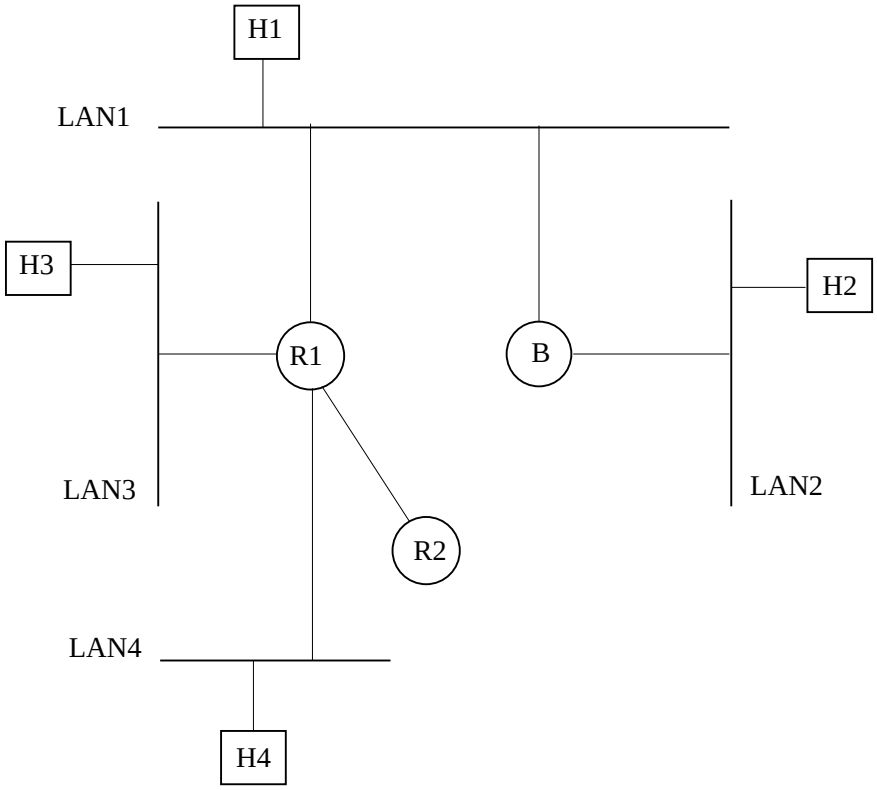
6. A message with data 1001000 is to be sent using the standard CRC method, with the CRC generator 1001. Calculate the actual bit string transmitted.

7. An organization has a network address of 210.10.10. As shown below, the network is organized as 4 Ethernet LANs, two of which are connected to each other through a bridge, and the entire network is connected via a router. LAN1 has 27 hosts, LAN2 has 72 hosts, and LAN3 has 54 hosts, and LAN4 has 20 hosts.

(a) Give a possible arrangement of subnet numbers and subnet masks to make the above organization possible.

(b) Draw the routing table at router R1. The fields of the table are SubnetNumber, SubnetMask, and NextHop. Set the default entry to be R2. (You may assign your own labels to all interfaces of R1.)

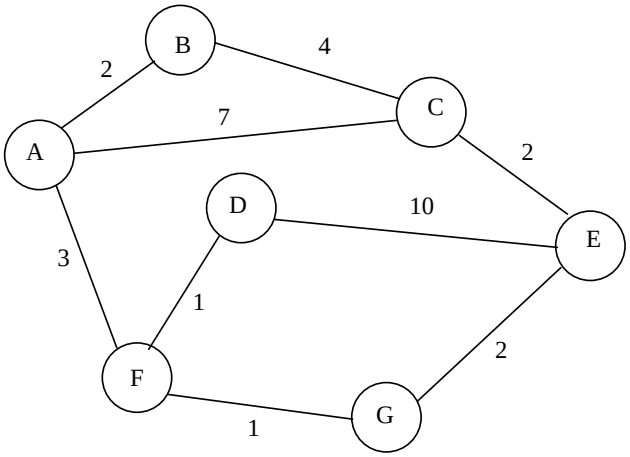
(c) Choose IP addresses for all interfaces of H1, H2, H3, H4, and R1.



(d) Now H1 sends a UDP packet to H3 and H3 replies with another UDP packet to H1. Initially, none of the hosts or routers know the Ethernet addresses of any interfaces. H1 knows the IP address of H3. Show the flow of packets sent and received in the process of this exchange. Specify the source and destination IP addresses, Ethernet addresses of the packets and the type of protocols that are used.

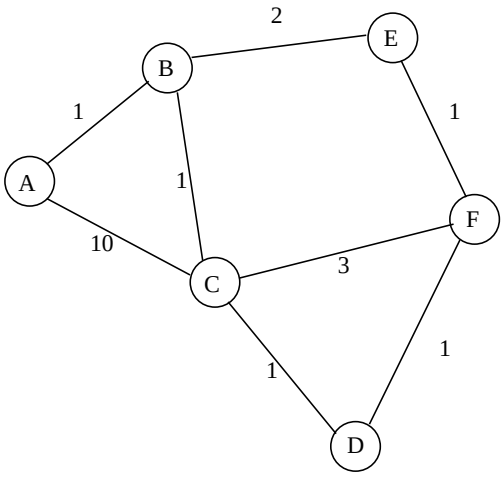
8. Suppose we use the distance vector protocol to compute the distances and next hops between different node pairs. Given the initial distance vector table (the first table), fill in the distance vector table entries of node A (the second table) after one round of distance vector exchange with its neighbors.

Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A	0	2	7	4	∞	3	3
B	2	0	4	∞	∞	∞	∞
C	7	4	0	∞	2	∞	4
D	4	∞	∞	0	10	1	2
E	∞	∞	2	10	0	3	2
F	3	∞	∞	1	3	0	1
G	4	∞	4	2	2	1	0



Information Stored at Node	Distance to Reach Node						
	A	B	C	D	E	F	G
A							

9. By computing the shortest path from node B to every other node in the following graph, determine the forwarding table that is stored at node B (assuming the network has reached a steady state).



10. Using RSA, choose $p = 3$ and $q = 11$, and encode the word "hello". Apply the decryption algorithm to the encrypted version to recover the original plaintext.