B1. Networks (25 points)

1. (25 pts) Security
   a. Explain 4 desirable properties of secure communications.
   b. Enumerate 3 general types of security attacks on computer and network systems.
   c. For each type in (b), explain 1 way to counter the attack.
   d. A sender S wants to send a plaintext P to a receiver R across a network using public key cryptography. Show the encryption and decryption steps needed to transmit P from S to R. How does R know that the incoming message is from the valid S?

B2. Networks (25 points)

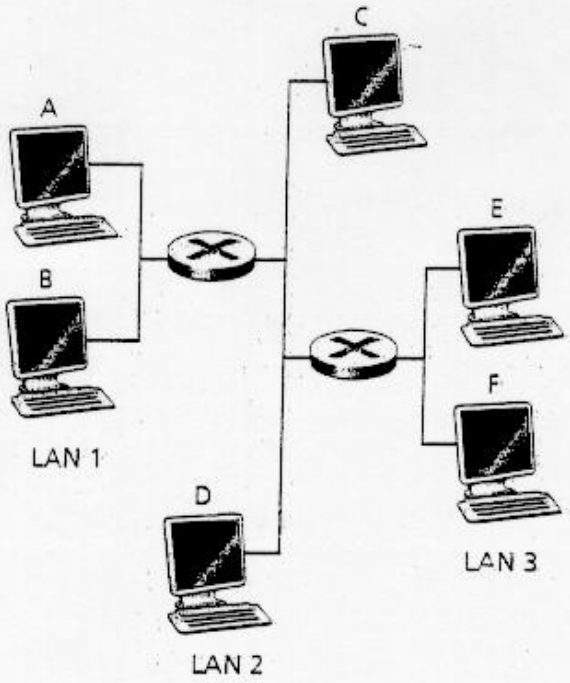
2. (25 pts) Using dotted-decimal/prefix notation, consider the network address 10.23.16.0/21

Note: $10_{10} = 00001010_2$ $23_{10} = 00010111_2$ $16_{10} = 00010000_2$ $21_{10} = 00010101_2$

a. (2 pts) How many potential hosts may exist in this network?
b. (3 pts) What are the host addresses in this network? (Give your answer as a range of two dotted-decimal addresses.)
c. (4 pts) From this network, allocate 5 subnets – 3 with exactly 16 host addresses, and 2 with exactly 8 host addresses. (Give your answers in dotted-decimal/prefix notation.)

Consider three LANs interconnected by two routers, as shown in the figure below.

d. (2 pts) Annotate the diagram to include adapters interfaces.
e. (3 pts) Assign IP addresses to all interfaces. For LANs 1,2,3, respectively use addresses from the 3 subnets with 16 hosts that you defined in part (b).
f. (2 pts) Assign MAC addresses to all of the interfaces. Use whatever addresses you want.
g. (5 pts) Consider sending a network layer packet, that is, an IP-Protocol Data Unit (PDU), from host B to host E. Assume all host and router ARP tables are up-to-date. Show all of the Ethernet-PDUs that will be generated. For each Ethernet-PDU generated, indicate clearly what are the MAC source/destination, and IP source/destination addresses.
h. (4 pts) Same question as (g) except now assume the ARP table in host B is empty, and all other ARP tables are all up-to-date. Show all additional Ethernet-PDUs that will be generated, i.e., Ethernet-PDUs that were not generated in your answer for (g). Indicate clearly what are the MAC and IP addresses in each of these additional Ethernet-PDUs.



B3. Networks (25 points)

3. (25 pts) Consider Link State and Distance Vector Routing. To help avoid ambiguity, please denote the protocol data units (PDUs) that the routers send between themselves in order to build up routing tables as "routing PDUs". Denote the generic IP packets that are later routed on the basis of each router's routing table – "IP-PDUs."
   a. (8 pts) Explain how routing tables are derived using Distance Vector routing.
   b. (8 pts) Explain how routing tables are derived using Link State routing.
   c. (9 pts) Explain and discuss the advantages and disadvantages of the two approaches.

   For (a) and (b), be sure to include a specification of what information is in a routing PDU, and how a router may or may not change its routing table in reaction to the receipt of a routing PDU. Use examples to help clarify your answer.

B4. Networks (25 points)

4. (25 pts) LANs
   a. (5 pts) What are the differences between an Ethernet switch and an Ethernet hub? Explain their relative advantages and disadvantages.
   b. (10 pts) Why is it required that the link layer packet (i.e., L-PDU) on a network using carrier sense multiple access with collision detection (CSMA/CD) not be "too small" (In other words, why is there a specified minimum size Ethernet-PDU?) Explain precisely how this minimum size is calculated.
   c. (10 pts) Unlike the IEEE 802.3 Ethernet protocol, the 802.11 MAC protocol for wireless networks does not implement collision detection. Rather, 802.11 implements collision avoidance. Explain two reasons why 802.11 does not perform collision detection.