1. What is flooding? Explain the need for sequence number and age in packets that are flooded.

Packets received over one interface of a node are relayed over all other interfaces. Sequence number keeps flooding in check as a packet with a specific source and sequence number can be relayed only once. Nodes remember the highest sequence number corresponding to every source and packets with lower sequence numbers are rejected. Age helps in ensuring that wrapping around of sequence numbers does not affect the process of deciding the higher sequence number.

2. What are the main differences between distance vector and link-state routing?

In DV algorithms information regarding every router in the subnet is conveyed to all neighbors. In LS information regarding neighbors is flooded to every node in the subnet. DV permits every node to learn the best next hop to reach a destination, and the cost of the path. LS enables routers to learn the complete topology.

3. An IP packet received by a router has a 20 byte header with source/dest address X/Y respectively, identification Z, and a payload of size 1000. The layer-2 protocol used by the router does not support payload sizes greater than 400. Indicate the contents of the IP packets before and after fragmentation. Make reasonable assumptions, and indicate the values in the IP headers of the received unfragmented packet and every fragment that is sent.

IP packets will need to be fragmented. All fragments have to be smaller than 380 bytes. So we need three fragments, and the payload size in first two fragments should be a multiple of eight – for example 376 bytes. (47x8 = 376) So 376 bytes in first two fragments and 248 in the third. In all three fragments all header fields will be the same except MF bit, offset and checksum. The first two will have MF flag set to 1. The offsets will be 0 in the first packet, 47 in the second and 94 in the third. Offset 47 in the second fragment indicates that the 376th byte is the first payload byte in the fragment. Offset 94 in the third fragment indicates that the 752nd byte is the first payload byte in the fragment.

4. A NAT with a public IP address 130.207.16.32 receives an IP packet source address 10.2.5.1 and destination IP 146.7.5.1, carrying a TCP payload with source port number 12345 and destination port 44. Make reasonable assumptions and depict the contents of the packet when it leaves the NAT.

The source IP is changed from 10.2..5.1 to 130.207.16.32
The source port number 12345 is changed to an available port number (say 20000) in the NAT
An entry is made of the form
10.2.5.1, TCP, 12345, 20000, TS=x
The record with a stale time stamp may be cleared.