2)

|  |  |  |  |
| --- | --- | --- | --- |
| Subnet | Host Range | Broadcast | Subnet Mask |
| 194.10.1.0 | 194.10.1.1 – 194.10.1.2 | 194.10.1.3 | 255.255.255.252 |
| 194.10.1.4 | 194.10.1.5 – 194.10.1.34 | 194.10.1.35 | 255.255.255.224 |
| 194.10.1.36 | 194.10.1.37 – 194.10.1.66 | 194.10.1.67 | 255.255.255.224 |
| 194.10.1.68 | 194.10.1.69 – 194.10.1.130 | 194.10.1.131 | 255.255.255.192 |

a)

b) Yes, it would be possible using a /26 subnet as 4 subnets would be created each with 62 usable host addresses. This is enough for each subnet needed in the network above.

3)

a)

i) The routing tables contains the destination address of the data and the interface over which it should be sent. For the routing function the tables are used to send data to the correct destination running a routing function also populates the routing table, for the forwarding function the protocol will look up the destination address and forward the packet to the next hop.

ii) The data plane routes traffic based on control plane logic, therefor it is a data plane function.

b)

i) The router shares each subnet connected to it, the network address and subnet mask in dot decimal form are usually shared.

ii) Any other router on the network that is running the same routing protocol.

c)

i) DA = [6, 10, infinite]

ii) Router A receives DB and DC from routers B and C.

DB = [6, 1, 9]

DC = [10, 1, 2]

Router A then updates its distance vectors.

DA(B) = min(6,11) = 6

DA(C) = min(10, 7) = 7

DA(D) = min(12,15) = 12

Updated DA = [6, 7, 12]

iii) Redistribute DA to surrounding routers.

4)

a) The transport layer allows processes to communicate logically, the network layer allows hosts to communicate.

b) The transport layer will optimise congestion control for applications on the network by changing the transmission speed to match the capacity available in the network. If this is still not enough to eliminate congestion, routers will send information to end devices to help troubleshoot. At this point the building of a new network that is more suited to the volume of traffic occurring may be the only option.

c) In connectionless demultiplexing, the socket is identified by the destination IP address and the destination port number. When the host receives segment, it checks the destination port number and directs the segment to the socket with that port number. In connectionless demultiplexing, the socket is identified by: the source IP address, source port number, destination IP address and destination port number. All these values are used to send data segments to the correct destination socket.

d) In the stop-and-wait protocol, the sender transmits a packet and waits for the receiver to transmit a special acknowledgment packet, then the sender can continue and transmit the next packet. This helps data integrity by making sure the receiver has every packet, eliminating the possibility of incomplete data. If the sender transmits a packet and does not receive an acknowledgment packet, the sender will time out and resend the packet until the receiver acknowledges that it has been received. Using checksums removes the possibility of the receiver acknowledging a corrupted packet as legitimate data. Using a set CRC such as CRC-4(x4+x+1) gives us the checksum of 10011, if the received data is divided by 10011 and the result is not zero then the data is corrupted, and a retransmission will occur.