1.

a. No, we can’t. An IP address consists of two parts: network part and host part. The network part is determined by the network interface. Therefore, we can’t assign an arbitrary IP address to a computer connected to a network.

b. 8190. For the mask 255.255.224.0, the network part is 19 bits long and the host part is 13 bits long. Therefore, the maximum number of hosts it can handle will be 2^13 - 2 = 8190.

c. No. In an IP packet, there is a field called Time to live (TTL). The TTL value can be thought of as an upper bound on the time that an IP datagram can exist in an Internet system. If the IP packet exists longer than the TTL value, it will be dropped. Therefore, an IP packet can not loop forever inside an IP network.

d. In every IP datagram, there is a field called “Identification” which is primarily used for uniquely identifying the group of fragments of a single IP datagram. By comparing the identification of IP datagrams, we can know whether the two datagrams belong to one single original IP datagram.

e. The main reason is that network links have maximum transfer size (MTU). In network links, datagrams that are larger than MTU have to be fragmented. Because of MTU, if intermediate routers reassemble datagrams, fragmentation will happen again and it only wastes time and causes delays. Therefore, IP datagram reassembly should only be done at the destination host.

2.

a. TCP congestion control uses a congestion window that limits the amount of data the TCP can send into the network to avoid network congestion. TCP congestion control also enables an algorithm to control the size of the congestion window based on different events.

b. CongWin = 8 KB and threshold = 12 KB. Since CongWin < threshold, the sender is a slow-start phrase. The congestion window will double its size after receiving the correct ACK and threshold does not have any change.

c. CongWin = 17 KB and threshold = 12 KB. Since CongWin > threshold, the sender is at a congestion avoidance phrase. The congestion window will increase its size by 1 MSS after receiving the correct ACK and threshold does not have any change.

d. CongWin = 1 KB and threshold = 12 KB. Since CongWin > threshold, the sender is at a congestion avoidance phrase. The congestion window will immediately decrease to 1 MSS after a timeout event and threshold will become half of the previous congestion window.

e. 24 KB is the maximum amount of data the sender can send in the next round. When a triple duplicate ACKs event occurs, threshold will be set to CongWin/2, and CongWin will be set to threshold, which is 24 KB. In addition, since 24 KB is smaller than 30 KB, which is the size of the receiver advertisement window, sending 24 KB would not cause overflow in the receiver’s buffer.

3.

a. TCP flow control ensures that the sender cannot send more bytes than space that is available in the receiver’s buffer. The receiver uses a receiver window to determine how much space is left in the receiver’s buffer and it would tell the sender the current size of its receiver window each time it sends an acknowledgment packet. TCP on the send's side can only transmit data when the window size is not zero.

b.

a) The intervals of time when TCP slow start is operating are [1, 6] and [23, 26].

b) The intervals of time when TCP congestion avoidance is operating are [6, 16] and [17, 22].

c) After the 16th transmission round, segment loss was detected by a triple duplicate ACK.

d) After the 22nd transmission round, segment loss was detected by a timeout.

4.

a.

Prefix	Link Interface
11100000 00	0
11100000 01000000	1
11100001 0	2
11100000	2
otherwise	3

b.

There is no specific prefix in the table that matches 11001000 10010001 01010001 01010101. Therefore, it would be forwarded to link interface 3.

11100001 01000000 11000011 00111100 matches the third prefix in the table. Therefore, it would be forwarded to link interface 2.

11100001 10000000 00010001 01110111 does not match any prefix in the first four entries. Therefore, it would be forwarded to link interface 3.

5.

a. In circuit switching, a dedicated path (e.g. cables) has to be established. Data transmission is fast and each node does not need to have any storage facility.
In virtual circuit switching, no dedicated path is actually established. It requires a storage facility and has packet transmission delay.

b.

Assume that the lowest unused VCI starts from 1.

VC Translation table of Router 1:

Input Port	Input VCI	Output Port	Output VCI
0	1	1	1
4	1	1	2
4	2	1	3
1	1	2	1
1	2	2	2

VC Translation table of Router 2:

Input Port	Input VCI	Output Port	Output VCI
3	1	0	1
3	2	1	1
3	3	2	1
2	1	3	1
0	1	3	2

VC Translation table of Router 3:

Input Port	Input VCI	Output Port	Output VCI
0	1	3	1
0	2	1	1

VC Translation table of Router 4:

Input Port	Input VCI	Output Port	Output VCI
3	1	1	1

VC Translation table of Router 5:

Input Port	Input VCI	Output Port	Output VCI
3	1	1	1

6.

a. First, host X will look up the MAC address of host Z in its ARP cache. But since there is no MAC address of host Z in its ARP cache, it will broadcast ARP request packets, asking for the MAC address of host Z. Switch S will detect a message sent from port 2. It will add a new entry that matches the MAC address and port number of host X in its switch table and continue the broadcast. After host Z receives the ARP packet, it will send a response to A with its MAC address through switch S. Switch S will add a new entry that matches the MAC address and port number of host Z in its switch table. Finally host X gets the MAC address of host Z from the ARP response message.

   Yes. Router R will also receive the ARP request. Router R will add a new entry containing the IP and MAC address of host X in its ARP table. But router R will not receive the ARP response message from host Z because that is sent by unicast.

   First, host X will send an IP datagram that contains the MAC address of host Z through the link to switch S. Switch S will look up the destination MAC address of the incoming datagram in its switch table and know that the MAC address is matched to port 3. Then switch S will forward the datagram to host Z from port 3.

b. First, host X will look up the MAC address of host H in its ARP cache. Since the MAC address of host H is cached, host X will directly send a normal IP datagram to host H. In the halfway, switch S will detect an incoming datagram from port 2 and it will add a new entry that matches the MAC address of host X and the port number in its switch table. Since switch S has already known host H is at port 1, it will forward the IP datagram to host H through port 1.

   No. The router will not receive any message (either ARP request or ARP response) because there is no broadcasting involved.

   First, host X will send an IP datagram that contains the MAC address of host H through the link to switch S. Switch S will look up the destination MAC address of the incoming datagram in its switch table and know that the MAC address is matched to port 1. Then switch S will forward the datagram to host H from port 1.

c. No. Because server W is not on the same network as host X, host X will not use ARP to map the IP address of server W to a physical Ethernet address.

   First, host X can find that server W is on a different network by comparing its subnet mask with the IP address of server W. Host X will look in its routing table for a router to the destination network, and then it will send its IP datagram to the appropriate (or default) router. In this case, it would forward the IP datagram to router R.

   Same as the above question, host X will send the datagram to router R. The destination IP and MAC addresses of the datagram are host X's. The destination IP address of the datagram is server W's but the destination MAC address is router R's. The datagram will go through switch S. It will detect that the incoming datagram is from port 1 and update its switch table with the MAC address of host X and port number 1. Then switch S will look up the destination MAC address of the datagram in its switch table and find out the port number mapped to the address. Finally, switch S will forward the datagram to router R through port 0.

7.

a. 1. After R1 receives the IP packet from host C, R1 checks its routing table and obtains the IP address 128.105.0.0 of the next hop, R2, on the route to the data packet's destination.
   2. Since R1 can identify R2 and the source IP address of the packet is actually on the same network, an ICMP Redirect message is sent to the host. The ICMP Redirect message advises the host C to send its traffic for the IP address 128.105.0.0 directly to R2 as this is a shorter path to the destination.
   3. R1 forwards the original data packet to the next hop, R2 .
   4. Finally, since R2 has the MAC address of host B, R2 delivers the IP packet to host B from port 1.

b. No, host C will not send another IP packet to router R1. Instead, it will send the packet to R2. To obtain R2's MAC address, host C will broadcast an ARP request to all the hosts on its network, including R2. Then R2 will know host C is asking for its MAC address and it will send back a ARP response to host C via unicast. Finally, host C can obtain the MAC address of host C from the ARP response and add it to its ARP table.

c. No, router R2 will not send an ICMP Redirect message to router R1. This is because ICMP messages are always sent to the source IP address of an IP packet and that is host C's IP address.
   No, the network layer at R2 cannot tell whether router R1 or host C send the packet to it. Because both of the source and destination IP addresses of the IP packet will not be changed throughout the whole transmission and the MAC address is not a network layer

address, R2 can’t tell whether R1 or host C send the packet to it solely based on the IP address.

d. The ICMP router discovery messages are called "Router Advertisements" and "Router Solicitations". Each router periodically multicasts a Router Advertisement from each of its multicast interfaces, announcing the IP address(es) of that interface. Since R3 and R1 are directly connected to switch S2, R1 will receive an ICMP router discovery message from R3 and know that R3 is directly connected to LAN3, which is a more preferred route source. Then R1 will replace R2 with R3 as “Next hop” in that entry for destination network prefix 131.16.143.0/20.

e. Router R3 may not be connected to switch S2 in the first place. Before R3 is connected to S2, R1, R2, R3 are not in the same network group. Therefore, the IP packet that is sent from LAN2 to LAN3 has to be forwarded to R2 first, and then R2 forward the packet to R3 through S1. That may explain why R1 has a “non-optimal" route entry that has router R2 as the next-hop to the destination network prefix 131.16.143.0/20 instead of router R3 in the first place.