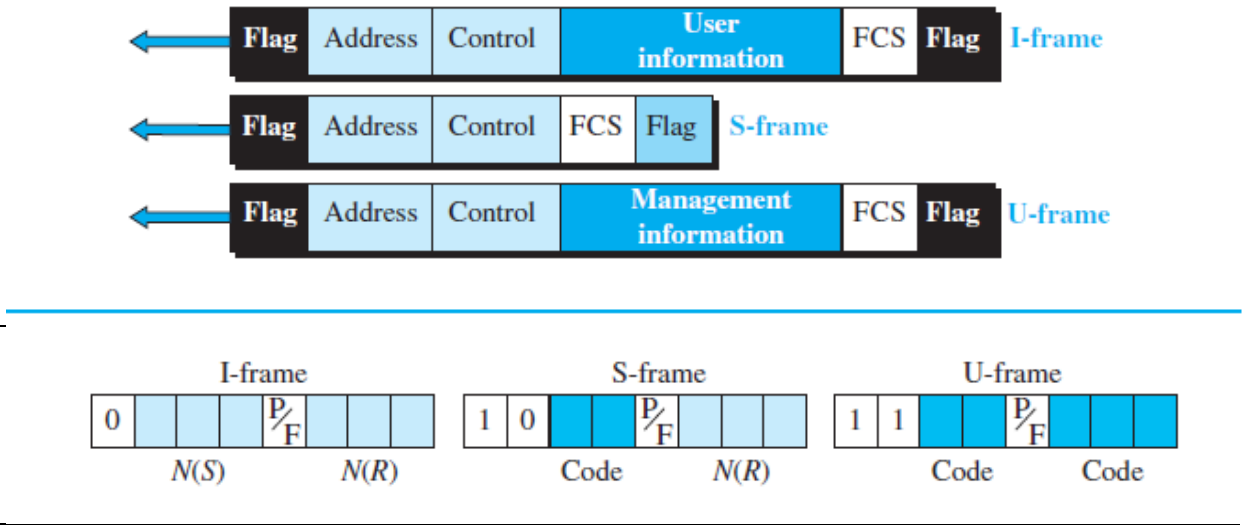
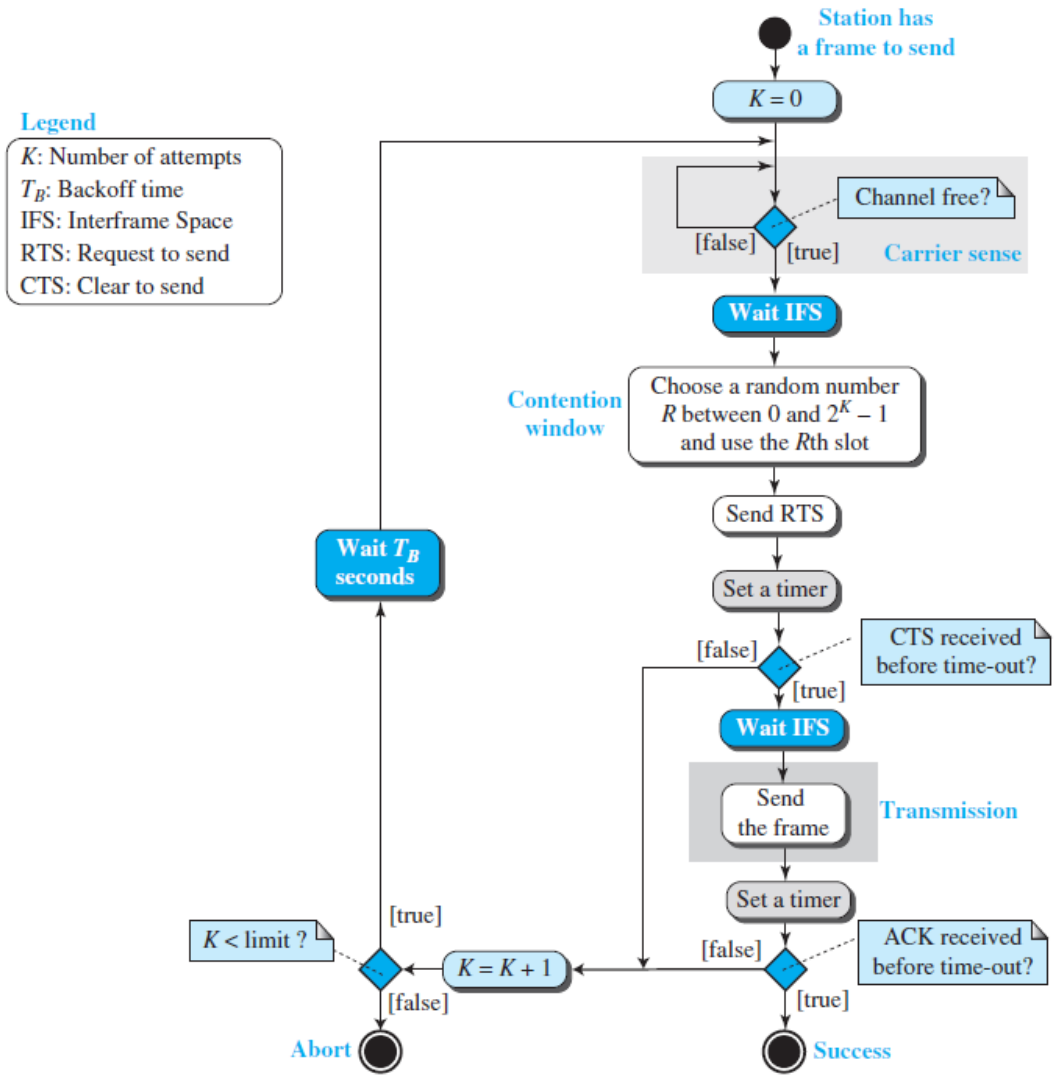
20ITT51 Computer Networks

CAT 2 Answer Key

1.	The bit-stuffed frame payload is 000111110110110111101010001111101111111100001110
2.	1. Password Authentication Protocol (PAP): Challenge Handshake Authentication Protocol (CHAP)
3.	piggybacking, additional data or control information is included in the same frame or packet as the primary data being transmitted. This additional information is typically related to acknowledgments (ACKs) or flow control, such as indicating the successful receipt of previously transmitted data or requesting retransmission of lost or corrupted data. Improved efficiency: Reduced latency Enhanced reliability Simplified protocol design
4.	Slot Duration = Frame Size / Transmission Rate Slot Duration = 1000 bits / 1 Mbps Slot Duration = 1000 microseconds In a slotted Aloha network, the vulnerable time is typically considered to be one slot duration. This is because if two or more stations start transmitting at the beginning of a slot, their frames will collide. Therefore, during the entire slot duration, collisions can occur. So, in this case, the vulnerable time for the network is 1000 microseconds or 1 millisecond.
5.	First, let's convert the frame size from bytes to bits: Frame Size = 1000 bytes * 8 bits/byte Frame Size = 8000 bits Next, we need to calculate the time it takes to transmit one frame. In Ethernet, the transmission rate is typically 10 Mbps (megabits per second). Transmission Time for One Frame = Frame Size / Transmission Rate Transmission Time for One Frame = 8000 bits / 10 Mbps Transmission Time for One Frame = 0.8 milliseconds (ms) Now, we can calculate the number of frames that can be transmitted during the 2 ms noise: Number of Frames Destroyed = Noise Duration / Transmission Time for One Frame Number of Frames Destroyed = 2 ms / 0.8 ms Number of Frames Destroyed = 2.5 frames
6.	A hub and a repeater are related in the sense that a hub can be considered a multi-port repeater or a multiple-port extension of a repeater. A repeater is a network device that regenerates or amplifies signals received on one port and transmits them to all other ports. Its purpose is to extend the reach of a network by boosting the signal strength and compensating for signal degradation over long distances.
7.	A.130.34.54.12 is a Class B IP address. b. 200.34.2.1 is a Class C IP address.
8.	he correct answer is option c. 255.255.255.6 cannot be a valid mask in CIDR (Classless Inter-

	Domain Routing).
9.	Flow control is not available in the Network layer of the TCP/IP protocol suite because it is more appropriate to be implemented at the transport layer. The Network layer focuses on routing and forwarding packets across networks, and implementing flow control at this layer would introduce complexity, hinder network independence, and potentially impact overall network performance.
10.	No, the value of the header length field in an IPv4 packet cannot be less than 5. The header length field specifies the length of the IPv4 header in 32-bit words (4-byte units). Since each word is 4 bytes long, the minimum header length is 5 words, which corresponds to 20 bytes. In the IPv4 header, the header length field is a 4-bit field, allowing values from 0 to 15. However, the field is multiplied by 4 to calculate the actual header length in bytes. Therefore, a value of 5 in the header length field corresponds to a header length of 5 * 4 = 20 bytes. The header length field is used to indicate the size of the IPv4 header, which can vary depending on the optional fields present in the header, such as options or extensions. If there are no optional fields, the header length will be 20 bytes (5 words). If there are additional options or extensions, the header length will be larger, but it will always be a multiple of 4 bytes due to the 32-bit word alignment requirement in IPv4.
PART B	
11.	

12.	To calculate the time it takes for the first bit to reach the destination, the time it takes for the last bit to reach the destination after the first bit has arrived, and the duration of the network's involvement with the frame (vulnerable to collision), we need to consider the propagation delay and the frame transmission time. Given: Propagation delay = 5 microseconds Frame transmission time = 10 microseconds a. Time for the first bit to reach the destination: The first bit will reach the destination after the propagation delay. Therefore, it takes 5 microseconds for the first bit to reach the destination. b. Time for the last bit to reach the destination after the first bit has arrived: The last bit will take additional time to reach the destination after the first bit has arrived. This additional time is equal to the frame transmission time. Therefore, it takes an additional 10 microseconds for the last bit to reach the destination after the first bit has arrived. c. Duration of the network's involvement with this frame (vulnerable to collision): The network is involved with the frame from the moment the first bit is transmitted until the last bit reaches the destination. This includes both the propagation delay and the frame transmission time. Therefore, the network is involved with this frame for a total time of 5 microseconds (propagation delay) + 10 microseconds (frame transmission time) = 15 microseconds.



13. a. The block 16.12.64.0/20 represents a block of IP addresses with a network prefix of 20 bits. The network prefix specifies the number of bits allocated for the network portion of the address.

To find the number and range of addresses in the ISP block, we can calculate the number of addresses based on the network prefix. In this case, the network prefix is /20, which means there are 20 network bits and 12 host bits.

The formula to calculate the number of addresses is 2^(32 - network prefix). Applying this formula, we have 2^(32 - 20) = 2^12 = 4096 addresses.

The range of addresses in the ISP block is from 16.12.64.0 to 16.12.79.255.

b. Each organization needs 256 addresses. Since each organization requires a block of addresses that is a power of 2, we can determine that each organization needs a network prefix of /24 (2^8 = 256).

To calculate the range of addresses for each organization, we can start with the first

	organization using the network address 16.12.64.0/24 and the broadcast address 16.12.64.255/24. The next organization can start from the next available network address, which is 16.12.65.0/24, and so on. The range of addresses for each organization is as follows: Organization 1: 16.12.64.0 to 16.12.64.255 Organization 2: 16.12.65.0 to 16.12.65.255 Organization 3: 16.12.66.0 to 16.12.66.255 Organization 4: 16.12.67.0 to 16.12.67.255 Organization 5: 16.12.68.0 to 16.12.68.255 Organization 6: 16.12.69.0 to 16.12.69.255 Organization 7: 16.12.70.0 to 16.12.70.255 Organization 8: 16.12.71.0 to 16.12.71.255 The range of unallocated addresses would be from 16.12.72.0 to 16.12.79.255. c. The outline of the address distribution and the forwarding table would look like this: ISP Block: 16.12.64.0/20 Organization 1: 16.12.64.0/24 Organization 2: 16.12.65.0/24 Organization 3: 16.12.66.0/24 Organization 4: 16.12.67.0/24 Organization 5: 16.12.68.0/24 Organization 6: 16.12.69.0/24 Organization 7: 16.12.70.0/24 Organization 8: 16.12.71.0/24 Forwarding Table: Destination: 16.12.64.0/20, Next Hop: ISP Gateway Destination: 16.12.64.0/24, Next Hop: Organization 1 Gateway Destination: 16.12.65.0/24, Next Hop: Organization 2 Gateway Destination: 16.12.66.0/24, Next Hop: Organization 3 Gateway Destination: 16.12.67.0/24, Next Hop: Organization 4 Gateway Destination: 16.12.68.0/24, Next Hop: Organization 5 Gateway Destination: 16.12.69.0/24, Next Hop: Organization 6 Gateway Destination: 16.12.70.0/24, Next Hop: Organization 7 Gateway Destination: 16.12.71.0/24, Next Hop: Organization 8 Gateway Default Route: Next Hop: ISP Gateway
14	***Congestion Control*** Congestion control refers to techniques and mechanisms that can either prevent congestion before it happens or remove congestion after it has happened. In general, we can divide congestion control mechanisms into two broad categories: **open-loop congestioncontrol** (prevention) and **closed-loop congestion control** (removal). ***Open-Loop Congestion Control*** . ***Retransmission Policy*** ***Window Policy***

	Acknowledgment Policy **Figure 18.13** ***.Discarding Policy*** ***Admission Policy*** ***Closed-Loop Congestion Control*** ***Backpressure*** **Figure 18.14** **Backpressure Backpressure Backpressure** **528** ***Choke Packet*** ***Implicit Signaling*** ***Explicit Signaling***