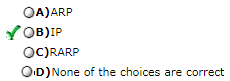
**UNIT-I**

**Multiple Choice Questions**

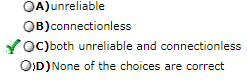
Note: **All the correct answer for each question is indicated by a  symbol.**

**1. Topic: IP Datagram, IP fragmentation**

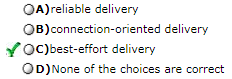
1. The \_\_\_\_\_\_\_\_ protocol is the transmission mechanism used by the TCP/IP suite.



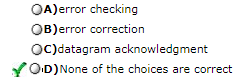
1. IP is \_\_\_\_\_\_\_\_\_ datagram protocol.



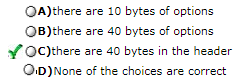
1. The term \_\_\_\_\_\_\_\_ means that IP provides no error checking or tracking. IP assumes the unreliability of the underlying layers and does its best to get a transmission through to its destination, but with no guarantees.



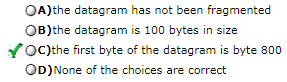
1. A best-effort delivery service such as IP includes \_\_\_\_\_\_\_.



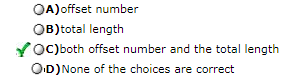
1. An HLEN value of decimal 10 means \_\_\_\_\_\_\_.



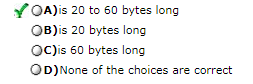
1. If the fragment offset has a value of 100, it means that \_\_\_\_\_\_\_.



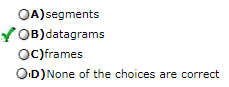
1. What is needed to determine the number of the last byte of a fragment?



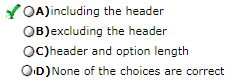
1. The IP header size \_\_\_\_\_\_\_.



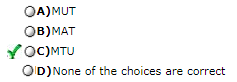
1. Packets in the IP layer are called \_\_\_\_\_\_\_\_\_.



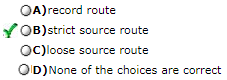
1. The total length field defines the total length of the datagram \_\_\_\_\_\_\_\_\_.



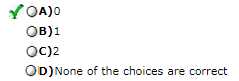
1. When a datagram is encapsulated in a frame, the total size of the datagram must be less than the \_\_\_\_\_\_\_.



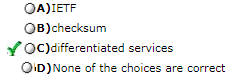
1. Which IP option is used if exactly four specific routers are to be visited by the datagram?



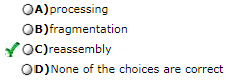
1. For the timestamp option, a flag value of \_\_\_\_\_\_\_ means that each visited router adds only the timestamp in the provided field.



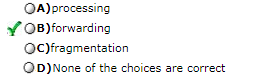
1. The IP header field formerly known as the service type field is now called the \_\_\_\_\_\_\_ field.



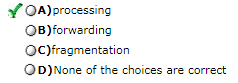
1. The \_\_\_\_\_\_\_ module takes fragments of a message and puts them back in order.



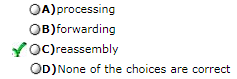
1. The \_\_\_\_\_\_\_ module sends out an IP packet, the next-hop address, and interface information.



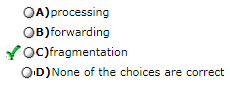
1. The \_\_\_\_\_\_\_ module discards datagrams with a TTL value of zero.



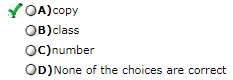
1. The output of the \_\_\_\_\_\_\_ module is an IP packet destined for an upper-layer protocol.



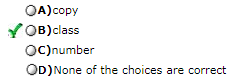
1. The \_\_\_\_\_\_\_ module consults the MTU table to determine the packet size necessary for transmission.



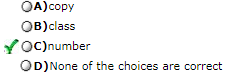
1. The value of the \_\_\_\_\_\_\_\_ subfield in an option controls the presence of the option in fragmentation.



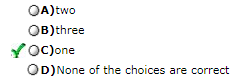
1. The value of the \_\_\_\_\_\_\_\_ subfield defines the general purpose of an option.



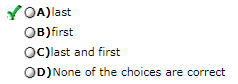
1. The value of the \_\_\_\_\_\_\_\_ subfield defines the types of an option.



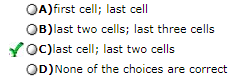
1. Only \_\_\_\_\_\_ end of option option can be used in a datagram.



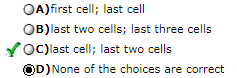
1. When we use IP over ATM, only the \_\_\_\_\_\_\_\_ cell carry(ies) the 8-byte trailer added to the IP datagram.



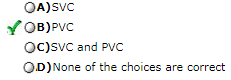
1. When we use IP over ATM, padding can be added only to the \_\_\_\_\_ or the \_\_\_\_\_\_\_.



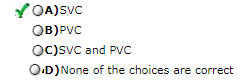
1. To find the physical address of the exiting-point router, ATM uses the services of \_\_\_\_\_\_\_\_\_.



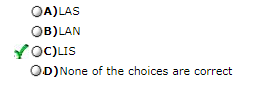
1. The inverse request and inverse reply messages can bind the physical address to an IP address in a(n) \_\_\_\_\_\_\_ situation.



1. The request and reply message can be used to bind a physical address to an IP address in a(n) \_\_\_\_\_\_\_ situation.

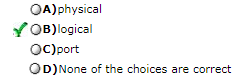


1. \_\_\_\_\_\_\_\_\_\_ allows an ATM network to be divided into several logical subnets.

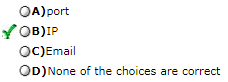


**2. Topic: ARP, RARP**

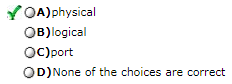
1. A \_\_\_\_\_\_\_ address is an internetwork address with universal jurisdiction.



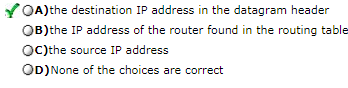
1. The logical addresses in the TCP/IP protocol suite are called \_\_\_\_\_\_\_ addresses.



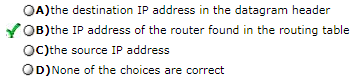
1. A \_\_\_\_\_\_\_\_ is a local address. Its jurisdiction is over a local network.



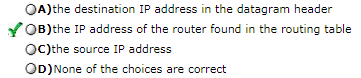
1. If the sender is a host and wants to send a packet to another host on the same network, the logical address that must be mapped to a physical address is \_\_\_\_\_\_.



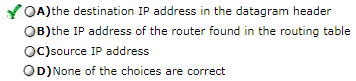
1. If the sender is a host and wants to send a packet to another host on another network, the logical address that must be mapped to a physical address is \_\_\_\_\_\_.



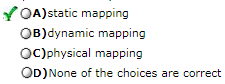
1. The sender is a router that has received a datagram destined for a host on another network. The logical address that must be mapped to a physical address is \_\_\_\_\_\_.



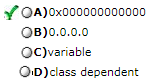
1. The sender is a router that has received a datagram destined for a host in the same network. The logical address that must be mapped to a physical address is \_\_\_\_\_\_.



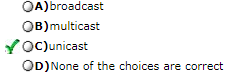
1. In \_\_\_\_\_\_\_, a table associating a logical address with a physical address is updated manually.



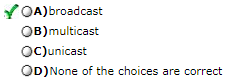
1. The target hardware address on an Ethernet is \_\_\_\_\_\_\_ in an ARP request.



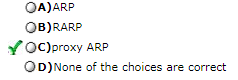
1. An ARP reply is normally \_\_\_\_\_\_\_.



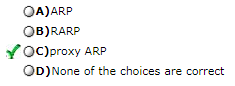
1. An ARP request is normally \_\_\_\_\_\_\_.



1. A technique called \_\_\_\_\_\_ is used to create a subnetting effect.

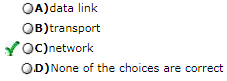


1. A \_\_\_\_\_\_\_ is an ARP that acts on behalf of a set of hosts.

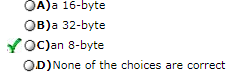


**3. Topic: Internet Control Message Protocol (ICMP)**

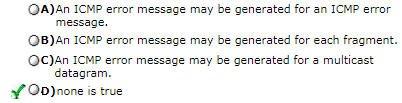
1. ICMP is a \_\_\_\_\_\_\_\_\_ layer protocol.



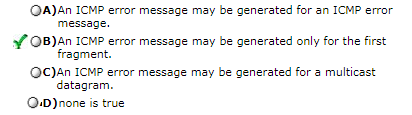
1. An ICMP message has \_\_\_\_\_ header and a variable-size data section.



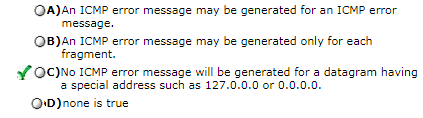
1. Which of the following is true about ICMP messages?



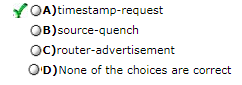
1. Which of the following is true about ICMP messages?



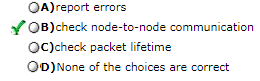
1. Which of the following is true about ICMP messages?



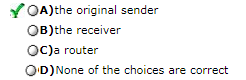
1. If a host needs to synchronize its clock with another host, it sends a \_\_\_\_\_\_\_ message.



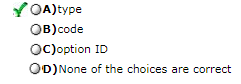
1. The purpose of echo request and echo reply is to \_\_\_\_\_\_\_



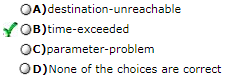
1. In error reporting the encapsulated ICMP packet goes to \_\_\_\_\_\_\_.



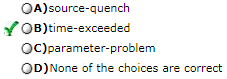
1. What field uniquely identifies the kind of ICMP message (for example, echo reply versus echo request)?



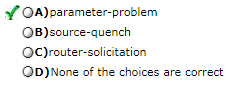
1. When the hop-count field reaches zero and the destination has not been reached, a \_\_\_\_\_\_\_ error message is sent.



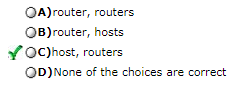
1. When all fragments of a message have not been received within the designated amount of time, a \_\_\_\_\_\_\_ error message is sent.



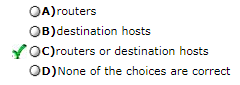
1. Errors in the header or option fields of an IP datagram require a \_\_\_\_\_\_\_ error message.



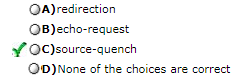
1. A \_\_\_\_\_\_\_ can learn about network \_\_\_\_\_\_\_ by sending out a router-solicitation packet.



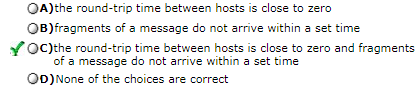
1. Who can send ICMP error-reporting messages?



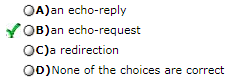
1. One method to alert a source host of congestion is the \_\_\_\_\_\_\_ message.



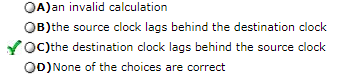
1. A time-exceeded message is generated if \_\_\_\_\_\_\_.



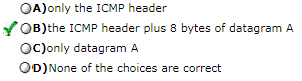
1. To determine whether or not a node is reachable, \_\_\_\_\_\_\_ message can be sent.



1. In calculating the time difference between two clocks, a negative value indicates \_\_\_\_\_\_\_.

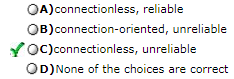


1. An IP datagram (datagram A) cannot reach its destination. An ICMP error message is sent to the source. The data field of the IP datagram (datagram B) that encapsulates the ICMP packet contains \_\_\_\_\_\_\_.

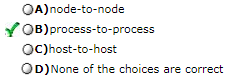


**4. Topic: User Datagram Protocol (UDP)**

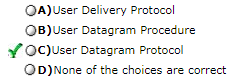
1. UDP is called a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_transport protocol.



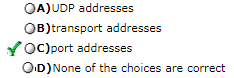
1. UDP does not add anything to the services of IP except for providing \_\_\_\_\_\_\_ communication.



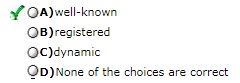
1. UDP is an acronym for \_\_\_\_\_\_\_.



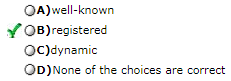
1. The local host and the remote host are defined using IP addresses. To define the processes, we need second identifiers called \_\_\_\_\_\_\_\_\_\_\_\_ .



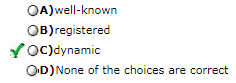
1. The ports ranging from 0 to 1,023 are assigned and controlled by ICANN. These are the \_\_\_\_\_\_\_\_\_\_\_ ports.



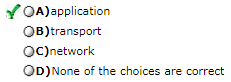
1. The ports ranging from 1,024 to 49,151 are called \_\_\_\_\_\_\_\_\_\_\_ ports.



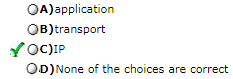
1. The ports ranging from 49,152 to 65,535 can be used as temporary or private port numbers. They are called the \_\_\_\_\_\_\_\_ ports.



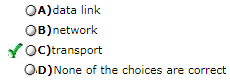
1. In the sending computer, UDP receives a data unit from the \_\_\_\_\_\_\_ layer.



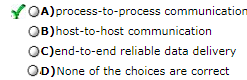
1. In the sending computer, UDP sends a data unit to the \_\_\_\_\_\_\_ layer.



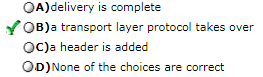
1. UDP and TCP are both \_\_\_\_\_\_\_ layer protocols.



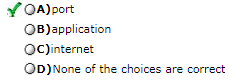
1. Which of the following functions does UDP perform?



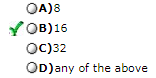
1. When the IP layer of a receiving host receives a datagram, \_\_\_\_\_\_\_.



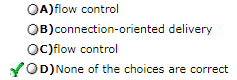
1. UDP needs the \_\_\_\_\_\_\_ address to deliver the user datagram to the correct application process.



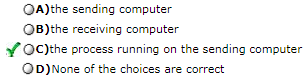
1. A port address in UDP is \_\_\_\_\_\_\_ bits long.



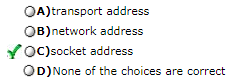
1. Which of the following does UDP guarantee?



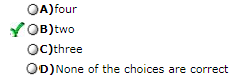
1. The source port address on the UDP user datagram header defines \_\_\_\_\_\_\_.



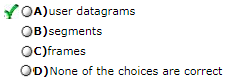
1. The combination of an IP address and a port number is called a \_\_\_\_\_\_\_\_\_\_\_\_.



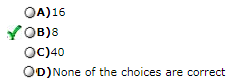
1. To use the services of UDP, we need \_\_\_\_\_\_\_\_ socket addresses.



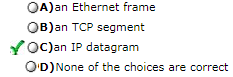
1. UDP packets are called \_\_\_\_\_\_\_\_\_\_ .



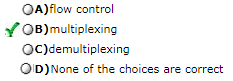
1. UDP packets have a fixed-size header of \_\_\_\_\_\_\_ bytes.



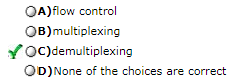
1. UDP packets are encapsulated in \_\_\_\_\_\_\_\_\_\_\_ .



1. UDP uses \_\_\_\_\_\_\_\_ to handle outgoing user datagrams from multiple processes on one host.

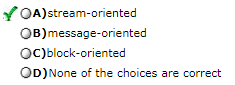


1. UDP uses \_\_\_\_\_\_\_ to handle incoming user datagrams that go to different processes on the same host.

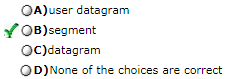


**5. Topic: Transmission Control Protocol (TCP)**

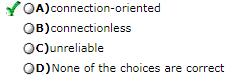
1. TCP is a \_\_\_\_\_\_\_\_\_\_protocol.



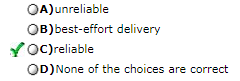
1. TCP groups a number of bytes together into a packet called a \_\_\_\_\_\_\_\_\_\_\_.



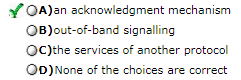
1. TCP is a(n) \_\_\_\_\_\_\_\_\_\_\_ protocol.



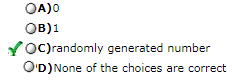
1. TCP is a(n) \_\_\_\_\_\_\_ transport protocol.



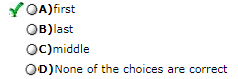
1. TCP uses \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ to check the safe and sound arrival of data.



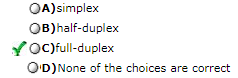
1. The bytes of data being transferred in each connection are numbered by TCP. The numbering starts with a \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



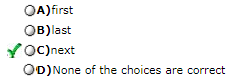
1. TCP assigns a sequence number to each segment that is being sent. The sequence number for each segment is the number of the \_\_\_\_\_\_\_ byte carried in that segment.



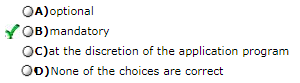
1. Communication in TCP is \_\_\_\_\_\_\_\_\_\_\_.



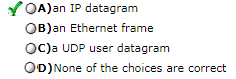
1. The value of the acknowledgment field in a segment defines the sequence number related to the \_\_\_\_\_\_byte a party expects to receive.



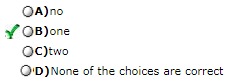
1. The inclusion of the checksum in the TCP segment is \_\_\_\_\_\_\_\_.



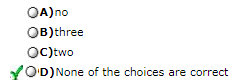
1. The inclusion of the checksum in the TCP segment is \_\_\_\_\_\_\_\_.



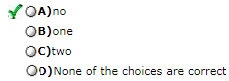
1. A SYN segment cannot carry data; it consumes \_\_\_\_\_ sequence number(s).



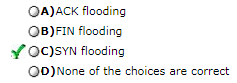
1. A SYN + ACK segment cannot carry data; it consumes \_\_\_\_\_ sequence numbers.



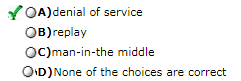
1. An ACK segment, if carrying no data, consumes \_\_\_\_\_\_ sequence number(s).



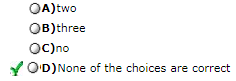
1. The connection establishment procedure in TCP is susceptible to a serious security problem called the \_\_\_\_\_\_\_\_\_ attack.



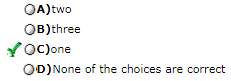
1. The SYN flooding attack belongs to a group of security attacks known as a \_\_\_\_\_ attack.



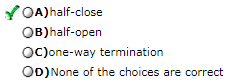
1. The FIN segment consumes \_\_\_\_ sequence numbers if it does not carry data.



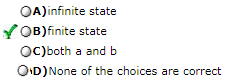
1. The FIN + ACK segment consumes \_\_\_\_\_ sequence number(s) if it does not carry data.



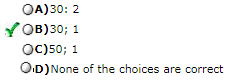
1. In TCP, one end can stop sending data while still receiving data. This is called a \_\_\_\_\_\_.



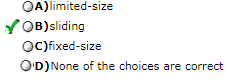
1. A(n) \_\_\_\_\_\_\_\_\_ machine is a machine that goes through a limited number of states.



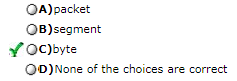
1. A common value for MSL is between\_\_\_ seconds and \_\_\_ minute(s).



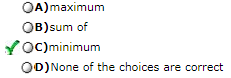
1. To accomplish flow control, TCP uses a \_\_\_\_\_\_\_\_\_\_\_ window protocol.



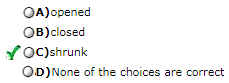
1. TCP sliding windows are \_\_\_\_\_\_\_\_\_\_ oriented.



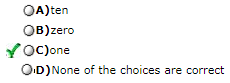
1. In TCP, the size of the send window is the \_\_\_\_\_\_\_\_ of rwnd and cwnd.



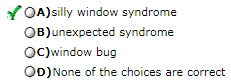
1. In TCP, the window should not be \_\_\_\_\_\_\_\_\_.



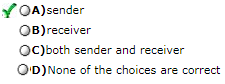
1. In TCP, the receiver can temporarily shut down the window; the sender, however, can always send a segment of \_\_\_\_\_ byte(s) after the window is shut down.



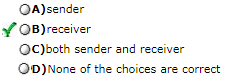
1. A serious problem can arise in the sliding window operation when either the sending application program creates data slowly or the receiving application program consumes data slowly, or both. This problem is called the \_\_\_\_\_\_.



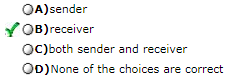
1. Nagle's algorithm can solve the silly window syndrome created by the \_\_\_\_\_\_\_\_\_.



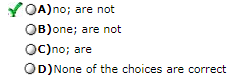
1. Clark's solution can solve the silly window syndrome created by the \_\_\_\_\_\_\_\_\_.



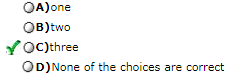
1. Delayed acknowledgment can solve the silly window syndrome created by the \_\_\_\_\_\_\_\_\_.



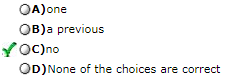
1. ACK segments consume \_\_\_\_\_\_\_ sequence number(s) and \_\_\_\_\_\_\_ acknowledged.



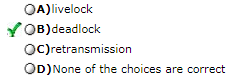
1. In modern implementations of TCP, a retransmission occurs if the retransmission timer expires or \_\_\_\_\_\_\_\_ duplicate ACK segments have arrived.



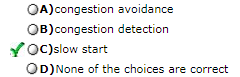
1. In TCP, \_\_\_\_\_\_\_\_ retransmission timer is set for an ACK segment.



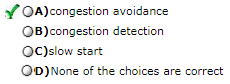
1. Lost acknowledgments may create a \_\_\_\_\_\_\_ if they are not handled properly.



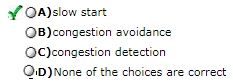
1. In the \_\_\_\_\_\_\_\_ algorithm the size of the congestion window increases exponentially until it reaches a threshold.



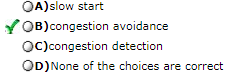
1. In the \_\_\_\_\_\_\_\_\_\_ algorithm the size of the congestion window increases additively until congestion is detected.



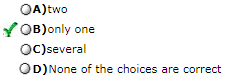
1. In the congestion detection algorithm, if detection is by a time-out, a new \_\_\_\_\_\_\_ phase starts.



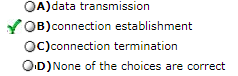
1. In the congestion detection algorithm, if detection is by three ACKs, a new \_\_\_\_\_\_\_ phase starts.



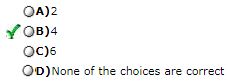
1. In TCP, there can be \_\_\_\_\_\_ RTT measurement(s) in progress at any time.



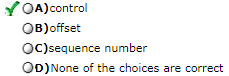
1. The value of the window scale factor can be determined during \_\_\_\_\_\_\_\_\_\_.



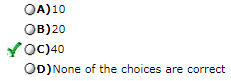
1. Multiply the header length field by \_\_\_\_\_\_\_ to find the total number of bytes in the TCP header.



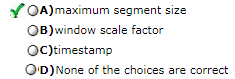
1. Urgent data requires the urgent pointer field as well as the URG bit in the \_\_\_\_\_\_\_ field.



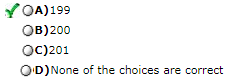
1. The options field of the TCP header ranges from 0 to \_\_\_\_\_\_\_ bytes.



1. Which option defines the maximum number of bytes in a TCP segment?

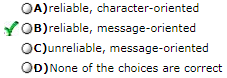


1. If the ACK value is 200, then byte \_\_\_\_\_\_\_ has been received successfully.

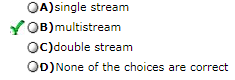


**6. Topic: Stream Control Transmission Protocol (SCTP)**

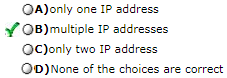
1. Stream Control Transmission Protocol (SCTP) is a new \_\_\_\_\_\_\_\_\_\_\_\_\_protocol.



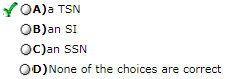
1. SCTP allows \_\_\_\_\_\_\_\_\_\_ service in each association.



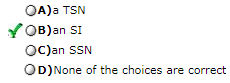
1. SCTP association allows \_\_\_\_\_\_\_\_\_\_\_\_\_ for each end.



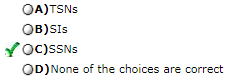
1. In SCTP, a data chunk is numbered using \_\_\_\_\_\_\_\_.



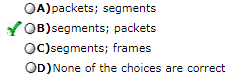
1. To distinguish between different streams, SCTP uses \_\_\_\_\_\_\_\_\_\_\_.



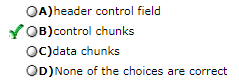
1. To distinguish between different data chunks belonging to the same stream, SCTP uses \_\_\_\_\_\_\_\_\_\_\_.



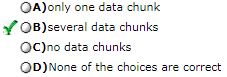
1. TCP has \_\_\_\_\_\_\_\_\_\_\_\_; SCTP has \_\_\_\_\_\_\_\_\_\_\_\_.



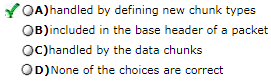
1. The control information in SCTP is included in the \_\_\_\_\_\_\_\_.



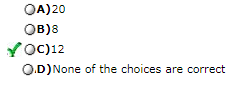
1. An SCTP packet can carry \_\_\_\_\_\_\_\_\_\_.



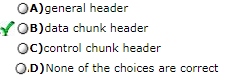
1. Options in SCTP are \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



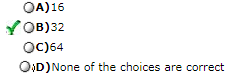
1. The general header in SCTP is \_\_\_\_\_\_\_ bytes.



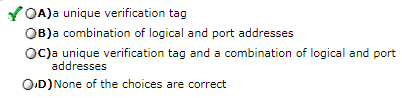
1. An SCTP sequence number (TSN) is located in the \_\_\_\_\_\_\_.



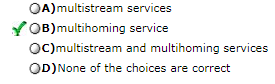
1. The checksum in SCTP is \_\_\_\_\_\_\_\_ bits.



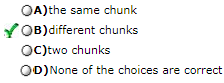
1. The association identifier in SCTP is \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



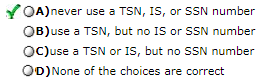
1. The association identifier in SCTP cannot be a combination of logical and port addresses because of \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



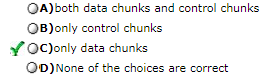
1. In SCTP, control information and data information are carried in \_\_\_\_\_\_\_.



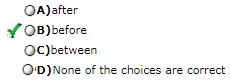
1. Control chunks in SCTP \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_.



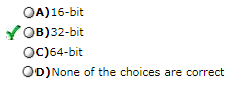
1. In SCTP, acknowledgment numbers are used to acknowledge \_\_\_\_\_\_\_\_\_\_\_\_\_.



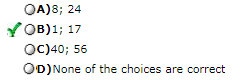
1. In an SCTP packet, control chunks come \_\_\_\_\_\_\_\_\_\_\_ data chunks.



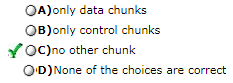
1. In SCTP, chunks need to terminate on a \_\_\_\_\_\_\_boundary.



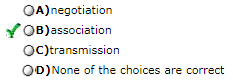
1. In SCTP, the data field of the DATA chunk must carry at least \_\_\_\_\_\_\_\_\_ byte of data, which means the value of length field cannot be less than \_\_\_\_\_\_\_\_\_\_\_.



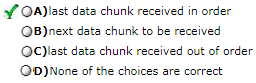
1. In SCTP, \_\_\_\_\_\_\_\_\_\_\_ can be carried in a packet that carries an INIT chunk.



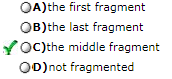
1. A connection in SCTP is called a(n) \_\_\_\_\_\_\_\_\_\_\_\_.



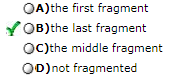
1. The acknowledgment in SCTP defines the cumulative TSN, the TSN of the \_\_\_\_\_\_\_\_\_\_\_\_ .



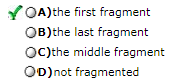
1. A DATA chunk arrives with its B/E bits equal to 0/0. It is \_\_\_\_\_\_\_\_\_\_\_.



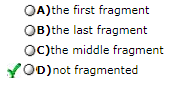
1. A DATA chunk arrives with its B/E bits equal to 0/1. It is



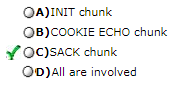
1. A DATA chunk arrives with its B/E bits equal to 1/0. It is \_\_\_\_\_\_\_\_\_\_\_.



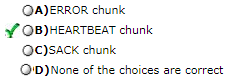
1. A DATA chunk arrives with its B/E bits equal to 1/1. It is \_\_\_\_\_\_\_\_\_\_\_.



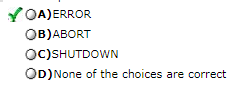
1. Which chunk is not involved in association establishment?



1. Which chunk probes the condition of an association?

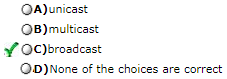


1. The \_\_\_\_\_\_\_ chunk is sent when an end point finds an error in a received packet.

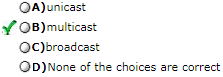


**7. Topic: Multicasting and Multicast Routing Protocol (MRP)**

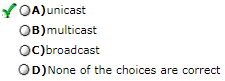
1. A one-to-all communication between one source and all hosts on a network is classified as a \_\_\_\_\_\_\_ communication.



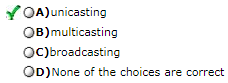
1. A one-to-many communication between one source and a specific group of hosts is classified as a \_\_\_\_\_\_\_ communication.



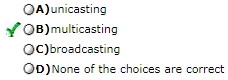
1. A one-to-one communication between one source and one destination is classified as a \_\_\_\_\_\_\_ communication.



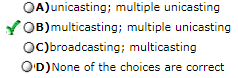
1. In \_\_\_\_\_\_, the router forwards the received packet through only one of its interfaces.



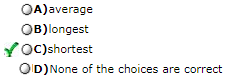
1. In \_\_\_\_\_\_\_, the router may forward the received packet through several of its interfaces.



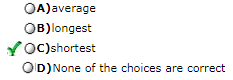
1. Emulation of \_\_\_\_\_\_\_\_ through \_\_\_\_\_\_\_\_\_\_\_ is not efficient and may create long delays.



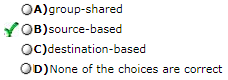
1. In unicast routing, each router in the domain has a table that defines a \_\_\_\_\_\_ path tree to possible destinations.



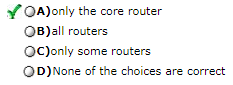
1. In multicast routing, each involved router needs to construct a \_\_\_\_\_\_\_\_ path tree for each group.



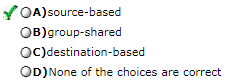
1. In the \_\_\_\_\_\_\_ tree approach, each router needs to have one shortest path tree for each group.



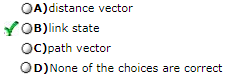
1. In the group-shared tree approach, \_\_\_\_\_\_\_\_ is/are involved in multicasting.



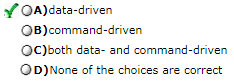
1. Multicast link state routing uses the \_\_\_\_\_\_\_ tree approach.



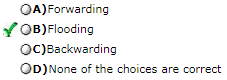
1. The Multicast Open Shortest Path First (MOSPF) protocol is an extension of the OSPF protocol that uses multicast routing to create source-based trees. The protocol is based on \_\_\_\_\_\_\_ routing.



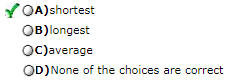
1. MOSPF is a \_\_\_\_\_\_\_ protocol.



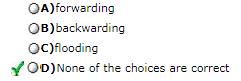
1. \_\_\_\_\_\_\_\_\_ broadcasts packets, but creates loops in the systems.



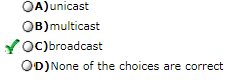
1. In RPF, a router forwards only the copy that has traveled the \_\_\_\_\_\_\_ path from the source to the router.



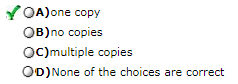
1. RPF eliminates the \_\_\_\_\_\_\_\_ in the flooding process.



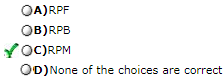
1. RPB creates a shortest path \_\_\_\_\_\_\_ tree from the source to each destination.



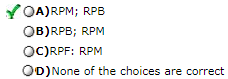
1. RPB guarantees that each destination receives \_\_\_\_\_\_\_\_\_ of the packet.



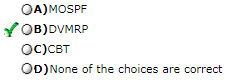
1. In \_\_\_\_\_\_\_\_, the multicast packet must reach only those networks that have active members for that particular group.



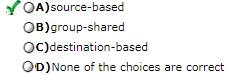
1. \_\_\_\_\_\_\_ adds pruning and grafting to \_\_\_\_\_\_\_ to create a multicast shortest path tree that supports dynamic membership changes.



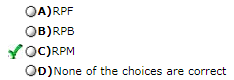
1. \_\_\_\_\_\_\_\_\_\_ is an implementation of multicast distance vector routing. It is a source-based routing protocol, based on RIP.



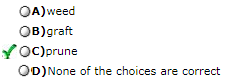
1. DVMRP is a \_\_\_\_\_\_\_\_routing protocol, based on RIP.



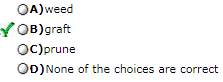
1. Pruning and grafting are strategies used in \_\_\_\_\_\_\_.



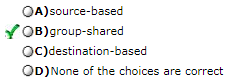
1. A \_\_\_\_\_\_\_ message tells an upstream router to stop sending multicast messages for a specific group through a specific router.



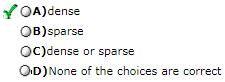
1. A \_\_\_\_\_\_\_ message tells an upstream router to start sending multicast messages for a specific group through a specific router.



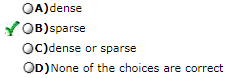
1. CBT is a \_\_\_\_\_\_\_\_ protocol that uses a core as the root of the tree.



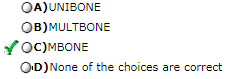
1. PIM-DM is used in a \_\_\_\_\_\_\_ multicast environment.



1. PIM-SM is used in a \_\_\_\_\_\_\_multicast environment such as a WAN.

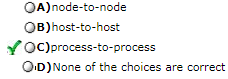


1. In \_\_\_\_\_\_\_, a logical tunnel is established by encapsulating the multicast packet inside a unicast packet.

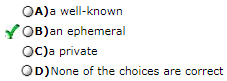


**8. Topic: Transport Layer**

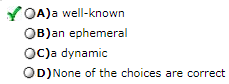
1. One of the main duties of the transport layer is \_\_\_\_\_\_\_\_\_\_\_\_ communication.



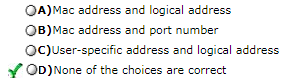
1. The client program normally uses \_\_\_\_\_\_\_\_\_\_\_\_ port number.



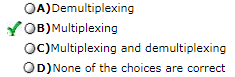
1. The server program normally uses \_\_\_\_\_\_\_\_\_\_ port number.



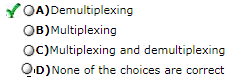
1. A socket address is a combination of \_\_\_\_\_\_\_\_\_\_



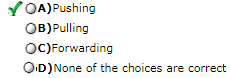
1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ means accepting items from more than one source.



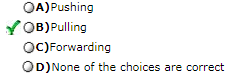
1. \_\_\_\_\_\_\_\_\_\_\_\_\_\_ means delivering items to more than one source.



1. \_\_\_\_\_\_\_\_\_ means the producer delivers the items when they are produced without waiting for the request from the consumer



1. \_\_\_\_\_\_\_\_\_ means the consumer takes the items when it is ready to do so.



1. In the stop-and-wait protocol, the send window size is \_\_\_\_\_\_ and the receive window size is \_\_\_\_\_\_\_ where n is related to the number of bits in the sequence.



1. In the go-back-N protocol, the send window size is \_\_\_\_\_\_ and the receive window size is \_\_\_\_\_\_\_, where n is related to the number of bits in the sequence number.



1. In the selective-repeat protocol, the send window size is \_\_\_\_\_\_ and the receive window size is \_\_\_\_\_\_\_, where n is related to the number of bits in the sequence.

