* **Question 1**

0.8 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | Select all statements that correctly describe IPv4 address assignment. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrecta.  Network managers can never assign IPv4 addresses manually, because such addresses are always set automatically by the network layer software anytime a new computer joins a given network. | |  | Incorrectd.  Anytime a computer joins an IP network, DHCP dynamically activates the computer’s configuration file that in turn assigns the computer’s IP address. | |  | Correcte.  One of the problems IPv6 is intended to address is a shortage of available IPv4 addresses. | | Answers: | a.  Network managers can never assign IPv4 addresses manually, because such addresses are always set automatically by the network layer software anytime a new computer joins a given network. | |  | b.  Each computer in an IPv4 network has only one address that is used to uniquely distinguish all layers of its protocol stack. | |  | Correctc.  Each IPv4 address is 32 bits in length. | |  | d.  Anytime a computer joins an IP network, DHCP dynamically activates the computer’s configuration file that in turn assigns the computer’s IP address. | |  | Correcte.  One of the problems IPv6 is intended to address is a shortage of available IPv4 addresses. |  |  |  | | --- | --- | | Response Feedback: | Each computer in an IP network has several addresses that distinguish it uniquely at different protocol layers, such as the application, network and data link layer. IP addresses are not always set automatically or dynamically when a new computer joins a given network; network managers can manually assign IP addresses as well. Any IPv4 address consists of 32 bits and is therefore a 32-bit number. Although the IPv4 address space is quite large (2^32), one problem with it is that it is running out of available addresses due to the extensive growth of the Internet; this shortage is one of the reasons for the development of IPv6. DHCP stands for Dynamic Host Configuration Protocol and is used to dynamically assign an IP address to a computer that connects to a given network. | |  |  |  |

* **Question 2**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Review the following scenario, which describes an asynchronous transmission between two computers, then follow the subsequent instructions.  -- Computer A uses asynchronous transmission to send characters to Computer B. Each character is encoded by 16 bits. Computer A adds two start bits and one stop bit for each character in order to separate the subsequent characters and enable their synchronization when they are received at Computer B. --  From the following statements, select the total number of bits that are sent on the circuit whenever Computer A transmits a character to Computer B. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcte.  The total number of bits per character transmitted over the circuit is equal to 19. | | Answers: | a.  The total number of bits per character transmitted over the circuit is equal to 21. | |  | b.  The total number of bits per character transmitted over the circuit is equal to 18. | |  | c.  The total number of bits per character transmitted over the circuit is equal to 16. | |  | d.  The total number of bits per character transmitted over the circuit is equal to 20. | |  | Correcte.  The total number of bits per character transmitted over the circuit is equal to 19. |  |  |  | | --- | --- | | Response Feedback: | For each character that is encoded by 16 bits we have two start bits and one stop bit. Therefore, the total number of bits per character that are transmitted over the circuit is equal to 16 + 2 + 1 = 19. | |  |  |  |

* **Question 3**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Review the following scenario, which describes a home automation system, then follow the subsequent instructions.  -- Megan uses a home automation system that enables her to control and manage her home appliances wirelessly. The appliances are connected to a central router through a wireless protocol whose speed is 10Mbps. Each message exchanged between an appliance and the router has 210 bytes of useful information and also a total of 30 bytes of overhead information. --  Select all statements that correctly define the transmission efficiency and effective data rate of the home automation system described in the scenario. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  The effective data rate is equal to 8.75Mbps. | |  | Correctd.  The transmission efficiency is equal to 87.5%. | | Answers: | Correcta.  The effective data rate is equal to 8.75Mbps. | |  | b.  The transmission efficiency is equal to 87%. | |  | c.  The transmission efficiency is equal to 70%. | |  | Correctd.  The transmission efficiency is equal to 87.5%. | |  | e.  The effective data rate is equal to 70Mbps. |  |  |  | | --- | --- | | Response Feedback: | The transmission efficiency is calculated by using the formula:  Transmission efficiency = Number of information bits / Number of total bits in transmission  The number of information bits is equal to 210 \* 8 = 1680 bits, while the number of total bits in transmission is equal to (210 + 30) \* 8 = 1920 bits. Therefore, the transmission efficiency is equal to 1680/1920=0.875 or 87.5%.  The effective data rate is calculated by using the formula:  Effective data rate = Maximum data rate \* Transmission efficiency  The speed of the wireless protocol is 10Mbps. Therefore, the effective data rate is equal to 10Mbps \* 0.875 = 8.75Mbps. | |  |  |  |

* **Question 4**

2.4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | Select all statements that correctly describe the Address Resolution Protocol (ARP). |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  ARP is used to determine the MAC address of a given computer whose IP address is known. | |  | Correctb.  An ARP request is received by all computers that belong to the same broadcast domain except the computer that issued that ARP request. | |  | Correctc.  Each ARP request is broadcast to computers on the same network as the computer sending the request. | |  | Incorrecte.  ARP operates at the network layer. | | Answers: | Correcta.  ARP is used to determine the MAC address of a given computer whose IP address is known. | |  | Correctb.  An ARP request is received by all computers that belong to the same broadcast domain except the computer that issued that ARP request. | |  | Correctc.  Each ARP request is broadcast to computers on the same network as the computer sending the request. | |  | Correctd.  The purpose of the address cache is to reduce the number of ARP requests that need to be sent on a given network for resolving addresses. | |  | e.  ARP operates at the network layer. |  |  |  | | --- | --- | | Response Feedback: | One computer cannot send a message to another computer in the same network if it does not know its data link layer address; for this reason the goal of the Address Resolution Protocol (ARP) is to determine the MAC address of a given computer based on its IP address. Therefore, ARP operates at the data link layer, not the network layer. ARP works by sending an ARP request to all computers that belong to the same network; the ARP request is specially formatted to ask the following question: “Whoever is IP address xxx.xxx.xxx.xxx, please send me your data link layer address”. An ARP request is received by all computers that belong to the same broadcast domain. A computer normally caches the addresses it resolved for some period of time which helps to reduce the number of ARP requests for addresses that the computer has already resolved. | |  |  |  |

* **Question 5**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Imagine that all IPv4 addresses in an organization use 21-bit network identifiers. Given the following CIDR entries and corresponding network addresses within the organization:  66.105.247.125/21 66.105.208.02/21 66.105.245.240/21 66.105.224.208/21  and the following IPv4 address in binary, which also has a 21-bit network identifier:  01000010 01101001 11010110 10100101  Select all statements that correctly describe which addresses are on the same network. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correctc.  66.105.247.125/21 is on the same network as 66.105.245.240/21. | |  | Correcte.  66.105.208.02/21 is on the same network as IPv4 address 01000010 01101001 11010110 10100101. | | Answers: | a.  66.105.224.208/21 is on the same network as 66.105.208.02/21. | |  | b.  66.105.245.240/21 is on the same network as 66.105.224.208/21. | |  | Correctc.  66.105.247.125/21 is on the same network as 66.105.245.240/21. | |  | d.  66.105.245.240/21 is on the same network as 66.105.208.02/21. | |  | Correcte.  66.105.208.02/21 is on the same network as IPv4 address 01000010 01101001 11010110 10100101. | |  | f.  66.105.224.208/21 is on the same network as IPv4 address 01000010 01101001 11010110 10100101. | |  | g.  66.105.247.125/21 is on the same network as 66.105.208.02/21. | |  | h.  66.105.247.125/21 is on the same network as 66.105.224.208/21. | |  | i.  66.105.224.208/21 is on the same network as IPv4 address 01000010 01101001 11010110 10100101. | |  | j.  66.105.247.125/21 is on the same network as IPv4 address 01000010 01101001 11010110 10100101. |  |  |  | | --- | --- | | Response Feedback: | The key to answering this question efficiently and correctly is recognizing that the first two octets are fully spanned by a 21-bit network identifier, the last octet is not spanned by the 21-bit network identifier at all, and only the first 5 bits in the third octet are used by the network identifier. Therefore if the first two octets and the first 5 bits in the third octet are identical, the address is on the same network. On the flipside, the last three bits in the third octet, and value in the last octet, have no effect on whether the address is on the same network, since these bits comprise the host identifier. With this in mind, we can now evaluate each address in turn:  66.105.247.125/21 and 66.105.224.208/21 are on *different* networks because, although the first two octets are identical, the first 5 bits of the third octet, 11110 and 11100, respectively, are different from each other.  66.105.247.125/21 and 66.105.245.240/21 are on *the same* network because the first two octets are identical, and the first 5 bits of the third octet, 11110, are also identical.  66.105.245.240/21 and 66.105.208.02/21 are on *different*networks because, although the first two octets are identical, the first 5 bits of the third octet, 11110and 11010, respectively, are different from each other  66.105.224.208/21 and IPv4 address 01000010 01101001 11010110 10100101 are on different networks because, although the bits for the first two octets are identical, the first 5 bits in the third octet, 11100 and 11010, respectively, are different from each other.  66.105.247.125/21 and 66.105.208.02/21 are on *different* networks because, although the first two octets are identical, the first 5 bits in the third octet, 11110 and 11010, respectively, are different from each other.  66.105.224.208/21 and 66.105.208.02/21 are on *different* networks because, although the first two octets are identical, the first 5 bits in the third octet, 11100 and 11010, respectively, are different from each other.  66.105.208.02/21 and IPv4 address 01000010 01101001 11010110 10100101 are on*the* *same* network because the first two octets are identical, and the first 5 bits of the third octet, 11010, are also identical.  66.105.245.240/21 and 66.105.224.208/21 are on *different* networks because, although the first two octets are identical, the first 5 bits in the third octet, 11110 and 11100, respectively, are different from each other.  66.105.247.125/21 and IPv4 address 01000010 01101001 11010110 10100101 are on *different* networks because, although the first two octets are identical, the first 5 bits in the third octet, 11110 and 11010, respectively, are different from each other.  66.105.224.208/21 and IPv4 address 01000010 01101001 11010110 10100101 are on *different* networks because, although the first two octets are identical, the first 5 bits in the third octet, 11100 and 11010, respectively, are different from each other. | |  |  |  |

* **Question 6**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Imagine that two (2) computers named Computer A and Computer B have only one network adapter each, and that both are connected to the same network.  Further imagine that Computer A’s IPv4 configuration is represented by the CIDR entry 112.62.156.241/23, and that Computer B’s IPv4 configuration is represented by the CIDR entry of 112.62.159.52/25. Select all true statements about this scenario. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Computer B’s network address in dotted decimal notation is 112.62.159.0. | |  | Correctc.  Computer B’s network identifier in binary is 01110000 00111110 10011111 0. | |  | Correctd.  Computer A’s network identifier in binary is 01110000 00111110 1001110. | | Answers: | Correcta.  Computer B’s network address in dotted decimal notation is 112.62.159.0. | |  | b.  Computer A’s network address in dotted decimal notation is 112.62.156.128. | |  | Correctc.  Computer B’s network identifier in binary is 01110000 00111110 10011111 0. | |  | Correctd.  Computer A’s network identifier in binary is 01110000 00111110 1001110. | |  | e.  Computer A’s network identifier in binary is 01110000 00111110 10011100 1. |  |  |  | | --- | --- | | Response Feedback: | The correct network identifier for Computer ‘A’ is 01110000 00111110 1001110 in binary notation, and the network address for Computer ‘A’ is 112.62.156.0 in dotted decimal.  By converting Computer A’s CIDR entry of 112.62.156.241/23 into binary we arrive at 01110000 00111110 10011100 11110001.  The ‘/23’ in the CIDR notation indicates that the network identifier spans the first 23 bits of the address.  This gives us 01110000 00111110 1001110 as the network identifier.  To arrive at the network address for Computer ‘A’, we fill in the remaining 9 bits of the address (the host bits) with 0 bits to arrive at 01110000 00111110 10011100 00000000.  Converted to dotted decimal to arrive at 112.62.156.0 as our network address for Computer ‘A’.  The correct network identifier for Computer ‘B’ is 01110000 00111110 10011111 0 in binary notation, and the network address for Computer ‘B’ is 112.62.159.0 in dotted decimal.  By converting Computer B’s CIDR entry of 112.62.159.52/25 into binary we arrive at 01110000 00111110 10011111 00110100.  The ‘/25’ in the CIDR notation indicates that the network identifier spans the first 24 bits of the address.  This gives us 01110000 00111110 10011111 0 as the network identifier.  To arrive at the network address for Computer ‘B’, we fill in the remaining 7 bits of the address (the host bits) with 0 bits to arrive at 01110000 00111110 10011111 00000000.  Converted to dotted decimal to arrive at 112.62.159.0 as our network address for Computer ‘B’. | |  |  |  |

* **Question 7**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Imagine that two (2) computers named Computer A and Computer B have only one network adapter each.  Further imagine that Computer A’s IPv4 configuration is represented by the CIDR entry 96.157.144.238/20, and that Computer B’s IPv4 configuration is represented by the CIDR entry 96.157.198.238/18. Select all true statements about this scenario. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Computer B’s subnet mask in dotted decimal notation is 255.255.192.0. | |  | Correctb.  Computer A’s subnet mask in binary notation is 11111111.11111111.11110000.00000000 | |  | Correctc.  Computer A’s subnet mask in dotted decimal notation is 255.255.240.0. | | Answers: | Correcta.  Computer B’s subnet mask in dotted decimal notation is 255.255.192.0. | |  | Correctb.  Computer A’s subnet mask in binary notation is 11111111.11111111.11110000.00000000 | |  | Correctc.  Computer A’s subnet mask in dotted decimal notation is 255.255.240.0. | |  | d.  Computer A’s subnet mask in binary notation is 00000000.00000000.00001111.11111111 | |  | e.  Computer B’s subnet mask in dotted decimal notation is 255.255.224.0. |  |  |  | | --- | --- | | Response Feedback: | The correct subnet mask for Computer A is 255.255.240.0 in dotted decimal notation. The reason is that the "/20" in CIDR notation indicates the mask spans 20 bits, which means the first two octets are fully spanned by 1 bits, and the first four bits of the third octet are spanned by 1 bits. All remaining bits which are the ‘host bits’ are spanned by 0 bits.  This results in a binary representation of 11111111.11111111.11110000.00000000 and 255.255.240.0 in dotted decimal.  The correct subnet mask for Computer B is 255.255.192.0 in dotted decimal notation. The reason is that the "/18" in CIDR notation indicates the mask spans 18 bits, which means the first two octets are fully spanned by 1 bits, and the first 2 bits of the third are spanned by 1 bits.  All remaining bits which are the ‘host bits’ are spanned by 0 bits. This results in a binary representation of 11111111.11111111.11000000.00000000 and 255.255.192.0 in dotted decimal. | |  |  |  |

* **Question 8**

0.8 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | From the following statements, select all that correctly describe error correction via retransmission |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrectc.  Flow control is an important component of both Stop-and-wait ARQ and Continuous ARQ. | |  | Correctd.  Stop-and-wait ARQ can be used on a half-duplex circuit. | |  | Incorrecte.  Retransmission requires the most overhead of all error correction techniques, but it is also the most effective. | | Answers: | a.  Retransmitting the first packet with an error and all those that followed it (referred to as Go-Back-N ARQ) is the most efficient method of continuous ARQ. | |  | Correctb.  The sliding window used in Continuous ARQ determines the number of protocol data units that can be sent by the sender without any acknowledgment from the receiver. | |  | c.  Flow control is an important component of both Stop-and-wait ARQ and Continuous ARQ. | |  | Correctd.  Stop-and-wait ARQ can be used on a half-duplex circuit. | |  | e.  Retransmission requires the most overhead of all error correction techniques, but it is also the most effective. |  |  |  | | --- | --- | | Response Feedback: | Retransmitting only those packets containing an error (referred to as Link Access Protocol for Modems or LAP-M) is the most efficient method of continuous ARQ.  Retransmission is simplest, most effective, and least expensive (in terms of overhead) method for error correction, especially when LAP-M is used.  Flow control is not necessary in Stop-and-wait ARQ, because the sender sends one packet at a time, and then waits for a response from the receiver before sending the next packet.  With continuous ARQ, flow control is important to ensure that the sender is not transmitting too quickly for the receiver. | |  |  |  |

* **Question 9**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | From the following statements, select all that correctly describe error detection in data transmissions. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correctb.  Adding extra data to each message in a transmission is one important strategy for detecting errors. | |  | Correctc.  Cyclic redundancy check detects a high percentage of transmission errors. | | Answers: | a.  If parity checking is used for error detection, the uppercase letter *B* in 8-bit ASCII (encoded as 01000010) would be transmitted as 010000101. | |  | Correctb.  Adding extra data to each message in a transmission is one important strategy for detecting errors. | |  | Correctc.  Cyclic redundancy check detects a high percentage of transmission errors. | |  | d.  Greater error-detection always results in more efficient transmission of data over the circuit. | |  | e.  Parity checking can be used to detect and correct all errors. will not only determine that an error occurred, but will also know what the error was. |  |  |  | | --- | --- | | Response Feedback: | Parity check can only determine that an error occurred, but not what the error was.  In fact, if two bits in the transmission are switched, parity check will not detect and error occurred as all.  As the amount of error-detection data sent with each message increases, the throughput of useful data is reduced; therefore the efficiency of data throughput is decreased, resulting in less efficient transmission of data of the circuit.  Parity is determined by the number of 1’s present in a transmission.  Given the example here, the uppercase letter *B* in 8-bit ASCII (encoded as 01000010) would be transmitted using even parity as 010000100.  Because there are two 1’s (an even number), the parity bit is set to 0. | |  |  |  |

* **Question 10**

3.4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | From the following statements, select all that correctly describe error prevention. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Echoes in computer networks can be caused by poorly connected cables. | |  | Incorrectb.  White noise can be completely avoided if proper error prevention methods are used. | |  | Correcte.  Changing the size of the guardbands in Frequency Division Multiplexing (FDM) may eliminate cross-talk or intermodulation noise. | | Answers: | Correcta.  Echoes in computer networks can be caused by poorly connected cables. | |  | b.  White noise can be completely avoided if proper error prevention methods are used. | |  | c.  Changing the multiplexing technique will never eliminate the negative effects of cross-talk or intermodulation noise. | |  | d.  Repeaters are used only in analog circuits. | |  | Correcte.  Changing the size of the guardbands in Frequency Division Multiplexing (FDM) may eliminate cross-talk or intermodulation noise. |  |  |  | | --- | --- | | Response Feedback: | White noise is a physical phenomenon that is caused by the thermal agitation of electrons in communication circuits and thus cannot be avoided by any error prevention methods. Poorly connected cables or poorly maintained equipment are possible reasons for echos in computer networks. Repeaters are used in digital circuits because a repeater receives the incoming signal, translates it into a digital message, and then retransmits the message. Cross-talk and intermodulation noise are often caused by improper multiplexing and one way to eliminate them is by changing the size of the guardbands in Frequency Division Multiplexing (FDM); another way would be to change the multiplexing technique: for example by using Time Division Multiplexing (TDM) instead of FDM. | |  |  |  |

* **Question 11**

2.06666 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | From the following statements, select all that correctly describe the Internet Protocols IPv4 and IPv6. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Internet Protocol (IP) protocol data units’ are referred to as packets. | |  | Correctb.  The IPv4 header contains a rarely used options field, and a typical header size of 20 bytes. | |  | Incorrectc.  Both IPv6 and IPv4 addresses are represented in dotted decimal notation. | | Answers: | Correcta.  Internet Protocol (IP) protocol data units’ are referred to as packets. | |  | Correctb.  The IPv4 header contains a rarely used options field, and a typical header size of 20 bytes. | |  | c.  Both IPv6 and IPv4 addresses are represented in dotted decimal notation. | |  | Correctd.  It is possible to represent IPv6 addresses using a ‘compressed notation’. | |  | e.  IPv6 has a 384-bit header, due to the increase in the length of the source and destination addresses from 32 to 128 bits. |  |  |  | | --- | --- | | Response Feedback: | IPv6 has a 320-bit header length.  This is primarily due to the increase in the address size from 32 bits to 128 bits, but there are also marked differences in the packet structure between IPv6 and the older IPv4.  IPv6 has a much simpler packet structure.  IPv6 is represented using hexadecimal, not dotted decimal, to express addresses. | |  |  |  |

* **Question 12**

2.8 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | From the following statements, select all that correctly describe Media Access Control. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Access request is a technique used with the Controlled Access approach to Media Access Control. | |  | Incorrectc.  Media Access control prevents any two computers on a circuit from transmitting data at the same time. | |  | Correctd.  Ethernet frequently uses the contention approach to Media Access Control. | |  | Incorrecte.  Media Access Control is not needed with a half-duplex point-to-point circuit. | | Answers: | Correcta.  Access request is a technique used with the Controlled Access approach to Media Access Control. | |  | b.  Polling is a technique used with the Contention approach to Media Access Control. | |  | c.  Media Access control prevents any two computers on a circuit from transmitting data at the same time. | |  | Correctd.  Ethernet frequently uses the contention approach to Media Access Control. | |  | e.  Media Access Control is not needed with a half-duplex point-to-point circuit. |  |  |  | | --- | --- | | Response Feedback: | Media Access Control becomes important when several computers share the same network, such as a point-to-point configuration with a half-duplex configuration that requires computers to take turns transmitting.  Polling is one of two techniques used with the Controlled Access approach to Media Access Control.  Media Access Control doesn’t prevent multiple computers on a circuit from transmitting data at the same time, but it does address ways to recover from the this problem using two fundamental approaches: Contention and Controlled Access. | |  |  |  |

* **Question 13**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | From the following statements, select all that correctly describe routing protocols. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  An autonomous system is a network operated by one organization. | |  | Correctb.  The routing protocols used inside an autonomous system are known as interior routing protocols. | |  | Correctd.  Intermediate System to Intermediate System (IS-IS) is a link state interior routing protocol. | | Answers: | Correcta.  An autonomous system is a network operated by one organization. | |  | Correctb.  The routing protocols used inside an autonomous system are known as interior routing protocols. | |  | c.  The best routing protocols determine all possible routes in a given network irrespective of the size of the network. | |  | Correctd.  Intermediate System to Intermediate System (IS-IS) is a link state interior routing protocol. | |  | e.  Exterior routing protocols calculate all possible routes between two autonomous systems. |  |  |  | | --- | --- | | Response Feedback: | The calculation of all possible routes in a given network becomes impractical if the network is large, because this process would take significant time and computational resources; therefore, it is not always advisable to determine all possible routes. For this reason, large networks are often subdivided into autonomous systems of networks. An autonomous system is a network operated by one organization. The routing protocols used inside an autonomous system are known as interior routing protocols. Exterior routing protocols do not calculate all possible routes between two autonomous systems, but rather determine only the preferred or the best routes. IS-IS is a link state interior routing protocol. | |  |  |  |

* **Question 14**

3.4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Partial Credit | From the following statements, select all that correctly describe server name resolution and the Domain Name Service (DNS). |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correctb.  Server name resolution is the process of translating application layer addresses into network addresses. | |  | Correctd.  The server name resolution process involves sending a DNS request to a DNS server. | |  | Incorrecte.  Server name resolution is the process of translating application layer addresses into data link layer addresses. | | Answers: | a.  The server name resolution process takes equal time to complete irrespective of the application layer address that needs to be resolved. | |  | Correctb.  Server name resolution is the process of translating application layer addresses into network addresses. | |  | c.  Sending a single DNS request to one DNS server is always sufficient to successfully perform server name resolution. | |  | Correctd.  The server name resolution process involves sending a DNS request to a DNS server. | |  | e.  Server name resolution is the process of translating application layer addresses into data link layer addresses. |  |  |  | | --- | --- | | Response Feedback: | Server name resolution resolves application layer addresses into IP addresses, not MAC addresses. If a computer does not know the IP address of another computer whose application layer address is known, then the computer needs to send a DNS request to a DNS server to determine the unknown IP address. If a DNS server does not have in its own database an IP address that has been requested by a DNS request, then that DNS server will forward the DNS request to another DNS server; therefore, sometimes it is not sufficient to send a DNS request only to one DNS server in order to find an unknown IP address. In addition, the time required to perform server name resolution is not fixed because a different number of DNS servers might be involved in the resolution process. | |  |  |  |

* **Question 15**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | From the following statements, select all that correctly describe sources of errors in data transmission. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  Echoes are a result of poor connections within the circuit, and are more common in analog circuits. | |  | Correctb.  Impulse noise is one of the most common source of errors in data communications. | |  | Correcte.  Increasing the signal strength in network media may help prevent white noise. | | Answers: | Correcta.  Echoes are a result of poor connections within the circuit, and are more common in analog circuits. | |  | Correctb.  Impulse noise is one of the most common source of errors in data communications. | |  | c.  Cross-talk can only occur on copper cables when multiplexing is used to carry many discrete signals. | |  | d.  With attenuation, low frequencies lose power more rapidly than higher frequencies. | |  | Correcte.  Increasing the signal strength in network media may help prevent white noise. |  |  |  | | --- | --- | | Response Feedback: | Cross-talk occurs between pairs of wires carrying separate signals, in multiplexed links carrying many discrete signals, and can also occur in microwave links where on antenna picks up a minute reflection from another antenna.  Higher frequencies are more susceptible to attenuation than lower frequencies – given the same circuit, as frequency increases, the degree of attenuation increases. | |  |  |  |

* **Question 16**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | From the following statements, select all that correctly describe Synchronous transmission and its associated standards and protocols. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | Correcta.  As little as one synchronization character (SYN) can be added to the start of a frame. | |  | Correctb.  The typical Synchronous data link control (SDLC) frame begins and ends with a flag, and contains and address field, a control field, and a frame check sequence field. | |  | c.  Synchronous transmission on multipoint circuits requires that only the destination address be included in each packet. | |  | Correctd.  One way in which an Ethernet 802.3ac frame differs from an Ethernet II frame is that a Type field is used to specify an ACK frame. | |  | e.  Ethernet is a commonly used synchronous data link protocol which also uses a controlled-access media access protocol. |  |  |  | | --- | --- | | Response Feedback: | Synchronous transmission on multipoint circuits requires that a destination address and a source address be included in each packet.  Unlike synchronous data link control (SDLC) and high-level data link control (HDLC) which use a controlled-access media access protocol; Ethernet uses a contention media access control. | |  |  |  |

* **Question 17**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | From the following statements, select all that correctly describe the Transmission Control Protocol (TCP). |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | Correcta.  The Application Layer determines which transport protocol will be used to transmit a particular message– TCP, User Datagram Protocol (UDP), or another. | |  | b.  TCP is the Transport Layer protocol that links the Network Layer to the Data-Link layer. | |  | c.  TCP encapsulates a message into a protocol data unit called a frame, and numbers each frame for reassembly at the Network Layer. | |  | Correctd.  TCP breaks data into smaller protocol data unit’s called segments. | |  | Correcte.  Excluding the option field which is rarely used, TCP has a header length of 20 bytes. |  |  |  | | --- | --- | | Response Feedback: | TCP is the Transport Layer protocol that links the application layer to the Network Layer.  TCP breaks the message into smaller PDU’s called segments, numbering them, ensuring each segment is reliably delivered, and reassembling them in the correct order at the destination. | |  |  |  |

* **Question 18**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | From the following statements, select all that correctly describe the transport layer in TCP/IP. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | a.  TCP does not need to segment the messages it receives from the application layer because the data link layer can handle any application message irrespective of its length. | |  | Correctb.  One of the functions of TCP is to segment the messages it receives from the application layer. | |  | c.  Any port address is represented by a 1-byte number. | |  | d.  FTP and Telnet have identical port addresses. | |  | Correcte.  Once TCP receives an IP packet from the network layer, it decides to which application it should deliver the packet based on the application’s unique port address. |  |  |  | | --- | --- | | Response Feedback: | The segmentation of the messages received from the application layer is one of the functions of the Transmission Control Protocol (TCP); the reason for segmenting messages at the transport layer is that the data link layer can transmit messages only of certain length. Any application has a unique port address; FTP servers use port 21, while Telnet uses port 23. TCP decides where to deliver an IP packet it receives based on the application’s port address which distinguishes the application uniquely from other applications. Finally, port addresses are 2-byte numbers, not 1-byte numbers. | |  |  |  |

* **Question 19**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | From the following statements, select all that correctly describe properties of transport layer protocols. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | Correcta.  The successful delivery of messages is not guaranteed if UDP is used as a transport layer protocol for communication between a sender and receiver. | |  | b.  A TCP connection between a sender and receiver is considered terminated if the sender transmits FIN to the receiver to announce that is has no more data to transmit. | |  | Correctc.  In connectionless messaging, a sender transmits data to a receiver without prior arrangement of a dedicated end-to-end connection between the sender and receiver. | |  | Correctd.  The process of establishing a TCP connection between a sender and receiver involves three control messages exchanged between the sender and receiver. | |  | e.  Once a TCP connection is established between a sender and receiver, all packets transmitted by the sender always follow one physical route on their way to the receiver. |  |  |  | | --- | --- | | Response Feedback: | A TCP connection between a sender and receiver is established after the completion of the three-way handshake process that involves the exchange of three control messages between the sender and receiver.  When a TCP connection is established between a sender and receiver, there is one logical connection or session between them at the transport layer, but the packets may follow different physical routes on their way to the destination. A TCP connection is considered terminated after successful completion of the four-way handshake, or namely when both the sender and receiver send a FIN and receive an ACK as a response to the FIN sent. UDP is connectionless protocol and thus does not guarantee successful delivery of UDP datagrams. | |  |  |  |

* **Question 20**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | Select all statements that correctly describe types of routing. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | Correcta.  Distance vector and link state routing protocols are types of dynamic routing protocols. | |  | b.  Static routing is used predominantly in networks that are expected to grow significantly or whose routing configuration needs to change often. | |  | Correctc.  Network topology is one of the factors that influence the routing decisions taken in networks with dynamic routing. | |  | Correctd.  In a network with centralized routing, there is one router that determines the routing decisions for all other routers that participate in the network. | |  | e.  Determining static routes in networks with static routing requires more capable routers in terms memory and processing power compared to determining dynamic routes in networks with dynamic routing. |  |  |  | | --- | --- | | Response Feedback: | With centralized routing, all routing decisions are made by one central computer or router. Static routing is normally used in simpler networks that are not expected to grow significantly and have few routing options that seldom change. The routing decisions in networks with dynamic routing are influenced by the network topology among other factors because the dynamic routing protocol intends to adapt to the topology change and reroute the traffic over different routes is possible. Dynamic routing normally requires more computing resources in terms of CPU and memory than static routing, because static routes are configured manually and seldom change, while dynamic routes may change often depending on the network conditions. Distance vector and link state routing protocols are types of dynamic routing protocols. | |  |  |  |

* **Question 21**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Select the most complete answer.  Which items in the list below can cause errors during data transmission? |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Correctb.  White noise, Impulse noise, Echo, Cross talk | | Answers: | a.  White noise, Impulse noise, Echo, Cross talk, Shielding | |  | Correctb.  White noise, Impulse noise, Echo, Cross talk | |  | c.  Impulse Noise, Echo, Cross talk | |  | d.  White noise, impulse noise | |  | e.  White noise, impulse noise, echo | |  |  |  |

* **Question 22**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Assume that a network interface card is configured as follows: IP Address: 192.168.37.17 Subnet Mask: 255.255.255.240 Select the subnet-directed broadcast address from the alternatives below. |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Correctd.  192.168.37.31 | | Answers: | a.  None of the other answers are correct | |  | b.  192.168.37.255 | |  | c.  192.168.37.240 | |  | Correctd.  192.168.37.31 | |  | e.  192.168.37.0 | |  |  |  |

* **Question 23**

0 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Incorrect | Select all statements that correctly describe the Address Resolution protocol (ARP). |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Incorrect [None Given] | | Answers: | Correcta.  A successful ARP request will ultimately lead to the sender receiving a MAC Address of another device on the network. | |  | Correctb.  A successful ARP request will ultimately map an IP Address to an associated MAC Address. | |  | c.  A successful ARP request will ultimately map a network (subnet) address to an associated IP address. | |  | d.  A successful ARP request will ultimately map an IP Address to an associated DNS name. |  |  |  | | --- | --- | | Response Feedback: | An ARP request is a data link layer address (MAC Address) resolution technique. It associates a MAC Address with an IP Address. | |  |  |  |

* **Question 24**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Imagine that all IPv4 addresses in an organization use 17-bit network identifiers. Given the following CIDR entries from the organization:  222.111.252.33/17 222.111.138.19/17 222.113.252.34/17  and the following IPv4 addresses in binary, which also have a 17-bit network identifier:  11011110 01110001 11111100 00100011 11011110 01101111 01010001 00010011  Select all statements that correctly describe which addresses are on the same network. |  |  |  |
| |  |  | | --- | --- | | Selected Answers: | Correcta.  222.111.252.33/17 is on the same network as 222.111.138.19/17. | |  | Correcth.  222.113.252.34/17 is on the same network as IPv4 address 11011110 01110001 11111100 00100011. | | Answers: | Correcta.  222.111.252.33/17 is on the same network as 222.111.138.19/17. | |  | b.  222.111.252.33/17 is on the same network as 222.113.252.34/17. | |  | c.  222.111.252.33/17 is on the same network as IPv4 address 11011110 01110001 11111100 00100011. | |  | d.  222.111.252.33/17 is on the same network as IPv4 address 11011110 01101111 01010001 00010011. | |  | e.  222.111.138.19/17 is on the same network as 222.113.252.34/17. | |  | f.  222.111.138.19/17 is on the same network as IPv4 address 11011110 01110001 11111100 00100011. | |  | g.  222.111.138.19/17 is on the same network as IPv4 address 11011110 01101111 01010001 00010011. | |  | Correcth.  222.113.252.34/17 is on the same network as IPv4 address 11011110 01110001 11111100 00100011. | |  | i.  222.113.252.34/17 is on the same network as IPv4 address 11011110 01101111 01010001 00010011. | |  | j.  IPv4 address 11011110 01110001 11111100 00100011 is on the same network as IPv4 address 11011110 01101111 01010001 00010011. |  |  |  | | --- | --- | | Response Feedback: | The key to answering this question efficiently and correctly is recognizing that the first two octets are fully spanned by a 17-bit network identifier, the last octet is not spanned by the 17-bit network identifier at all, and only the first bit in the third octet is used by the network identifier. Therefore if the first two octets and the first bit in the third octet are identical, the address is on the same network. On the flipside, the last seven bits in the third octet, and the last octet, have no effect on whether the address is on the same network, since these bits comprise the host identifier. With this in mind, we can now evaluate each address in turn:  222.111.252.33/17 is on the *same* network as 222.111.138.19/17, because the first two octets are the same, and because the first bit in the third octet for each address is the same (1).  222.111.252.33/17 and 222.113.252.34/17 are on a *different*network, because the second octet differs between the two.  222.111.252.33/17 and IPv4 address 11011110 01110001 11111100 00100011 are on a *different*network, because the second octet in the second address is 113, which differs from 111 in the first address.  222.111.252.33/17 is on a *different*network than IPv4 address 11011110 01101111 01010001 00010011, because although the first two octets are identical, the first bit in the third octet is a 1 for the first address and a 0 for the second address.  222.111.138.19/17 is on a *different*network than 222.113.252.34/17, because the second octet is 111 in the first address, and 113 in the second address.  222.111.138.19/17 is on a *different*network than IPv4 address 11011110 01110001 11111100 00100011, because the second octet is 111 for the first address, and 113 in the second address (when converted to decimal).  222.111.138.19/17 is on a *different*network than IPv4 address 11011110 01101111 01010001 00010011 because although the first two octets are identical, the third octet begins with a 1 bit in the first address, but begins with a 0 bit in the second octet.  222.113.252.34/17 is on the *same*network as IPv4 address 11011110 01110001 11111100 00100011, because the first two octets are identical (222.113), and because the first bit in the third octet for both address is the same (1).  222.113.252.34/17 is on a *different*network than IPv4 address 11011110 01101111 01010001 00010011, because the second octet is 113 in the first address, and 111 in the second address (when converted to decimal).  IPv4 address 11011110 01110001 11111100 00100011 is on a different network than IPv4 address 11011110 01101111 01010001 00010011, because the second octet differs between both addresses (01110001 and 01101111). | |  |  |  |

* **Question 25**

4 out of 4 points

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  |  | | | |
| Correct | Assume that a 1,700 byte file is transmitted using Ethernet over a circuit that has no errors. Further assume that up to 1,500 bytes of data can be transmitted in a single Ethernet frame, in addition to the frame's header and trailer which is comprised of 26 bytes. Select this transmission's efficiency, rounded to two decimal places, from the alternatives. |  |  |  |
| |  |  | | --- | --- | | Selected Answer: | Correctb.  97.03% | | Answers: | a.  None of the other answers are correct | |  | Correctb.  97.03% | |  | c.  100.03% | |  | d.  2.97% | |  | e.  98.49% | |  |  |  |

Wednesday, November 6, 2019 7:08:46 PM EST