computer-network-questions-answers

1. The IETF standards documents are called ________
a) RFC
b) RCF
c) ID
d) DFC

Answer: a
Explanation: RFC stands for Request For Comments and they are documents that describe methods, behaviors, research, or innovations applicable to the working of the Internet.

2. In the layer hierarchy as the data packet moves from the upper to the lower layers, headers are ___________
a) Added
b) Removed
c) Rearranged
d) Modified

Answer: a
Explanation: Each layer adds its own header to the packet from the previous layer. For example, in the Internet layer, the IP header is added over the TCP header on the data packet that came from the transport layer.

3. The structure or format of data is called ___________
a) Syntax
b) Semantics
c) Struct
d) Formatting

Answer: a
Explanation: The structure and format of data are defined using syntax. Semantics defines how a particular pattern to be interpreted, and what action is to be taken based on that interpretation. In programming languages, syntax of the instructions plays a vital role in designing of the program.

4. Communication between a computer and a keyboard involves ______________ transmission.
a) Automatic
b) Half-duplex
c) Full-duplex
d) Simplex

Answer: d
Explanation: In simplex transmission, data flows in single direction which in this case refers to the data flowing from the keyboard to the computer. Another example would be of the mouse where the data flows from the mouse to the computer only.

5. The first Network was called ________
a) CNNET
b) NSFNET
c) ASAPNET
d) ARPANET

Answer: d
Explanation: ARPANET stands for Advanced Research Projects Agency Networks. It was the first network to be implemented which used the TCP/IP protocol in the year 1969.

6. A _______ is the physical path over which a message travels.
a) Path
b) Medium

c) Protocol
d) Route

Answer: b
Explanation: Messages travel from sender to receiver via a physical path called the medium using a set of methods/rules called protocol. Mediums can be guided (wired) or unguided (wireless).

7. Which organization has authority over interstate and international commerce in the communications field?
a) ITU-T
b) IEEE
c) FCC
d) ISOC

Answer: c
Explanation: FCC is the abbreviation for Federal Communications Commission. FCC is responsible for regulating all interstate communications originating or terminating in USA. It was founded in the year 1934.

8. Which of this is not a network edge device?
a) PC
b) Smartphones
c) Servers
d) Switch

Answer: d
Explanation: Network edge devices refer to host systems, which can host applications like web browser. A switch can't operate as a host, but as a central device which can be used to manage network communication.

9. A _________ set of rules that governs data communication.
a) Protocols
b) Standards
c) RFCs
d) Servers

Answer: a
Explanation: In communications, a protocol refers to a set of rules and regulations that allow a network of nodes to transmit and receive information. Each layer in the network model has a protocol set, for example, the transport layer has TCP and UDP protocols.

10. Three or more devices share a link in ________ connection.
a) Unipoint
b) Multipoint
c) Point to point
d) Simplex

Answer: b
Explanation: A multipoint communication is established when three or many network nodes are connected to each other. Frame relay, Ethernet and ATM are some examples of multipoint connections.

1. When collection of various computers seems a single coherent system to its client, then it is called _________
a) computer network
b) distributed system
c) networking system
d) mail system

Answer: b
Explanation: A Computer network is defined as a collection of interconnected computers which uses a single technology for connection.
A distributed system is also the same as computer network but the main difference is that the whole collection of

computers appears to its users as a single coherent system.
Example:- World wide web

2. Two devices are in network if __________
a) a process in one device is able to exchange information with a process in another device
b) a process is running on both devices
c) PIDs of the processes running of different devices are same
d) a process is active and another is inactive

Answer: a
Explanation: A computer network, or data network, is a digital telecommunications network which allows nodes to share resources. In computer networks, computing devices exchange data with each other using connections between nodes. The nodes have certain processes which enable them to share a specific type of data using a distinct protocol.

3. Which of the following computer networks is built on the top of another network?
a) prior network
b) chief network
c) prime network
d) overlay network

Answer: d
Explanation: An overlay network is a computer network that is built on top of another network. Some examples of an overlay network are Virtual Private Networks (VPN) and Peer-to-Peer Networks (P2P).

4. In computer network nodes are _________
a) the computer that originates the data
b) the computer that routes the data
c) the computer that terminates the data
d) all of the mentioned

Answer: d
Explanation: In a computer network, a node can be anything that is capable of sending data or receiving data or even routing the data to its destination. Routers, Computers and Smartphones are some examples of network nodes.

5. Communication channel is shared by all the machines on the network in ________
a) broadcast network
b) unicast network
c) multicast network
d) anycast network

Answer: a
Explanation: In a broadcast network, information is sent to all stations in a network whereas in a multicast network the data or information is sent to a group of stations in the network. In unicast network, information is sent to only one specific station. The broadcast address of the network is the last assigned address of the network.

6. Bluetooth is an example of __________
a) personal area network
b) local area network
c) virtual private network
d) wide area network

Answer: a
Explanation: Bluetooth is a wireless technology used to create a wireless personal area network for data transfer up to a distance of 10 meters. It operates on 2.45 GHz frequency band for transmission.

7. A __________ is a device that forwards packets between networks by processing the routing information included in the packet.
a) bridge

b) firewall
c) router
d) hub

Answer: c
Explanation: A router is a networking device that forwards data packets between computer networks. Routers perform the traffic directing functions on the Internet. They make use of routing protocols like RIP to find the cheapest path to the destination.

8. A list of protocols used by a system, one protocol per layer, is called ________
a) protocol architecture
b) protocol stack
c) protocol suite
d) protocol system

Answer: b
Explanation: A protocol stack refers to a group of protocols that are running concurrently that are employed for the implementation of network protocol suite. Each layer in the network model has to use one specific protocol from the protocol stack.

9. Network congestion occurs _________
a) in case of traffic overloading
b) when a system terminates
c) when connection between two nodes terminates
d) in case of transfer failure

Answer: a
Explanation: Network congestion occurs when traffic in the network is more than the network could handle. To avoid network congestion, the network management uses various open-loop and closed-loop congestion control techniques.

10. Which of the following networks extends a private network across public networks?
a) local area network
b) virtual private network
c) enterprise private network
d) storage area network

Answer: b
Explanation: A virtual private network extends a private network across a public network, and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites which are unavailable in certain regions.

1. Which of this is not a constituent of residential telephone line?
a) A high-speed downstream channel
b) A medium-speed downstream channel
c) A low-speed downstream channel
d) An ultra-high speed downstream channel

Answer: c
Explanation: A low-speed downstream channel is not a constituent of a residential telephone line. But it might be just a two-way telephone channel. Internet can be provided through a high-speed downstream channel in a residential telephone line.

2. DSL telcos provide which of the following services?
a) Wired phone access
b) ISP
c) Wired phone access and ISP
d) Network routing and ISP

Answer: c
Explanation: DSL stands for Digital Subscriber Line and ISP stands for Internet Service Provider. In a Digital Subscriber Line system, the same company which provides phone connection is also an ISP. The internet is provided through the pre-installed telephone lines.

3. The function of DSLAM is to __________
a) Convert analog signals into digital signals
b) Convert digital signals into analog signals
c) Amplify digital signals
d) De-amplify digital signals

Answer: a
Explanation: DSLAM stands for Digital Subscriber Line Access Multiplexer and it's used by Telcos to convert the analog signals to digital signals for the purpose of providing internet. The DSLAM located in a telco's Central Office does this function.

4. Which of the following terms is not associated with DSL?
a) DSLAM
b) CO
c) Splitter
d) CMTS

Answer: d
Explanation: CMTS stands for Cable modem termination system. It is used in cable internet access. In cable internet access, internet is not provided through telephone lines and the companies that provide such connections don't necessarily provide telephone access.

5. HFC contains _______
a) Fibre cable
b) Coaxial cable
c) A combination of Fibre cable and Coaxial cable
d) Twisted Pair Cable

Answer: c
Explanation: Hybrid fiber-coaxial (HFC) is a telecommunications industry term for a broadband network that combines optical fiber and coaxial cable. It has been popularly used since the early 1990s. It is stronger than the optical fiber cables and faster than the co-axial cables.

6. Which of the following statements is not applicable for cable internet access?
a) It is a shared broadcast medium
b) It includes HFCs
c) Cable modem connects home PC to Ethernet port
d) Analog signal is converted to digital signal in DSLAM

Answer: d
Explanation: CMTS stands for Cable modem termination system. In cable access analog signal is converted to digital signal by CMTS. In cable internet access, internet is not provided through telephone lines. DSLAM is used by Telecom companies.

7. Among the optical-distribution architectures that are essentially switched ethernet is __________
a) AON
b) PON
c) NON
d) MON

Answer:a
Explanation: AON stands for Active optical networks which are essentially switched Ethernets. Each user has his/her own dedicated optical fiber line connecting to the ISP in an AON.

8. StarBand provides __________
a) FTTH internet access
b) Cable access
c) Telephone access
d) Satellite access

Answer: d
Explanation: StarBand was a two-way satellite broadband Internet service available in the U.S. from 2000–2015. It was discontinued from September 30 2015 due to increasing competition from other ISPs.

9. Home Access is provided by __________
a) DSL
b) FTTP
c) Cable
d) All of the mentioned

Answer: d
Explanation: Home Internet Access is provided by DSL, FTTP, and Cable. FTTP provides the fastest speeds followed by the cable connections and then the DSLs. FTTP is popularly used in modern connections.

10. ONT is connected to splitter using _________
a) High speed fibre cable
b) HFC
c) Optical cable
d) Twisted pair cable

Answer: c
Explanation: ONT stands for Optical Network Terminal. The ONT connects to the Termination Point (TP) with an optical fibre cable. It translates light signals from the fibre optic line to electric signals that the router can read.

11. Which of the following factors affect transmission rate in DSL?
a) The gauge of the twisted-pair line
b) Degree of electrical interfernece
c) Shadow fading
d) The gauge of the twisted-pair line and degree of electrical interference

Answer: d
Explanation: Because DSL is made of twisted wire copper pair, the gauge of twisted pair line i.e. the protection and electrical interference would affect the transmission rate in DSL. Unlike DSL, FTTP is not really affected by these factors.

1. How many layers are present in the Internet protocol stack (TCP/IP model)?
a) 5
b) 7
c) 6
d) 10

Answer: a
Explanation: There are five layers in the Internet Protocol stack. The five layers in Internet Protocol stack is Application, Transport, Network, Data link and Physical layer. The internet protocol stack model is also called the TCP/IP model and it's used in modern Internet Communication.

2. The number of layers in ISO OSI reference model is __________
a) 5
b) 7
c) 6
d) 10

Answer: b
Explanation: The seven layers in ISO OSI reference model is Application, Presentation, Session, Transport, Network, Data link and Physical layer. OSI stands for Open System Interconnect and it is a generalized model.

3. Which of the following layers is an addition to OSI model when compared with TCP IP model?
a) Application layer
b) Presentation layer
c) Session layer
d) Session and Presentation layer

Answer: d
Explanation: The only difference between OSI model and TCP/IP model is that the functions of Presentation and Session layer in the OSI model are handled by the transport layer itself in TCP/IP. OSI is a generalized model and TCP/IP is an application specific model.

4. Application layer is implemented in ____________
a) End system
b) NIC
c) Ethernet
d) Packet transport

Answer: a
Explanation: Not only application layer, but presentation layer, session layer and transport layer are also implemented in the end system. The layers below are implemented outside the end system, for example, the network layer is implemented on the routers and the physical layer is implemented for the medium.

5. Transport layer is implemented in ______________
a) End system
b) NIC
c) Ethernet
d) Signal transmission

Answer: a
Explanation: Application, Presentation, Session and Transport layer are implemented in the end system. The transport layer handles the process to process delivery of the packet through ports.

6. The functionalities of the presentation layer include ____________
a) Data compression
b) Data encryption
c) Data description
d) All of the mentioned

Answer: d
Explanation: Some functions of the presentation layer include character-code translation, data conversion, data encryption and decryption, and data translation. It connects the application layer with the layers below converting the human readable text and media to machine readable format and vice-versa.

7. Delimiting and synchronization of data exchange is provided by __________
a) Application layer
b) Session layer
c) Transport layer
d) Link layer

Answer: b
Explanation: The session layer provides the mechanism for opening, closing and managing a session between end-user application processes. The session layer 5 is responsible for establishing managing synchronizing and terminating sessions. In TCP/IP protocol stack, the functions of the session layer are handled by the transport layer itself and thus the session layer is missing from the TCP/IP model.

8. In OSI model, when data is sent from device A to device B, the 5th layer to receive data at B is _________
a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: d
Explanation: In OSI reference model, the fifth layer is Session layer. Session layer provides the mechanism for opening, closing and managing a session between end-user application processes. In TCP/IP protocol stack, the functions of the session layer are handled by the transport layer itself and thus the session layer is missing from the TCP/IP model.

9. In TCP IP Model, when data is sent from device A to device B, the 5th layer to receive data at B is ____________
a) Application layer
b) Transport layer
c) Link layer
d) Session layer

Answer: a
Explanation: In TCP/IP model, the fifth layer is application layer. When data is sent from device A to device B, the 5th layer to receive data at B is application layer. Application layer provides the interface between applications and the network. The user interacts with only this layer.

10. In the OSI model, as a data packet moves from the lower to the upper layers, headers are _______
a) Added
b) Removed
c) Rearranged
d) Randomized

Answer: b
Explanation: In OSI reference model, when data packet moves from lower layers to higher layer, headers get removed. Whereas when the data packet moves from higher layer to lower layers, headers are added. These headers contain the essential control information for the protocols used on the specific layer.

11. Which of the following statements can be associated with OSI model?
a) A structured way to discuss and easier update system components
b) One layer may duplicate lower layer functionality
c) Functionality at one layer no way requires information from another layer
d) It is an application specific network model

Answer: c
Explanation: One layer may use the information from another layer, for example timestamp value. The information is contained in the header inserted by the previous layer. The headers are added as the packet moves from higher layers to the lower layers.

1. OSI stands for __________
a) open system interconnection
b) operating system interface
c) optical service implementation
d) open service Internet

Answer: a
Explanation: OSI is the abbreviation for Open System Interconnection. OSI model provides a structured plan on how applications communicate over a network, which also helps us to have a structured plan for troubleshooting. It is recognized by the ISO as the generalized model for computer network i.e. it can be modified to design any kind of computer network.

2. The number of layers in ISO OSI reference model is __________
a) 4

b) 5
c) 6
d) 7

Answer: d
Explanation: In OSI reference model, there are 7 layers namely Application, Presentation, Session, Transport, Network, Data Link and Physical layer. Each layer uses a protocol to perform its designated function, for example, the data link layer uses error detection protocols for error control functions.

3. TCP/IP model does not have ______ layer but OSI model have this layer.
a) session layer
b) transport layer
c) application layer
d) network layer

Answer: a
Explanation: In OSI reference model, there are two layers which are not present in TCP/IP model. They are Presentation and Session layer. The functions of Presentation and Session layer in the OSI model are handled by the transport layer itself in TCP/IP.

4. Which layer is used to link the network support layers and user support layers?
a) session layer
b) data link layer
c) transport layer
d) network layer

Answer: c
Explanation: Physical, data link and network layers are network support layers and session, presentation and application layers are user support layers. The transport layer links these layers by segmenting and rearranging the data. It uses protocols like TCP and UDP.

5. Which address is used on the internet for employing the TCP/IP protocols?
a) physical address and logical address
b) port address
c) specific address
d) all of the mentioned

Answer: d
Explanation: The physical, logical, port and specific addresses are used in TCP/IP protocol. All the addressing schemes, that is physical (MAC) and logical address, port address and specific address are employed in both TCP/IP model and OSI model. In TCP/IP, the addresses are more focused on the internet implementation of these addresses.

6. TCP/IP model was developed _____ the OSI model.
a) prior to
b) after
c) simultaneous to
d) with no link to

Answer: a
Explanation: Several TCP/IP prototypes were developed at multiple research centers between 1978 and 1983, whereas OSI reference model was developed in the year 1984. TCP/IP was developed with the intention to create a model for the Internet while OSI was intended to be a general network model.

7. Which layer is responsible for process to process delivery in a general network model?
a) network layer
b) transport layer
c) session layer
d) data link layer

Answer: b
Explanation: The role of Transport layer (Layer 4) is to establish a logical end to end connection between two systems in a network. The protocols used in Transport layer is TCP and UDP. The transport layer is responsible for segmentation of the data. It uses ports for the implementation of process-to-process delivery.

8. Which address is used to identify a process on a host by the transport layer?
a) physical address
b) logical address
c) port address
d) specific address

Answer: c
Explanation: A port number is a way to identify a specific process to which an Internet or other network message is to be forwarded when it arrives at a server. Some examples of port numbers are port 20 which is used for FTP data, port 22 which is used for SSH remote login ,and port 23 which is used for TELNET.

9. Which layer provides the services to user?
a) application layer
b) session layer
c) presentation layer
d) physical layer

Answer: a
Explanation: In networking, a user mainly interacts with application layer to create and send information to other computer or network. Application layer provides the interface between applications and the network. It is the top-most layer in both the TCP/IP and the OSI model.

10. Transmission data rate is decided by ____________
a) network layer
b) physical layer
c) data link layer
d) transport layer

Answer: b
Explanation: Physical layer is a layer 1 device which deals with network cables or the standards in use like connectors, pins, electric current used etc. Basically the transmission speed is determined by the cables and connectors used. Hence it is physical layer that determines the transmission speed in network. Some of the cables used for high speed data transmission are optical fiber cables and twisted pair cables.

1. The physical layer is concerned with ___________
a) bit-by-bit delivery
p) process to process delivery
c) application to application delivery
d) port to port delivery

Answer: a
Explanation: Physical layer deals with bit to bit delivery in networking. The data unit in the physical layer is bits. Process to process delivery or the port to port delivery is dealt in the transport layer. The various transmission mediums aid the physical layer in performing its functions.

2. Which transmission media provides the highest transmission speed in a network?
a) coaxial cable
b) twisted pair cable
c) optical fiber
d) electrical cable

Answer: c
Explanation: Fiber optics is considered to have the highest transmission speed among the all mentioned above. The fiber

optics transmission runs at 1000Mb/s. It is called as 1000Base-Lx whereas IEEE standard for it is 802.3z. It is popularly used for modern day network connections due to its high transmission rate.

3. Bits can be sent over guided and unguided media as analog signal by ___________
a) digital modulation
b) amplitude modulation
c) frequency modulation
d) phase modulation

Answer: a
Explanation: In analog modulation, digital low frequency baseband signal (digital bit stream) is transmitted over a higher frequency. Whereas in digital modulation the only difference is that the base band signal is of discrete amplitude level. The bits are represented by only two frequency levels, one for high and one for low.

4. The portion of physical layer that interfaces with the media access control sublayer is called ___________
a) physical signalling sublayer
b) physical data sublayer
c) physical address sublayer
d) physical transport sublayer

Answer: a
Explanation: The portion of physical layer that interfaces with the medium access control sublayer is Physical Signaling Sublayer. The main function of this layer is character encoding, reception, decoding and performs optional isolation functions. It handles which media connection the signal should be forwarded to physically.

5. The physical layer provides __________
a) mechanical specifications of electrical connectors and cables
b) electrical specification of transmission line signal level
c) specification for IR over optical fiber
d) all of the mentioned

Answer: d
Explanation: Anything dealing with a network cable or the standards in use – including pins, connectors and the electric current used is dealt in the physical layer (Layer 1). Physical layer deals with bit to bit delivery of the data aided by the various transmission mediums.

6. In asynchronous serial communication the physical layer provides ___________
a) start and stop signalling
b) flow control
c) both start & stop signalling and flow control
d) only start signalling

Answer: c
Explanation: In asynchronous serial communication, the communication is not synchronized by clock signal. Instead of a start and stop signaling and flow control method is followed. Unlike asynchronous serial communication, in synchronous serial communication a clock signal is used for communication, so the start and stop method is not really required.

7. The physical layer is responsible for __________
a) line coding
b) channel coding
c) modulation
d) all of the mentioned

Answer: d
Explanation: The physical layer is responsible for line coding, channel coding and modulation that is needed for the transmission of the information. The physical configuration including pins, connectors and the electric current used is dealt in the physical layer based on the requirement of the network application.

8. The physical layer translates logical communication requests from the ______ into hardware specific operations.
a) data link layer
b) network layer
c) trasnport layer
d) application layer

Answer: a
Explanation: Physical layer accepts data or information from the data link layer and converts it into hardware specific operations so as to transfer the message through physical cables. Some examples of the cables used are optical fiber cables, twisted pair cables and co-axial cables.

9. A single channel is shared by multiple signals by ____________
a) analog modulation
b) digital modulation
c) multiplexing
d) phase modulation

Answer: c
Explanation: In communication and computer networks, the main goal is to share a scarce resource. This is done by multiplexing, where multiple analog or digital signals are combined into one signal over a shared medium. The multiple kinds of signals are designated by the transport layer which is the layer present on a higher level than the physical layer.

10. Wireless transmission of signals can be done via ___________
a) radio waves
b) microwaves
c) infrared
d) all of the mentioned

Answer: d
Explanation: Wireless transmission is carried out by radio waves, microwaves and IR waves. These waves range from 3 Khz to above 300 Ghz and are more suitable for wireless transmission. Radio waves can penetrate through walls and are used in radio communications, microwaves and infrared (IR) waves cannot penetrate through walls and are used for satellite communications and device communications respectively.

1. The data link layer takes the packets from _________ and encapsulates them into frames for transmission.
a) network layer
b) physical layer
c) transport layer
d) application layer

Answer: a
Explanation: In computer networks, the data from application layer is sent to transport layer and is converted to segments. These segments are then transferred to the network layer and these are called packets. These packets are then sent to data link layer where they are encapsulated into frames. These frames are then transferred to physical layer where the frames are converted to bits. Error control and flow control data is inserted in the frames at the data link layer.

2. Which of the following tasks is not done by data link layer?
a) framing
b) error control
c) flow control
d) channel coding

Answer: d
Explanation: Channel coding is the function of physical layer. Data link layer mainly deals with framing, error control and flow control. Data link layer is the layer where the packets are encapsulated into frames.

3. Which sublayer of the data link layer performs data link functions that depend upon the type of medium?
a) logical link control sublayer

b) media access control sublayer
c) network interface control sublayer
d) error control sublayer

Answer: b
Explanation: Media access control (MAC) deals with transmission of data packets to and from the network-interface card, and also to and from another remotely shared channel. The MAC sublayer also prevents collision using protocols like CSMA/CD.

4. Header of a frame generally contains ______________
a) synchronization bytes
b) addresses
c) frame identifier
d) all of the mentioned

Answer: d
Explanation: In a frame, the header is a part of the data that contains all the required information about the transmission of the file. It contains information like synchronization bytes, addresses, frame identifier etc. It also contains error control information for reducing the errors in the transmitted frames.

5. Automatic repeat request error management mechanism is provided by ________
a) logical link control sublayer
b) media access control sublayer
c) network interface control sublayer
d) application access control sublayer

Answer: a
Explanation: The logical link control is a sublayer of data link layer whose main function is to manage traffic, flow and error control. The automatic repeat request error management mechanism is provided by the LLC when an error is found in the received frame at the receiver's end to inform the sender to re-send the frame.

6. When 2 or more bits in a data unit has been changed during the transmission, the error is called ____________
a) random error
b) burst error
c) inverted error
d) double error

Answer: b
Explanation: When a single bit error occurs in a data, it is called single bit error. When more than a single bit of data is corrupted or has error, it is called burst error. If a single bit error occurs, the bit can be simply repaired by inverting it, but in case of a burst error, the sender has to send the frame again.

7. CRC stands for __________
a) cyclic redundancy check
b) code repeat check
c) code redundancy check
d) cyclic repeat check

Answer: a
Explanation: Cyclic redundancy check is a code that is added to a data which helps us to identify any error that occurred during the transmission of the data. CRC is only able to detect errors, not correct them. CRC is inserted in the frame trailer.

8. Which of the following is a data link protocol?
a) ethernet
b) point to point protocol
c) hdlc
d) all of the mentioned

Answer: d
Explanation: There are many data link layer protocols. Some of them are SDLC (synchronous data link protocol), HDLC (High level data link control), SLIP (serial line interface protocol), PPP (Point to point protocol) etc. These protocols are used to provide the logical link control function of the Data Link Layer.

9. Which of the following is the multiple access protocol for channel access control?
a) CSMA/CD
b) CSMA/CA
c) Both CSMA/CD & CSMA/CA
d) HDLC

Answer: c
Explanation: In CSMA/CD, it deals with detection of collision after collision has occurred, whereas CSMA/CA deals with preventing collision. CSMA/CD is abbreviation for Carrier Sensing Multiple Access/Collision detection. CSMA/CA is abbreviation for Carrier Sensing Multiple Access/Collision Avoidance. These protocols are used for efficient multiple channel access.

10. The technique of temporarily delaying outgoing acknowledgements so that they can be hooked onto the next outgoing data frame is called ____________
a) piggybacking
b) cyclic redundancy check
c) fletcher's checksum
d) parity check

Answer: a
Explanation: Piggybacking is a technique in which the acknowledgment is temporarily delayed so as to be hooked with the next outgoing data frame. It saves a lot of channel bandwidth as in non-piggybacking system, some bandwidth is reserved for acknowledgement.

1. The network layer is concerned with __________ of data.
a) bits
b) frames
c) packets
d) bytes

Answer: c
Explanation: In computer networks, the data from the application layer is sent to the transport layer and is converted to segments. These segments are then transferred to the network layer and these are called packets. These packets are then sent to data link layer where they are encapsulated into frames. These frames are then transferred to physical layer where the frames are converted to bits.

2. Which one of the following is not a function of network layer?
a) routing
b) inter-networking
c) congestion control
d) error control

Answer: d
Explanation: In the OSI model, network layer is the third layer and it provides data routing paths for network communications. Error control is a function of the data link layer and the transport layer.

3. A 4 byte IP address consists of __________
a) only network address
b) only host address
c) network address & host address
d) network address & MAC address

Answer: c

Explanation: An ip address which is 32 bits long, that means it is of 4 bytes and is composed of a network and host portion and it depends on address class. The size of the host address and network address depends upon the class of the address in classful IP addressing.

4. In virtual circuit network each packet contains ___________
a) full source and destination address
b) a short VC number
c) only source address
d) only destination address

Answer: b
Explanation: A short VC number also called as VCID (virtual circuit identifier) is a type of identifier which is used to distinguish between several virtual circuits in a connection oriented circuit switched network. Each virtual circuit is used to transfer data over a larger packet switched network.

5. Which of the following routing algorithms can be used for network layer design?
a) shortest path algorithm
b) distance vector routing
c) link state routing
d) all of the mentioned

Answer: d
Explanation: The routing algorithm is what decides where a packet should go next. There are several routing techniques like shortest path algorithm, static and dynamic routing, decentralized routing, distance vector routing, link state routing, Hierarchical routing etc. The routing algorithms go hand in hand with the operations of all the routers in the networks. The routers are the main participants in these algorithms.

6. Which of the following is not correct in relation to multi-destination routing?
a) is same as broadcast routing
b) contains the list of all destinations
c) data is not sent by packets
d) there are multiple receivers

Answer: c
Explanation: In multi-destination routing, there is more than one receiver and the route for each destination which is contained in a list of destinations is to be found by the routing algorithm. Multi-destination routing is also used in broadcasting.

7. A subset of a network that includes all the routers but contains no loops is called ________
a) spanning tree
b) spider structure
c) spider tree
d) special tree

Answer: a
Explanation: Spanning tree protocol (STP) is a network protocol that creates a loop free logical topology for ethernet networks. It is a layer 2 protocol that runs on bridges and switches. The main purpose of STP is to ensure that you do not create loops when you have redundant paths in your network.

8. Which one of the following algorithm is not used for congestion control?
a) traffic aware routing
b) admission control
c) load shedding
d) routing information protocol

Answer: d
Explanation: The Routing Information Protocol (RIP) is used by the network layer for the function of dynamic routing. Congestion control focuses on the flow of the traffic in the network and uses algorithms like traffic aware routing,

admission control and load shedding to deal with congestion.

9. The network layer protocol for internet is __________
a) ethernet
b) internet protocol
c) hypertext transfer protocol
d) file transfer protocol

Answer: b
Explanation: There are several protocols used in Network layer. Some of them are IP, ICMP, CLNP, ARP, IPX, HRSP etc. Hypertext transfer protocol is for application layer and ethernet protocol is for data link layer.

10. ICMP is primarily used for __________
a) error and diagnostic functions
b) addressing
c) forwarding
d) routing

Answer: a
Explanation: ICMP abbreviation for Internet Control Message Protocol is used by networking devices to send error messages and operational information indicating a host or router cannot be reached. ICMP operates over the IP packet to provide error reporting functionality as IP by itself cannot report errors.

1. Transport layer aggregates data from different applications into a single stream before passing it to ____________
a) network layer
b) data link layer
c) application layer
d) physical layer

Answer: a
Explanation: The flow of data in the OSI model flows in following manner Application -> Presentation -> Session -> Transport -> Network -> Data Link -> Physical. Each and every layer has its own set of functions and protocols to ensure efficient network performance.

2. Which of the following are transport layer protocols used in networking?
a) TCP and FTP
b) UDP and HTTP
c) TCP and UDP
d) HTTP and FTP

Answer: c
Explanation: Both TCP and UDP are transport layer protocol in networking. TCP is an abbreviation for Transmission Control Protocol and UDP is an abbreviation for User Datagram Protocol. TCP is connection oriented whereas UDP is connectionless.

3. User datagram protocol is called connectionless because _____________
a) all UDP packets are treated independently by transport layer
b) it sends data as a stream of related packets
c) it is received in the same order as sent order
d) it sends data very quickly

Answer: a
Explanation: UDP is an alternative for TCP and it is used for those purposes where speed matters most whereas loss of data is not a problem. UDP is connectionless whereas TCP is connection oriented.

4. Transmission control protocol ___________
a) is a connection-oriented protocol
b) uses a three way handshake to establish a connection

c) receives data from application as a single stream
d) all of the mentioned

Answer: d
Explanation: TCP provides reliable and ordered delivery of a stream of bytes between hosts communicating via an IP network. Major internet applications like www, email, file transfer etc rely on TCP. TCP is connection oriented and it is optimized for accurate delivery rather than timely delivery.

5. An endpoint of an inter-process communication flow across a computer network is called __________
a) socket
b) pipe
c) port
d) machine

Answer: a
Explanation: Socket is one end point in a two way communication link in the network. TCP layer can identify the application that data is destined to be sent by using the port number that is bound to socket.

6. Socket-style API for windows is called ____________
a) wsock
b) winsock
c) wins
d) sockwi

Answer: b
Explanation: Winsock is a programming interface which deals with input output requests for internet applications in windows OS. It defines how windows network software should access network services.

7. Which one of the following is a version of UDP with congestion control?
a) datagram congestion control protocol
b) stream control transmission protocol
c) structured stream transport
d) user congestion control protocol

Answer: a
Explanation: The datagram congestion control is a transport layer protocol which deals with reliable connection setup, teardown, congestion control, explicit congestion notification, and feature negotiation. It is used in modern day systems where there are really high chances of congestion. The protocol was last updated in the year 2008.

8. A _____ is a TCP name for a transport service access point.
a) port
b) pipe
c) node
d) protocol

Answer: a
Explanation: Just as the IP address identifies the computer, the network port identifies the application or service running on the computer. A port number is 16 bits. The combination of IP address preceded with the port number is called the socket address.

9. Transport layer protocols deals with ____________
a) application to application communication
b) process to process communication
c) node to node communication
d) man to man communication

Answer: b
Explanation: Transport layer is 4th layer in TCP/IP model and OSI reference model. It deals with logical communication

between process. It is responsible for delivering a message between network host.

10. Which of the following is a transport layer protocol?
a) stream control transmission protocol
b) internet control message protocol
c) neighbor discovery protocol
d) dynamic host configuration protocol

Answer: a
Explanation: The Stream Control Transmission Protocol (SCTP) is a transport layer protocol used in networking system where streams of data are to be continuously transmitted between two connected network nodes. Some of the other transport layer protocols are RDP, RUDP, TCP, DCCP, UDP etc.

1. Physical or logical arrangement of network is __________
a) Topology
b) Routing
c) Networking
d) Control

Answer: a
Explanation: Topology in networks is the structure or pattern in which each and every node in the network is connected. There are many topologies in networking like bus, tree, ring, star, mesh, and hybrid topology. There is no particular best topology and a suitable topology can be chosen based on the kind of application of the network .

2. Which network topology requires a central controller or hub?
a) Star
b) Mesh
c) Ring
d) Bus

Answer: a
Explanation: In star topology, no computer is connected to another computer directly but all the computers are connected to a central hub. Every message sent from a source computer goes through the hub and the hub then forwards the message only to the intended destination computer.

3. _______ topology requires a multipoint connection.
a) Star
b) Mesh
c) Ring
d) Bus

Answer: d
Explanation: In bus topology, there is a single cable to which all the network nodes are connected. So whenever a node tries to send a message or data to other nodes, this data passes through all other nodes in the network through the cable. It is really simple to install but it's not secure enough to be used in most of the computer network applications.

4. Data communication system spanning states, countries, or the whole world is ________
a) LAN
b) WAN
c) MAN
d) PAN

Answer: b
Explanation: WAN is the abbreviation for Wide Area Network. This network extends over a large geographical area. WANs are used to connect cities, states or even countries. A wireless connection is required to build a WAN. The best example of WAN is the Internet.

5. Data communication system within a building or campus is________

a) LAN
b) WAN
c) MAN
d) PAN

Answer: a
Explanation: LAN is an abbreviation for Local Area Network. This network interconnects computers in a small area such as schools, offices, residence etc. It is the most versatile kind of data communication system where most of the computer network concepts can be visibly used.

6. WAN stands for __________
a) World area network
b) Wide area network
c) Web area network
d) Web access network

Answer: b
Explanation: WAN is the abbreviation for Wide Area Network. This network extends over a large geographical area. These are used to connect cities, states or even countries. They can be connected through leased lines or satellites.

7. In TDM, slots are further divided into __________
a) Seconds
b) Frames
c) Packets
d) Bits

Answer: b
Explanation: TDM is the abbreviation for Time division multiplexing. It is technique for combining several low rate channels to a single high rate channel. For a certain time slot, the several channels could use the maximum bandwidth. Each channel is inactive for a period of time too. Some other multiplexing techniques are Frequency division multiplexing and Phase division multiplexing.

8. _____ is the multiplexing technique that shifts each signal to a different carrier frequency.
a) FDM
b) TDM
c) Both FDM & TDM
d) PDM

Answer: a
Explanation: FDM is an abbreviation for Frequency Division Multiplexing. This technique is used when the bandwidth of the channel is greater than the combined bandwidth of all the signals which are to be transmitted. The channel is active at all times unless a collision occurs with another channel trying to use the same frequency. Some other multiplexing techniques are Time division multiplexing and Phase division multiplexing.

1. The sharing of a medium and its link by two or more devices is called _________
a) Fully duplexing
b) Multiplexing
c) Micropleixng
d) Duplexing

Answer: b
Explanation: Multiplexing is a method using which one can send multiples signals through a shared medium at the same time. This helps in using less resources and thus saving the cost of sending messages.

2. Multiplexing is used in _______
a) Packet switching
b) Circuit switching
c) Data switching

d) Packet & Circuit switching

Answer: b
Explanation: Circuit switching is a switching method by which one can obtain a physical path between end points. Circuit switching method is also called a connection oriented network. Two nodes must be physically and logically connected to each other to create a circuit switching network.

3. Which multiplexing technique used to transmit digital signals?
a) FDM
b) TDM
c) WDM
d) FDM & WDM

Answer: b
Explanation: TDM abbreviation for Time Division Multiplexing is a method used for digital signals. Whereas FDM and WDM abbreviation for Frequency Division Multiplexing, and Wavelength Division Multiplexing, are used for analog signals. TDM is used in applications like ISDN (Integrated Services Digital Network) and PSTN (Public Switched Telephone Network).

4. If there are n signal sources of same data rate, then the TDM link has _______ slots.
a) n
b) n/2
c) n*2
d) 2^n

Answer: a
Explanation: In TDM, the total unit of time is divided equally among all the signal sources and each and every source has access to the complete channel bandwidth during its allotted time slot. When the time slot of the source is not active, it remains idle and waits for its slot to begin.

5. If link transmits 4000frames per second, and each slot has 8 bits, the transmission rate of circuit this TDM is __________
a) 32kbps
b) 500bps
c) 500kbps
d) 32bps

Answer: a
*Explanation: Transmission rate= frame rate * number of bits in a slot.*
Given: Frame rate = 4000/sec and number of bits in slot = 8
*Thus, Transmission rate = (4000 * 8) bps*
= 32000bps
= 32kbps

6. The state when dedicated signals are idle are called __________
a) Death period
b) Poison period
c) Silent period
d) Stop period

Answer: c
Explanation: There are instances when connection between two endpoints has been established, but no communication or transfer of messages occurs. This period of time is called silent period. The silent period ends when either of the two endpoints starts the communication.

7. Multiplexing provides _________
a) Efficiency

b) Privacy
c) Anti jamming
d) Both Efficiency & Privacy

Answer: d
Explanation: Multiplexing helps us to transfer our messages over a shared channel. This brings up the issue of privacy and efficiency. Fortunately, Multiplexing has high efficiency and high privacy when implemented because in the implementation, the transport layer of the OSI network model handles the function of multiplexing through interfaces called ports which provide the required efficiency and privacy.

8. In TDM, the transmission rate of a multiplexed path is always _______ the sum of the transmission rates of the signal sources.
a) Greater than
b) Lesser than
c) Equal to
d) Equal to or greater than

Answer: a
Explanation: In TDM the transmission rate provided by the path that is multiplexed will always be greater than the sum of transmission rates of the single sources. This happens because the transmission rate is provided to each source only for a small period of time.

9. In TDM, slots are further divided into _________
a) Seconds
b) Frames
c) Packets
d) Bits

Answer: b
Explanation: TDM is the abbreviation for Time division multiplexing. It is technique for combining several low rate channels to a single high rate channel. For a certain time slot, the several channels could use the maximum bandwidth. Each channel is inactive for a period of time too. Some other multiplexing techniques are Frequency division multiplexing and Phase division multiplexing.

1. Which of the following delay is faced by the packet in travelling from one end system to another?
a) Propagation delay
b) Queuing delay
c) Transmission delay
d) All of the mentioned

Answer: d
Explanation: When a packet has to travel from one end system to another, it first faces the queuing delay when there are multiple packets which are to be sent, then it faces the transmission delay to convert the packet into bits to be transmitted, and then it faces the propagation delay to propagate the bits through the physical medium.

2. For a 10Mbps Ethernet link, if the length of the packet is 32bits, the transmission delay is ____________ (in microseconds)
a) 3.2
b) 32
c) 0.32
d) 320

Answer: a
Explanation: Transmission rate = length / transmission rate = 32/10 = 3.2 microseconds.

3. The time required to examine the packet's header and determine where to direct the packet is part of __________
a) Processing delay
b) Queuing delay

c) Transmission delay
d) Propagation delay

Answer: a
Explanation: Processing delay is induced at a router's or other network processor's end in the path of the packet and is caused by the time taken by the processor to examine the packet's header to decide the further path of the packet.

4. Given L = number of bits in the packet, a = average rate and R = transmission rate. The Traffic intensity in the network is given by ____________
a) La/R
b) LR/a
c) R/La
d) Ra/L

Answer: a
*Explanation: Traffic Intensity = (Number of bits in packet * Average Transmission rate)/Current Transmission rate.*

5. In the transfer of file between server and client, if the transmission rates along the path is 10Mbps, 20Mbps, 30Mbps, 40Mbps. The throughput is usually ___________
a) 20Mbps
b) 10Mbps
c) 40Mbps
d) 50Mbps

Answer: b
Explanation: The throughput is generally the transmission rate of bottleneck link.

6. If end to end delay is given by dend-end = N(dproc + dtrans + dprop) is a non congested network. The number of routers between source and destination is?
a) N/2
b) N
c) N-1
d) 2N

Answer: c
Explanation: In the equation N (dproc + dtrans + dprop), N is the number of checkpoints/stops that the packet makes as it reaches the destination. The stops are made at each router and the final destination node. Now, since N = number of routers + final node, then number of routers = N – final node. As we know, there is only 1 final node in a path, thus, number of routers = N – 1. Suppose, There is a path A->R1->R2->B for a packet where A is the source node, B is the final node and R1 and R2 are routers. The total delay would be given by N (dproc + dtrans + dprop) where N = 3, since the packet would stop at R1, R2 and B. The number of routers here are 2, and (N – 1) is also 2.

7. The total nodal delay is given by ____________
a) dnodal = dproc – dqueue + dtrans + dprop
b) dnodal = dproc + dtrans – dqueue
c) dnodal = dproc + dqueue + dtrans + dprop
d) dnodal = dproc + dqueue – dtrans – dprop

Answer: c
Explanation: The total node-to-node delay, that is, nodal delay is the sum of all, the processing delay, queuing delay, transmission delay and propagation delay. Ideally, the nodal delay must be low as possible for a better Quality of Service of the network.

8. In a network, If P is the only packet being transmitted and there was no earlier transmission, which of the following delays could be zero?
a) Propagation delay
b) Queuing delay
c) Transmission delay

d) Processing delay

Answer: b
Explanation: Since there is no other packet to be transmitted, there is no need for a queue. Therefore, the delay caused due to the queuing would be none i.e. 0.

9. Transmission delay does not depend on _____________
a) Packet length
b) Distance between the routers
c) Transmission rate
d) Bandwidth of medium

Answer: b
Explanation: Transmission delay = packet length / transmission rate. The transmission rate depends upon the bandwidth of the medium.

10. Propagation delay depends on ___________
a) Packet length
b) Transmission rate
c) Distance between the routers
d) Speed of the CPU

Answer: c
Explanation: Propagation delay is caused when the packet is in its electric signal form and is travelling through a medium (a wire or a electromagnetic wave). Propagation delay is the time it takes a bit to propagate from one router to the next. If the distance between the routers is increased, it will take longer time to propagate, that is, there would be more propagation delay.

1. _____________ allows LAN users to share computer programs and data.
a) Communication server
b) Print server
c) File server
d) Network

Answer: c
Explanation: A file server allows LAN users to share computer programs and data. It uses the File Transfer Protocol to provide this feature on ports 20 and 21. The file server works as a medium for the transfer.

2. With respect to physical media, STP cables stands for _________
a) Shielded Twisted Pair Cable
b) Spanning Tree Protocol Cable
c) Static Transport Protocol Cable
d) Shielded Two Power Cable

Answer: a
Explanation: For physical media, STP cable stands for Shielded twisted pair cable. 100 Mbps is the max data capacity of STP cable and its default connector is RJ45. It is popularly used in LANs due to its ease of maintenance and installation.

3. A standalone program that has been modified to work on a LAN by including concurrency controls such as file and record locking is an example of ___________
a) LAN intrinsic software
b) LAN aware software
c) Groupware
d) LAN ignorant software

Answer: a
Explanation: A standalone program that has been modified to work on a LAN by including concurrency controls such as file and record locking is an example of LAN intrinsic software. They are used to give better functionality of the program

and the applications working over it to the users of the LAN.

4. The __________ portion of LAN management software restricts access, records user activities and audit data, etc.
a) Configuration management
b) Security management
c) Performance management
d) Recovery management

Answer: b
Explanation: The Security management portion of LAN management software restricts access, records user activities, and audit data. It is responsible for controlling access to the network based on predefined policy. The security management ensures authentication, confidentiality, and integrity in the LAN.

5. What is the max length of the Shielded twisted pair cable?
a) 100 ft
b) 200 ft
c) 100 m
d) 200 m

Answer: c
Explanation: The max the Shielded twisted pair cable is 100 meters. If the length exceeds 100 meters, the loss of signals flowing through the cable would be really high. Thus, STP cable is more suitable for smaller networks like LANs.

6. What is the max data transfer rate of STP cables?
a) 10 Mbps
b) 100 Mbps
c) 1000 Mbps
d) 10000 Mbps

Answer: b
Explanation: 100 Mbps is the max data transfer rate that can be handled by STP cables, and its default connector is RJ-45. 100 Mbps is a feasible data transfer rate for small networks like LANs.

7. Which connector does the STP cable use?
a) BNC
b) RJ-11
c) RJ-45
d) RJ-69

Answer: c
Explanation: RJ-45 is used for STP cable. 100 Mbps is the max data transfer rate that can be handled by STP. RJ-45 is popularly used to connect to modern-day routers, computer network cards, and other network devices.

8. What is the central device in star topology?
a) STP server
b) Hub/switch
c) PDC
d) Router

Answer: b
Explanation: In star topology, no computer is connected to another computer directly but all the computers are connected to a central switch or hub. Every message sent from a source computer goes through the switch or hub and the switch or hub then forwards the message only to the intended destination computer.

9. What is the max data transfer rate for optical fiber cable?
a) 10 Mbps
b) 100 Mbps
c) 1000 Mbps

d) 10000 Mbps

Answer: d
Explanation: Fiber channel speeds have been increasing over the years. 10000 Mbps is the max data transfer rate for optical fiber cables. It is said to be the fastest among the other kinds of cables like STP cables and co-axial cables. People are now using optical fiber cables instead of STP cables for LANs due to their fast data transfer capability.

10. Which of the following architecture uses the CSMA/CD access method?
a) ARC net
b) Ethernet
c) Router
d) STP server

Answer: b
Explanation: Collision detection is not possible in Ethernet without extensions. Collision detection techniques for multiple access like CSMA/CD are used to detect collisions in the Ethernet architecture.

1. The attacker using a network of compromised devices is known as _____________
a) Internet
b) Botnet
c) Telnet
d) D-net

Answer: b
Explanation: Botnet is a network of compromised devices used by the attacker without the owner's knowledge to perform unethical activities such as spamming. The attacker usually uses the least secure devices to create the botnet.

2. Which of the following is a form of DoS attack?
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) All of the mentioned

Answer: d
Explanation: In a DoS attack, the attacker won't let the victims access the network by using a certain method that ensures that an essential network resource is unavailable to the victim. In vulnerability attack, the attacker exploits any obvious vulnerable entity in the network to deny the victim access into the network. In bandwidth flooding, the attacker floods the victim with a huge flow of packets and uses up all the bandwidth. In connection flooding, the attacker floods the victim network with a huge number of connections, so that, no other machine can connect to it.

3. The DoS attack, in which the attacker establishes a large number of half-open or fully open TCP connections at the target host is ________
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) UDP flooding

Answer: c
Explanation: In Vulnerability attack, the attacker exploits the vulnerable control points of the network to deny access to the victims. In Bandwidth flooding, the attacker intentionally uses up all the bandwidth by flooding the victim with a deluge of packets and makes sure that the victim can't use any bandwidth. In UDP flooding, too many UDP packets are sent by the attacker to the victim at random ports.

4. The DoS attack, in which the attacker sends deluge of packets to the targeted host is ________
a) Vulnerability attack
b) Bandwidth flooding
c) Connection flooding
d) UDP flooding

Answer: b
Explanation: In Bandwidth flooding, the attacker floods the victim machine with a deluge of packets to make sure that no bandwidth is available. The victim then cannot utilize the complete bandwidth to perform its operation.

5. Packet sniffers involve ____________
a) Active receiver
b) Passive receiver
c) Legal receiver
d) Partially-active receiver

Answer: b
Explanation: The function of packet sniffers is to just silently receive the packets flowing in the channel. If they inject any packets into the channel, they might alert the other users about the intrusion.

6. Sniffers can be prevented by using _______________
a) Wired environment
b) WiFi
c) Ethernet LAN
d) Switched network

Answer: d
Explanation: Switches make sure that the packet is sent to the intended receiver and no one else, thus preventing Sniffers to perform their function. Intelligent switches are hence used preferably for the network.

7. Firewalls are often configured to block ___________
a) UDP traffic
b) TCP traffic
c) Sensitive traffic
d) Best-effort traffic

Answer: a
Explanation: UDP is more vulnerable to attacks, so firewalls are often configured to block suspicious UDP traffic.

8. In a network, If P is the only packet being transmitted and there was no earlier transmission, which of the following delays could be zero?
a) Propagation delay
b) Queuing delay
c) Transmission delay
d) Processing delay

Answer: b
Explanation: Since there is no other packet to be transmitted, there is no need for a queue. Therefore, the delay caused due to the queuing would be none i.e. 0.

1. Which of this is not a guided media?
a) Fiber optical cable
b) Coaxial cable
c) Wireless LAN
d) Copper wire

Answer: c
Explanation: Wireless LAN is unguided media.

2. UTP is commonly used in __________
a) DSL
b) FTTP
c) HTTP
d) None of the mentioned

Answer: a
Explanation: Unshielded twisted pair(UTP) is commonly used in home access.

3. Coaxial cable consists of _______ concentric copper conductors.
a) 1
b) 2
c) 3
d) 4

Answer: b
Explanation: Coaxial cable has an inner conductor surrounded by a insulating layer, which is surrounded by a conducting shield. Coaxial cable is used to carry high frequency signals with low losses.

4. Fiber optics posses following properties __________
a) Immune electromagnetic interference
b) Very less signal attenuation
c) Very hard to tap
d) All of the mentioned

Answer: d
Explanation: In fibre optics the transmission of information is in the form of light or photons. Due to all above properties mentioned in options fibre optics can be submerged in water and are used at more risk environments.

5. If an Optical Carrier is represented as OC-n, generally the link speed equals(in Mbps) __________
a) n*39.8
b) n*51.8
c) 2n*51.8
d) None of the mentioned

Answer: b
*Explanation: The base unit of transmission rates in optical fibre is 51.8 Mbits/s. So an optical carrier represented as OC-n has n*51.8 Mbits/s transmission speed. For eg. OC-3 has 3*51.8 Mbits/s speed.*

6. Terrestrial radio channels are broadly classifed into _____ groups.
a) 2
b) 3
c) 4
d) 1

Answer: b
Explanation: The three types are those that operate over very short distance, those that operate in local areas, those that operate in the wide area.

7. Radio channels are attractive medium because __________
a) Can penetrate walls
b) Connectivity can be given to mobile user
c) Can carry signals for long distance
d) All of the mentioned

Answer: d
Explanation: Radio channels can penetrate walls, can be used to provide connectivity to mobile users and can also carry signals for long distances.

8. Geostationary satellites ___________
a) Are placed at a fixed point above the earth
b) Rotate the earth about a fixed axis
c) Rotate the earth about a varying axis
d) All of the mentioned

Answer: a
Explanation: They are placed in orbit at 36,000km above Earth's surface.

1. A local telephone network is an example of a _______ network.
a) Packet switched
b) Circuit switched
c) Bit switched
d) Line switched

Answer: b
Explanation: Circuit switching is connection oriented switching technique, whereas in the case of packet switching, it is connectionless. Circuit switching is implemented in the Physical layer, whereas packet switching is implemented in the Network layer. Internet too is based on the concept of circuit switching.

2. Most packet switches use this principle ____________
a) Stop and wait
b) Store and forward
c) Store and wait
d) Stop and forward

Answer: b
Explanation: The packet switch will not transmit the first bit to outbound link until it receives the entire packet. If the entire packet is not received and the time-out period expires, the packet switch will inform the sender to resend the part of packet or the entire packet based on the algorithm being used.

3. If there are N routers from source to destination, the total end to end delay in sending packet P(L-> number of bits in the packet R-> transmission rate) is equal to ______________
a) N
b) (N*L)/R
c) (2N*L)/R
d) L/R

Answer: b
*Explanation: The equation to find the end to end delay when no. of bits, transmission rate and no. of routers is given by (N*L)/R. The total end to end delay, that is, nodal delay is the sum of all, the processing delay, queuing delay, transmission delay and propagation delay.*

4. What are the Methods to move data through a network of links and switches?
a) Packet switching and Line switching
b) Circuit switching and Line switching
c) Line switching and bit switching
d) Packet switching and Circuit switching

Answer: d
Explanation: Packet switching and Circuit switching are two different types of switching methods used to connect the multiple communicating devices with one another. Packet switching is used in conventional LAN systems and circuit switching is used in telephonic systems.

5. The required resources for communication between end systems are reserved for the duration of the session between end systems in ________ method.
a) Packet switching
b) Circuit switching
c) Line switching
d) Frequency switching

Answer: b
Explanation: In circuit switching, a physical path between the sender and receiver is established. This path is maintained until the connection is needed. Circuit switching is implemented in the Physical layer and is used in telephonic systems.

6. As the resources are reserved between two communicating end systems in circuit switching, ___________ is achieved.
a) authentication
b) guaranteed constant rate
c) reliability
d) store and forward

Answer: b
Explanation: Circuit switching is connection oriented and is always implemented in the physical layer. Once a path is set, all transmission occurs through the same path. It is used since the early times in telephonic systems.

7. In _________ systems, resources are allocated on demand.
a) packet switching
b) circuit switching
c) line switching
d) frequency switching

Answer: a
Explanation: In packet switching, the bits are received in out of order and need to be assembled at the receiver end, whereas in the case of Circuit switching, all the bits are received in order. All transmissions may not occur through the same path in case of packet switching.

8. Which of the following is not an application layer service?
a) Network virtual terminal
b) File transfer, access, and management
c) Mail service
d) Error control

Answer: d
Explanation: Application layer is the topmost layer in the OSI model. Network virtual terminal, mail service, file transfer, access and management are all services of the application layer. It uses protocols like HTTP, FTP, and DNS etc. to provide these services.

1. Which is not a application layer protocol?
a) HTTP
b) SMTP
c) FTP
d) TCP

Answer: d
Explanation: TCP is transport layer protocol.

2. The packet of information at the application layer is called __________
a) Packet
b) Message
c) Segment
d) Frame

Answer: b
Explanation: For Application, Presentation and Session layers there is no data format for message. Message is message as such in these three layers. But when it comes to Transport, Network, Data and Physical layer they have data in format of segments, packets, frames and bits respectively.

3. Which one of the following is an architecture paradigms?
a) Peer to peer
b) Client-server
c) HTTP
d) Both Peer-to-Peer & Client-Server

Answer: d
Explanation: HTTP is a protocol.

4. Application developer has permission to decide the following on transport layer side
a) Transport layer protocol
b) Maximum buffer size
c) Both Transport layer protocol and Maximum buffer size
d) None of the mentioned

Answer: c
Explanation: Application layer provides the interface between applications and the network. So application developer can decide what transport layer to use and what should be its maximum buffer size.

5. Application layer offers _______ service.
a) End to end
b) Process to process
c) Both End to end and Process to process
d) None of the mentioned

Answer: a
Explanation: End to End service is provided in the application layer. Whereas process to process service is provided at the transport layer.

6. E-mail is _________
a) Loss-tolerant application
b) Bandwidth-sensitive application
c) Elastic application
d) None of the mentioned

Answer: c
Explanation: Because it can work with available throughput.

7. Pick the odd one out.
a) File transfer
b) File download
c) E-mail
d) Interactive games

Answer: d
Explanation: File transfer, File download and Email are services provided by the application layer and there are message and data oriented.

8. Which of the following is an application layer service?
a) Network virtual terminal
b) File transfer, access, and management
c) Mail service
d) All of the mentioned

Answer: d
Explanation: The services provided by the application layer are network virtual terminal, file transfer, access and management, mail services, directory services, various file and data operations.

9. To deliver a message to the correct application program running on a host, the _______ address must be consulted.
a) IP
b) MAC
c) Port
d) None of the mentioned

Answer: c
Explanation: IP address lets you know where the network is located. Whereas MAC address is a unique address for every device. Port address identifies a process or service you want to carry on.

10. Which is a time-sensitive service?
a) File transfer
b) File download
c) E-mail
d) Internet telephony

Answer: d
Explanation: Internet telephony is Loss-tolerant other applications are not.

11. Transport services available to applications in one or another form _________
a) Reliable data transfer
b) Timing
c) Security
d) All of the mentioned

Answer: d
Explanation: The transport services that are provided to application are reliable data transfer, security and timing. These are very important for proper end to end services.

12. Electronic mail uses which Application layer protocol?
a) SMTP
b) HTTP
c) FTP
d) SIP

Answer: a
Explanation: Email uses various protocols like SMTP, IMAP and POP. The most prominent one used in application layer is SMTP.

1. The ____________ translates internet domain and host names to IP address.
a) domain name system
b) routing information protocol
c) network time protocol
d) internet relay chat

Answer: a
Explanation: Domain name system is the way the internet domain names are stored and translated to IP addresses. The domain names systems matches the name of website to ip addresses of the website.

2. Which one of the following allows a user at one site to establish a connection to another site and then pass keystrokes from local host to remote host?
a) HTTP
b) FTP
c) Telnet
d) TCP

Answer: c
Explanation: Telnet is used for accessing remote computers. Using telnet a user can access computer remotely. With Telnet, you can log on as a regular user with whatever privileges you may have been granted to the specific application and data on the computer.

3. Application layer protocol defines ____________
a) types of messages exchanged
b) message format, syntax and semantics

c) rules for when and how processes send and respond to messages
d) all of the mentioned

Answer: d
Explanation: Application layer deals with the user interface, what message is to be sent or the message format, syntax and semantics. A user has access to application layer for sending and receiving messages.

4. Which one of the following protocol delivers/stores mail to reciever server?
a) simple mail transfer protocol
b) post office protocol
c) internet mail access protocol
d) hypertext transfer protocol

Answer: a
Explanation: SMTP, abbreviation for Simple Mail Transfer Protocol is an application layer protocol. A client who wishes to send a mail creates a TCP connection to the SMTP server and then sends the mail across the connection.

5. The ASCII encoding of binary data is called
a) base 64 encoding
b) base 32 encoding
c) base 16 encoding
d) base 8 encoding

Answer: a
Explanation: Base64 is used commonly in a number of applications including email via MIME, and storing complex data in XML. Problem with sending normal binary data to a network is that bits can be misinterpreted by underlying protocols, produce incorrect data at receiving node and that is why we use this code.

6. Which one of the following is an internet standard protocol for managing devices on IP network?
a) dynamic host configuration protocol
b) simple network management protocol
c) internet message access protocol
d) media gateway protocol

Answer: b
Explanation: SNMP is a set of protocols for network management and monitoring. This protocol is included in the application layer. SNMP uses 7 protocol data units.

7. Which one of the following is not an application layer protocol?
a) media gateway protocol
b) dynamic host configuration protocol
c) resource reservation protocol
d) session initiation protocol

Answer: c
Explanation: Resource reservation protocol is used in transport layer. It is designed to reserve resources across a network for quality of service using the integrated services model.

8. Which protocol is a signaling communication protocol used for controlling multimedia communication sessions?
a) session initiation protocol
b) session modelling protocol
c) session maintenance protocol
d) resource reservation protocol

Answer: a
Explanation: SIP is a signaling protocol in which its function includes initiating, maintaining and terminating real time sessions. SIP is used for signaling and controlling multimedia sessions.

9. Which one of the following is not correct?
a) Application layer protocols are used by both source and destination devices during a communication session
b) HTTP is a session layer protocol
c) TCP is an application layer protocol
d) All of the mentioned

Answer: d
Explanation: HTTP is an application layer protocol. Whereas TCP is a transport layer protocol.

10. When displaying a web page, the application layer uses the _____________
a) HTTP protocol
b) FTP protocol
c) SMTP protocol
d) TCP protocol

Answer: a
Explanation: HTTP is abbreviation for hypertext transfer protocol. It is the foundation of data communication for world wide web. This protocol decides how the message is formatted and transmitted etc.

1. The number of objects in a Web page which consists of 4 jpeg images and HTML text is ________
a) 4
b) 1
c) 5
d) 7

Answer: c
Explanation: 4 jpeg images + 1 base HTML file.

2. The default connection type used by HTTP is _________
a) Persistent
b) Non-persistent
c) Can be either persistent or non-persistent depending on connection request
d) None of the mentioned

Answer: a
Explanation: By default the http connection is issued with persistent connection. In persistent connection server leaves connection open after sending response. As little as one RTT (Time for a small packet to travel from client to server and back) is required for all referenced objects.

3. The time taken by a packet to travel from client to server and then back to the client is called __________
a) STT
b) RTT
c) PTT
d) JTT

Answer: b
Explanation: RTT stands for round-trip time.

4. The HTTP request message is sent in _________ part of three-way handshake.
a) First
b) Second
c) Third
d) Fourth

Answer: c
Explanation: In first step client sends a segment to establish a connection with the server. In the second the step the client waits for the acknowledgement to be received from the server. After receiving the acknowledgement, the client sends actual data in the third step.

5. In the process of fetching a web page from a server the HTTP request/response takes __________ RTTs.
a) 2
b) 1
c) 4
d) 3

Answer: b
Explanation: By default the http connection will be persistent connection. Hence it will take only 1 RTT to fetch a webpage from a server.

6. The first line of HTTP request message is called _____________
a) Request line
b) Header line
c) Status line
d) Entity line

Answer: a
Explanation: The line followed by request line are called header lines and status line is the initial part of response message.

7. The values GET, POST, HEAD etc are specified in ____________ of HTTP message
a) Request line
b) Header line
c) Status line
d) Entity body

Answer: a
Explanation: It is specified in the method field of request line in the HTTP request message.

8. The __________ method when used in the method field, leaves entity body empty.
a) POST
b) SEND
c) GET
d) PUT

Answer: c
Explanation: There are two methods which help to request a response from a server. Those are GET and POST. In GET method, the client requests data from server. In POST method the client submits data to be processed to the server.

9. The HTTP response message leaves out the requested object when ____________ method is used
a) GET
b) POST
c) HEAD
d) PUT

Answer: c
Explanation: HEAD method is much faster than GET method. In HEAD method much smaller amount of data is transferred. The HEAD method asks only for information about a document and not for the document itself.

10. Find the oddly matched HTTP status codes
a) 200 OK
b) 400 Bad Request
c) 301 Moved permanently
d) 304 Not Found

Answer: d
Explanation: 404 Not Found.

11. Which of the following is not correct?
a) Web cache doesnt has its own disk space
b) Web cache can act both like server and client
c) Web cache might reduce the response time
d) Web cache contains copies of recently requested objects

Answer: a
Explanation: Web cache or also known as HTTP cache is a temporary storage where HTML pages and images are stored temporarily so that server lag could be reduced.

12. The conditional GET mechanism
a) Imposes conditions on the objects to be requested
b) Limits the number of response from a server
c) Helps to keep a cache upto date
d) None of the mentioned

Answer: c
Explanation: The HTTP protocol requests the server of the website its trying to access so that it can store its files, images etc. in cache memory. This request of asking the server for a document considering a specific parameter is called conditional GET Request.

13. Which of the following is present in both an HTTP request line and a status line?
a) HTTP version number
b) URL
c) Method
d) None of the mentioned

Answer: a
Explanation: Status line is the the start line of an HTTP response. It contains the information such as the protocol version, a status text, status code.
Answer: a
Explanation: Persistent connections are kept active after completing transaction so that multiple objects can be sent over the same TCP connection.

2. HTTP is ________ protocol.
a) application layer
b) transport layer
c) network layer
d) data link layer

Answer: a
Explanation: HTTP is an Application layer protocol used to define how messages are formatted and transmitted through the World Wide Web.

3. In the network HTTP resources are located by
a) uniform resource identifier
b) unique resource locator
c) unique resource identifier
d) union resource locator

Answer: a
Explanation: The Uniform Resource Identifier is a name and locator for the resource to be located by the HTTP. The URLs and URNs are derived through the identifier.

4. HTTP client requests by establishing a __________ connection to a particular port on the server.
a) user datagram protocol
b) transmission control protocol
c) border gateway protocol

d) domain host control protocol

Answer: b
Explanation: HTTP clients perform requests using a TCP connection, because the TCP connection provides a more reliable service. UDP is not a reliable protocol, border gateway protocol is used on top of TCP, while domain host control protocol is a network layer protocol.

5. In HTTP pipelining ________________
a) multiple HTTP requests are sent on a single TCP connection without waiting for the corresponding responses
b) multiple HTTP requests can not be sent on a single TCP connection
c) multiple HTTP requests are sent in a queue on a single TCP connection
d) multiple HTTP requests are sent at random on a single TCP connection

Answer: a
Explanation: HTTP pipelining helps the client make multiple requests without having to waiting for each response, thus saving a lot of time and bandwidth for the client.

6. FTP server listens for connection on port number ____________
a) 20
b) 21
c) 22
d) 23

Answer: b
Explanation: Port 20 is used for FTP data. Port 22 is used for SSH remote login. Port 23 is used for TELNET.

7. In FTP protocol, client contacts server using ____ as the transport protocol.
a) transmission control protocol
b) user datagram protocol
c) datagram congestion control protocol
d) stream control transmission protocol

Answer: a
Explanation: The clients use the Transmission Control Protocol for FTP as it's more reliable than UDP, DCCP, and SCTP, and reliability of file transfer is required to be as high as possible for FTP.
Answer: b
Explanation: In Passive mode of FTP, the client initiates both data and control connections, while in Active mode, the client initiates the control connection and then the server initiates the data connection.

9. The File Transfer Protocol is built on ______________
a) data centric architecture
b) service oriented architecture
c) client server architecture
d) connection oriented architecture

Answer: c
Explanation: The FTP connection includes a Server and a Client which wish to share files. The server can have multiple clients at the same time while the client communicates with only one server at a time.

10. In File Transfer Protocol, data transfer cannot be done in ___________
a) stream mode
b) block mode
c) compressed mode
d) message mode

Answer: d
Explanation: In Stream mode, the data is transferred in a continuous stream. In Block mode, data is transferred after being divided into smaller blocks. In Compressed mode, data is transferred after being compressed using some

compression algorithm.

1. Expansion of FTP is __________
a) Fine Transfer Protocol
b) File Transfer Protocol
c) First Transfer Protocol
d) Fast Transfer Protocol

Answer: b
Explanation: File Transfer Protocol is an application layer protocol used to share "files" between a server and a client. The protocol uses two separate ports for data and control connections: port 20 for data and port 21 for control.

2. FTP is built on _____ architecture.
a) Client-server
b) P2P
c) Data centric
d) Service oriented

Answer: a
Explanation: An FTP connection includes a Server and a Client which wish to share a number of data files. The server can transfer files with multiple clients at the same time while the client communicates with only one server at a time.

3. FTP uses _________ parallel TCP connections to transfer a file.
a) 1
b) 2
c) 3
d) 4

Answer: b
Explanation: Control connection using FTP port: 21, and data connection using FTP port: 20. The FTP session is started or ended using port 21 and the actual data i.e. files are sent through port 20.

4. Identify the incorrect statement regarding FTP.
a) FTP stands for File Transfer Protocol
b) FTP uses two parallel TCP connections
c) FTP sends its control information in-band
d) FTP sends exactly one file over the data connection

Answer: c
Explanation: FTP is out-of-band because the data connection is done separately through port 20 and control connection is done separately through port 21.

5. If 5 files are transferred from server A to client B in the same session. The number of TCP connections between A and B is _______
a) 5
b) 10
c) 2
d) 6

Answer: d
Explanation: The client would first initiate the TCP control connection through port 21. Then for every file transfer, a separate connection would be made through port 20. Now, since we have five files to be transferred, 1 control connection + 5 data connections = 6 total TCP connections.

6. FTP server _____________
a) Maintains state information
b) Is stateless
c) Has single TCP connection for a file transfer

d) Has UDP connection for file transfer

Answer: a
Explanation: FTP server maintains state information of every control connection to keep track of the active and inactive connections in the session. This helps the server decide which connection to terminate, in case the connection is inactive for too long.

7. The commands, from client to server, and replies, from server to client, are sent across the control connection in ________ bit ASCII format.
a) 8
b) 7
c) 3
d) 5

Answer: b
Explanation: FTP was designed to transmit commands only in English characters that are possible with just 7 bits in ASCII. Even the media has to be converted to ASCII before transmission.

8. Find the FTP reply whose message is wrongly matched.
a) 331 – Username OK, password required
b) 425 – Can't open data connection
c) 452 – Error writing file
d) 452 – Can't open data connection

Answer: d
Explanation: The correct response code for the message "Can't open data connection" is 425. Response code 452 is sent usually when the connection is suddenly closed.

9. The data transfer mode of FTP, in which all the fragmenting has to be done by TCP is ________
a) Stream mode
b) Block mode
c) Compressed mode
d) Message mode

Answer: a
Explanation: Stream mode is the default mode of FTP, in which the TCP transforms/fragments the data into segments, and then after the transmission is completed, converts it back to stream of bytes.

10. The password is sent to the server using ________ command.
a) PASSWD
b) PASS
c) PASSWORD
d) PWORD

Answer: b
Explanation: The PASS command, preceded by the username, completes the user's identification for access control in an FTP session. Without the valid password, the user won't be able to initiate the FTP connection.

1. When the mail server sends mail to other mail servers it becomes ____________
a) SMTP server
b) SMTP client
c) Peer
d) Master

Answer: b
Explanation: SMTP clients are the entities that send mails to other mail servers. The SMTP servers cannot send independent mails to other SMTP servers as an SMTP server. There are no masters or peers in SMTP as it is based on the client-server architecture.

2. If you have to send multimedia data over SMTP it has to be encoded into _______
a) Binary
b) Signal
c) ASCII
d) Hash

Answer: c
Explanation: Since only 7-bit ASCII codes are transmitted through SMTP, it is mandatory to convert binary multimedia data to 7-bit ASCII before it is sent using SMTP.

3. Expansion of SMTP is ________
b) Simple Message Transfer Protocol
c) Simple Mail Transmission Protocol
d) Simple Message Transmission Protocol

Answer: a
Explanation: SMTP or Simple Mail Transfer Protocol is an application layer protocol used to transport e-mails over the Internet. Only 7-bit ASCII codes can be sent using SMTP.

4. In SMTP, the command to write receiver's mail address is written with the command _______
a) SEND TO
b) RCPT TO
c) MAIL TO
d) RCVR TO

Answer: b
Explanation: RCPT TO command is followed by the recipient's mail address to specify where or to whom the mail is going to through the internet. If there is more than one receiver, the command is repeated for each address continually.

5. The underlying Transport layer protocol used by SMTP is ________
a) TCP
b) UDP
c) Either TCP or UDP
d) IMAP

Answer: a
Explanation: TCP is a reliable protocol, and Reliability is a mandatory requirement in e-mail transmission using SMTP.

6. Choose the statement which is wrong incase of SMTP?
a) It requires message to be in 7bit ASCII format
b) It is a pull protocol
c) It transfers files from one mail server to another mail server
d) SMTP is responsible for the transmission of the mail through the internet

Answer: b
Explanation: In SMTP, the sending mail server pushes the mail to receiving mail server hence it is push protocol. In a pull protocol such as HTTP, the receiver pulls the resource from the sending server.

7. Internet mail places each object in _________
a) Separate messages for each object
b) One message
c) Varies with number of objects
d) Multiple messages for each object

Answer: b
Explanation: It places all objects into one message as it wouldn't be efficient enough if there are different messages for each object. The objects include the text and all the multimedia to be sent.

8. Typically the TCP port used by SMTP is _________
a) 25
b) 35
c) 50
d) 15

Answer: a
Explanation: The ports 15, 35 and 50 are all UDP ports and SMTP only uses TCP port 25 for reliability.

9. A session may include ________
a) Zero or more SMTP transactions
b) Exactly one SMTP transactions
c) Always more than one SMTP transactions
d) Number of SMTP transactions cant be determined

Answer: a
Explanation: An SMTP session consists of SMTP transactions only even if no transactions have been performed. But no transactions in the session might mean that the session is inactive or is just initiated.

10. Which of the following is an example of user agents for e-mail?
a) Microsoft Outlook
b) Facebook
c) Google
d) Tumblr

Answer: a
Explanation: Among the options, only Microsoft Outlook is an e-mail agent. Google is a search engine and Facebook, and Tumblr are social networking platforms. Gmail and Alpine are some other examples of e-mail agent.

11. When the sender and the receiver of an email are on different systems, we need only _________
a) One MTA
b) Two UAs
c) Two UAs and one MTA
d) Two UAs and two MTAs

Answer: d
Explanation: The sender's User Agent (UA) submits the message to a Message Transfer Agent (MTA). Then the MTA sends the message to another MTA i.e. a mail relay. Then the receiver receives the message from the mail relay whenever it is available.

12. User agent does not support this ___________
a) Composing messages
b) Reading messages
c) Replying messages
d) Routing messages

Answer: d
Explanation: The user agent is basically a software program that allows the user to send, and receive e-mail messages. Routing of the message is done by the Message Transfer Agent.

1. Simple mail transfer protocol (SMTP) utilizes _________ as the transport layer protocol for electronic mail transfer.
a) TCP
b) UDP
c) DCCP
d) SCTP

Answer: a

Explanation: Since TCP is a reliable protocol, it's more efficient to use TCP protocol for e-mail transfer. TCP also provides more security than other transport layer protocols.

2. SMTP connections secured by SSL are known as _____________
a) SMTPS
b) SSMTP
c) SNMP
d) STARTTLS

Answer: a
Explanation: SSMTP is a simple mail transfer program to send mail from a local PC to a mail host. SNMP is a network management protocol. STARTTLS connections are secured by TLS.

3. SMTP uses which of the following TCP port?
a) 22
b) 23
c) 21
d) 25

Answer: d
Explanation: Port 21 is used for FTP control connection, port 22 is used by SSH, and port 23 is used by TELNET.

4. Which one of the following protocol is used to receive mail messages?
a) SMTP
b) Post Office Protocol (POP)
c) Internet Message Access Protocol (IMAP)
d) FTP

Answer: d
Explanation: FTP is used to share files. SMTP, POP and IMAP are the protocols used to send and receive mails on the internet.

5. What is on-demand mail relay (ODMR)?
a) protocol for SMTP security
b) an SMTP extension
c) protocol for web pages
d) protocol for faster mail transfer

Answer: b
Explanation: ODMR is an extension to SMTP, in which mails are relayed to the receivers after they are authenticated. It allows only the authorized receivers to receive the mail.

6. An email client needs to know the _________ of its initial SMTP server.
a) IP address
b) MAC address
c) URL
d) Name

Answer: a
Explanation: The client needs to know the IP of its initial SMTP server as it has to send the mail first to that server and then the server forwards the mail ahead on behalf of the user.

7. An SMTP session may not include _______
a) zero SMTP transaction
b) one SMTP transaction
c) more than one SMTP transaction
d) one HTTP transaction

Answer: d
Explanation: An SMTP session can only include SMTP transactions regardless the number. Any other protocol's transaction is not included in an SMTP session.

8. SMTP defines _______
a) message transport
b) message encryption
c) message content
d) message password

Answer: a
Explanation: As the name suggests, Simple Mail Transfer Protocol is only responsible for "how" the message is transferred i.e. Transport of the message. Other protocols such as TCP are used to provide other services like encryption for the messages.

9. Which one of the following is an SMTP server configured in such a way that anyone on the internet can send e-mail through it?
a) open mail relay
b) wide mail reception
c) open mail reception
d) short mail reception

Answer: a
Explanation: Anyone can send an e-mail through an Open Mail Relay server so it acted like a free relay for email agents to forward their mails through. Open Mail Relays are now unpopular because they can be used by attackers to perform man-in-the-middle attacks.

10. SMTP is not used to deliver messages to ______
a) user's terminal
b) user's mailbox
c) user's word processor
d) user's email client

Answer: c
Explanation: SMTP can only be used to send messages to user's terminal, email client or mailbox. A stand-alone word processor cannot be connected to a network, so it won't be possible to deliver messages to it.

1. The entire hostname has a maximum of ___________
a) 255 characters
b) 127 characters
c) 63 characters
d) 31 characters

Answer: a
Explanation: An entire hostname can have a maximum of 255 characters. Although each label must be from 1 to 63 characters long. Host name is actually a label that is given to a device in a network.

2. A DNS client is called _________
a) DNS updater
b) DNS resolver
c) DNS handler
d) none of the mentioned

Answer: b
Explanation: DNS client also known as DNS resolver also known as DNS lookup helps to resolve DNS requests using an external DNS server.

3. Servers handle requests for other domains _______

a) directly
b) by contacting remote DNS server
c) it is not possible
d) none of the mentioned

Answer: b
Explanation: Whenever a request is received at server from other domains, it handles this situation by contacting remote DNS server.

4. DNS database contains _______
a) name server records
b) hostname-to-address records
c) hostname aliases
d) all of the mentioned

Answer: d
Explanation: Domain Name system not only deals with mapping IP addresses with the hostname but also deals with exchange of information in the server.

5. If a server has no clue about where to find the address for a hostname then _______
a) server asks to the root server
b) server asks to its adjcent server
c) request is not processed
d) none of the mentioned

Answer: a
Explanation: Root name servers are actually very important and critical as they are the first step in translating human readable hostnames into IP addresses for carrying out communication.

6. Which one of the following allows client to update their DNS entry as their IP address change?
a) dynamic DNS
b) mail transfer agent
c) authoritative name server
d) none of the mentioned

Answer: a
Explanation: Dynamic DNS or in short DDNS or DynDNS helps in automatically updating a name server in the DNS. This does not require manual editing.

7. Wildcard domain names start with label _______
a) @
b) *
c) &
d) #

Answer: b
Explanation: A wildcard DNS record matches requests to a non existent domain name. This wildcard DNS record is specified by using asterisk "" as the starting of a domain name.*

8. The right to use a domain name is delegated by domain name registers which are accredited by _______
a) internet architecture board
b) internet society
c) internet research task force
d) internet corporation for assigned names and numbers

Answer: d
Explanation: The ICANN (Internet Corporation for Assigned Names and Numbers) deals with IP address space allocation, protocol identifier assignment, generic and country code Top Level domain name system management (gTLD

and ccTLD).

9. The domain name system is maintained by _______
a) distributed database system
b) a single server
c) a single computer
d) none of the mentioned

Answer: a
Explanation: A domain name system is maintained by a distributed database system. It is a collection of multiple, logically interrelated databases distributed over a computer network.

10. Which one of the following is not true?
a) multiple hostnames may correspond to a single IP address
b) a single hostname may correspond to many IP addresses
c) a single hostname may correspond to a single IP address
d) none of the mentioned

Answer: c
Explanation: It need not be that a single hostname will correspond to a ip address. For example facebook.com and fb.com both correspond to same ip address. So there can be multiple hostnames for a single ip address.

1. Secure shell (SSH) network protocol is used for __________
a) secure data communication
b) remote command-line login
c) remote command execution
d) all of the mentioned

Answer: d
Explanation: SSH provides high encryption and security features while communicating through a network. It is a cryptographic network protocol.

2. SSH can be used in only _____________
a) unix-like operating systems
b) windows
c) both unix-like and windows systems
d) none of the mentioned

Answer: c
Explanation: SSH isn't confined to a certain network or operating system. It can be implemented over different networks and on different operating systems.

3. SSH uses ___________ to authenticate the remote computer.
a) public-key cryptography
b) private-key cryptography
c) any of public-key or private-key
d) both public-key & private-key

Answer: a
Explanation: Public encryption key is slower but more flexible. Every cryptographic security system requires a private key for private access and a public key for location.

4. Which standard TCP port is assigned for contacting SSH servers?
a) port 21
b) port 22
c) port 23
d) port 24

Answer: b
Explanation: Port 22 is used for contacting ssh servers, used for file transfers (scp, sftp) and also port forwarding.

5. Which one of the following protocol can be used for login to a shell on a remote host except SSH?
a) telnet
b) rlogin
c) both telnet and rlogin
d) none of the mentioned

Answer: c
Explanation: SSH is more secured then telnet and rlogin.

6. Which one of the following is a file transfer protocol using SSH?
a) SCP
b) SFTP
c) Rsync
d) All of the mentioned

Answer: d
Explanation: SCP (Secure copy protocol), SFTP (SSH File Transfer Protocol) and Rsync all are file transfer protocols which are used by SSH.

7. SSH-2 does not contain _______________
a) transport layer
b) user authentication layer
c) physical layer
d) connection layer

Answer: c
Explanation: SSH2 is a more secure, portable and efficient version of SSH that includes SFTP, which is functionally similar to FTP, but is SSH2 encrypted.

8. Which one of the following feature was present in SSH protocol, version 1?
a) password changing
b) periodic replacement of session keys
c) support for public-key certificates
d) none of the mentioned

Answer: d
Explanation: All of the mentioned features are provided by SSH-2 and that SSH-1 only provide strong authentication and guarantee confidentiality.

9. SCP protocol is evolved from ___________ over SSH.
a) RCP protocol
b) DHCP protocol
c) MGCP protocol
d) GCP protocol

Answer: a
Explanation: RCP is the abbreviation for Rate Control Protocol is a congestion control algorithm for fast user response times.

10. Which one of the following authentication method is used by SSH?
a) public-key
b) host based
c) password
d) all of the mentioned

Answer: d
Explanation: SSH used public key authentication, Password authentication, Host based authentication, keyboard authentication and authentication of servers.

1. DHCP (dynamic host configuration protocol) provides __________ to the client.
a) IP address
b) MAC address
c) Url
d) None of the mentioned

Answer: a
Explanation: We use DHCP to allow the hosts to acquire their ip addresses dynamically which is better than visiting each and every host on the network and configure all of this information manually.

2. DHCP is used for ________
a) IPv6
b) IPv4
c) Both IPv6 and IPv4
d) None of the mentioned

Answer: c
Explanation: DHCP is used for both IPv4 and IPv6 addressing. With DHCP you get to let the hosts know about the change dynamically, and hosts update their info themselves.

3. The DHCP server _________
a) maintains a database of available IP addresses
b) maintains the information about client configuration parameters
c) grants a IP address when receives a request from a client
d) all of the mentioned

Answer: d
Explanation: Whenever a DHCP server gets a request from a client it responds with a DHCP offer containing IP address being offered, network mask offered, the amount of time that the client can use and keep it, the ip address of the DHCP server making this offer.

4. IP assigned for a client by DHCP server is
a) for a limited period
b) for an unlimited period
c) not time dependent
d) none of the mentioned

Answer: a
Explanation: The IP address offered to a client is only for a limited period of time. There is actually a certain amount of time that the client can use and keep this IP address.

5. DHCP uses UDP port _________ for sending data to the server.
a) 66
b) 67
c) 68
d) 69

Answer: b
Explanation: 67 is the UDP port number that is used as the destination port of a server. Whereas UDP port number 68 is used by the client.

6. The DHCP server can provide the _______ of the IP addresses.
a) dynamic allocation
b) automatic allocation

c) static allocation
d) all of the mentioned

Answer: d
Explanation: When a host acquires multiple offers of IP addresses from different DHCP servers, the host will broadcast a dhcp request identifying the server whose offer has been accepted.

7. DHCP client and servers on the same subnet communicate via _________
a) UDP broadcast
b) UDP unicast
c) TCP broadcast
d) TCP unicast

Answer: a
Explanation: DHCP actually employs a connectionless service, which is provided by UDP, since TCP is connection oriented. It is implemented with two UDP port numbers 67 and 68 for its operations.

8. After obtaining the IP address, to prevent the IP conflict the client may use _________
a) internet relay chat
b) broader gateway protocol
c) address resolution protocol
d) none of the mentioned

Answer: c
Explanation: ARP abbreviation for address resolution protocol is used for mapping IP addresses to MAC addresses that are present in the local network.

9. What is DHCP snooping?
a) techniques applied to ensure the security of an existing DHCP infrastructure
b) encryption of the DHCP server requests
c) algorithm for DHCP
d) none of the mentioned

Answer: a
Explanation: DHCP snooping is a security feature that is used in OS of a network in the layer 2. This technology prevents unauthorized DHCP servers offering IP addresses to DHCP clients.

10. If DHCP snooping is configured on a LAN switch, then clients having specific ______ can access the network.
a) MAC address
b) IP address
c) Both MAC address and IP address
d) None of the mentioned

Answer: c
Explanation: The DHCP snooping is done to prevent unauthorized IP addresses being offered by unauthorized servers. This features allows only specific mac addresses and IP addresses to access the network.

1. IPSec is designed to provide security at the _________
a) Transport layer
b) Network layer
c) Application layer
d) Session layer

Answer: b
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

2. In tunnel mode, IPSec protects the ______

a) Entire IP packet
b) IP header
c) IP payload
d) IP trailer

Answer: a
Explanation: In the tunnel mode, IPSec adds control bits into the packets to encrypt the entire packet between the IPSec endpoints. Using encryption, it provides secure communication between the two endpoints.

3. Which component is included in IP security?
a) Authentication Header (AH)
b) Encapsulating Security Payload (ESP)
c) Internet key Exchange (IKE)
d) All of the mentioned

Answer: d
Explanation: AH ensures that there is no retransmission of data from an unauthorized source, and protects against data tampering. ESP provides with content protection and ensures that there is integrity and confidentiality for the message. IKE is used to make sure that only the intended sender and receiver can access the message.

4. WPA2 is used for security in _______
a) Ethernet
b) Bluetooth
c) Wi-Fi
d) Email

Answer: c
Explanation: WPA2 or WiFi Protected Access 2 is a security protocol used to provide users and firms with strong data security and protection for their wireless networks (WiFi) to give them confidence that only authorized users can access their network.

5. An attempt to make a computer resource unavailable to its intended users is called ______
a) Denial-of-service attack
b) Virus attack
c) Worms attack
d) Botnet process

Answer: a
Explanation: In a Denial of Service attack, the attacker won't let the victims access the network by using a certain method that ensures that an essential network resource is unavailable to the victim. The methods that the attacker can use are vulnerability attack, bandwidth flooding and connection flooding.

6. Extensible authentication protocol is authentication framework frequently used in ______
a) Wired personal area network
b) Wireless networks
c) Wired local area network
d) Wired metropolitan area network

Answer: b
Explanation: The Extensible Authentication Protocol (EAP) is an authentication protocol used to connect a network node to the Internet. It designed through extending the methods used by the Point-to-Point Protocol for authentication.

7. Pretty good privacy (PGP) is used in ______
a) Browser security
b) Email security
c) FTP security
d) WiFi security

Answer: b
Explanation: PGP is an encryption method used in e-mail security to encrypt and decrypt the content of an e-mail transmitted over the internet. It makes sure that the message cannot be stolen by other unauthorized users.

8. PGP encrypts data by using a block cipher called ______
a) International data encryption algorithm
b) Private data encryption algorithm
c) Internet data encryption algorithm
d) Local data encryption algorithm

Answer: a
Explanation: The IDEA was designed in 1991 by Xuejia Lai and James Massey. Before IDEA, PGP used the cipher method BassOmatic.

9. When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called _________
a) DNS lookup
b) DNS hijacking
c) DNS spoofing
d) DNS authorizing

Answer: c
Explanation: In DNS spoofing, also known as DNS cache poisoning, an attacker gets the valid credentials from a victim by spoofing the intended resource, and tricking the victim to give his/her valid authorization credentials.

1. A ___________ is an extension of an enterprise's private intranet across a public network such as the internet, creating a secure private connection.
a) VNP
b) VPN
c) VSN
d) VSPN

Answer: b
Explanation: VPN provides enhanced security and online anonymity to users on the internet. It is also used to unblock websites that are unavailable in certain regions.

2. When were VPNs introduced into the commercial world?
a) Early 80's
b) Late 80's
c) Early 90's
d) Late 90's

Answer: d
Explanation: VPNs were first introduced in the year 1996. Then as the internet started to get popularized, the need for connection security increased. VPN was a great solution to this, and that's when VPNs were implemented in the commercial world.

3. What protocol is NOT used in the operation of a VPN?
a) PPTP
b) IPsec
c) YMUM
d) L2TP

Answer: c
Explanation: PPTP is a tunneling protocol which was initially used for the creation of VPNs. IPSec is used in encrypting the traffic flowing in the VPN. L2TP is used to tunnel all the L2 traffic on the VPN.

4. Which of the following statements is NOT true concerning VPNs?

a) Financially rewarding compared to leased lines
b) Allows remote workers to access corporate data
c) Allows LAN-to-LAN connectivity over public networks
d) Is the backbone of the Internet

Answer: d
Explanation: VPNs are not the backbone of the Internet as they are just a method to create private intranets on the internet. They are used for enhancing the connection security for the users.

5. Traffic in a VPN is NOT ____________
a) Invisible from public networks
b) Logically separated from other traffic
c) Accessible from unauthorized public networks
d) Restricted to a single protocol in IPsec

Answer: c
Explanation: Traffic in a VPN is not accessible from any unauthorized public networks because it is secured with the masking IP address. This provides the benefit of access to blocked resources to the users.

6. VPNs are financially speaking __________
a) Always more expensive than leased lines
b) Always cheaper than leased lines
c) Usually cheaper than leased lines
d) Usually more expensive than leased lines

Answer: c
Explanation: The services of a VPN are cheaper for moderate to large scale institutional networks than the services of leased lines. Though for a small scale network, it does not prove to be as beneficial as the costs are not reduced to a great degree as compared to leased lines.

7. Which layer 3 protocols can be transmitted over an L2TP VPN?
a) Only IP
b) Only IPX
c) Only ICMP
d) IP and IPX

Answer: d
Explanation: L2TP stands for Layer 2 Tunneling Protocol. It is used to tunnel all the L2 traffic on an IP network and is able to transmit network layer's IP and IPX protocol data.

8. ESP (Encapsulating Security Protocol) is defined in which of the following standards?
a) IPsec
b) PPTP
c) PPP
d) L2TP

Answer: a
Explanation: ESP is a security component of IPSec. ESP provides content protection and ensures that there is integrity and confidentiality of the message. The other security components of IPSec are Authentication Header and Internet Key Exchange.

9. L2F was developed by which company?
a) Microsoft
b) Cisco
c) Blizzard Entertainment
d) IETF

Answer: b

Explanation: L2F stands for Layer 2 Forwarding protocol. It was designed by Cisco to tunnel PPP traffic, helping create VPNs over the internet.

10. Which layer of the OSI reference model does PPTP work at?
a) Layer 1
b) Layer 2
c) Layer 3
d) Layer 4

Answer: b
Explanation: PPTP stands for Point-to-Point Tunneling Protocol. PPTP is a tunneling protocol that was primitively used to create VPNs. It is no longer used for VPNs due to the lack of security it provides.

11. Which layer of the OSI reference model does IPsec work at?
a) Layer 1
b) Layer 2
c) Layer 3
d) Layer 4

Answer: c
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. It operates in the network layer.

1. Storage management comprises of _______________
a) SAN Management
b) Data protection
c) Disk operation
d) All of the mentioned

Answer: d
Explanation: SAN management, data protection and disk operation are the main components of the Storage Management Initiative Specification. SMI-S was developed by the Storage Networking Industry Association.

2. Which of the following is not a storage device?
a) Switch
b) RAID Arrays
c) Tape drives
d) Hub

Answer: d
Explanation: Switches, RAID arrays and tape drives are the main storage devices in SMI-S, while a Hub is simple networking device that cannot be used as storage.

3. Which protocols are used for Storage management?
a) SNMP
b) LDAP
c) POP3
d) MIB

Answer: a
Explanation: Simple Network Management Protocol is used for storage management. Lightweight Directory Access Protocol is used to access or locate information about directories and other resources on a network. Post Office Protocol 3 is used for e-mailing on the internet. Management Information Base is a part of SNMP and contains hierarchically organized information.

4. Identify the difficulty a SAN administrator does not incur while dealing with diverse vendors.
a) Proprietary management interfaces
b) Multiple applications to manage storage in the data center

c) No single view
d) Single view

Answer: d
Explanation: A single view is not possible with diverse vendors present. Proprietary management interfaces, multiple applications management and no single view are the main difficulties incurred by a SAN administrator in such a situation.

5. How do Storage administrators ensure secure access to storage devices?
a) By using Zoning
b) By putting a physical lock on the storage device
c) By keeping devices shutdown when not in use
d) By keeping devices when used

Answer: a
Explanation: Zoning is a method in SAN that can be used by a storage administrator to specify who can see what in the SAN. Zoning might complicate the scaling process if the size of the SAN increases.

6. Effective Storage management does not include __________
a) security
b) backups
c) reporting
d) connection

Answer: d
Explanation: Connection is the responsibility of the connection manager. Storage management includes management of all necessities such as security, backups and reporting facilities.

7. Among the following, identify which task is not involved in Storage Capacity management?
a) Identifying storage systems are approaching full capacity
b) Monitoring trends for each resource
c) Tracking Total capacity, total used, total available
d) Preventing unauthorized access to the storage

Answer: d
Explanation: Prevention of unauthorized access to storage is the task of Security management. Identifying when the storage is approaching full capacity, monitoring trends, reporting and tracking capacity are the tasks of Storage Capacity management.

8. Effect of open standards like SMI(s) is _______________
a) standardization drives software interoperability and interchange ability
b) breaks the old-style dependence on proprietary methods, trade secrets, and single providers
c) builds a strong foundation on which others can quickly build and innovate
d) all of the mentioned

Answer: d
Explanation: Open standards like SMI-S inculcate a general ideal through which the normal designers are able to easily implement the standard into their software and its scalability. Since it is open-source, nothing is hidden from its users and they can implement it as they like or require to. As a whole lot of time is spent to build it as strong and scalable, it provides an efficient foundation to the designers to build and innovate on.

9. Task of Distributed Management Task Force is not ________
a) to promote interoperability among the management solution providers
b to act as an interface between the various budding technologies and provide solution to manage various environments
c) to track the operation of the different management solution providers
d) to manage the facility by itself if one of the management solution providers fail

Answer: d
Explanation: The Distributed Management Task Force is used just to simplify the overall management of the network. It cannot manage a network facility by itself in case one of the management solution providers fails. It provides an interface for promoting interoperability among management solution providers.

10. SMI-S Standard uses which of the following?
a) Java RMI
b) CIM-XML/HTTP
c) CORBA
d) .NET

Answer: b
Explanation: The Distributed Management Task Force maintains a Common Information Model (CIM) to represent a common set of network objects and their relationships. CIM-XML/HTTP refers to the operations of CIM being performed over HTTP or XML. SMI-S uses CIM-XML/HTTP.

1. The application-level protocol in which a few manager stations control a set of agents is called ______
a) HTML
b) TCP
c) SNMP
d) SNMP/IP

Answer: c
Explanation: SNMP stands for Simple Network Management Protocol. It is an application-level protocol in which a few manager stations control a set of agents. It is used under the TCP/IP protocol suite and is used for managing devices on the internet.

2. Full duplex mode increases the capacity of each domain by ________
a) 10 to 20 mbps
b) 20 to 30 mbps
c) 30 to 40 mbps
d) 40 to 50 mbps

Answer: a
Explanation: In full duplex mode, both endpoints share a single channel bandwidth to achieve two-way transmission. This results in complete utilization of the band capacity increasing the capacity by 10 to 20 mbps than half-duplex mode.

3. Configuration management can be divided into which two subsystems?
a) Reconfiguration and documentation
b) Management and configuration
c) Documentation and dialing up
d) Configuration and dialing up

Answer: a
Explanation: The best current practices report is created by a management group to ensure the most effective configuration management. The group also makes a MIB (Management Information Base) module to help with the configuration management.

4. To use a Simple Network Management System, we need _______
a) Servers
b) IP
c) Protocols
d) Rules

Answer: d
Explanation: Rules are a collection of expression containing parameters to observe the attributes of the user's device, and then execute some actions. It specifies the parameters for the managed objects inside the application and performs operations that would support the expression. The input of a rule may be many expressions or even a single expression

that end in an output of single object invoking some action.

5. The main difference between SNMPv3 and SNMPv2 is _______
a) Management
b) Integration
c) Classification
d) Enhanced security

Answer: d
Explanation: SNMPv3 has introduced new cryptographic security, through which confidentiality is provided by encrypting packets and blocking intruders. It also ensures that the message is coming from a reliable source.

6. In Network Management System, the division that is responsible for controlling access to network based on a predefined policy is called _________
a) Fault Management
b) Secured Management
c) Active Management
d) Security Management

Answer: d
Explanation: Security management is also responsible to provide confidentiality, authentication and encryption in addition to controlling access to network. Without security management, the network and its traffic would be vulnerable to be exploited by attackers.

7. BER stands for ________
a) Basic Encoding Rules
b) Basic Encoding Resolver
c) Basic Encoding Rotator
d) Basic Encoding Router

Answer: a
Explanation: The Basic Encoding Rules are a set of rules that specify the guidelines to encode the SNMP messages in binary form. Each SNMP message is encoded into 3 parts namely data, length and type of message.

8. Control of the users' access to network resources through charges is the main responsibility of ________
a) Reactive Fault Management
b) Reconfigured Fault Management
c) Accounting Management
d) Security Management

Answer: c
Explanation: The accounting management keeps track of the users and their access rights to the network and controls the user's access by communicating with the security management. The accounting management takes support of the Management Information Block to perform its operations.

9. SNMP is the framework for managing devices in an internet using the ______
a) TCP/IP protocol
b) UDP
c) SMTP
d) None

Answer: a
Explanation: SNMP is a management protocol in which a few manager stations control a set of agents using the TCP/IP protocol suite. SNMP stands for Simple Network Management Protocol.

10. Structure of Management Information (SMI), is the guideline of ________
a) HTTP
b) SNMP

c) URL
d) MIB

Answer: b
Explanation: SMI was developed by the Storage Networking Industry Association (SNIA) and it defines a standard that can be manipulated by SNMP. Basically, it defines the standard format and hierarchy of management data which is used by the SNMP. It does not describe how the objects are to be managed.

1. The application layer protocol used by a Telnet application is ________
a) Telnet
b) FTP
c) HTTP
d) SMTP

Answer: a
Explanation: Telnet is an application layer protocol that provides access to the command-line interface on a remote host. Telnet stands for teletype network.

2. Which amongst the following statements is correct for "character at a time" mode?
a) Character processing is done on the local system under the control of the remote system
b) Most text typed is immediately sent to the remote host for processing
c) All text is echoed locally, only completed lines are sent to the remote host
d) All text is processed locally, and only confirmed lines are sent to the remote host

Answer: b
Explanation: In character at a time mode, the typed text is sent immediately to the remote host while the user is typing. Another mode used in Telnet is "Old line by line" mode in which only completed lines are sent to the remote host.

3. _______ allows you to connect and login to a remote computer
a) Telnet
b) FTP
c) HTTP
d) SMTP

Answer: a
Explanation: Telnet provides access to the command-line interface on a remote computer. One can login to the computer from the command-line interface.

4. What is the correct syntax to be written in the web browser to initiate a Telnet connection to www.sanfoundry.com?
a) telnet//www.sanfoundry.com
b) telnet:www.sanfoundry.com
c) telnet://www.sanfoundry.com
d) telnet www.sanfoundry.com

Answer: c
Explanation: telnet://" is the header to be used to initiate a Telnet connection to a web server. One can browse the website using telnet if they are authorized to.

5. Telnet is used for _______
a) Television on net
b) Network of Telephones
c) Remote Login
d) Teleshopping site

Answer: c
Explanation: Telnet is an application layer protocol that provides access to the command line interface of a remote computer that can be used to perform remote login.

6. Which one of the following is not correct?
a) telnet is a general purpose client-server program
b) telnet lets user access an application on a remote computer
c) telnet can also be used for file transfer
d) telnet can be used for remote login

Answer: c
Explanation: File Transfer Protocol is used for file transfer. Telnet provides access to the command-line interface on a remote host.

7. Which operating mode of telnet is full duplex?
a) default mode
b) server mode
c) line mode
d) character mode

Answer: c
Explanation: In line mode, terminal character processing is done on the client side but editing is enabled on the server side. Line mode reduces the number of packets and is useful for long delay networks.

8. If we want that a character be interpreted by the client instead of server _________
a) interpret as command (IAC) escape character has to be used
b) control functions has to be disabled
c) it is not possible
d) cli character has to be used

Answer: a
Explanation: The client must look at each byte that arrives and look for IAC escape character. If IAC is found, the client moves on to look for any other code or IAC. If the next byte is IAC – a single byte is presented by the client to the terminal. If IAC is followed by any other code than IAC, the client interprets this as a command.

1. Telnet protocol is used to establish a connection to __________
a) TCP port number 21
b) TCP port number 22
c) TCP port number 23
d) TCP port number 25

Answer: c
Explanation: TCP port 21 is used for FTP, TCP port 22 is used for SSH and TCP port 25 is used for SMTP. Telnet provides access to a command line interface on a remote computer using the TCP port number 23.

2. Which one of the following is not true?
a) telnet defines a network virtual terminal (NVT) standard
b) client programs interact with NVT
c) server translates NVT operations
d) client can transfer files using to remote server using NVT

Answer: d
Explanation: The client can use the NVT only to interact with the programs already present on the remote server, not to transfer files to it. To transfer files, an FTP connection has to be used.

3. All telnet operations are sent as ________
a) 4 bits
b) 8 bits
c) 16 bits
d) 32 bits

Answer: b

Explanation: Telnet provides a bi-directional, 8-bit byte oriented communications facility through which operations are sent as 8-bit bytes for the server to interpret.

4. AbsoluteTelnet is a telnet client for _______ Operating system.
a) windows
b) linux
c) mac
d) ubuntu

Answer: a
Explanation: AbsoluteTelnet was originally released in 1999. It was developed by Brian Pence of Celestial Software.

5. The decimal code of Interpret as Command (IAC) character is _______
a) 252
b) 253
c) 254
d) 255

Answer: d
Explanation: If we want that a character be interpreted by the client instead of server, we use the IAC character. If IAC is followed by any other code than IAC, the client interprets it as a character.

6. Which of the following is true for character mode operation of telnet implementation?
a) each character typed is sent by the client to the server
b) each character typed is discarded by the server
c) each character typed is aggregated into a word and then sent to the server
d) each character type is aggregated into a line and then sent to the server

Answer: a
Explanation: In character mode, each character that the user is typing is immediately sent to the server which then interprets it only after the complete operation command is received.

7. In which mode of telnet, the client echoes the character on the screen but does not send it until a whole line is completed?
a) default mode
c) character mode
c) server mode
d) command mode

Answer: a
Explanation: In the default mode, the client does not send each character typed by the user to the server, thus saving the amount of packet transmissions required for executing each operation. But the server has to remain idle until the client sends the completed line wasting a lot of time.

8. Which one of the following is not correct?
a) telnet is a general purpose client-server program
b) telnet lets user access an application on a remote computer
c) telnet can also be used for file transfer
d) telnet can be used for remote login

Answer: c
Explanation: File Transfer Protocol is used for file transfer. Telnet provides access to the command-line interface on a remote host.

1. Which of the following is false with respect to TCP?
a) Connection-oriented
b) Process-to-process
c) Transport layer protocol

d) Unreliable

Answer: d
Explanation: TCP is a transport layer protocol that provides reliable and ordered delivery of a stream of bytes between hosts communicating via an IP network.

2. In TCP, sending and receiving data is done as _______
a) Stream of bytes
b) Sequence of characters
c) Lines of data
d) Packets

Answer: a
Explanation: TCP provides stream oriented delivery between hosts communicating via an IP network and there are no message boundaries. TCP can concatenate data from a number of send () commands into one stream of data and still transmit it reliably.

3. TCP process may not write and read data at the same speed. So we need __________ for storage.
a) Packets
b) Buffers
c) Segments
d) Stacks

Answer: b
Explanation: A TCP receiver has a receive buffer that is used to store the unprocessed incoming packets in case the sender is sending packets faster than the processing rate of the received packets.

4. TCP groups a number of bytes together into a packet called _______
a) Packet
b) Buffer
c) Segment
d) Stack

Answer: c
Explanation: A segment may be collection of data from many send () statements. TCP transmits each segment as a stream of bytes.

5. Communication offered by TCP is ________
a) Full-duplex
b) Half-duplex
c) Semi-duplex
d) Byte by byte

Answer: a
Explanation: Data can flow both the directions at the same time during a TCP communication hence, it is full-duplex. This is the reason why TCP is used in systems that require full-duplex operation such as e-mail systems.

6. To achieve reliable transport in TCP, ___________ is used to check the safe and sound arrival of data.
a) Packet
b) Buffer
c) Segment
d) Acknowledgment

Answer: d
Explanation: Acknowledgment mechanism is used to check the safe and sound arrival of data. The sender actively checks for acknowledgement from the receiver and once a specific time period has passed, it retransmits the data.

7. In segment header, sequence number and acknowledgement number fields refer to _______

a) Byte number
b) Buffer number
c) Segment number
d) Acknowledgment

Answer: a
Explanation: As TCP has to ensure ordered delivery of packets, sequence number and acknowledgement number are used to identify the byte number of the packet in the stream of bytes being transmitted.

8. Suppose a TCP connection is transferring a file of 1000 bytes. The first byte is numbered 10001. What is the sequence number of the segment if all data is sent in only one segment?
a) 10000
b) 10001
c) 12001
d) 11001

Answer: b
Explanation: The sequence number given to first byte of a segment, with respect to its order among the previous segments, is the sequence number of that segment.

9. Bytes of data being transferred in each connection are numbered by TCP. These numbers start with a _________
a) Fixed number
b) Random sequence of 0's and 1's
c) One
d) Sequence of zero's and one's

Answer: d
Explanation: One might expect the sequence number of the first byte in the stream to be 0, or 1. But that does not happen in TCP, Instead, the sender has to choose an Initial Sequence Number (ISN), which is basically a random 32 bit sequence of 0's and 1's, during the connection handshake.

10. The value of acknowledgement field in a segment defines _______
a) sequence number of the byte received previously
b) total number of bytes to receive
c) sequence number of the next byte to be received
d) sequence of zeros and ones

Answer: c
Explanation: The acknowledgement field in a segment defines the sequence number of the byte which is to be received next i.e. sequence number of byte that the sender should transmit next.

1. The receiver of the data controls the amount of data that are to be sent by the sender is referred to as ___________
a) Flow control
b) Error control
c) Congestion control
d) Error detection

Answer: a
Explanation: Flow control is done to prevent the receiver from being overflowed with data. It is done using various open-loop (prevention) methods and closed-loop (recovery) methods.

2. Size of TCP segment header ranges between ___________
a) 16 and 32 bytes
b) 16 and 32 bits
c) 20 and 60 bytes
d) 20 and 60 bits

Answer: c
Explanation: The size of the header can be 20 bytes at a minimum if there are no options and can go up to 60 bytes at maximum with 40 bytes in the options field. The header contains all the control information required to ensure ordered, error-free and reliable delivery of the segment.

3. Connection establishment in TCP is done by which mechanism?
a) Flow control
b) Three-Way Handshaking
c) Forwarding
d) Synchronization

Answer: b
Explanation: A three-way handshake allows both, the server and the client to choose their Initial Sequence Number and inform about it to the other party. This won't be possible using the two-way handshake mechanism.

4. The server program tells its TCP that it is ready to accept a connection. This process is called ___________
a) Active open
b) Active close
c) Passive close
d) Passive open

Answer: d
Explanation: This is the first step in the Three-Way Handshaking process and is started by the server. Then the Client picks an ISN (Initial Sequence Number) and synchronizes (shares) it with the Server requesting a connection. The Server acknowledges the clients ISN, and then picks an ISN and synchronizes it with the Client. At last, the Client acknowledges the servers ISN.

5. A client that wishes to connect to an open server tells its TCP that it needs to be connected to that particular server. The process is called ___________
a) Active open
b) Active close
c) Passive close
d) Passive open

Answer: a
Explanation: This is the second step in the Three-Way Handshaking process and is done by the client once it finds the open server and picks an ISN. The Server acknowledges the clients request, and then picks an ISN and synchronizes it with the Client. At last, the Client acknowledges the servers ISN.

6. In Three-Way Handshaking process, the situation where both the TCP's issue an active open is ___________
a) Mutual open
b) Mutual Close
c) Simultaneous open
d) Simultaneous close

Answer: c
Explanation: In simultaneous open situation, two nodes send an SYN signal to each other and start a TCP connection. Here, both TCP nodes transmit a SYNC+ACK segment to each other and a connection is established between them. This doesn't happen usually, because both sides have to know which port on the other side to send to.

7. A malicious attacker sends a large number of SYNC segments to a server, pretending that each of them is coming from a different client by faking the source IP address in the datagram. Which type of attack is being performed in this situation?
a) SYNC flooding attack
b) Active attack
c) Passive attack
d) Denial-of-service attack

Answer: a
Explanation: SYNC flooding attack is a form of Denial of Service attack. Due to the overflow of SYNC segments sent to the server, the victims are not able to request for a connection to the server, thus resulting in Denial of Service.

8. SYNC flooding attack belongs to a type of security attack known as ___________
a) SYNC flooding attack
b) Active attack
c) Passive attack
d) Denial-of-service attack

Answer: d
Explanation: During SYNC flooding the system collapses and denies service to every request, making it a DoS attack. Some other DoS attacks are bandwidth flooding, connection flooding and UDP flooding.

9. The sizes of source and destination port address in TCP header are ___________ respectively.
a) 16-bits and 32-bits
b) 16-bits and 16-bits
c) 32-bits and 16-bits
d) 32-bits and 32-bits

Answer: b
Explanation: All port addresses are of 16 bits and they specify the type of service being used by the network entity. For example, port 21 is used for FTP connections and port 25 is used for ICMP connections.

10. What allows TCP to detect lost segments and in turn recover from that loss?
a) Sequence number
b) Acknowledgment number
c) Checksum
d) Both Sequence & Acknowledgment number

Answer: b
Explanation: TCP header contains separate fields for sequence number and acknowledgment number. Comparing these values is what allows TCP to detect lost segments and in turn recover from that loss. After detecting the lost segments, the recovery may require retransmission of the lost segments of data.

1. Which of the following is false with respect to UDP?
a) Connection-oriented
b) Unreliable
c) Transport layer protocol
d) Low overhead

Answer: a
Explanation: UDP is an unreliable, connectionless transport layer protocol that provides message-based data transmission. TCP is an example of connection-oriented protocols.

2. Return value of the UDP port "Chargen" is _______
a) String of characters
b) String of integers
c) Array of characters with integers
d) Array of zero's and one's

Answer: a
Explanation: Using Chargen with UDP on port 19, the server sends a UDP datagram containing a random number of characters every time it receives a datagram from the connecting host. The number of characters is between 0 and 512.

3. Beyond IP, UDP provides additional services such as _______
a) Routing and switching
b) Sending and receiving of packets

c) Multiplexing and demultiplexing
d) Demultiplexing and error checking

Answer: d
Explanation: De-multiplexing is the delivering of received segments to the correct application layer processes at the recipients end using UDP. Error checking is done through checksum in UDP.

4. What is the main advantage of UDP?
a) More overload
b) Reliable
c) Low overhead
d) Fast

Answer: c
Explanation: As UDP does not provide assurance of delivery of packet, reliability and other services, the overhead taken to provide these services is reduced in UDP's operation. Thus, UDP provides low overhead, and higher speed.

5. Port number used by Network Time Protocol (NTP) with UDP is ________
a) 161
b) 123
c) 162
d) 124

Answer: b
Explanation: The Network Time Protocol is a clock synchronization network protocol implemented by using UDP port number 123 to send and receive time stamps.

6. What is the header size of a UDP packet?
a) 8 bytes
b) 8 bits
c) 16 bytes
d) 124 bytes

Answer: a
Explanation: The fixed size of the UDP packet header is 8 bytes. It contains four two-byte fields: Source port address, Destination port address, Length of packet, and checksum.

7. The port number is "ephemeral port number", if the source host is _______
a) NTP
b) Echo
c) Server
d) Client

Answer: d
Explanation: Port numbers from 1025 to 5000 are used as ephemeral port numbers in Windows Operating System. Ephemeral port numbers are short-lived port numbers which can be used for clients in a UDP system where there are temporary clients all the time.

8. "Total length" field in UDP packet header is the length of _________
a) Only UDP header
b) Only data
c) Only checksum
d) UDP header plus data

Answer: d
Explanation: Total length is the 16 bit field which contains the length of UDP header and the data. The maximum value of the Total length field and the maximum size of a UDP datagram is 65,535 bytes (8 byte header + 65,527 bytes of data).

9. Which is the correct expression for the length of UDP datagram?
a) UDP length = IP length – IP header's length
b) UDP length = UDP length – UDP header's length
c) UDP length = IP length + IP header's length
d) UDP length = UDP length + UDP header's length

Answer: a
Explanation: A user datagram is encapsulated in an IP datagram. There is a field in the IP header that defines the total length of the IP packet. There is another field in the IP header that defines the length of the header. So if we subtract the length of the IP header that is encapsulated in the IP packet, we get the length of UDP datagram.

10. The ______ field is used to detect errors over the entire user datagram.
a) udp header
b) checksum
c) source port
d) destination port

Answer: b
Explanation: Checksum field is used to detect errors over the entire user datagram. Though it is not as efficient as CRC which is used in TCP, it gets the job done for the UDP datagram as UDP doesn't have to ensure the delivery of the packet.

1. Which mode of IPsec should you use to assure the security and confidentiality of data within the same LAN?
a) AH transport mode
b) ESP transport mode
c) ESP tunnel mode
d) AH tunnel mode

Answer: b
Explanation: ESP transport mode should be used to ensure the integrity and confidentiality of data that is exchanged within the same LAN. ESP tunnel mode is comparatively more secure and should be used to assure the security of the data within different LANs.

2. Which two types of encryption protocols can be used to secure the authentication of computers using IPsec?
a) Kerberos V5
b) SHA
c) MD5
d) Both SHA and MD5

Answer: d
Explanation: SHA or MD5 can be used. Kerberos V5 is an authentication protocol, not an encryption protocol; therefore, answer A is incorrect. Certificates are a type of authentication that can be used with IPsec, not an encryption protocol; therefore, answer B is incorrect.

3. Which two types of IPsec can be used to secure communications between two LANs?
a) AH tunnel mode
b) ESP tunnel mode
c) Both AH tunnel mode and ESP tunnel mode
d) ESP transport mode

Answer: c
Explanation: The AH and ESP tunnel mode IPSec should be used for data transfer purpose, option d is for integrity & confidentiality purpose. Tunnel mode provides security for the entire original IP packet unlike transport mode which is not as secure as it only encrypts the data portion and not the whole packet.

4. ______ provides authentication at the IP level.
a) AH
b) ESP

c) PGP
d) SSL

Answer: a
Explanation: The Authentication Header (AH) authenticates the origin of data, and guarantees the integrity of the information that's being sent using IPSec. It also provides anti-reply security.

5. IPsec defines two protocols: _______ and ________
a) AH; SSL
b) PGP; ESP
c) AH; ESP
d) PGP; SSL

Answer: c
Explanation: AH ensures that there is no retransmission of data from an unauthorized source, and protects against data tampering. ESP provides with content protection and ensures that there is integrity and confidentiality for the message.

6. IP Security operates in which layer of the OSI model?
a) Network
b) Transport
c) Application
d) Physical

Answer: a
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

7. ESP does not provide ________
a) source authentication
b) data integrity
c) privacy
d) error control

Answer: d
Explanation: The ESP provides data confidentiality, integrity and authentication. It provides confidentiality through encryption. ESP can operate in two modes, transport mode and tunnel mode.

8. In computer security _______ means that computer system assets can be modified only by authorized parities.
a) confidentiality
b) integrity
c) availability
d) authenticity

Answer: b
Explanation: Integrity means that computer system assets can be modified only by authorized parities. Confidentiality means that the assets can only be accessed by authorized parties. Availability refers to the accessibility of the resource to the authorized parties. Authenticity means that the asset is not unethically changed.

9. In computer security _______ means that the information in a computer system only be accessible for reading by authorized parities.
a) confidentiality
b) integrity
c) availability
d) authenticity

Answer: a
Explanation: Confidentiality means that the assets can only be accessed by authorized parties. Integrity means that computer system assets can be modified only by authorized parities. Availability refers to the accessibility of the resource

to the authorized parties. Authenticity means that the asset is not unethically changed.

10. Which of the following organizations is primarily concerned with military encryption systems?
a) NSA
b) NIST
c) IEEE
d) ITU

Answer: a
Explanation: The NSA is primarily responsible for military encryption systems. The NSA designs evaluates, and implements encryption systems for the military and government agencies with high security needs.

1. Two broad categories of congestion control are
a) Open-loop and Closed-loop
b) Open-control and Closed-control
c) Active control and Passive control
d) Active loop and Passive loop

Answer: a
Explanation: Open loop congestion control techniques are used to prevent congestion before it even happens by enforcing certain policies. Closed loop congestion control techniques are used to treat congestion after it has happened.

2. In open-loop control, policies are applied to __________
a) Remove after congestion occurs
b) Remove after sometime
c) Prevent before congestion occurs
d) Prevent before sending packets

Answer: c
Explanation: Open loop congestion control techniques are used to prevent congestion before it even happens by enforcing certain policies. Retransmission policy, window policy and acknowledgement policy are some policies that might be enforced.

3. Retransmission of packets must not be done when _______
a) Packet is lost
b) Packet is corrupted
c) Packet is needed
d) Packet is error-free

Answer: d
Explanation: Retransmission refers to the sender having to resend the packet to the receiver. It needs to be done only when some anomaly occurs with the packet like when the packet is lost or corrupted.

4. In Go-Back-N window, when the timer of the packet times out, several packets have to be resent even some may have arrived safe. Whereas in Selective Repeat window, the sender resends ___________
a) Packet which are not lost
b) Only those packets which are lost or corrupted
c) Packet from starting
d) All the packets

Answer: b
Explanation: In Selective Repeat, the sender side uses a searching algorithm to find the packets which need to be retransmitted based on the negative acknowledgements received and then resends only those packets thus saving bandwidth.

5. Discarding policy is mainly done by _______
a) Sender
b) Receiver

c) Router
d) Switch

Answer: c
Explanation: The discarding policy adopted by the routers mainly states that the routers discard sensitive or corrupted packets that it receives, thus controlling the integrity of the packet flow. The discarding policy is adopted as an open loop congestion control technique.

6. Closed-Loop control mechanisms try to _________
a) Remove after congestion occurs
b) Remove after sometime
c) Prevent before congestion occurs
d) Prevent before sending packets

Answer: a
Explanation: In closed loop congestion control, methods are implemented to remove congestion after it occurs. Some of the methods used are backpressure and choke packet.

7. The technique in which a congested node stops receiving data from the immediate upstream node or nodes is called as _______
a) Admission policy
b) Backpressure
c) Forward signaling
d) Backward signaling

Answer: b
Explanation: In this closed loop congestion control technique, the congested node propagates in the opposite direction of the data flow to inform the predecessor node to reduce the flow of packets. This is why this technique is called a node-to-node congestion control technique.

8. Backpressure technique can be applied only to _______
a) Congestion networks
b) Closed circuit networks
c) Open circuit networks
d) Virtual circuit networks

Answer: d
Explanation: In Virtual circuit networks, each node knows the upstream node from which a flow data is coming. So, it makes possible for the congested node to track the source of the congestion and then inform that node to reduce the flow to remove congestion.

9. The packet sent by a node to the source to inform it of congestion is called _______
a) Explicit
b) Discard
c) Choke
d) Backpressure

Answer: c
Explanation: Choke packet is sent by a node to the source to inform it of congestion. Two choke packet techniques can be used for the operation called hop-by-hop choke packet and source choke packet.

10. In the slow-start algorithm, the size of the congestion window increases __________ until it reaches a threshold.
a) exponentially
b) additively
c) multiplicatively
d) suddenly

Answer: a

Explanation: In slow-start algorithm, the size of the congestion window increases exponentially until it reaches a threshold. When it reaches the threshold, it stops increasing and continues sending packets through the threshold window thus preventing congestion.

11. In the congestion avoidance algorithm, the size of the congestion window increases ____________ until congestion is detected.
a) exponentially
b) additively
c) multiplicatively
d) suddenly

Answer: b
Explanation: In the congestion avoidance algorithm, the size of the congestion window increases additively until congestion is detected. Once congestion is detected, the size of congestion window is decreased once and then the packets are transmitted to achieve congestion avoidance.

1. Which of the following is not a characteristic of Virtual Circuit Network?
a) There are setup and teardown phases in addition to the data transfer phase
b) Resources can be allocated during setup phase or on demand
c) All packets follow the same path established during the connection
d) Virtual circuit network is implemented in application layer

Answer: d
Explanation: Virtual circuit network is normally implemented in data link layer. It is a combination of circuit-switched network and datagram network which are implemented in the physical layer and network layer respectively.

2. The address that is unique in the scope of the network or internationally if the network is part of an international network is called as ______
a) Global address
b) Network address
c) Physical address
d) IP address

Answer: a
Explanation: Global address is a network address that is unique internationally and is used as a common address by all the users of the network. It is used to create a virtual circuit identifier.

3. The Identifier that is used for data transfer in virtual circuit network is called _______
a) Global address
b) Virtual circuit identifier
c) Network identifier
d) IP identifier

Answer: b
Explanation: A virtual circuit identifier is a type of numeric identifying address that is used to distinguish between different virtual circuits in a circuit-switched network. It is used for data transfer and has a switch scope.

4. Which of the following is not a phase of virtual circuit network?
a) Setup phase
b) Data transfer phase
c) Termination phase
d) Teardown phase

Answer: c
Explanation: There are three phases in a virtual circuit network: setup, data transfer and teardown phase. There is no termination phase in it.

5. Steps required in setup process are ___________

a) Setup request and acknowledgement
b) Setup request and setup response
c) Setup request and setup termination
d) Setup and termination steps

Answer: a
Explanation: Setup request (sent by a source) and acknowledgement (sent by the destination) are the steps in the setup process. Both the ends' switches make table entries during the setup process.

6. During teardown phase, the source, after sending all the frames to destination, sends a _____ to notify termination.
a) teardown response
b) teardown request
c) termination request
d) termination response

Answer: b
Explanation: The source, after sending all the frames to destination sends teardown request to which, destination sends teardown response. The switches then delete the corresponding table entries.

7. Delay of the resource allocated during setup phase during data transfer is ________
a) constant
b) increases for each packet
c) same for each packet
d) different for each packet

Answer: c
Explanation: If a resource is allocated during setup phase, delay is same for each packet as there is only one-time delay during the setup phase and no delay during the data transfer phase.

8. Delay of the resource allocated on demand during data transfer is ________
a) constant
b) increases for each packet
c) same for each packet
d) different for each packet

Answer: d
Explanation: If a resource is to be allocated on demand during the data transfer phase, the delay for each packet would be different depending upon the resource requirement of the packets.

9. In virtual circuit network, the number of delay times for setup and teardown respectively are _______
a) 1 and 1
b) 1 and 2
c) 2 and 1
d) 2 and 2

Answer: a
Explanation: There is one-time delay for both setup and teardown phase. The one-time delay in setup phase is for resource allocation and the one-time delay in teardown phase is for the de-allocation of the resources.

10. In data transfer phase, how many columns does the table contain?
a) 1
b) 2
c) 3
d) 4

Answer: d
Explanation: The switch maintains a table for each Virtual Circuit Network. In the data transfer phase, it maintains 2 columns each for incoming data and outgoing data. The columns are in the following order: Source port, Source VCI,

Destination port, Destination VCI.

1. ATM and frame relay are ________
a) virtual circuit networks
b) datagram networks
c) virtual private networks
d) virtual public networks

Answer: a
Explanation: ATM and frame relay are transmission modes in which information is transferred through electric circuit layer as packets. ATM has fixed packet size and frame relay has variable packet size.

2. ATM uses _______________
a) asynchronous frequency division multiplexing
b) asynchronous time division multiplexing
c) asynchronous space division multiplexing
d) asynchronous amplitude division multiplexing

Answer: b
Explanation: ATM uses a constant data stream consisting of transmission cells to transmit information in a fixed division of time. The packet size remains fixed.

3. ATM standard defines _______ layers.
a) 2
b) 3
c) 4
d) 5

Answer: b
Explanation: The three layers are physical layer, ATM layer and application adoption layer. The physical layer corresponds to the physical layer, ATM layer corresponds to the data link layer and the AAL layer corresponds to the network layer of the OSI model.

4. ATM can be used for ________
a) local area network
b) wide area network
c) campus area network
d) networks covering any range

Answer: d
Explanation: ATM is a connection oriented network for cell relay which can be implemented for networks covering any area. It uses Time Division Multiplexing and supports voice, video and data communications.

5. An ATM cell has the payload field of __________
a) 32 bytes
b) 48 bytes
c) 64 bytes
d) 128 bytes

Answer: b
Explanation: An ATM field contains a header and a payload. The header is of 5 bytes and the payload is of 48 bytes. The size of the header remains fixed.

6. Frame relay has error detection at the ______
a) physical layer
b) data link layer
c) network layer
d) transport layer

Answer: b
Explanation: The Frame Relay header contains an 8-bit Header Error Control field (HEC). The HEC field contains an 8-bit CRC which is used for error control.

7. Virtual circuit identifier in frame relay is called ______
a) data link connection identifier
b) frame relay identifier
c) cell relay identifier
d) circuit connection identifier

Answer: a
Explanation: The Data Link Connection Identifier is 10-bit virtual circuit identifier. It is used to assign frames to the specified Permanent Virtual Circuits or Switched Virtual Circuits.

8. Frame relay has _______
a) only physical layer
b) only data link layer
c) only network layer
d) both physical and data link layer

Answer: d
Explanation: The physical layer is guided by the protocols recognized by the ANSI. The data link layer supports the simplified core functions specified by the OSI model.

9. In frame relay networks, extended address is used _______
a) to increase the range of data link connection identifiers
b) for error detection
c) for encryption
d) for error recovery

Answer: a
Explanation: Extended address is indicated by the last bit of every address byte in the DLCI. It specifies whether the byte is the last in the addressing field. It is used to increase the range of data link connection identifiers.

10. What is FRAD in frame relay network?
a) FRAD assembles and disassembles the frames coming from other protocols
b) FRAD is used for modulation and demodulation
c) FRAD is used for error detection
d) FRAD is used for error recovery

Answer: a
Explanation: FRAD stands for Frame Relay Assembler/Disassembler. It converts packets into frames that can be transmitted over Frame Relay Networks. It operates at the physical layer.

1. Frame Relay is cheaper than other _____
a) LANs
b) WANs
c) MANs
d) Multipoint Networks

Answer: b
Explanation: Frame relay is a standardized wide area network technology and is popularly used because it is cheaper than leased line WANs. It is also very simple to configure user equipment in a Frame Relay network.

2. Frame Relay networks offer an option called _______
a) Voice Over For Relay
b) Voice Over Fine Relay
c) Voice On Frame Relay

d) Voice Over Frame Relay

Answer: d
Explanation: Frame Relay networks offer an option called Voice over Frame Relay, which transmits voice and voice-band data over a Frame Relay network. It has two sub-protocols FRF11 and FRF12.

3. There are ________ total features of Frame Relay.
a) Five
b) Seven
c) Nine
d) Ten

Answer: c
Explanation: Frame relay is a wide area network technology used to transmit information over a network in the form of frames using relays. The frames are of variable size. It is cheaper than other WANs and it's simple to configure user equipment in the network.

4. Frame Relay does not provide flow or error control, they must be provided by the ______
a) Lower Level Protocol
b) Highest Level Protocol
c) Upper Level Protocol
d) Lowest Level Protocol

Answer: c
Explanation: Frame relay only provides error detection using CRC. If errors are detected, the upper-layer protocols, such as TCP are expected to provide error correction features. Network layer provides flow control.

5. Frame Relay deploys physical layer carriers such as _______
a) ADMs
b) UPSR
c) BLSR
d) SONET

Answer: d
Explanation: Frame Relays uses carriers such as SONET (for fiber-optic connections) to physically transmit data frames over a Frame Relay network. SONET is cheaper and provides better network reliability than other carriers.

6. Frame relay provides error detection at the ______
a) physical layer
b) data link layer
c) network layer
d) transport layer

Answer: b
Explanation: Frame relay provides error detection using CRC in the data link layer. The transport layer then provides the error correction features if an error is detected.

7. Virtual circuit identifier in frame relay is called _______
a) data link connection identifier
b) frame relay identifier
c) cell relay identifier
d) circuit connection identifier

Answer: a
Explanation: The Data Link Connection Identifier is 10-bit virtual circuit identifier. It is used to assign frames to the specified Permanent Virtual Circuits or Switched Virtual Circuits.

8. Frame relay has only _______

a) physical layer
b) data link layer
c) physical layer and data link layer
d) network layer and data link layer

Answer: c
Explanation: The physical layer is guided by the protocols recognized by the ANSI and provides conversion to frames. The data link layer supports the simplified core functions specified by the OSI model like error detection.

9. In frame relay networks, extended address is used ________
a) to increase the range of data link connection identifiers
b) for error detection
c) for encryption
d) for error recovery

Answer: a
Explanation: Extended address is indicated by the last bit of every address byte in the DLCI. It specifies whether the byte is the last in the addressing field. It is used to increase the range of data link connection identifiers.

10. What is FRAD in frame relay network?
a) FRAD assembles and disassembles the frames coming from other protocols
b) FRAD is used for modulation and demodulation
c) FRAD is used for error detection
d) FRAD is used for error recovery

Answer: a
Explanation: FRAD stands for Frame Relay Assembler/Disassembler. It converts packets into frames that can be transmitted over Frame Relay Networks. It operates at the physical layer.

1. A piece of icon or image on a web page associated with another webpage is called ______
a) url
b) hyperlink
c) plugin
d) extension

Answer: b
Explanation: URLs are locators for resources present on the World Wide Web. A plugin provides extra functionality to the webpage. An extension provides modification allowance for the core functionality of a webpage. Hyperlink is piece of icon or image on a web page associated with another webpage.

2. Dynamic web page ______
a) is same every time whenever it displays
b) generates on demand by a program or a request from browser
c) both is same every time whenever it displays and generates on demand by a program or a request from browser
d) is different always in a predefined order

Answer: b
Explanation: A dynamic web page provides different content every time the user opens it based on some events like new additions or time of the day. Languages such as JavaScript are used to respond to client-side events while languages such as PHP as used to respond to server-side events.

3. What is a web browser?
a) a program that can display a web page
b) a program used to view html documents
c) it enables user to access the resources of internet
d) all of the mentioned

Answer: d

Explanation: A web browser is an application program that is used to access the World Wide Web resources, applications and websites. Some examples of web browsers are Google Chrome, Internet Explorer and Safari.

4. Common gateway interface is used to _______
a) generate executable files from web content by web server
b) generate web pages
c) stream videos
d) download media files

Answer: a
Explanation: CGI is an interface through servers can run execute console-based executable files on a web server that generates dynamic web pages. A CGI script executes only when a request is made. The script then generates HTML.

5. URL stands for ________
a) unique reference label
b) uniform reference label
c) uniform resource locator
d) unique resource locator

Answer: c
Explanation: The Uniform Resource Locator is a locator for the resource to be located by HTTP on the World Wide Web. The URL is derived from the Uniform Resource Identifier.

6. A web cookie is a small piece of data that is _______
a) sent from a website and stored in user's web browser while a user is browsing a website
b) sent from user and stored in the server while a user is browsing a website
c) sent from root server to all servers
d) sent from the root server to other root servers

Answer: a
Explanation: A web cookie is a small piece of data sent from a website and stored in user's web browser while a user is browsing the website and is used to remember stateful information about the user's operations on the website. This can help the website provide a better browsing experience to the user.

7. Which one of the following is not used to generate dynamic web pages?
a) PHP
b) ASP.NET
c) JSP
d) CSS

Answer: d
Explanation: CSS alone cannot be used to generate dynamic web pages as it does not provide many event handling functions. It can be used along with JavaScript to generate dynamic web pages which are visually compelling.

8. An alternative to JavaScript on windows platform is _______
a) VBScript
b) ASP.NET
c) JSP
d) PHP

Answer: a
Explanation: VBScript is a general-purpose, lightweight and active scripting language which can be used on Microsoft Visual Basic. It was first released in 1996.

9. What is document object model (DOM)?
a) convention for representing and interacting with objects in html documents
b) application programming interface
c) hierarchy of objects in ASP.NET

d) scripting language

Answer: a
Explanation: DOM is a hierarchical model i.e. a tree used to represent an HTML or XML document. Every node of the tree an object that represents a part of the document.

10. AJAX stands for _______
a) asynchronous javascript and xml
b) advanced JSP and xml
c) asynchronous JSP and xml
d) advanced javascript and xml

Answer: a
Explanation: AJAX is a group of technologies that works on the client-side to create asynchronous web applications. It is used to modify only a part of a webpage and not the whole webpage whenever some event occurs.

1. Which of the following is not applicable for IP?
a) Error reporting
b) Handle addressing conventions
c) Datagram format
d) Packet handling conventions

Answer: a
Explanation: The Internet Protocol is the networking protocol which establishes the internet by relaying datagrams across network boundaries. ICMP is a supporting protocol for IP which handles the Error Reporting functionality.

2. Which of the following field in IPv4 datagram is not related to fragmentation?
a) Flags
b) Offset
c) TOS
d) Identifier

Answer: c
Explanation: TOS-type of service identifies the type of packets. It is not related to fragmentation but is used to request specific treatment such as high throughput, high reliability or low latency for the IP packet depending upon the type of service it belongs to.

3. The TTL field has value 10. How many routers (max) can process this datagram?
a) 11
b) 5
c) 10
d) 1

Answer: c
Explanation: TTL stands for Time to Live. This field specifies the life of the IP packet based on the number of hops it makes (Number of routers it goes through). TTL field is decremented by one each time the datagram is processed by a router. When the value is 0, the packet is automatically destroyed.

4. If the value in protocol field is 17, the transport layer protocol used is _____________
a) TCP
b) UDP
c) ICMP
d) IGMP

Answer: b
Explanation: The protocol field enables the demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type. Its most used values are 17 and 6 for UDP and TCP respectively. ICMP and IGMP are network layer protocols.

5. The data field cannot carry which of the following?
a) TCP segment
b) UDP segment
c) ICMP messages
d) SMTP messages

Answer: c
Explanation: Data field usually has transport layer segments, but it can also carry ICMP messages. SMTP is an application layer protocol. First it must go through the transport layer to be converted into TCP segments and then it can be inserted into IP packets.

6. What should be the flag value to indicate the last fragment?
a) 0
b) 1
c) TTl value
d) Protocol field value

Answer: a
Explanation: The Flag field in the IP header is used to control and identify the fragments. It contains three bits: reserved, don't fragment and more fragments. If the more fragments bit is 0, it means that the fragment is the last fragment.

7. Which of these is not applicable for IP protocol?
a) is connectionless
b) offer reliable service
c) offer unreliable service
d) does not offer error reporting

Answer: b
Explanation: IP does not provide reliable delivery service for the data. It's dependent upon the transport layer protocols like TCP to offer reliability.

8. Which of the following demerits does Fragmentation have?
a) complicates routers
b) open to DOS attack
c) overlapping of fragments.
d) all of the mentioned

Answer: d
Explanation: Fragmentation makes the implementation of the IP protocol complex and can also be exploited by attackers to create a DOS attack such as a teardrop attack. Fragmentation won't be required if the transport layer protocols perform wise segmentation.

9. Which field helps to check rearrangement of the fragments?
a) offset
b) flag
c) ttl
d) identifer

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

1. Which of these is not applicable for IP protocol?
a) Connectionless
b) Offer reliable service
c) Offer unreliable service
d) Does not offer error reporting

Answer: b
Explanation: IP does not provide reliable delivery service for the data. It's dependent upon the transport layer protocols like TCP to offer reliability.

2. Which of the following demerits does Fragmentation have?
a) Complicates routers
b) Open to DOS attack
c) Overlapping of fragments
d) All of the mentioned

Answer: d
Explanation: Fragmentation makes the implementation of the IP protocol complex and can also be exploited by attackers to create a DOS attack such as a teardrop attack. Fragmentation won't be required if the transport layer protocols perform wise segmentation.

3. Which field helps to check rearrangement of the fragments?
a) Offset
b) Flag
c) TTL
d) Identifier

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

4. In classless addressing, there are no classes but addresses are still granted in ______
a) IPs
b) Blocks
c) Codes
d) Sizes

Answer: b
Explanation: In classless addressing, there are no classes but addresses are still granted in blocks. The total number of addresses in a block of classless IP addresses = $2^{(32 - CIDR\_value)}$.

5. In IPv4 Addresses, classful addressing is replaced with ________
a) Classless Addressing
b) Classful Addressing
c) Classful Advertising
d) Classless Advertising

Answer: a
Explanation: Classful addressing is replaced with classless addressing as a large ratio of the available addresses in a class in calssful addressing is wasted. In classless addressing, one can reserve the number of IP addresses required by modifying the CIDR value and make sure that not many addresses are wasted.

6. First address in a block is used as network address that represents the ________
a) Class Network
b) Entity
c) Organization
d) Codes

Answer: c
Explanation: First address in a block is used as network address that represents the organization. The network address can be found by AND'ing any address in the block by the default mask. The last address in a block represents the broadcast address.

7. In classful addressing, a large part of available addresses are ________

a) Organized
b) Blocked
c) Wasted
d) Communicated

Answer: c
Explanation: In classful addressing, a large part of available addresses are wasted. Thus to solve this classful addressing is replaced with classless addressing where one can reserve the number of IP addresses required by modifying the CIDR value and make sure that not many addresses are wasted.

8. Network addresses are a very important concept of ________
a) Routing
b) Mask
c) IP Addressing
d) Classless Addressing

Answer: c
Explanation: Network addresses are a very important concept of IP addressing. The first address in a block is used as network address that represents the organization. The network address can be found by AND'ing any address in the block or class by the default mask.

9. Which of this is not a class of IP address?
a) Class E
b) Class C
c) Class D
d) Class F

Answer: d
Explanation: Class F is not a class of IP addressing. There are only five classes of IP addresses: Class A (0.0.0.0 to 127.255.255.255), Class B (128.0.0.0 to 191.255.255.255), Class C (192.0.0.0 to 223.255.255.255), Class D (224.0.0.0 to 239.255.255.255), and Class E (240.0.0.0 to 255.255.255.255).

1. The size of an IP address in IPv6 is _________
a) 4 bytes
b) 128 bits
c) 8 bytes
d) 100 bits

Answer: b
Explanation: An IPv6 address is 128 bits long. Therefore, 2128 i.e. 340 undecillion addresses are possible in IPv6. IPv4 has only 4 billion possible addresses and IPv6 would be a brilliant alternative in case IPv4 runs out of possible new addresses.

2. The header length of an IPv6 datagram is ___________
a) 10bytes
b) 25bytes
c) 30bytes
d) 40bytes

Answer: d
Explanation: IPv6 datagram has fixed header length of 40bytes, which results in faster processing of the datagram. There is one fixed header and optional headers which may or may not exist. The fixed header contains the mandatory essential information about the packet while the optional headers contain the optional "not that necessary" information.

3. In the IPv6 header, the traffic class field is similar to which field in the IPv4 header?
a) Fragmentation field
b) Fast-switching
c) ToS field

d) Option field

Answer: c
Explanation: The traffic class field is used to specify the priority of the IP packet which is a similar functionality to the Type of Service field in the IPv4 header. It's an 8-bit field and its values are not defined in the RFC 2460.

4. IPv6 does not use _________ type of address.
a) broadcast
b) multicast
c) anycast
d) unicast

Answer: a
Explanation: There is no concept of broadcast address in IPv6. Instead, there is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

5. Which among the following features is present in IPv6 but not in IPv4?
a) Fragmentation
b) Header checksum
c) Options
d) Anycast address

Answer: d
Explanation: There is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

6. The _________ field determines the lifetime of IPv6 datagram
a) Hop limit
b) TTL
c) Next header
d) Type of traffic

Answer: a
Explanation: The Hop limit value is decremented by one by a router when the datagram is forwarded by the router. When the value becomes zero the datagram is discarded. The field is 8-bits wide, so an IPv6 packet can live up to 255 router hops only.

7. Dual-stack approach refers to _________
a) implementing Ipv4 with 2 stacks
b) implementing Ipv6 with 2 stacks
c) node has both IPv4 and IPv6 support
d) implementing a MAC address with 2 stacks

Answer: c
Explanation: Dual-stack is one of the approaches used to support IPv6 in already existing systems. ISPs are using it as a method to transfer from IPv4 to IPv6 completely eventually due to the lower number of possible available addresses in IPv4.

8. Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is ________
a) Use dual-stack approach
b) Tunneling
c) No solution
d) Replace the system

Answer: b
Explanation: The IPv4 routers can form a tunnel in which at the sender's side, the IPv6 datagram is encapsulated in to IPv4, and at the receiver's side of the tunnel, the IPv4 packet is stripped and the IPv6 packet is sent to the receiver.

9. Teredo is an automatic tunneling technique. In each client the obfuscated IPv4 address is represented by bits ______
a) 96 to 127
b) 0 to 63
c) 80 to 95
d) 64 to 79

Answer: a
Explanation: Teredo is a technique through which gives the possibility for full IPv6 network connectivity to IPv6 capable hosts which are currently on an IPv4 network. Bits 96 to 127 in the datagram represents obfuscated 1Pv4 address of the IPv4 network.

1. Dual-stack approach refers to _________
a) Implementing Ipv4 with 2 stacks
b) Implementing Ipv6 with 2 stacks
c) Node has both IPv4 and IPv6 support
d) Implementing a MAC address with 2 stacks

Answer: c
Explanation: Dual-stack is one of the approaches used to support IPv6 in already existing systems. ISPs are using it as a method to transfer from IPv4 to IPv6 completely eventually due to the lower number of possible available addresses in IPv4.

2. Suppose two IPv6 nodes want to interoperate using IPv6 datagrams, but they are connected to each other by intervening IPv4 routers. The best solution here is ________
a) Use dual-stack approach
b) Tunneling
c) No solution
d) Replace the system

Answer: b
Explanation: The IPv4 routers can form a tunnel in which at the sender's side, the IPv6 datagram is encapsulated in to IPv4, and at the receiver's side of the tunnel, the IPv4 packet is stripped and the IPv6 packet is sent to the receiver.

3. Teredo is an automatic tunneling technique. In each client the obfuscated IPv4 address is represented by bits ______
a) 96 to 127
b) 0 to 63
c) 80 to 95
d) 64 to 79

Answer: a
Explanation: Teredo is a technique through which gives the possibility for full IPv6 network connectivity to IPv6 capable hosts which are currently on an IPv4 network. Bits 96 to 127 in the datagram represents obfuscated 1Pv4 address of the IPv4 network.

4. A link local address of local addresses is used in an _______
a) Isolated router
b) Isolated mask
c) Isolated subnet
d) Isolated net

Answer: c
Explanation: Isolated subnet is very huge sharing network area in this link local address of local addresses is used. A link local address can be configured on any subnet with the prefix "FE80::".

5. In subcategories of reserved address in IPv6, address that is used by a host to test itself without going into network is called _________

a) Unspecified address
b) Loopback address
c) Compatible address
d) Mapped address

Answer: b
Explanation: In subcategories of reserved address in IPv6, address that is used by a host to test itself without going into network is called loop back address. IPv6 loopback address is 0000:0000:0000:0000:0000:0000:0000:0001. IPv4 loopback address is 127.0.0.1. It's a reserved address.

6. A few leftmost bits in each address of IPv6 address define its category is called ________
a) Prefix type
b) Postfix type
c) Reserved type
d) Local type

Answer: a
Explanation: Prefix is the bits in the IP address which are placed in leftmost position. A network prefix in IPv6 is given by a CIDR format-liked number at the end of the address.

7. In IPv6 addresses, addresses that start with eight 0s are called ________
a) Unicast addresses
b) Multicast addresses
c) Any cast addresses
d) Reserved addresses

Answer: d
Explanation: In IPv6 address format, the starting bits are specified with eight 0s to represent reserved addresses. These reserved addresses have a certain function pre-defined like the loop-back address is used to test a network card. Reserved addresses cannot be allotted to a machine.

8. Which statement(s) about IPv6 addresses are true?
a) Leading zeros are required
b) Two colons (::) are used to represent successive hexadecimal fields of zeros
c) Two colons (::) are used to separate fields
d) A single interface cannot have multiple IPv6 addresses of different types

Answer: b
Explanation: In order to shorten the written length of an IPv6 address, successive fields of zeros may be replaced by double colons. In trying to shorten the address further, leading zeros may also be removed. Just as with IPv4, a single device's interface can have more than one address; with IPv6 there are more types of addresses and the same rule applies. There can be link-local, global unicast, and multicast addresses all assigned to the same interface.

9. When was IPv6 launched?
a) June 2, 2012
b) June 4, 2012
c) June 5, 2012
d) June 6, 2012

Answer: d
Explanation: IPv6 is the latest version of the Internet Protocol released on 6th June 2012. An IPv6 address is 128 bits long. Therefore, 2^{128} i.e. 340 undecillion addresses are possible in IPv6.

1. Which layer is responsible for process-to-process delivery?
a) Physical layer
b) Network layer
c) Transport layer

d) Application layer

Answer: c
Explanation: The transport layer is responsible for process-to-process delivery, error control and flow control. It provides an interface for the implementation of process to process delivery through ports. There are 65,535 port numbers.

2. In process-to-process delivery, two processes communicate in which of the following methods?
a) Client/Server
b) Source/Destination
c) Message Transfer
d) Peer to Peer

Answer: a
Explanation: The most common method used for this communication is Client/Server. The client requests a service through a particular port number to the port of the server using its socket address. Then the server responds by giving the requested service to the client port.

3. Multiple processes on destinations at transport layer are identified by __________
a) Mac address
b) Port number
c) Host number
d) Host address

Answer: b
Explanation: Multiple processes on destinations are identified by a transport layer address also called as port number. The IP address along with the port number is called the socket address.

4. Range of port numbers in Internet model is __________
a) 0 and 32,765(8-bit)
b) 0 and 32,765(16-bit)
c) 0 and 65,535(32-bit)
d) 0 and 65,535(16-bit)

Answer: d
Explanation: Port numbers are 16-bit integers between 0 and 65,535. They are an interface for the implementation of process to process delivery for the transport layer.

5. According to Internet Assigned Numbers Authority (IANA), which of the following ranges is not a part of port number ranges?
a) Well-known ports
b) Registered ports
c) Dynamic ports
d) Static ports

Answer: d
Explanation: IANA divided port numbers into three ranges i.e., Well-known, Registered and Dynamic ports. Well-known port numbers range from 0 to 1023, registered port numbers are from 1024 to 49151 and dynamic port numbers are from 49152 to 65535.

6. The combination of an IP address and port number is called as ________
a) Socket address
b) Port address
c) MAC address
d) Host address

Answer: a
Explanation: Socket address is the combination of an IP address and a port number and it is used to define the client-end and server-end processes uniquely.

7. Which of the following is false with respect to Connectionless service of transport layer protocol?
a) Packets are not numbered
b) Packets are not delayed
c) No acknowledgement
d) Packet may arrive out of sequence

Answer: b
Explanation: There is a high probability in connectionless services like UDP that the packet gets delayed or lost because there is no connection made between the two end nodes. No connection means that there is no unique pathway for the packets to travel.Answer: d
Explanation: First the client has to request a connection and the server has to accept the connection to establish a connection. Then data transfer can start between the two ends. Then both client and server need to terminate their ends to terminate the connection.

9. In transport layer, Multiplexing is done at _________
a) Channel
b) Receiver site
c) Sender site
d) Packet

Answer: c
Explanation: At the sender's side, there are multiple processes which may want to send packets. But there is only one transport layer protocol like TCP or UDP working at a time. So the transport layer protocol gets the messages from these processes and separates them with different port numbers. This process is called multiplexing and it is done before sending packets to the receivers side.

10. The process of error checking and dropping of the header, delivering messages to appropriate process based on port number is called as _______
a) Delivery of packets
b) Error correction
c) Multiplexing
d) Demultiplexing

Answer: d
Explanation: Demultiplexing is the process of error checking and dropping of the header, delivering messages to appropriate process based on port number. The transport layer does this on the receiver's end after the packet is received and takes help of the header attached by the sender's side transport layer during multiplexing.

1. Internet Control Message Protocol (ICMP) has been designed to compensate _________
a) Error-reporting
b) Error-correction
c) Host and management queries
d) All of the mentioned

Answer: d
Explanation: IP by itself does not provide the features of error reporting or error correction. So, to address these issues a network layer protocol called Internet Control Message Protocol is used. ICMP operates over the IP packet to provide error reporting functionality.

2. Header size of the ICMP message is _________
a) 8-bytes
b) 8-bits
c) 16-bytes
d) 16-bits

Answer: a
Explanation: An ICMP message has an 8-byte header and a variable size data section. Out of the 8 bytes, the first 4

bytes are of a fixed format having the type, code and checksum fields and the next 4 bytes depend upon the type of the message.

3. During error reporting, ICMP always reports error messages to ________
a) Destination
b) Source
c) Next router
d) Previous router

Answer: b
Explanation: ICMP notifies the source about the error when an error is detected because the datagram knows information about source and destination IP address. The source can then retransmit the data again or try to correct those errors.

4. Which of these is not a type of error-reporting message?
a) Destination unreachable
b) Source quench
c) Router error
d) Time exceeded

Answer: c
Explanation: Router error is not a type of error-reporting message in ICMP. The type of error reporting message is specified in the ICMP header. Destination unreachable is type 3 error message, source quench is type 4, and time exceeded is type 11 error message.

5. ICMP error message will not be generated for a datagram having a special address such as _______
a) 127.0.0.0
b) 12.1.2
c) 11.1
d) 127

Answer: a
Explanation: 127.0.0.0 is a special address known as the loopback address which is used for testing purpose of a machine without actually communicating with a network. Thus no error reporting message will be generated for such special addresses.

6. When a router cannot route a datagram or host cannot deliver a datagram, the datagram is discarded and the router or the host sends a ____________ message back to the source host that initiated the datagram.
a) Destination unreachable
b) Source quench
c) Router error
d) Time exceeded

Answer: a
Explanation: Router sends destination unreachable message if the destination is not found. Destination unreachable is type 3 error reporting message. It is invoked when the router can't find a path to the intended destination to forward the packet through.

7. The source-quench message in ICMP was designed to add a kind of ____________ to the IP.
a) error control
b) flow control
c) router control
d) switch control

Answer: b
Explanation: Firstly, it informs the source that the datagram has been discarded. Secondly, it warns the source that there is congestion in the network. It's type 4 error reporting message after which the source is expected to reduce the flow of packets.

8. In case of time exceeded error, when the datagram visits a router, the value of time to live field is _________
a) Remains constant
b) Decremented by 2
c) Incremented by 1
d) Decremented by 1

Answer: d
Explanation: This field will be decremented by 1 at every router, and will be zero by the time it reaches source. This error reporting message is type 11 and is used to prevent the router from travelling forever in case some unknown path anomaly occurs.

9. Two machines can use the timestamp request and timestamp replay messages to determine the ___________ needed for an IP datagram to travel between them.
a) Half-trip time
b) Round-trip time
c) Travel time for the next router
d) Time to reach the destination/source

Answer: b
Explanation: The round-trip time refers to the total time taken combining the time taken for a packet sent from a source to reach a destination and the time taken the acknowledgement sent by the destination to reach the source. The Router sends destination unreachable message if the destination is not found.

10. During debugging, we can use the ____________ program to find if a host is alive and responding.
a) traceroute
b) shell
c) ping
d) java

Answer: c
Explanation: Ping program is used to find if a host is alive and responding. It is to be entered into a command line with the syntax "ping (IP address)" to be executed. Traceroute is a program used to find the shortest route to the destination IP.

11. In windows ____________ can be used to trace the route of the packet from the source to the destination.
a) traceroute
b) tracert
c) ping
d) locater

Answer: b
Explanation: Tracert is used in case of windows, whereas Traceroute in UNIX. Tracert is a program used to find the shortest route to the destination IP. The Router sends destination unreachable message if a path to the destination IP is not found.

12. In a simple echo-request message, the value of the sum is 01010000 01011100. Then, value of checksum is ___________
a) 10101111 10100011
b) 01010000 01011100
c) 10101111 01011100
d) 01010000 10100011

Answer: a
Explanation: The sender side adds the bits of the fragmented packet to find a sum. Checksum is the compliment of the sum (exchange 0's and 1's). The receiver then has to verify the checksum by adding the bits of the received packet to ensure that the packet is error-free.

1. The main reason for transition from IPv4 to IPv6 is _________

a) Huge number of systems on the internet
b) Very low number of system on the internet
c) Providing standard address
d) To provide faster internet

Answer: a
Explanation: Due to huge number of systems on the internet and the lower number of available addresses on IPv4, transition from IPv4 to IPv6 needs to happen. IPv4 provides around 4 billion unique IP addresses whereas IPv6 provides over 340 undecillion unique IP addresses.

2. Which of the following is not a transition strategy?
a) Dual stack
b) Tunneling
c) Conversion
d) Header translation

Answer: c
Explanation: As IPv4 addresses are of 32 bits and IPv6 addresses are of 128 bits, it is not possible to convert IPv4 address to IPv6 address. So, Dual stack, tunneling and header translation are the three strategies which might help in the transition from IPv4 to IPv6.

3. To determine which version to use when sending a packet to a destination, the source host queries which of the following?
a) Dual stack
b) Domain Name Server
c) Header information
d) Transport layer

Answer: b
Explanation: Source host queries DNS to determine which version to use when sending a packet to a destination. The DNS contains both, the IPv4 and IPv6 addresses of the modern dual stack host servers.

4. The strategy used when two computers using IPv6 want to communicate with each other and the packet must pass through a region that uses IPv4 is ______________
a) Dual stack
b) Header translation
c) Conversion
d) Tunneling

Answer: d
Explanation: In tunneling, The IPv4 routers can form a tunnel in which at the sender's side, the IPv6 datagram is encapsulated in to IPv4, and at the receiver's side of the tunnel, the IPv4 packet is stripped and the IPv6 packet is sent to the receiver.Answer: a
Explanation: At the sender's side, the IPv6 datagram is encapsulated in to IPv4 i.e. An IPv4 header is inserted on top of the IPv6 header, and then the packet is sent through the tunnel.

6. ___________ is necessary when the sender wants to use IPv6, but the receiver does not understand IPv6.
a) Dual stack
b) Header translation
c) Conversion
d) Tunneling

Answer: b
Explanation: Header translation is used when the sender wants to use IPv6, but the receiver does not understand IPv6. It is made possible through a Network Address Translation – Protocol Translation enabled device such as a gateway.

7. Header translation uses ___________ to translate an IPv6 address to an IPv4 address.
a) IP address

b) Physical address
c) Mapped address
d) MAC address

Answer: c
Explanation: A mapped IPv6 address contains the IPv4 address in its last 32-bits and is preceded by 16 1s and 80 0s. It can be used to translate an IPv6 address to an IPv4 address.

8. Which of the following is not a step in the Header translation procedure?
a) The IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32bits
b) The value of the IPv6 priority field is discarded
c) The type of service field in IPv4 is set to zero
d) The IPv6 flow label is considered

Answer: d
Explanation: In the header translation procedure, first the IPv6 mapped address is changed to an IPv4 address by extracting the rightmost 32bits, then the value of the IPv6 priority field is discarded, and finally the ToS field in the IPv4 header is set to zero. IPv6 flow label is ignored in the procedure.

1. Which of the following is not applicable for IP?
a) Error reporting
b) Handle addressing conventions
c) Datagram format
d) Packet handling

Answer: a
Explanation: The Internet Protocol is the networking protocol that establishes the internet by relaying datagram across network boundaries. ICMP is a supporting protocol for IP which handles the Error Reporting functionality.

2. Which of the following field in IPv4 datagram is not related to fragmentation?
a) Flags
b) Offset
c) TOS
d) Identifier

Answer: c
Explanation: TOS-type of service identifies the type of packets. It is not related to fragmentation but is used to request specific treatment such as high throughput, high reliability or low latency for the IP packet depending upon the type of service it belongs to.

3. The TTL field has value 10. How many routers (max) can process this datagram?
a) 11
b) 5
c) 10
d) 1

Answer: c
Explanation: TTL stands for Time to Live. This field specifies the life of the IP packet based on the number of hops it makes (Number of routers it goes through). TTL field is decremented by one each time the datagram is processed by a router. When the value is 0, the packet is automatically destroyed.

4. If the value in protocol field is 17, the transport layer protocol used is _________
a) TCP
b) UDP
c) ICMP
d) IGMP

Answer: b

Explanation: The protocol field enables the demultiplexing feature so that the IP protocol can be used to carry payloads of more than one protocol type. Its most used values are 17 and 6 for UDP and TCP respectively. ICMP and IGMP are network layer protocols.

5. Which field helps to check rearrangement of the fragments?
a) offset
b) flag
c) ttl
d) identifier

Answer: a
Explanation: The Fragment Offset field specifies where the fragment fits in the original datagram. The offset of the first fragment will always be 0. The size of the field (13 bits) is 3-bits shorter than the size of the total length field (16 bits).

6. The size of an IP address in IPv6 is _________
a) 4bytes
b) 128bits
c) 8bytes
d) 100bits

Answer: b
Explanation: An IPv6 address is 128 bits long. Therefore, 2^{128} i.e. 340 undecillion unique addresses are available in IPv6. IPv4 has only 4 billion possible addresses and IPv6 would be a brilliant alternative in case IPv4 runs out of possible new addresses.

7. The header length of an IPv6 datagram is ___________
a) 10bytes
b) 25bytes
c) 30bytes
d) 40bytes

Answer: d
Explanation: IPv6 datagram has fixed header length of 40bytes, which results in faster processing of the datagram. There is one fixed header and optional headers which may or may not exist. The fixed header contains the mandatory essential information about the packet while the optional headers contain the optional "not that necessary" information.

8. In an IPv6 header, the traffic class field is similar to which field in the IPv4 header?
a) Fragmentation field
b) Fast switching
c) TOS field
d) Option field

Answer: c
Explanation: The traffic class field is used to specify the priority of the IP packet which is a similar functionality to the Type of Service field in the IPv4 header. It's an 8-bit field and its values are not defined in the RFC 2460.

9. IPv6 does not use ________ type of address.
a) Broadcast
b) Multicast
c) Any cast
d) Unicast

Answer: a
Explanation: There is no concept of broadcast address in IPv6. Instead, there is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

10. Which are the features present in IPv4 but not in IPv6?
a) Fragmentation

b) Header checksum
c) Options
d) Anycast address

Answer: d
Explanation: There is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network. Anycast address is not standardized in IPv4.

1. Which of the following is the broadcast address for a Class B network ID using the default subnetmask?
a) 172.16.10.255
b) 255.255.255.255
c) 172.16.255.255
d) 172.255.255.255

Answer: c
Explanation: In this case, the class B network ID is 172.16.0.0. We know that the default mask of a class B network is 255.255.0.0. If we OR any address in a network with the complement of the default mask (0.0.255.255), we get the broadcast address of the network. In this case, the result of OR would be 172.16.255.255.

2. You have an IP address of 172.16.13.5 with a 255.255.255.128 subnet mask. What is your class of address, subnet address, and broadcast address?
a) Class A, Subnet 172.16.13.0, Broadcast address 172.16.13.127
b) Class B, Subnet 172.16.13.0, Broadcast address 172.16.13.127
c) Class B, Subnet 172.16.13.0, Broadcast address 172.16.13.255
d) Class B, Subnet 172.16.0.0, Broadcast address 172.16.255.255

Answer: b
Explanation: We know that the prefix 172 lies in class B (128 to 191) of IPv4 addresses. From the subnet mask, we get that the class is divided into 2 subnets: 172.16.13.0 to 172.16.13.127 and 172.16.13.128 to 172.16.13.255. The IP 172.16.13.5 lies in the first subnet. So the starting address 172.16.13.0 is the subnet address and last address 172.16.13.127 is the broadcast address.

3. If you wanted to have 12 subnets with a Class C network ID, which subnet mask would you use?
a) 255.255.255.252
b) 255.255.255.255
c) 255.255.255.240
d) 255.255.255.248

Answer: c
Explanation: If you have eight networks and each requires 10 hosts, you would use the Class C mask of 255.255.255.240. Why? Because 240 in binary is 11110000, which means you have four subnet bits and four host bits. Using our math, we'd get the following:
24-2=14 subnets
24-2=14 hosts.

4. The combination of _________ and __________ is often termed the local address of the local portion of the IP address.
a) Network number and host number
b) Network number and subnet number
c) Subnet number and host number
d) Host number

Answer: c
Explanation: It is termed as the local address because the address won't be applicable outside the subnet. Sub networking is implemented for remote sensing in transparent way from that host which is contained in the sub network which called a local operation.

5. _________ implies that all subnets obtained from the same subnet mask.

a) Static subnetting
b) Dynamic subnetting
c) Variable length subnetting
d) Dynamic length subnetting

Answer: a
Explanation: Static subnetting is used when the requirement is of same number of hosts in each subnet for the institution. The same subnet mask can be used to find the subnet id of each subnet. It is usually used to divide large networks into smaller parts.Answer: a
Explanation: In a connection oriented protocol, the host can only establish connection with another host on one unique channel, that's why it can only use unicast addresses. In IPv6, there is an anycast address in IPv6 which allows sending messages to a group of devices but not all devices in a network.

7. __________ is a high performance fiber optic token ring LAN running at 100 Mbps over distances upto 1000 stations connected.
a) FDDI
b) FDDT
c) FDDR
d) FOTR

Answer: a
Explanation: FDDI stands for Fiber Distributed Data Interface. It is a set of standards for fiber optic token ring LANs running at 100 Mbps over distances up to 200 km in diameter and 1000 stations connected.

8. Which of the following are Gigabit Ethernets?
a) 1000 BASE-SX
b) 1000 BASE-LX
c) 1000 BASE-CX
d) All of the mentioned

Answer: d
Explanation: In computer networking, Gigabit Ethernet (GbE or 1 GigE) is a term describing various technologies for transmitting Ethernet frames at a rate of a gigabit per second (1,000,000,000 bits per second), as defined by the IEEE 802.3-2008 standard. It came into use beginning in 1999, gradually supplanting Fast Ethernet in wired local networks, as a result of being considerably faster.

9. _________ is a collective term for a number of Ethernet Standards that carry traffic at the nominal rate of 1000 Mbit/s against the original Ethernet speed of 10 Mbit/s.
a) Ethernet
b) Fast Ethernet
c) Gigabit Ethernet
d) Gigabyte Ethernet

Answer: b
Explanation: Fast Ethernet is a set of Ethernet Standards which were introduced in 1995, that carry traffic at the nominal rate of 1000 Mbit/s. 100BASE-TX is the most commonly used Fast Ethernet standard.

10. _________ is another kind of fiber optic network with an active star for switching.
a) S/NET
b) SW/NET
c) NET/SW
d) FS/NET

Answer: a
Explanation: A 50-MBd active star fiber optical Local area network (LAN) and its optical combiner and mixing rod splitter are presented. The limited power budget and relatively large tapping losses of light wave technology, which limit the use of fiber optics in tapped bus LAN topologies, are examined and proven tolerable in optical star topologies.

a) i only
b) ii only
c) iii and iv only
d) i and v only

Answer: d
Explanation: First, if you have two hosts directly connected, as shown in the graphic, then you need a crossover cable. A straight-through cable won't work. Second, the hosts have different masks, which puts them in different subnets. The easy solution is just to set both masks to 255.255.255.0 (/24).

a) i only
b) ii and iii only
c) iii and iv only
d) ii only

Answer: c
Explanation: The router's IP address on the E0 interface is 172.16.2.1/23, which is 255.255.254.0. This makes the third octet a block size of 2. The router's interface is in the 172.16.2.0 subnet, and the broadcast address is 172.16.3.255 because the next subnet is 172.16.4.0. The valid host range is 172.16.2.1 to 172.16.3.254. The router is using the first valid host address in the range.

a) i and iii
b) ii and iv
c) i, ii and iv
d) ii, iii and iv

Answer: b
Explanation: The mask 255.255.254.0 (/23) used with a Class A address means that there are 15 subnet bits and 9 host bits. The block size in the third octet is 2 (256 – 254). So this makes the subnets in the interesting octet 0, 2, 4, 6, etc., all the way to 254. The host 10.16.3.65 is in the 10.16.2.0 subnet. The next subnet is 10.16.4.0, so the broadcast address for the 10.16.2.0 subnet is 10.16.3.255. The valid host addresses are 10.16.2.1 to 10.16.3.254.

4. What is the maximum number of IP addresses that can be assigned to hosts on a local subnet that uses the 255.255.255.224 subnet mask?
a) 14
b) 15
c) 16
d) 30

Answer: d
Explanation: A /27 (255.255.255.224) is 3 bits on and 5 bits off. This provides 8 subnets, each with 30 hosts. Does it matter if this mask is used with a Class A, B, or C network address? Not at all. The number of host bits would never change.

5. You need to subnet a network into 5 subnets, each with at least 16 hosts. Which classful subnet mask would you use?
a) 255.255.255.192
b) 255.255.255.224
c) 255.255.255.240
d) 255.255.255.248

Answer: b
Explanation: You need 5 subnets, each with at least 16 hosts. The mask 255.255.255.240 provides 16 subnets with 14 hosts which is less than 15, so this will not work. The mask 255.255.255.224 provides 8 subnets, each with 30 hosts so this may work. The mask 255.255.255.192 provides 4 subnets, each with 60 hosts so this may work. Comparing both the possible masks, 255.255.255.224 provides the best answer.

6. You have a network that needs 29 subnets while maximizing the number of host addresses available on each

subnet. How many bits must you borrow from the host field to provide the correct subnet mask?
a) 2
b) 3
c) 4
d) 5

Answer: d
Explanation: A 240 mask is 4 subnet bits and provides 16 subnets, each with 14 hosts. We need more subnets, so let's add subnet bits. One more subnet bit would be a 248 mask. This provides 5 subnet bits (32 subnets) with 3 host bits (6 hosts per subnet). This is the best answer.

7. If an Ethernet port on a router were assigned an IP address of 172.16.112.1/25, what would be the valid subnet address of this host?
a) 172.16.112.0
b) 172.16.0.0
c) 172.16.96.0
d) 172.16.255.0

Answer: a
Explanation: A /25 mask is 255.255.255.128. Used with a Class B network, the third and fourth octets are used for subnetting with a total of 9 subnet bits, 8 bits in the third octet and 1 bit in the fourth octet. Since there is only 1 bit in the fourth octet, the bit is either off or on-which is a value of 0 or 128. The host in the question is in the 0 subnet, which has a broadcast address of 127 since 128 is the next subnet

8. You have an interface on a router with the IP address of 192.168.192.10/29. Including the router interface, how many hosts can have IP addresses on the LAN attached to the router interface?
a) 6
b) 8
c) 30
d) 32

Answer: a
Explanation: A /29 (255.255.255.248), regardless of the class of address, has only 3 host bits. Six hosts are the maximum number of hosts on this LAN, including the router interface. Out of the 8 addresses possible with the host bits, the first and the last address are for the subnet id and broadcast address respectively.

9. What is the subnet id of a host with an IP address 172.16.66.0/21?
a) 172.16.36.0
b) 172.16.48.0
c) 172.16.64.0
d) 172.16.0.0

Answer: c
Explanation: A /21 is 255.255.248.0, which means we have a block size of 8 in the third octet, so we just count by 8 until we reach 66. The subnet in this question is 64.0. The next subnet is 72.0, so the broadcast address of the 64 subnet is 71.255.

10. The network address of 172.16.0.0/19 provides how many subnets and hosts?
a) 7 subnets, 30 hosts each
b) 8 subnets, 8,190 hosts each
c) 8 subnets, 2,046 hosts each
d) 7 subnets, 2,046 hosts each

Answer: b
Explanation: A CIDR address of /19 is 255.255.224.0. This is a Class B address, so that is only 3 subnet bits, but it provides 13 host bits, or 8 subnets, each with 8,190 hosts.

1. Which type of Ethernet framing is used for TCP/IP and DEC net?

a) Ethernet 802.3
b) Ethernet 802.2
c) Ethernet II
d) Ethernet SNAP

Answer: c
Explanation: The Ethernet 802.3 framing is used for NetWare versions 2 to 3.11, and the Ethernet 802.2 framing is used for NetWare versions 3.12 and later plus OSI routing, Ethernet II is used with TCP/IP and DEC net, and Ethernet SNAP is used with TCP/IP and AppleTalk. The type field in Ethernet 802.2 frame is replaced by a length field in Ethernet 802.3.

2. Consider a situation in which you are a system administrator on a NetWare network, you are running NetWare 4.11 and you cannot communicate with your router. What is the likely problem?
a) NetWare 4.11 defaults to 802.2 encapsulation
b) NetWare 4.11 defaults to 802.3 encapsulation
c) Cisco routers only work with NetWare 3.11
d) NetWare 3.11 defaults to 802.2 encapsulation

Answer: a
Explanation: The default encapsulation on Cisco routers is Novell Ethernet_802.3 and NetWare 3.12and later defaults to 802.2 encapsulation, 3.11 and earlier defaults to 802.3.

3. NetWare IPX addressing uses a network number and a node number. Which statement is not true?
a) The network address is administratively assigned and can be up to 16 hexadecimal digits long
b) The node address is always administratively assigned
c) The node address is usually the MAC address
d) If the MAC address is used as the node address, then IPX eliminates the use of ARP

Answer: b
Explanation: The network address can be up to 16 hexadecimal digits in length. The node number is 12 hexadecimal digits. The node address is usually the MAC address. An example IPX address is 4a1d.0000.0c56.de33. The network part is 4a1d. The node part is 0000.0c56.de33. The network number is assigned by the system administrator of the Novell network and the MAC address/node address is not assigned by the administrator.

4. Which NetWare protocol works on layer 3–network layer—of the OSI model?
a) IPX
b) NCP
c) SPX
d) NetBIOS

Answer: a
Explanation: IPX (Internetwork Packet Exchange) is the NetWare network layer 3 protocol used for transferring information on LANs that use Novell's NetWare.

5. Which NetWare protocol provides link-state routing?
a) NLSP
b) RIP
c) SAP
d) NCP

Answer: a
Explanation: NetWare Link Services Protocol (NLSP) provides link-state routing. SAP (Service Advertisement Protocol) advertises network services. NCP (NetWare Core Protocol) provides client-to-server connections and applications. RIP is a distance vector routing protocol. NLSP was developed by Novell to replace RIP routing protocols.

6. As a system administrator, you want to debug IGRP but are worried that the "debug IP IGRP transaction" command will flood the console. What is the command that you should use?
a) Debug IP IGRP event
b) Debug IP IGRP-events

c) Debug IP IGRP summary
d) Debug IP IGRP events

Answer: d
Explanation: The "debug IP IGRP events" is used to display a short summary of IGRP routing information. You can append an IP address onto either console's command-line to see only the IGRP updates from a neighbor. The command will only give a short summary and hence won't flood the command line.Answer: a
Explanation: It isolates network 10.0.0.0 and 172.68.7.0 and associates autonomous systems 109 and71 with IGRP. IGRP does not disable RIP, both can be used at the same time.

8. The "IPX delay number" command will allow an administrator to change the default settings. What are the default settings?
a) For LAN interfaces, one tick; for WAN interfaces, six ticks
b) For LAN interfaces, six ticks; for WAN interfaces, one tick
c) For LAN interfaces, zero ticks; for WAN interfaces, five ticks
d) For LAN interfaces, five ticks; for WAN interfaces, zero Ticks

Answer: a
Explanation: Tick is basically the update rate of clients in the network. The IPX delay number will give the ticks at a certain time. The default ticks are–for LAN interfaces, one tick, and for WAN interfaces, six ticks.Answer: d
Explanation: The following commands setup the sub interfaces to allow for two types of encapsulation:interface Ethernet 0.1 IPX encapsulation Novell-ether IPX network 9e interface Ethernet0.2 IPX encapsulation sap IPX network 6c.

10. What does the "IPX maximum-paths 2" command accomplish?
a) It enables load sharing on 2 paths if the paths are equal metric paths
b) It sets up routing to go to network 2
c) It is the default for Cisco IPX load sharing
d) It enables load sharing on 2 paths if the paths are unequal metric paths

Answer: a
Explanation: It enables load sharing on 2 paths if the paths are equal metric paths. The default is 1 path and the maximum is 512 paths. The value must always be greater than 1 and must be a natural number.

11. You want to enable both arpa and snap encapsulation on one router interface. How do you do this?
a) The interface can handle multiple encapsulation types with no extra configuration
b) Assign two network numbers, one for each encapsulation type
c) Enable Novell-ether to run multiple encapsulation types
d) Both arpa and snap are enabled by default so you don't have to configure anything

Answer: b
Explanation: To assign multiple network numbers, you usually use sub interfaces. A sample configuration follows: IPXEthernet 0.1 IPX encapsulation novell-ether ipx network 9e interface ethernet 0.2 ipx encapsulation sap ipx network 6cAnswer: a
Explanation: GNS is Novell's protocol to Get Nearest Server. If there is a server on the local network,that server will respond. If there isn't, the Cisco router has to be configured to forward theGNS SAP.

13. To prevent Service Advertisements (SAPs) from flooding a network, Cisco routers do not forward them. How are services advertised to other networks?
a) Each router builds its own SAP table and forwards that every 60 seconds
b) Each router assigns a service number and broadcasts that
c) SAPs aren't necessary with Cisco routers
d) Cisco routers filter out all SAPs

Answer: a
Explanation: Cisco routers build SAP tables and forward the table every 60 seconds. All SAPs can't befiltered even with 4.x since NDS and time synchronization uses SAPs.

14. Novell's implementation of RIP updates routing tables every _________ seconds.
a) 60
b) 90
c) 10
d) 30

Answer: a
Explanation: Novell's RIP updates routing tables every 60 seconds, Apple's RTMP is every 10 seconds, routers ARP every 60 seconds, IGRP signal every 90 seconds, and Banyan VINES signals every 90 seconds.

15. In Novell's use of RIP, there are two metrics used to make routing decisions. Select the correct metrics.
a) Ticks & Hops
b) Hops & Loops
c) Loops & Counts
d) Counts & Ticks

Answer: a
Explanation: It first uses ticks (which is about 1/18 sec.); if there is a tie, it uses hops; if hops are equal, then it uses an administratively assigned tiebreaker.

1. Which routing protocol has a maximum network diameter (hop count) of 15?
a) RIPv1
b) RIPv2
c) EIGRP
d) Both RIPv1 and RIPv2

Answer: d
Explanation: Both RIPv1 and RIPv2 support a maximum hop count of 15 because they use 4-bits to store this value. RIPv1 uses classful routing whereas RIPv2 uses classless routing. The routing updates are broadcasted over the network. It notifies routers about the update so that they update their own routing tables.

2. How often does a RIPv1 router broadcast its routing table by default?
a) Every 30 seconds
b) Every 60 seconds
c) Every 90 seconds
d) RIPv1 does not broadcast periodically

Answer: a
Explanation: RIPv1 router broadcasts its routing table every 30 seconds by default. The broadcasted routing table can be used by other routers to find the shortest path among the network devices.

3. Which command displays RIP routing updates?
a) Show IP route
b) Debug IP rip
c) Show protocols
d) Debug IP route

Answer: b
Explanation: The debug IP rip command is used to show the Internet Protocol (IP) Routing Information Protocol (RIP) updates being sent and received on the router. It verifies that the updates are being broadcasted and not multicasted.

4. Two connected routers are configured with RIP routing. What will be the result when a router receives a routing update that contains a higher-cost path to a network already in its routing table?
a) The updated information will be added to the existing routing table Debug IP rip
b) The update will be ignored and no further action will occur Debug IP route
c) The updated information will replace the existing routing table entry
d) The existing routing table entry will be deleted from the routing table and all routers will exchange routing updates to reach convergence

Answer: b
Explanation: When a routing update is received by a router, the router first checks the administrative distance (AD) and always chooses the route with the lowest AD. However, if two routes are received and they both have the same AD, then the router will choose the one route with the lowest metrics, or in RIP's case, hop count.

5. You type debug IP rip on your router console and see that 172.16.10.0 is being advertised to you with a metric of 16. What does this mean?
a) The route is 16 hops away Debug IP rip
b) The route has a delay of 16 microseconds Debug IP route
c) The route is inaccessible
d) The route is queued at 16 messages a second

Answer: c
Explanation: You cannot have 16 hops on a RIP network by default, because the max default hops possible is 15. If you receive a route advertised with a metric of 16, this means it is inaccessible.

6. Default administrative distance of a static route is ________
a) 0
b) 90
c) 100
d) 1

Answer: d
Explanation: 1 is the default administrative distance of Static Route. It is used by routers to select the best path when there are different routes to the same destination. It's used only two different routing protocols are being used.

7. Which protocol gives a full route table update every 30 seconds?
a) IEGRP
b) RIP
c) ICMP
d) IP

Answer: b
Explanation: RIP gives a full route table update every 30 seconds. The broadcasted routing table can be used by other routers to find the shortest path among the network devices.

8. _________ is the default administrative distance of RIP.
a) 0
b) 90
c) 120
d) 130

Answer: c
Explanation: The default administrative distance is the default count of numbers assigned to arbitrary routes to a destination. The default administrative distance of RIP is 120. It is used to find the shortest route amongst the number of paths available.

9. Which statement is true regarding classless routing protocol?
a) The use of discontinuous networks is not allowed
b) Use of variable length subnet masks is permitted
c) RIPv1 is a classless routing protocol
d) IGRP supports classes routing within the same autonomous system

Answer: b
Explanation: Use of variable length subnet masks is permitted in classless routing protocols. Also use of discontinuous networks is allowed in such routing protocols. RIPv1 is a classful routing protocol but RIPv2 is classless routing protocol.

10. Where should we use default routing?

a) On stub networks- which have only one exit path out of the network
b) Which have more than one exit path out of the network
c) Minimum five exit paths out of the network
d) Maximum five exit paths out of the network

Answer: a
Explanation: We must use default routing on stub networks. They have only one exit path out of the network, so there can be no specific path decided for such networks.

1. Which statement is true regarding classless routing protocols?
a) The use of discontinuous networks is not allowed
b) The use of variable length subnet masks is permitted
c) RIPv1 is a classless routing protocol
d) RIPv2 supports classless routing

Answer: b
Explanation: Classful routing means that all hosts in the internetwork use the same mask. Classless routing means that you can use Variable Length Subnet Masks (VLSMs) and can also support discontinuous networking.

2. What is route poisoning?
a) It sends back the protocol received from a router as a poison pill, which stops the regular updates. The use of variable length subnet masks is permitted
b) It is information received from a router that can't be sent back to the originating router.RIPv2 supports classless routing
c) It prevents regular update messages from reinstating a route that has just come up
d) It describes when a router sets the metric for a downed link to infinity

Answer: d
Explanation: When a network goes down, the distance-vector routing protocol initiates route poisoning by advertising the network with a metric of 16, or unreachable.

3. Which of the following is true regarding RIPv2?
a) It has a lower administrative distance than RIPv1
b) It converges faster than RIPv1
c) It has the same timers as RIPv1
d) It is harder to configure than RIPv1

Answer: c
Explanation: RIPv2 is pretty much just like RIPv1. It has the same administrative distance and timers and is configured just like RIPv1.

4. Which of the situations might not require multiple routing protocols in a network?
a) When a new Layer 2-only switch is added to the network
b) When you are migrating from one routing protocol to another
c) When you are using routers from multiple vendors
d) When there are host-based routers from multiple vendors

Answer: a
Explanation: Multiple routing protocols are required only when we need to migrate from one routing protocol to another, or when we are using routers from multiple vendors, or when there are host-based routers from multiple vendors. Routing is not a layer-2 function so we don't require multiple routing protocols when new layer-2 switch is added.

5. Which two routing protocols can be redistributed into OSPF by a Cisco router?
a) IP EIGRP and AppleTalk EIGRP
b) AppleTalk EIGRP and RIPv2
c) RIPv2 and IP EIGRP
d) IPX RIP & AppleTalk EIGRP

Answer: c
Explanation: OSPF stands for Open Shortest Path First. It is a Link state routing protocol. IP EIGRP and RIPv2 can be redistributed into OSPF by a Cisco router.

6. Which is a reason for avoiding doing route redistribution on two routers between the same two routing domains?
a) Higher cost of two routers
b) Routing feedback
c) Cisco IOS incompatibility
d) Not possible to use two routers

Answer: b
Explanation: Routing feedback is an anomaly in which the routing protocols go back and forth between one route and another. Routing feedback is a reason for avoiding doing route redistribution on two routers between the same two routing domains.

7. What does administrative distance rank?
a) Metrics
b) Sources of routing information
c) Router reliability
d) Best paths

Answer: b
Explanation: Sources of routing information is the administrative distance rank. It is used by routers to select the best path when there are different routes to the same destination. It's used only two different routing protocols are being used.

8. Which protocol maintains neighbor adjacencies?
a) RIPv2 and EIGRP
b) IGRP and EIGRP
c) RIPv2
d) EIGRP

Answer: c
Explanation: Neighbor adjacency refers to the formal handshake performed by neighboring routers. It is to be done before the router share any routing information. RIP V2 maintains neighbor adjacencies.

9. Which routing protocol implements the diffusing update algorithm?
a) IS-IS
b) IGRP
c) EIGRP
d) OSPF

Answer: c
Explanation: The diffusing update algorithm (DUAL) is used to maintain backup routes to a destination for when the primary route fails. EIGRP routing protocol implements the diffusing update algorithm.

1. In cryptography, what is cipher?
a) algorithm for performing encryption and decryption
b) encrypted message
c) both algorithm for performing encryption and decryption and encrypted message
d) decrypted message

Answer: a
Explanation: Cipher is a method to implement encryption and decryption of messages travelling in a network. It's used to increase the confidentiality of the messages.

2. In asymmetric key cryptography, the private key is kept by __________
a) sender
b) receiver

c) sender and receiver
d) all the connected devices to the network

Answer: b
Explanation: The private key is kept only by the receiver of the message. Its aim is to make sure that only the intended receiver can decipher the message.

3. Which one of the following algorithm is not used in asymmetric-key cryptography?
a) rsa algorithm
b) diffie-hellman algorithm
c) electronic code book algorithm
d) dsa algorithm

Answer: c
Explanation: Electronic code book algorithm is a block cipher method in which each block of text in an encrypted message corresponds to a block of data. It is not feasible for block sizes smaller than 40 bits.

4. In cryptography, the order of the letters in a message is rearranged by __________
a) transpositional ciphers
b) substitution ciphers
c) both transpositional ciphers and substitution ciphers
d) quadratic ciphers

Answer: a
Explanation: In transposition ciphers, the order of letters in a plaintext message is shuffled using a pre-defined method. Some of such ciphers are Rail fence cipher and Columnar transposition.

5. What is data encryption standard (DES)?
a) block cipher
b) stream cipher
c) bit cipher
d) byte cipher

Answer: a
Explanation: DES is a symmetric key block cipher in which the block size is 64 bits and the key size is 64 bits. It is vulnerable to some attacks and is hence not that popularly used.

6. Cryptanalysis is used __________
a) to find some insecurity in a cryptographic scheme
b) to increase the speed
c) to encrypt the data
d) to make new ciphers

Answer: a
Explanation: Cryptanalysis is a field of study in which a cryptographic scheme is intentionally tried to breach in order to find flaws and insecurities. It is used to make sure that the scheme is least vulnerable to attacks.

7. Which one of the following is a cryptographic protocol used to secure HTTP connection?
a) stream control transmission protocol (SCTP)
b) transport layer security (TLS)
c) explicit congestion notification (ECN)
d) resource reservation protocol

Answer: b
Explanation: TLS has strong message authentication and key-material generation to prevent eavesdropping, tampering and message forgery. It has been used since the year 1996.

8. Voice privacy in GSM cellular telephone protocol is provided by _______

a) A5/2 cipher
b) b5/4 cipher
c) b5/6 cipher
d) b5/8 cipher

Answer: a
Explanation: The A5/2 cipher was published in the year 1996 and was cryptanalysed in the same year within a month. It's use was discontinued from the year 2006 as it was really weak.

9. ElGamal encryption system is __________
a) symmetric key encryption algorithm
b) asymmetric key encryption algorithm
c) not an encryption algorithm
d) block cipher method

Answer: b
Explanation: The ELGamal encryption system was made by Taher Elgamal in the year 1985 and is an asymmetric key algorithm. It is popularly used in PGP and other systems.

10. Cryptographic hash function takes an arbitrary block of data and returns _________
a) fixed size bit string
b) variable size bit string
c) both fixed size bit string and variable size bit string
d) variable sized byte string

Answer: a
Explanation: Cryptographic hash functions are used in digital signatures and message authentication codes. The only issue with it is that it returns the same hash value every time for a message making it vulnerable to attackers to evaluate and break the cipher.
Answer: a
Explanation: Persistent connections are kept active after completing transaction so that multiple objects can be sent over the same TCP connection.

2. HTTP is ________ protocol.
a) application layer
b) transport layer
c) network layer
d) data link layer

Answer: a
Explanation: HTTP is an Application layer protocol used to define how messages are formatted and transmitted through the World Wide Web.

3. In the network HTTP resources are located by __________
a) Uniform resource identifier
b) Unique resource locator
c) Unique resource identifier
d) Union resource locator

Answer: a
Explanation: The Uniform Resource Identifier is a name and locator for the resource to be located by the HTTP. The URLs and URNs are derived through the identifier.

4. HTTP client requests by establishing a __________ connection to a particular port on the server.
a) User datagram protocol
b) Transmission control protocol
c) Border gateway protocol
d) Domain host control protocol

Answer: b
Explanation: HTTP clients perform requests using a TCP connection, because the TCP connection provides a more reliable service. UDP is not a reliable protocol, border gateway protocol is used on top of TCP, while domain host control protocol is a network layer protocol.

5. In HTTP pipelining __________
a) multiple HTTP requests are sent on a single TCP connection without waiting for the corresponding responses
b) multiple HTTP requests cannot be sent on a single TCP connection
c) multiple HTTP requests are sent in a queue on a single TCP connection
d) multiple HTTP requests are sent at random on a single TCP connection

Answer: a
Explanation: HTTP pipelining helps the client make multiple requests without having to waiting for each response, thus saving a lot of time and bandwidth for the client.

6. FTP server listens for connection on which port number?
a) 20
b) 21
c) 22
d) 23

Answer: b
Explanation: Port 20 is used for FTP data. Port 22 is used for SSH remote login. Port 23 is used for TELNET.

7. In FTP protocol, a client contacts a server using ______ as the transport protocol.
a) Transmission control protocol
b) User datagram protocol
c) Datagram congestion control protocol
d) Stream control transmission protocol

Answer: a
Explanation: The clients use the Transmission Control Protocol for FTP as it's more reliable than UDP, DCCP, and SCTP, and reliability of file transfer is required to be as high as possible for FTP.Answer: b
Explanation: In Passive mode of FTP, the client initiates both data and control connections, while in Active mode, the client initiates the control connection and then the server initiates the data connection.

9. The File Transfer Protocol is built on __________
a) data centric architecture
b) service oriented architecture
c) client server architecture
d) connection oriented architecture

Answer: c
Explanation: The FTP connection includes a Server and a Client which wish to share files. The server can have multiple clients at the same time while the client communicates with only one server at a time.

10. In File Transfer Protocol, data transfer cannot be done in __________
a) stream mode
b) block mode
c) compressed mode
d) message mode

Answer: d
Explanation: In Stream mode, the data is transferred in a continuous stream. In Block mode, data is transferred after being divided into smaller blocks. In Compressed mode, data is transferred after being compressed using some compression algorithm.

1. Which methods are commonly used in Server Socket class?

a) Public Output Stream get Output Stream ()
b) Public Socket accept ()
c) Public synchronized void close ()
d) Public void connect ()

Answer: b
Explanation: The Public socket accept () method is used by the ServerSocket class to accept the connection request of exactly one client at a time. The client requests by initializing the socket object with the servers IP address.

2. Which constructor of Datagram Socket class is used to create a datagram socket and binds it with the given Port Number?
a) Datagram Socket(int port)
b) Datagram Socket(int port, Int Address address)
c) Datagram Socket()
d) Datagram Socket(int address)

Answer: b
Explanation: Datagram Socket (int port, Int Address address) is used to create a datagram socket. A datagram socket is created for connection-less communication between the server and the client. There is no accept() method in this class.

3. The client in socket programming must know which information?
a) IP address of Server
b) Port number
c) Both IP address of Server & Port number
d) Only its own IP address

Answer: c
Explanation: The client in socket programming must know IP address of Server as it has to use that IP address in order to initialize the socket class constructor. That is how the client requests a connection to the server.Answer: a
Explanation: The URL Connection class can be used to read and write data to the specified resource referred by the URL. A connection to the URL is initialized by the OpenConnection() method of the class.Answer: a
Explanation: Datagram is basically some information travelling between the sender and the receiver, but there is no guarantee of its content, arrival or arrival time. A Datagram socket class object is created to make a datagram connection between the server and the client.

6. TCP, FTP, Telnet, SMTP, POP etc. are examples of ___________
a) Socket
b) IP Address
c) Protocol
d) MAC Address

Answer: c
Explanation: TCP, FTP, Telnet, SMTP, POP etc. are examples of Protocol. Out of them, TCP is a transport layer protocol and FTP, TELNET, SMTP and POP are application layer protocols.

7. What does the java.net.InetAddress class represent?
a) Socket
b) IP Address
c) Protocol
d) MAC Address

Answer: b
Explanation: The java.net.InetAddress class represents IP Address of a particular specified host. It can be used to resolve the host name from the IP address or the IP address from the host name.Answer: a
Explanation: The flush () method of Print Stream class flushes any un cleared buffers in memory.

9. Which classes are used for connection-less socket programming?
a) Datagram Socket

b) Datagram Packet
c) Both Datagram Socket & Datagram Packet
d) Server Socket

Answer: c
Explanation: Datagram is basically some information travelling between the sender and the receiver, but there is no guarantee of its content, arrival or arrival time. Datagram Socket, Datagram Packet are used for connection-less socket programming, while Server Socket is used for connection-oriented socket programming.

10. In Inet Address class, which method returns the host name of the IP Address?
a) Public String get Hostname()
b) Public String getHostAddress()
c) Public static InetAddress get Localhost()
d) Public getByName()

Answer: a
Explanation: In Inet Address class public String getHostname() method returns the host name of the IP Address. The getHostAddress() method returns the IP address of the given host name.

1. Cookies were originally designed for ____________
a) Client side programming
b) Server side programming
c) Both Client side programming and Server side programming
d) Socket programming

Answer: b
Explanation: Cookies were originally designed for server side programming, and at the lowest level, they are implemented as an extension to the HTTP protocol. They were introduced with the intention of providing a better user experience for the websites.

2. The Cookie manipulation is done using which property?
a) cookie
b) cookies
c) manipulate
d) manipulate cookie

Answer: a
Explanation: The cookie property sets or returns all name/value pairs of cookies in the current document. There are no methods involved: cookies are queried, set, and deleted by reading and writing the cookie property of the Document object using specially formatted strings.

3. Which of the following explains Cookies nature?
a) Non Volatile
b) Volatile
c) Intransient
d) Transient

Answer: d
Explanation: Cookies are transient by default; the values they store last for the duration of the web browser session but are lost when the user exits the browser. While the browsing session is active the cookie stores the user values in the user's storage itself and accesses them.

4. Which attribute is used to extend the lifetime of a cookie?
a) Higher-age
b) Increase-age
c) Max-age
d) Lifetime

Answer: c
Explanation: If you want a cookie to last beyond a single browsing session, you must tell the browser how long (in seconds) you would like it to retain the cookie by specifying a max-age attribute. A number of seconds until the cookie expires. A zero or negative number will kill the cookie immediately.

5. Which of the following defines the Cookie visibility?
a) Document Path
b) LocalStorage
c) SessionStorage
d) All of the mentioned

Answer: d
Explanation: sessionStorage, localStorage and Document path all are used to store data on the client-side. Each one has its own storage and expiration limit. Cookie visibility is scoped by the document origin as Local Storage and Session Storage are, and also by document path.

6. Which of the following can be used to configure the scope of the Cookie visibility?
a) Path
b) Domain
c) Both Path and Domain
d) Server

Answer: d
Explanation: The Cookie visibility scope is configurable through cookie attributes path and domain. Domain attribute in the cookie is used to specify the domain for which the cookie is sent. Path includes the Path attribute in the cookie to specify the path for which this cookie is sent.

7. How can you set a Cookie visibility scope to local Storage?
a) /
b) %
c) *
d) #

Answer: a
Explanation: Setting the path of a cookie to "/" gives scoping like that of localStorage and also specifies that the browser must transmit the cookie name and value to the server whenever it requests any web page on the site.

8. Which of the following is a Boolean cookie attribute?
a) Bool
b) Secure
c) Lookup
d) Domain

Answer: b
Explanation: The final cookie attribute is a boolean attribute named secure that specifies how cookie values are transmitted over the network. By default, cookies are insecure, which means that they are transmitted over a normal, insecure HTTP connection. If a cookie is marked secure, however, it is transmitted only when the browser and server are connected via HTTPS or another secure protocol.

9. Which of the following function is used as a consequence of not including semicolons, Commas or whitespace in the Cookie value?
a) EncodeURIComponent()
b) EncodeURI()
c) EncodeComponent()
d) Encode()

Answer: a
Explanation: Cookie values cannot include semicolons, commas, or whitespace. For this reason, you may want to use

the core JavaScript global function encodeURIComponent() to encode the value before storing it in the cookie.

10. What is the constraint on the data per cookie?
a) 2 KB
b) 1 KB
c) 4 KB
d) 3 KB

Answer: c
Explanation: Each cookie can hold up to only 4 KB. In practice, browsers allow many more than 300 cookies total, but the 4 KB size limit may still be enforced by some. Storage of a session has to be a minimum of 5MB.

1. What does REST stand for?
a) Represent State Transfer
b) Representational State Transfer
c) Representing State Transfer
d) Representation State Transfer

Answer: b
Explanation: REST stands for Representational State Transfer and is a software architecture style in which the server sends a representation of the state of the resource that it requests. It provides interoperability between the systems.

2. Which of the following protocol is used by Restful web services as a medium of communication between client and server?
a) HTTP
b) FTP
c) Gopher
d) TELNET

Answer: a
Explanation: Restful web services make use of HTTP protocol as a medium of communication between client and server. The REST architecture was known as the HTTP object model back in the year 1994.

3. Which of the following is not a good practice to create a standard URI for a web service?
a) Maintain Backward Compatibility
b) Use HTTP Verb
c) Using spaces for long resource names
d) Use lowercase letters

Answer: c
Explanation: We must use hyphens (-) or underscores (_) instead of spaces to represent long resource names. It may lead to the resource to be less recognizable for the system if we use spaces instead.

4. Which of the following HTTP methods should be idempotent in nature?
a) OPTIONS
b) DELETE
c) POST
d) HEAD

Answer: b
Explanation: DELETE operation should be idempotent, means their result will always same no matter how many times these operations are invoked. Also, the PUT operation is supposed to be idempotent.

5. Which of the following directive of Cache Control Header of HTTP response indicates that resource is cachable by only client and server?
a) Public
b) Private
c) Nocache/nostore

d) Maxage

Answer: b
Explanation: Private directive indicates that resource is cachable by only client and server; no intermediary can cache the resource. But if we use the public directive, it indicates that the resource may be cachable by any intermediary component.

6. Which of the following HTTP Status code means CREATED, when a resource is successful created using POST or PUT request?
a) 200
b) 201
c) 204
d) 304

Answer: b
Explanation: HTTP Status Code 201 means CREATED, when a resource is successful created using POST or PUT request. The code 200 means success i.e. OK, code 204 means NO CONTENT, and the code 304 means NOT MODIFIED.

7. Which of the following annotation of JAX RS API is used to annotate a method used to create resource?
a) @Path
b) @GET
c) @PUT
d) @POST

Answer: C
Explanation: @PUT is the HTTP request that is used to create resource and also define a complete resource path. @POST may also be used to create a resource but it won't define a resource path i.e. an accessing medium.

8. Which of the following annotation of JAX RS API binds the parameter passed to method to a HTTP matrix parameter in path?
a) @PathParam
b) @QueryParam
c) @MatrixParam
d) @HeaderParam

Answer: c
Explanation: @MatrixParam is the annotation that binds the parameter passed to method to a HTTP matrix parameter in path, while @QueryParam binds to a query parameter, @PathParam binds to a value and @HeaderParam binds to the HTTP header in the path. Answer: b
Explanation: In REST architecture, a REST Server simply provides access to resources and REST client accesses and presents the resources. It is popularly used because it makes efficient use of the bandwidth and can be cached for better performance and scalability. Answer: b
Explanation: POST operation can cause different result so they are not idempotent. The DELETE and PUT operations are idempotent as they invoke the same result every time they are called.

1. The term that is used to place packet in its route to its destination is called __________
a) Delayed
b) Urgent
c) Forwarding
d) Delivering

Answer: c
Explanation: Forwarding is done by the nodes in the path from source to destination, that are not the intended destination for the packet in order to pass the packet to the next node in the path. The destination machine does not forward the packet to any other node.

2. A second technique to reduce routing table and simplify searching process is called __________

a) Network-Specific Method
b) Network-Specific Motion
c) Network-Specific Maintaining
d) Network-Specific Membership

Answer: a
Explanation: In the network specific forwarding method, there is only one record, the destination of the packet, in the routing table and not the other hosts of the network. The other two forwarding methods are the default method and the next-hop method.

3. Next-Hop Method is used to reduce contents of a _________
a) Revolving table
b) Rotating Table
c) Routing Table
d) Re-allocate table

Answer: c
Explanation: In the next-hop forwarding method, the routing table of each router in the path contains the address of only the next hop in the path of packet. This method is suitable for short distances only.

4. Several techniques can make size of routing table manageable and also handle issues such as __________
a) Maturity
b) Error reporting
c) Tunneling
d) Security

Answer: d
Explanation: The size of the routing table in the technique must be manageable for the network nodes i.e. it must not be too big. Security of the forwarding packet is the highest priority for a technique and must be high enough so that only authorized senders and receivers can access the packet's content.

5. Host-specific routing is used for purposes such as checking route or providing _____
a) Network Measures
b) Security Measures
c) Routing Measures
d) Delivery Measures

Answer: b
Explanation: In host-specific routing, the route of the packet is defined based on the exact match of the packet's IP with the routing table entry of the host. It provides the best security for the packet as the packet is forwarded only to routers in the pre-defined path.

6. In Unicast routing, if instability is between three nodes, stability cannot be ________
a) Stable
b) Reversed
c) Guaranteed
d) Forward

Answer: c
Explanation: In Unicast routing, there is only sender and one receiver. So, if there is instability between three nodes, in which one is sender, one is receiver and one is the router in the path, there is no other path available for the packet and the stability of the network is not guaranteed.

7. In Unicast Routing, Dijkstra algorithm creates a shortest path tree from a ________
a) Graph
b) Tree
c) Network
d) Link

Answer: a
Explanation: The Djikstra's shortest path algorithm is the fastest among the algorithms for finding the shortest path in a graph. But it is a greedy method based algorithm so it does not guarantee the shortest path every time.

8. In Multicast Routing Protocol, flooding is used to broadcast packets but it creates ________
a) Gaps
b) Loops
c) Holes
d) Links

Answer: b
Explanation: In multicast routing, there is one sender and many receivers. So flooding is the most basic method to forward packets to many receivers. The one issue with flooding is that it creates routing loops. One loop prevention method is that the routers will not send the packet to a node where the packet has been received before.

9. RPF stands for __________
a) Reverse Path Forwarding
b) Reverse Path Failure
c) Reverse Packet Forwarding
d) Reverse Protocol Failure

Answer: a
Explanation: Reverse Path Forwarding is a loop-free forwarding method for multi-cast routing in modern systems. The method focuses on forwarding the packet away from the source IP in each iteration to make sure there is no loops.

10. LSP stands for __________
a) Link Stable Packet
b) Link State Packet
c) Link State Protocol
d) Link State Path

Answer: b
Explanation: A Link State Packet is a packet created by a router that lists its neighboring nodes and routers in link state routing protocol. It is shared with other routers to find the shortest path from a source to the destination.

1. IPSec is designed to provide security at the _________
a) transport layer
b) network layer
c) application layer
d) session layer

Answer: b
Explanation: IPSec is a set of protocols used to provide authentication, data integrity and confidentiality between two machines in an IP network. In the TCP/IP model, it provides security at the IP layer i.e. the network layer.

2. In tunnel mode, IPSec protects the ______
a) Entire IP packet
b) IP header
c) IP payload
d) IP trailer

Answer: a
Explanation: In the tunnel mode, IPSec adds control bits into the packets to encrypt the entire packet between the IPSec endpoints. Using encryption, it provides secure communication between the two endpoints.

3. Network layer firewall works as a ________
a) frame filter
b) packet filter

c) signal filter
d) content filter

Answer: b
Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

4. Network layer firewall has two sub-categories called ____________
a) stateful firewall and stateless firewall
b) bit oriented firewall and byte oriented firewall
c) frame firewall and packet firewall
d) network firewall and data firewall

Answer: a
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

5. WPA2 is used for security in _______
a) ethernet
b) bluetooth
c) wi-fi
d) e-mail

Answer: c
Explanation: WPA2 or WiFi Protected Access 2 is a security protocol used to provide users and firms with strong data security and protection for their wireless networks (WiFi) to give them confidence that only authorized users can access their network.

6. An attempt to make a computer resource unavailable to its intended users is called ______
a) denial-of-service attack
b) virus attack
c) worms attack
d) botnet process

Answer: a
Explanation: In a Denial of Service attack, the attacker won't let the victims access the network by using a certain method that ensures that an essential network resource is unavailable to the victim. The methods that the attacker can use are vulnerability attack, bandwidth flooding and connection flooding.

7. Extensible authentication protocol is authentication framework frequently used in ______
a) wired personal area network
b) wireless networks
c) wired local area network
d) wired metropolitan area network

Answer: b
Explanation: The Extensible Authentication Protocol (EAP) is an authentication protocol used to connect a network node to the Internet. It designed through extending the methods used by the Point-to-Point Protocol for authentication.

8. Pretty good privacy (PGP) is used in ______
a) browser security
b) email security

c) FTP security
d) wifi security

Answer: b
Explanation: PGP is an encryption method used in e-mail security to encrypt and decrypt the content of an e-mail transmitted over the internet. It makes sure that the message cannot be stolen by other unauthorized users.

9. PGP encrypts data by using a block cipher called ______
a) international data encryption algorithm
b) private data encryption algorithm
c) internet data encryption algorithm
d) local data encryption algorithm

Answer: a
Explanation: The IDEA was designed in 1991 by Xuejia Lai and James Massey. Before IDEA, PGP used the cipher method BassOmatic.

10. When a DNS server accepts and uses incorrect information from a host that has no authority giving that information, then it is called _________
a) DNS lookup
b) DNS hijacking
c) DNS spoofing
d) DNS authorizing

Answer: c
Explanation: In DNS spoofing, also known as DNS cache poisoning, an attacker gets the valid credentials from a victim by spoofing the intended resource, and tricking the victim to give his/her valid authorization credentials.

1. Open Shortest Path First (OSPF) is also called as _____________
a) Link state protocol
b) Error-correction protocol
c) Routing information protocol
d) Border gateway protocol

Answer: a
Explanation: In OSPF, the link state of each path is checked, and then the shortest path is chosen among only the open state links. Each OSPF router monitors the cost of the link to each of its neighbors and then floods the link state information to other routers in the network.

2. The computation of the shortest path in OSPF is usually done by ____________
a) Bellman-ford algorithm
b) Routing information protocol
c) Dijkstra's algorithm
d) Distance vector routing

Answer: c
Explanation: Shortest path in OSPF is usually computed by Dijkstra's algorithm. It was proposed by Edsger W. Dijkstra in the year 1956. It is a greedy method algorithm and hence may not guarantee the shortest path every time, but is really fast.

3. Which of the following is false with respect to the features of OSPF?
a) Support for fixed-length subnetting by including the subnet mask in the routing message
b) More flexible link cost than can range from 1 to 65535
c) Use of designated router
d) Distribution of traffic over multiple paths that have equal cost to the destination

Answer: a
Explanation: OSPF provides support for variable-length sunbathing by including the subnet mask in the routing

message. For fixed length subnets, there is no requirement for including the subnet mask in the routing message as there is just one subnet mask for all the subnets.

4. In OSPF, which protocol is used to discover neighbour routers automatically?
a) Link state protocol
b) Error-correction protocol
c) Routing information protocol
d) Hello protocol

Answer: d
Explanation: Hello protocol is used to discover neighboring routers automatically. It makes sure that the communication between neighbors is bidirectional. It's similar to the real world moral construct of saying "Hello" to initialize the communication.

5. Which of the following is not a type of OSPF packet?
a) Hello
b) Link-state request
c) Link-state response
d) Link-state ACK

Answer: c
Explanation: The five types of OSPF packets are: Hello, Database description, Link-state request, Link-state update, and Link-state ACK. There is no Link-state response packet; the neighbor router sends a Link-state update packet as a response to the Link-state request packet if there is an update in the routing table.Answer: b
Explanation: OSPF first implements a hello protocol. Then it later on tries to establish synchronisation with database. Later on building of routing tables is done.

7. In OSPF header, which field is used to detect errors in the packet?
a) Type
b) Area ID
c) Authentication type
d) Checksum

Answer: d
Explanation: Checksum field is used to detect errors. It makes sure that the data portions that are being sent are all in integrity. It can detect duplicated bits. Once an error is detected, the sender has to re-transmit the data as it won't receive an acknowledgement.

8. In OSPF database descriptor packet, if there are more database descriptor packets in the flow, 'M' field is set to ____________
a) 1
b) 0
c) more
d) -1

Answer: a
Explanation: The "M" bit is the more bit, which indicates that there are more packets to be received in the descriptor packet flow whenever it is set to 1. There is also an "I" bit which indicates if the packet is first in the flow.

9. In OSPF database descriptor packet, which field is used to indicate that the router is master?
a) M
b) MS
c) I
d) Options

Answer: b
Explanation: The MS bit is used to indicate if the origin of the packet is a master or a slave. If it is set to 1, the source of the packet is a master, and if it is set to 0, the source of the packet is a slave.

10. In OSPF database descriptor packet, which field is used to detect a missing packet?
a) LSA header
b) MS
c) Database descriptor sequence number
d) Options

Answer: c
Explanation: Sequence number field is used to detect a missing packet. The packets are to be received in order of the sequence number, so if the receiver detects that there is a sequence number skipped or missing in the order, it stops processing the further received packets and informs the sender to retransmit the packets in sequence.

1. An OSPF router receives an LSA, the router checks its sequence number, and this number matches the sequence number of the LSA that the receiving router already has. What does the receiving router do with the LSA?
a) Ignores the LSA
b) Adds it to the database
c) Sends newer LSU update to source router
d) Floods the LSA to the other routers

Answer: a
Explanation: When the OSPF router receives an LSA, the router checks its sequence number. If this number matches the sequence number of the LSA that the receiving router already has, the router ignores the LSA.

2. An OSPF router receives an LSA. The router checks its sequence number and finds that this number is higher than the sequence number it already has. Which two tasks does the router perform with the LSA?
a) Ignores the LSA
b) Adds it to the database
c) Sends newer LSU update to source router
d) Floods the LSA to the other routers

Answer: b
Explanation: An OSPF router receives an LSA. If the router checks its sequence number and finds that the number is higher than the sequence number of the LSA that it already has, the router adds it to the database, and then floods the LSA to the other routers.

3. An OSPF router receives an LSA. The router checks its sequence number and finds that this number is lower than the sequence number it already has. What does the router do with the LSA?
a) ignores the LSA
b) adds it to the database
c) sends newer LSU update to source router
d) floods the LSA to the other routers

Answer: c
Explanation: An OSPF router receives an LSA. If the router checks its sequence number and finds that this number is lower than the sequence number that it already has, the router sends newer LSU update to source router. The router then adds it to the database and floods it to the other routers.

4. Each LSA has its own age timer. By default, how long does an LSA wait before requiring an update?
a) 30 seconds
b) 1 minute
c) 30 minutes
d) 1 hour

Answer: c
Explanation: Each LSA has its own age timer. By default, an LSA waits for 30 minutes before requiring an update. The router then has to send a LSR (Link State Request) to its neighbors to get an update.Answer: b
Explanation: In Distance vector routing protocols, there is a problem called count-to-infinity which occurs regularly. So, to make sure that it does not occur, the split horizon algorithm is used. There is no requirement for it in OSPF.

6. The outcome of Dijkstra's calculation is used to populate the __________
a) Topology table
b) Routing table
c) Neighbor table
d) Adjacency table

Answer: b
Explanation: The outcome of Djikstra's calculation is the main source of entries in the routing table as it is the algorithm that is used to find the shortest path in OSPF. The calculations are done after receiving every new LSU.

7. What is the IP protocol number for OSPF packets?
a) 89
b) 86
c) 20
d) 76

Answer: a
Explanation: 89 is the IP protocol number for OSPF packets. 86 is the protocol number for DGP, 76 is the protocol number for Backroom-SATNET-Monitoring and 20 is the protocol number for Host Monitoring Protocol.

8. Which packet is NOT an OSPF packet type?
a) LSU
b) LSR
c) DBD
d) Query

Answer: d
Explanation: LSU is the Link State Update packet, LSR is the Link State Request packet and DBD is the Database Descriptor packet in OSPF. Query packet is NOT an OSPF packet type.

9. Which multicast address does the OSPF Hello protocol use?
a) 224.0.0.5
b) 224.0.0.6
c) 224.0.0.7
d) 224.0.0.8

Answer: a
Explanation: Hello protocol is used to discover neighboring routers automatically. It makes sure that the communication between neighbors is bidirectional. The multicast address that the OSPF Hello protocol uses is 224.0.0.5.Answer: a
Explanation: The Hello protocol sends periodic updates to ensure that a neighbor relationship is maintained between adjacent routers. It's similar to the real world moral construct of saying "Hello" to initialize the communication.

11. DBD packets are involved during which two states?
a) Exstart and exchange
b) Loading and Two-way
c) Init and Full
d) Down and Loading

Answer: a
Explanation: DBD stands for Database Descriptor. DBD packets are involved during the two states Exstart and Exchange. In exstart, the master and the slaves are decided and in the exchange state, the DBD is exchanged among the neighbors.

12. At which interval does OSPF refresh LSAs?
a) 10 seconds
b) 30 seconds
c) 30 minutes
d) 1 hour

Answer: d
Explanation: Each LSA has its own age timer. By default, an LSA waits for 30 minutes before requiring an update. So to make sure that each router first has an up-to-date LSA, OSPF refreshes LSAs after every 1 hour.

13. Which field is NOT a field within an OSPF packet header?
a) Packet length
b) Router ID
c) Authentication type
d) Maxage time

Answer: d
Explanation: The packet length field gives the length of the packet in bits. The Authentication type field gives the type of authentication used. The router ID field gives the ID of the source router of the packet. In an OSPF packet header, there is no field called Maxage time.

14. Which two commands are required for basic OSPF configuration?
a) "[Network mask] area [area-id]" and "Router ospf [process-id]"
b) "[Wildcard-mask] area [area-id]" and "[Network mask] area [area-id]"
c) Only "Router ospf [process-id]"
d) "[Wildcard-mask] area [area-id]" and "Router ospf [process-id]"

Answer: d
Explanation: The "Router ospf [process-id]" command enables OSPF routing protocol in the router and the "[Wildcard-mask] area [area-id]" command is used to select the interfaces that we want to include in the OSPF process. That is enough for the basic configuration of OSPF in a router.

15. Which OSPF show command describes a list of OSPF adjacencies?
a) Show ip ospf interface
b) Show ip ospf
c) Show ip route
d) Show ip ospf neighbor

Answer: d
Explanation: The "Show ip ospf neighbor" command is the OSPF show command that can describe a list of OSPF adjacencies i.e. the list of adjacent nodes or neighbors. The router will only communicate with its neighbors directly.

1. Datagram switching is done at which layer of OSI model?
a) Network layer
b) Physical layer
c) Application layer
d) Transport layer

Answer: a
Explanation: Datagram switching is normally done at network layer. In datagram switching, the datagram stream need not be in order as each datagram can take different routes to the destination.

2. Packets in datagram switching are referred to as ________
a) Switches
b) Segments
c) Datagrams
d) Data-packets

Answer: c
Explanation: As the name suggests, in datagram switching packets are called as datagram. Each datagram/packet is treated as an individual entity and routed independently through the network.

3. Datagram networks mainly refers to _________
a) Connection oriented networks

b) Connection less networks
c) Telephone networks
d) Internetwork

Answer: b
Explanation: The switch does not keep the information about the connection state, hence it is connection less. There is no need for establishing a handshake to begin the transmission in such networks.

4. Datagrams are routed to their destinations with the help of ________
a) Switch table
b) Segments table
c) Datagram table
d) Routing table

Answer: d
Explanation: Routing table is used to route the packets to their destinations. The packet/datagram header contains the destination header for the whole journey to source to the destination through the routers.

5. The main contents of the routing table in datagram networks are ___________
a) Source and Destination address
b) Destination address and Output port
c) Source address and Output port
d) Input port and Output port

Answer: b
Explanation: Routing table contains destination address and output port to route the packets to their destinations. The port address specifies the particular application that the packet has to be forwarded to after it has reached the destination.

6. Which of the following remains same in the header of the packet in a datagram network during the entire journey of the packet?
a) Destination address
b) Source address
c) Checksum
d) Padding

Answer: a
Explanation: Destination address remains same in the header during the entire journey of the packet. There is no pre-decided route for the packets so each datagram/packet is treated as an individual entity and routed independently through the network.

7. Which of the following is true with respect to the delay in datagram networks?
a) Delay is greater than in a virtual circuit network
b) Each packet may experience a wait at a switch
c) Delay is not uniform for the packets of a message
d) All of the mentioned

Answer: d
Explanation: The delay of each packet in a datagram network is different as each packet might take a different route to the destination. The delay includes the propagation delay and the processing delay that is induced at each stop/switch that the packet encounters in its journey.

8. During datagram switching, the packets are placed in __________ to wait until the given transmission line becomes available.
a) Stack
b) Queue
c) Hash
d) Routing table

Answer: b
Explanation: When there are too many packets to be transmitted and the transmission line gets blocked while transmitting some packets, the remaining packets are stored in queue during delay and are served as first in first out. The delay is called as queuing delay.

9. The probability of the error in a transmitted block _________ with the length of the block
a) Remains same
b) Decreases
c) Increases
d) Is not proportional

Answer: c
Explanation: Probability of the error in a transmitted block increases with the length of the block. Hence, the blocks should be as short as possible for ideal transmission with low possibility of an error.

10. Which of the following is false with respect to the datagram networks?
a) Number of flows of packets are not limited
b) Packets may not be in order at the destination
c) Path is not reserved
d) Delay is the same for all packets in a flow

Answer: d
Explanation: The delay of each packet in a datagram network is different as each packet might take a different route to the destination. This happens because there is no pre-decided route for the packets.

1. Network layer firewall works as a __________
a) Frame filter
b) Packet filter
c) Content filter
d) Virus filter

Answer: b
Explanation: As you know, firewalls are available as hardware appliances, as software-only, or a combination of the two. In every case, the purpose of a firewall is to isolate your trusted internal network (or your personal PC) from the dangers of unknown resources on the Internet and other network connections that may be harmful. The firewall prevents unauthorized access to your internal, trusted network from outside threats.

2. Network layer firewall has two sub-categories as _________
a) State full firewall and stateless firewall
b) Bit oriented firewall and byte oriented firewall
c) Frame firewall and packet firewall
d) Network layer firewall and session layer firewall

Answer: a
Explanation: Most network layer firewalls can operate as stateful or stateless firewalls, creating two subcategories of the standard network layer firewall. Stateful firewalls have the advantage of being able to track packets over a period of time for greater analysis and accuracy — but they require more memory and operate more slowly. Stateless firewalls do not analyze past traffic and can be useful for systems where speed is more important than security, or for systems that have very specific and limited needs. For example, a computer that only needs to connect to a particular backup server does not need the extra security of a stateful firewall.

3. A firewall is installed at the point where the secure internal network and untrusted external network meet which is also known as __________
a) Chock point
b) Meeting point
c) Firewall point
d) Secure point

Answer: a

Explanation: A firewall can be a PC, a router, a midrange, a mainframe, a UNIX workstation, or a combination of these that determines which information or services can be accessed from the outside and who is permitted to use the information and services from outside. Generally, a firewall is installed at the point where the secure internal network and untrusted external network meet, which is also known as a chokepoint.

4. Which of the following is / are the types of firewall?
a) Packet Filtering Firewall
b) Dual Homed Gateway Firewall
c) Screen Host Firewall
d) Dual Host Firewall

Answer: a

Explanation: A firewall can be a PC, a midrange, a mainframe, a UNIX workstation, a router, or combination of these. Depending on the requirements, a firewall can consist of one or more of the following functional components: Packet-filtering router

5. A proxy firewall filters at _________
a) Physical layer
b) Data link layer
c) Network layer
d) Application layer

Answer: d

Explanation: The application firewall is typically built to control all network traffic on any layer up to the application layer. It is able to control applications or services specifically, unlike a stateful network firewall, which is – without additional software – unable to control network traffic regarding a specific application. There are two primary categories of application firewalls, network-based application firewalls and host-based application firewalls.

6. A packet filter firewall filters at __________
a) Physical layer
b) Data link layer
c) Network layer or Transport layer
d) Application layer

Answer: c

Explanation: In computing, a firewall is a network security system that monitors and controls the incoming and outgoing network traffic based on predetermined security rules.[1] A firewall typically establishes a barrier between a trusted, secure internal network and another outside network, such as the Internet, that is assumed not to be secure or trusted.[2] Firewalls are often categorized as either network firewalls or host-based firewalls.

7. What is one advantage of setting up a DMZ with two firewalls?
a) You can control where traffic goes in three networks
b) You can do stateful packet filtering
c) You can do load balancing
d) Improved network performance

Answer: c

Explanation: DMZ stands for De-Militarized Zone. In a topology with a single firewall serving both internal and external users (LAN and WAN), it acts as a shared resource for these two zones. So load balancing can be done by adding another firewall.

8. What tells a firewall how to reassemble a data stream that has been divided into packets?
a) The source routing feature
b) The number in the header's identification field
c) The destination IP address
d) The header checksum field in the packet header

Answer: a
Explanation: The source routing feature provides a path address for the packet to help the firewall to reassemble the data stream that was divided into packets. After reassembling, the firewall can then filter the stream.

9. A stateful firewall maintains a ___________ which is a list of active connections.
a) Routing table
b) Bridging table
c) State table
d) Connection table

Answer: a
Explanation: The routing table basically gives the state of each connection i.e. whether the connection is active or not. A routing table ensures the best performance for the stateful firewall.

10. A firewall needs to be __________ so that it can grow proportionally with the network that it protects.
a) Robust
b) Expansive
c) Fast
d) Scalable

Answer: b
Explanation: The firewall has to be expansive because a network is expected to grow with time and if the firewall is unable to grow with it, the firewall won't be able to handle the growing network traffic flow and will hence fail.

1. Complex networks today are made up of hundreds and sometimes thousands of _________
a) Documents
b) Components
c) Servers
d) Entities

Answer: b
Explanation: Complex networks today are made up of hundreds and sometimes thousands of components. For effective functioning of these thousands of components, good network management is essential.

2. Performance management is closely related to _________
a) Proactive Fault Management
b) Fault management
c) Reactive Fault Management
d) Preventive Fault Management

Answer: b
Explanation: Fault management is really closely related to performance management. It is important to ensure that the network handles faults as effectively as it handles it's normal functioning to achieve better performance management.

3. Configuration management can be divided into two subsystems: reconfiguration and __________
a) Documentation
b) Information
c) Servers
d) Entity

Answer: a
Explanation: The documentation subsystem of configuration management handles the log making and reporting functions of the configuration management. It also reports the errors in the network caused by the configuration's failure.

4. In Network Management System, the term that is responsible for controlling access to network based on predefined policy is called ___________
a) Fault Management

b) Secured Management
c) Active Management
d) Security Management

Answer: d
Explanation: In Network Management System, the term that is responsible for controlling access to the network based on predefined policy is called security management. The security management ensures authentication, confidentiality and integrity in the network.

5. Control of users' access to network resources through charges is the main responsibility of ______________
a) Reactive Fault Management
b) Reconfigured Fault Management
c) Accounting Management
d) Security Management

Answer: c
Explanation: Control of users' access to network resources through charges is the main responsibility of accounting management. The accounting management creates a log of the users activity on the network too and goes hand-in-hand with the configurations management.

6. The physical connection between an end point and a switch or between two switches is __________
a) Transmission path
b) Virtual path
c) Virtual circuit
d) Transmission circuit

Answer: a
Explanation: The physical connection between an end point and a switch or between two switches is transmission path. The transmission path is the physical roadway that the packet needs to propagate in order to travel through the network.

7. Which of the following networks supports pipelining effect?
a) Circuit-switched networks
b) Message-switched networks
c) Packet-switched networks
d) Stream-switched networks

Answer: c
Explanation: Packet switched network is most preferred for pipelining process. Pipelining exponentially reduces the time taken to transmit a large number of packets in the network.

8. In Network Management System, maps track each piece of hardware and its connection to the _________
a) IP Server
b) Domain
c) Network
d) Data

Answer: c
Explanation: Network is the main entity connecting different components in a place. A network map is made to track each component and its connection to the network to ensure better network management.

9. MIB is a collection of groups of objects that can be managed by __________
a) SMTP
b) UDP
c) SNMP
d) TCP/IP

Answer: c
Explanation: MIB stands for Management Information Base. Simple network management controls the group of objects

in management information base. It is usually used with SNMP (Simple Network Management Protocol).

10. A network management system can be divided into ___________
a) three categories
b) five broad categories
c) seven broad categories
d) ten broad categories

Answer: b
Explanation: The five broad categories of network management are
• Fault Management
• Configuration Management
• Accounting (Administration)
• Performance Management
• Security Management.

1. Ping can _________
a) Measure round-trip time
b) Report packet loss
c) Report latency
d) All of the mentioned

Answer: d
Explanation: PING (Packet Internet Groper) command is the best way to test connectivity between two nodes, whether it is Local Area Network (LAN) or Wide Area Network (WAN). Ping uses ICMP (Internet Control Message Protocol) to communicate to other devices.

2. Ping sweep is a part of _________
a) Traceroute
b) Nmap
c) Route
d) Ipconfig

Answer: b
Explanation: A ping sweep is a method that can establish a range of IP addresses which map to live hosts and are mostly used by network scanning tools like nmap. A ping sweep is basically a collective ping command execution on a range of IP addresses.

3. ICMP is used in _________
a) Ping
b) Traceroute
c) Ifconfig
d) Both Ping & Traceroute

Answer: d
Explanation: ICMP stands for Internet Control Message Protocol. ICMP operates over the IP packet to provide error reporting functionality, so in case the node is not active or there is no route, ICMP will be used to report the specific errors for Ping and Traceroute.

4. __________ command is used to manipulate TCP/IP routing table.
a) route
b) Ipconfig
c) Ifconfig
d) Traceroute

Answer: a
Explanation: The route command is used to view and manipulate the TCP/IP routing table in Windows OS. The manipulations done in the routing table with the help of this command will count as static routes.

5. If you want to find the number of routers between a source and destination, the utility to be used is ___________
a) route
b) Ipconfig
c) Ifconfig
d) Traceroute

Answer: d
Explanation: Traceroute command is available on Linux OS to find the path i.e. the number of the routers that the packet has to go through to reach the destination. In Windows, Tracert command is used to perform the function.

6. Which of the following is not related to ipconfig in Microsoft Windows?
a) Display all current TCP/IP network configuration values
b) Modify DHCP settings
c) Modify DNS settings
d) Trace the routers in the path to destination

Answer: d
Explanation: The Tracert command is available on Microsoft Windows to find the path i.e. the number of the routers that the packet has to go through to reach its destination.

7. __________ allows checking if a domain is available for registration.
a) Domain Check
b) Domain Dossier
c) Domain Lookup
d) Domain registers

Answer: a
Explanation: There are billions of domains available for registration on the World Wide Web, and many of them are already registered. So when one wants to register a domain, they need to check whether the domain is available through a domain check.

8. Choose the wrong statement from the following.
a) Nslookup is used to query a DNS server for DNS data
b) Ping is used to check connectivity
c) Pathping combines the functionality of ping with that of route
d) Ifconfig can configure TCP/IP network interface parameters

Answer: c
Explanation: Pathping combines the functionality of ping with that of traceroute (tracert). The Ping command is used to test connectivity between two nodes and the Tracert/Traceroute command is used to find the path i.e. the number of the routers that the packet has to go through to reach its destination.

1. Ethernet frame consists of ____________
a) MAC address
b) IP address
c) Default mask
d) Network address

Answer: a
Explanation: The Ethernet frame has a header that contains the source and destination MAC address. Each MAC address is of 48 bits.

2. What is start frame delimeter (SFD) in ethernet frame?
a) 10101010
b) 10101011
c) 00000000
d) 11111111

Answer: b
Explanation: The start frame delimiter is a 1 byte field in the Ethernet frame that indicates that the preceding bits are the start of the frame. It is always set to 10101011.

3. MAC address is of ___________
a) 24 bits
b) 36 bits
c) 42 bits
d) 48 bits

Answer: d
Explanation: MAC address is like a local address for the NIC that is used to make a local Ethernet (or wifi) network function. It is of 48 bits.

4. What is autonegotiation?
a) a procedure by which two connected devices choose common transmission parameters
b) a security algorithm
c) a routing algorithm
d) encryption algorithm

Answer: a
Explanation: autonegotiation is a procedure by which two connected devices choose common transmission parameters. It is a signaling mechanism used in Ethernet over Twisted pair cables.

5. Ethernet in metropolitan area network (MAN) can be used as ___________
a) pure ethernet
b) ethernet over SDH
c) ethernet over MPLS
d) all of the mentioned

Answer: d
Explanation: A metropolitan area network (MAN) that is based on Ethernet standards is called an Ethernet MAN. It is commonly used to connect nodes to the Internet. Businesses also use Ethernet MANs to connect their own offices to each other.

6. A point-to-point protocol over ethernet is a network protocol for __________
a) encapsulating PPP frames inside ethernet frames
b) encapsulating ehternet framse inside PPP frames
c) for security of ethernet frames
d) for security of PPP frames

Answer: a
Explanation: PPoE or Point-to-Point protocol over Ethernet was first introduced in 1999. It is popularly used by modern day Internet Service Providers for Dial-up connectivity.

7. High speed ethernet works on _________
a) coaxial cable
b) twisted pair cable
c) optical fiber
d) unshielded twisted pair cable

Answer: c
Explanation: Fast Ethernet is mostly used in networks along with Category 5 (Cat-5) copper twisted-pair cable, but it also works with fiber-optic cable. Based on the cable being used, There can be three types of Fast Ethernet.

8. The maximum size of payload field in ethernet frame is __________
a) 1000 bytes
b) 1200 bytes

c) 1300 bytes
d) 1500 bytes

Answer: d
Explanation: The minimum size of the payload field is 40 bytes and the maximum size is 1500 bytes. If the payload size exceeds 1500 bytes, the frame is called a jumbo frame.

9. What is interframe gap?
a) idle time between frames
b) idle time between frame bits
c) idle time between packets
d) idle time between networks

Answer: a
Explanation: The inter-frame gap is the idle time for the receiver between the incoming frame flow. The inter-frame gap must be as low as possible for idle connections.

10. An ethernet frame that is less than the IEEE 802.3 minimum length of 64 octets is called _______
a) short frame
b) runt frame
c) mini frame
d) man frame

Answer: b
Explanation: An ethernet frame that is less than the IEEE 802.3 minimum length of 64 octets is called a runt frame. Such frames are a result of collisions or software malfunctions.

1. What is the access point (AP) in a wireless LAN?
a) device that allows wireless devices to connect to a wired network
b) wireless devices itself
c) both device that allows wireless devices to connect to a wired network and wireless devices itself
d) all the nodes in the network

Answer: a
Explanation: Access point in a wireless network is any device that will allow the wireless devices to a wired network. A router is the best example of an Access Point.

2. In wireless ad-hoc network _________
a) access point is not required
b) access point is must
c) nodes are not required
d) all nodes are access points

Answer: a
Explanation: An ad-hoc wireless network is a decentralized kind of a wireless network. An access point is usually a central device and it would go against the rules of the ad-hoc network to use one. Hence it is not required.

3. Which multiple access technique is used by IEEE 802.11 standard for wireless LAN?
a) CDMA
b) CSMA/CA
c) ALOHA
d) CSMA/CD

Answer: b
Explanation: CSMA/CA stands for Carrier-sense multiple access/collision avoidance. It is a multiple access protocol used by IEEE 802.11 standard for wireless LAN. It’s based on the principle of collision avoidance by using different algorithms to avoid collisions between channels.

4. In wireless distribution system __________
a) multiple access point are inter-connected with each other
b) there is no access point
c) only one access point exists
d) access points are not required

Answer: a
Explanation: A Wireless Distribution System allows the connection of multiple access points together. It is used to expand a wireless network to a larger network.

5. A wireless network interface controller can work in _______
a) infrastructure mode
b) ad-hoc mode
c) both infrastructure mode and ad-hoc mode
d) WDS mode

Answer: c
Explanation: A wireless network interface controller works on the physical layer and the data link layer of the OSI model. Infrastructure mode WNIC needs access point but in ad-hoc mode access point is not required.

6. In wireless network an extended service set is a set of ________
a) connected basic service sets
b) all stations
c) all access points
d) connected access points

Answer: a
Explanation: The extended service set is a part of the IEEE 802.11 WLAN architecture and is used to expand the range of the basic service set by allowing connection of multiple basic service sets.

7. Mostly ________ is used in wireless LAN.
a) time division multiplexing
b) orthogonal frequency division multiplexing
c) space division multiplexing
d) channel division multiplexing

Answer: b
Explanation: In orthogonal frequency division multiplexing, digital data is encoded on multiple carrier frequencies. It is also used in digital television and audio broadcasting in addition to Wireless LANs.

8. Which one of the following event is not possible in wireless LAN?
a) collision detection
b) acknowledgement of data frames
c) multi-mode data transmission
d) connection to wired networks

Answer: a
Explanation: Collision detection is not possible in wireless LAN with no extensions. Collision detection techniques for multiple access like CSMA/CD are used to detect collisions in Wireless LANs.

9. What is Wired Equivalent Privacy (WEP)?
a) security algorithm for ethernet
b) security algorithm for wireless networks
c) security algorithm for usb communication
d) security algorithm for emails

Answer: b
Explanation: WEP is a security algorithm for wireless network which intended to provide data confidentiality

comparable to that of traditional wired networks. It was introduced in 1997.

10. What is WPA?
a) wi-fi protected access
b) wired protected access
c) wired process access
d) wi-fi process access

Answer: a
Explanation: WPA or WiFi Protected Access is a security protocol used to provide users and firms with strong data security and protection for their wireless networks (WiFi) to give them confidence that only authorized users can access their network.

1. What is internet?
a) a single network
b) a vast collection of different networks
c) interconnection of local area networks
d) interconnection of wide area networks

Answer: b
Explanation: Internet is nothing but an interconnected computer network providing a variety of communication facilities, consisting of a huge amount of small networks using standardized communication protocols.

2. To join the internet, the computer has to be connected to a _________
a) internet architecture board
b) internet society
c) internet service provider
d) different computer

Answer: c
Explanation: The ISPs (Internet Service Providers) are the main agents through which every computer is connected to the internet. They are licensed to allot public IP addresses to its customers in order to connect them to the internet.

3. Internet access by transmitting digital data over the wires of a local telephone network is provided by _______
a) leased line
b) digital subscriber line
c) digital signal line
d) digital leased line

Answer: b
Explanation: DSL (Digital Subscriber Line) is the technology designed to use the existing telephone lines to transport high-bandwidth data to service subscribers. DSL was used to allow the early users access to the internet and it provides dedicated, point-to-point, public network access.

4. ISP exchanges internet traffic between their networks by __________
a) internet exchange point
b) subscriber end point
c) isp end point
d) internet end point

Answer: a
Explanation: ISPs exchange internet traffic between their networks by using Internet Exchange Points. ISPs and CDNs are connected to each other at these physical locations are they help them provide better service to their customers.

5. Which of the following protocols is used in the internet?
a) HTTP
b) DHCP
c) DNS

d) DNS, HTTP and DNS

Answer: d
Explanation: HTTP is used to browse all the websites on the World Wide Web, DHCP is used to allot IPs automatically to the users on the internet, and DNS is used to connect the users to the host servers on the internet based on the Domain Name.

6. The size of an IP address in IPv6 is _________
a) 32 bits
b) 64 bits
c) 128 bits
d) 265 bits

Answer: c
Explanation: An IPv6 address is 128 bits long. Therefore, 2128 i.e. 340 undecillion addresses are possible in IPv6. IPv4 has only 4 billion possible addresses and IPv6 would be a brilliant alternative in case IPv4 runs out of possible new addresses.

7. Internet works on _______
a) packet switching
b) circuit switching
c) both packet switching and circuit switching
d) data switching

Answer: a
Explanation: Packet switching is the method based on which the internet works. Packet switching features delivery of packets of data between devices over a shared network.

8. Which one of the following is not an application layer protocol used in internet?
a) remote procedure call
b) internet relay chat
c) resource reservation protocol
d) local procedure call

Answer: c
Explanation: Resource reservation protocol is a transport layer protocol used on the internet. It operates over IPv4 and IPv6 and is designed to reserve resources required by the network layer protocols.

9. Which protocol assigns IP address to the client connected in the internet?
a) DHCP
b) IP
c) RPC
d) RSVP

Answer: a
Explanation: DHCP stands for Domain Host Control Protocol. It is responsible to remotely assign IP address to the clients connected to the internet. The server that performs this fuction is called the DHCP server.

10. Which one of the following is not used in media access control?
a) ethernet
b) digital subscriber line
c) fiber distributed data interface
d) packet switching

Answer: d
Explanation: Packet switching is not really related to media access control as it just features delivery of packets of data between devices over a shared network. Internet is actually based on packet switching.

1. An interconnected collection of piconet is called ___________
a) scatternet
b) micronet
c) mininet
d) multinet

Answer: a
Explanation: Piconet is the basic unit of a bluetooth system having a master node and upto seven active slave nodes. A collection of piconets is called scatternet and a slave node of a piconet may act as a master in a piconet that is part of the scatternet.

2. In a piconet, there can be up to ________ parked nodes in the network.
a) 63
b) 127
c) 255
d) 511

Answer: c
Explanation: A slave node in a piconet can be instructed by the master node to go into parked mode. Then the slave node enters the parked mode in which the node is not disconnected from the network but is inactive unless the master wakes it up.

3. Bluetooth is the wireless technology for __________
a) local area network
b) personal area network
c) metropolitan area network
d) wide area network

Answer: b
Explanation: Bluetooth is a wireless technology used to create a wireless personal area network for data transfer up to a distance of 10 meters. It operates on 2.45 GHz frequency band for transmission.

4. Bluetooth uses __________
a) frequency hopping spread spectrum
b) orthogonal frequency division multiplexing
c) time division multiplexing
d) channel division multiplexing

Answer: a
Explanation: Frequency hopping spread spectrum is a method of transmitting radio signals by rapidly changing the carrier frequency and is controlled by the codes known to the sender and receiver only.

5. Unauthorised access of information from a wireless device through a bluetooth connection is called _________
a) bluemaking
b) bluesnarfing
c) bluestring
d) bluescoping

Answer: b
Explanation: Unauthorised access of information from a wireless device through a bluetooth connection is called Bluesnarfing. It is done through exploiting the vulnerabilities of the Bluetooth device to steal the transmitted information.

6. What is A2DP (advanced audio distribution profile)?
a) a bluetooth profile for streaming audio
b) a bluetooth profile for streaming video
c) a bluetooth profile for security
d) a bluetooth profile for file management

Answer: a
Explanation: A2DP stands for Advanced Audio Distribution Profile is a transfer standard use to transmit high definition audio through Bluetooth. It is mainly used in Bluetooth speakers and wireless headphones.

7. In a piconet, one master device ________
a) can not be slave
b) can be slave in another piconet
c) can be slave in the same piconet
d) can be master in another piconet

Answer: b
Explanation: In a scatternet, a slave node of one piconet may act as a master in a piconet that is part of the scatternet. The scatternet uses this property to connect many piconets together to create a larger network.

8. Bluetooth transceiver devices operate in ______ band.
a) 2.4 GHz ISM
b) 2.5 GHz ISM
c) 2.6 GHz ISM
d) 2.7 GHz ISM

Answer: a
Explanation: Bluetooth operates on 2.45 GHz frequency ISM band for transmission. It is used to create a wireless personal area network for data transfer up to a distance of 10 meters.

9. Bluetooth supports _______
a) point-to-point connections
b) point-to-multipoint connection
c) both point-to-point connections and point-to-multipoint connection
d) multipoint to point connection

Answer: c
Explanation: In Bluetooth, each slave node communicates with the master of the piconet independently i.e. each master-slave connection is independent. The slave is not allowed to communicate with other slaves directly.

10. A scatternet can have maximum __________
a) 10 piconets
b) 20 piconets
c) 30 piconets
d) 40 piconets

Answer: a
Explanation: A scatternet can have maximum of 10 piconets and minimum of 2 piconets. To connect these piconets, a slave node of one piconet may act as a master in a piconet that is part of the scatternet.

1. WiMAX stands for ___________
a) wireless maximum communication
b) worldwide interoperability for microwave access
c) worldwide international standard for microwave access
d) wireless internet maximum communication

Answer: b
Explanation: WiMAX or worldwide interoperability for microwave access is a set of wireless communication standards. It provides support for multiple physical layer (PHY) and Media Access Control (MAC) options. It is based on IEEE 802.16 standards.

2. WiMAX provides ________
a) simplex communication
b) half duplex communication

c) full duplex communication
d) no communication

Answer: c
Explanation: WiMax was developed to provide wireless broadband access to buildings. It can also be used to connect WLAN hotspots to the Internet. It is based on IEEE 802.16 standards.

3. WiMAX uses the _________
a) orthogonal frequency division multiplexing
b) time division multiplexing
c) space division multiplexing
d) channel division multiplexing

Answer: a
Explanation: WiMAX physical layer uses orthogonal frequency division multiplexing as it provides simplified reception in multipath and allows WiMAX to operate in NLOS conditions.

4. Which of the following modulation schemes is supported by WiMAX?
a) binary phase shift keying modulation
b) quadrature phase shift keying modulation
c) quadrature amplitude modulation
d) all of the mentioned

Answer: d
Explanation: WiMAX supports a variety of modulation schemes such as binary phase shift keying modulation, quadrature phase shift keying modulation, and quadrature amplitude modulation and allows for the scheme to change on a burst-by-burst basis per link, depending on channel conditions.

5. WiMAX MAC layer provides an interface between ___________
a) higher transport layers and physical layer
b) application layer and network layer
c) data link layer and network layer
d) session layer and application layer

Answer: a
Explanation: WiMAX provides support for multiple physical layer (PHY) on the physical layer and Media Access Control (MAC) options for higher layers to provide wireless broadband access to buildings.

6. For encryption, WiMAX supports _______
a) advanced encryption standard
b) triple data encryption standard
c) advanced encryption standard and triple data encryption standard
d) double data encryption standard

Answer: c
Explanation: Both advanced encryption standard and triple data encryption standard are block cipher techniques and are popularly used in WiMAX and other applications for secure encryption.

7. WiMAX provides _______
a) VoIP services
b) IPTV services
c) Both VoIP and IPTV services
d) no IPTV services

Answer: c
Explanation: IPTV can be transmitted over WiMAX, and relies on packet-switching to offer reliable delivery. VoIP can be operated over a WiMax network with no special hardware or software.

8. Devices that provide the connectivity to a WiMAX network are known as _________
a) subscriber stations
b) base stations
c) gateway
d) switch stations

Answer: a
Explanation: Subscriber stations in WiMAX are transceivers (transmitter and receivers). They are used to convert radio signals into digital signals that can be routed to and from communication devices. There is a variety of types of WiMAX subscriber stations like portable PCMCIA cards and fixed stations that provide service to multiple users.

9. WiMAX is mostly used for __________
a) local area network
b) metropolitan area network
c) personal area network
d) wide area network

Answer: b
Explanation: WiMAX provides Wi-Fi connectivity within the home or business for computers and smartphones. WiMAX network operators typically provide a WiMAX Subscriber Unit to do so. The subscriber unit is used to connect to the metropolitan WiMAX network.

10. Which of the following frequencies is not used in WiMAX for communication?
a) 2.3 GHz
b) 2.4 GHz
c) 2.5 GHz
d) 3.5 GHz

Answer: b
Explanation: The 2.4GHz ISM frequency band is used for personal area network technologies such as Bluetooth and hence is not suitable for WiMAX which is mostly used for Metropolitan Area Networks.

1. SONET stands for ___________
a) synchronous optical network
b) synchronous operational network
c) stream optical network
d) shell operational network

Answer: a
Explanation: SONET stands for synchronous optical network. Frame relay uses SONET to physically transmit data frames over a Frame Relay network as SONET is cheaper and provides better network reliability than other carriers.

2. In SONET, STS-1 level of electrical signalling has the data rate of _________
a) 51.84 Mbps
b) 155.52 Mbps
c) 2488.320 Mbps
d) 622.080 Mbps

Answer: a
Explanation: STS-1 level provides the data rate of 51.84 Mbps, STS-3 provides a data rate of 155.52 Mbps, STS-12 provides a data rate of 622.080 Mbps and STS-48 provides a data rate of 2488.320 Mbps.

3. The path layer of SONET is responsible for the movement of a signal _________
a) from its optical source to its optical destination
b) across a physical line
c) across a physical section
d) back to its optical source

Answer: b
Explanation: The path layer in SONET is responsible for finding the path of the signal across the physical line to reach the optical destination. It is ideally expected to find the shortest and the most reliable path to the destination.

4. The photonic layer of the SONET is similar to the __________ of OSI model.
a) network layer
b) data link layer
c) physical layer
d) transport layer

Answer: c
Explanation: The photonic layer in SONET is like the physical layer of the OSI model. It is the lowest layer among the four layers of SONET namely the photonic, the section, the line, and the path layers.

5. In SONET, each synchronous transfer signal STS-n is composed of __________
a) 2000 frames
b) 4000 frames
c) 8000 frames
d) 16000 frames

Answer: c
Explanation: SONET defines the electrical signal as STS-N (Synchronous Transport Signal Level-N) and the optical signal as OC-N (Optical Carrier Level-N). The building block of SONET is the STS-1/OC-1 signal, which is based on an 8-kHz frame rate and operates at 51.84 Mbps.

6. Which one of the following is not true about SONET?
a) frames of lower rate can be synchronously time-division multiplexed into a higher-rate frame
b) multiplexing is synchronous TDM
c) all clocks in the network are locked to a master clock
d) STS-1 provides the data rate of 622.080Mbps

Answer: d
Explanation: In SONET, STS-N stands for Synchronous Transport Signal Level-N. STS-1 level provides the data rate of 51.84 Mbps, and STS-12 provides a data rate of 622.080 Mbps.

7. A linear SONET network can be ________
a) point-to-point
b) multi-point
c) both point-to-point and multi-point
d) single point

Answer: c
Explanation: Synchronous Optical Network (SONET) is basically an optical fiber point-to-point or ring network backbone that provides a way to accommodate additional capacity as the needs of the organization increase to multipoint networks.

8. Automatic protection switching in linear network is defined at the _______
a) line layer
b) section layer
c) photonic layer
d) path layer

Answer: a
Explanation: The Line layer in SONET operates like the data link layer in the OSI model and it is responsible for the movement of signal across a physical line. The Synchronous Transport Signal Mux/Demux and Add/Drop Mux provide the Line layer functions.

9. A unidirectional path switching ring is a network with __________

a) one ring
b) two rings
c) three rings
d) four rings

Answer: b
Explanation: One ring is used as the working ring and other as the protection ring in which each node is connected to its respective adjacent nodes by two fibers, one to transmit, and one to receive.

10. What is SDH?
a) sdh is similar standard to SONET developed by ITU-T
b) synchronous digital hierarchy
c) sdh stands for synchronous digital hierarchy and is a similar standard to SONET developed by ITU-T
d) none of the mentioned

Answer: c
Explanation: SDH is a standard that allows low bit rates to be combined into high-rate data streams and as it is synchronous, each individual bit stream can be embedded into and extracted from high-rate data streams easily.

1. Real-time transport protocol (RTP) is mostly used in _________
a) streaming media
b) video teleconference
c) television services
d) all of the mentioned

Answer: d
Explanation: RTP stands for Real-time transport protocol and is for delivering audio and video over IP networks. Its applications include streaming media, video teleconference, and television services.

2. RTP is used to ________
a) carry the media stream
b) monitor transmission statistics of streams
c) monitor quality of service of streams
d) secure the stream

Answer: a
Explanation: RTP is used to carry the media stream for delivering audio and video over IP networks. Its applications include streaming media, video teleconference, and television services.

3. RTP provides the facility of jitter ____________
a) media stream
b) expansion
c) media modification
d) security

Answer: a
Explanation: RTP provides the facility of jitter media stream through a jitter buffer which works by reconstructing the sequence of packets on the receiving side. Then an even audio / video stream is generated.

4. Which protocol provides the synchronization between media streams?
a) RTP
b) RTCP
c) RPC
d) RTCT

Answer: b
Explanation: RTCP stands for Real-time Transport Control Protocol and it works with RTP to send control packets to the users of the networks while RTP handles the actual data delivery.

5. An RTP session is established for ___________
a) each media stream
b) all media streams
c) some predefined number of media streams
d) no media stream

Answer: a
Explanation: An RTP session is required to be established for each media stream for delivering audio and video over the IP network. Each session has independent data transmission.

6. RTP can use __________
a) unprevileleged UDP ports
b) stream control transmission protocol
c) datagram congestion control protocol
d) all of the mentioned

Answer: d
Explanation: RTP uses unprevileleged UDP ports, stream control transmission protocol, and datagram congestion control protocol for data delivery over IP networks.

7. Which one of the following multimedia formats can not be supported by RTP?
a) MPEG-4
b) MJPEG
c) MPEG
d) TXT

Answer: d
Explanation: RTP is suitable only for multimedia and not for simple text files as the operation would result into wastage of resources. Other protocols like FTP are suitable for such transmissions.

8. An RTP header has a minimum size of _________
a) 12 bytes
b) 16 bytes
c) 24 bytes
d) 32 bytes

Answer: a
Explanation: Each RTP packet has a fixed header of size 12 bytes that contains essential control information like timestamp, payload type etc. for the receiving system processing.

9. Which one of the following is not correct?
a) RTCP provides canonical end-point identifiers to all session participants
b) RTCP reports are expected to be sent by all participants
c) RTCP itself does not provide any flow encryption or authentication methods
d) RTCP handles the actual data delivery

Answer: d
Explanation: RTCP works with RTP to send control packets to the users of the networks and provide canonical end-point identifiers to all session participants while RTP handles the actual data delivery.

10. Which protocol defines a profile of RTP that provides cryptographic services for the transfer of payload data?
a) SRTP
b) RTCP
c) RCP
d) RTCT

Answer: a
Explanation: SRTP stands for Secure Real-time Transport Protocol. It is like an extension to RTP which provides stream

security through encryption, message authentication and integrity, and replay attack protection.

1. An RPC (remote procedure call) is initiated by the _________
a) server
b) client
c) client after the sever
d) a third party

Answer: b
Explanation: Remote Procedure Call is a method used for constructing distributed, client-server applications based on extending the conventional local procedure calling where the client initiates an RPC to start a connection process.

2. In RPC, while a server is processing the call, the client is blocked ________
a) unless the client sends an asynchronous request to the server
b) unless the call processing is complete
c) for the complete duration of the connection
d) unless the server is disconnected

Answer: a
Explanation: While the server is processing the call i.e. looking through the specifications, the client is blocked, unless the client sends an asynchronous request to the server for another operation.

3. A remote procedure call is _______
a) inter-process communication
b) a single process
c) a single thread
d) a single stream

Answer: a
Explanation: Remote procedure calls is a form of inter-process communication where the client initiates an RPC to start a connection process. It is used to construct distributed, client-server applications.

4. RPC allows a computer program to cause a subroutine to execute in _________
a) its own address space
b) another address space
c) both its own address space and another address space
d) applications address space

Answer: b
Explanation: RPC allows a computer program to cause a subroutine to execute in another address space which is usually the servers address space in a conventional client-server network.

5. RPC works between two processes. These processes must be ____________
a) on the same computer
b) on different computers connected with a network
c) on the same computer and also on different computers connected with a network
d) on none of the computers

Answer: c
Explanation: For the operation of RPC between two processes, it is mandatory that the processes are present on the same computer and also on different computers connected with its network.

6. A remote procedure is uniquely identified by _________
a) program number
b) version number
c) procedure number
d) all of the mentioned

Answer: d
Explanation: Each remote procedure can be uniquely identified by the program number, version number and the procedure number in the networks scope. The identifiers can be used to control the remote procedure by parties involved in the process.

7. An RPC application requires _________
a) specific protocol for client server communication
b) a client program
c) a server program
d) all of the mentioned

Answer: d
Explanation: The RPC technique for constructing distributed, client-server applications based on extending the conventional local procedure calling. It requires a client program, a server program and specific protocol for client server communication to build the system.

8. RPC is used to _________
a) establish a server on remote machine that can respond to queries
b) retrieve information by calling a query
c) establish a server on remote machine that can respond to queries and retrieve information by calling a query
d) to secure the client

Answer: c
Explanation: RPC or Remote Procedure Call is used to establish a server on remote machine that can respond to queries and to retrieve information by calling a query by other computers.

9. RPC is a _________
a) synchronous operation
b) asynchronous operation
c) time independent operation
d) channel specific operation

Answer: a
Explanation: RPC is a synchronous operation where the remote machine works in sync with the other machines to act as a server that can respond to queries called by the other machines.

10. The local operating system on the server machine passes the incoming packets to the ___________
a) server stub
b) client stub
c) client operating system
d) client process

Answer: a
Explanation: The local operating system on the server machine passes the incoming packets to the server stub which then processes the packets which contain the queries from the client machines for retrieving information.

1. Which of the following is an advantage of anomaly detection?
a) Rules are easy to define
b) Custom protocols can be easily analyzed
c) The engine can scale as the rule set grows
d) Malicious activity that falls within normal usage patterns is detected

Answer: c
Explanation: Once a protocol has been built and a behavior defined, the engine can scale more quickly and easily than the signature-based model because a new signature does not have to be created for every attack and potential variant.

2. A false positive can be defined as ________
a) An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent

legitimate network traffic or behavior
b) An alert that indicates nefarious activity on a system that is not running on the network
c) The lack of an alert for nefarious activity
d) Both An alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior and An alert that indicates nefarious activity on a system that is not running on the network

Answer: d
Explanation: A false positive is any alert that indicates nefarious activity on a system that, upon further inspection, turns out to represent legitimate network traffic or behavior.

3. One of the most obvious places to put an IDS sensor is near the firewall. Where exactly in relation to the firewall is the most productive placement?
a) Inside the firewall
b) Outside the firewall
c) Both inside and outside the firewall
d) Neither inside the firewall nor outside the firewall.

Answer: a
Explanation: There are legitimate political, budgetary and research reasons to want to see all the "attacks" against your connection, but given the care and feeding any IDS requires, do yourself a favor and keep your NIDS sensors on the inside of the firewall.

4. What is the purpose of a shadow honeypot?
a) To flag attacks against known vulnerabilities
b) To help reduce false positives in a signature-based IDS
c) To randomly check suspicious traffic identified by an anomaly detection system
d) To enhance the accuracy of a traditional honeypot

Answer: c
Explanation: "Shadow honeypots," as researchers call them, share all the same characteristics of protected applications running on both the server and client side of a network and operate in conjunction with an ADS.

5. At which two traffic layers do most commercial IDSes generate signatures?
a) Application layer and Network layer
b) Network layer and Session Layer
c) Transport layer and Application layer
d) Transport layer and Network layer

Answer: d
Explanation: Most commercial IDSes generate signatures at the network and transport layers. These signatures are used to ensure that no malicious operation is contained in the traffic. Nemean generates signature at application and session layer.

6. IDS follows a two-step process consisting of a passive component and an active component. Which of the following is part of the active component?
a) Inspection of password files to detect inadvisable passwords
b) Mechanisms put in place to reenact known methods of attack and record system responses
c) Inspection of system to detect policy violations
d) Inspection of configuration files to detect inadvisable settings

Answer: b
Explanation: Secondary components of mechanism are set in place to reenact known methods of attack and to record system responses. In passive components, the system I designed just to record the system's responses in case of an intrusion.

7. When discussing IDS/IPS, what is a signature?
a) An electronic signature used to authenticate the identity of a user on the network

b) Attack-definition file
c) It refers to "normal," baseline network behavior
d) It is used to authorize the users on a network

Answer: b
Explanation: IDSes work in a manner similar to modern antivirus technology. They are constantly updated with attack-definition files (signatures) that describe each type of known malicious activity. Nemean is a popular signature generation method for conventional computer networks.

8. "Semantics-aware" signatures automatically generated by Nemean are based on traffic at which two layers?
a) Application layer and Transport layer
b) Network layer and Application layer
c) Session layer and Transport layer
d) Application layer and Session layer

Answer: d
Explanation: Nemean automatically generates "semantics-aware" signatures based on traffic at the session and application layers. These signatures are used to ensure that no malicious operation is contained in the traffic.

9. Which of the following is used to provide a baseline measure for comparison of IDSes?
a) Crossover error rate
b) False negative rate
c) False positive rate
d) Bit error rate

Answer: a
Explanation: As the sensitivity of systems may cause the false positive/negative rates to vary, it's critical to have some common measure that may be applied across the board.

10. Which of the following is true of signature-based IDSes?
a) They alert administrators to deviations from "normal" traffic behavior
b) They identify previously unknown attacks
c) The technology is mature and reliable enough to use on production networks
d) They scan network traffic or packets to identify matches with attack-definition files

Answer: d
Explanation: They are constantly updated with attack-definition files (signatures) that describe each type of known malicious activity. They then scan network traffic for packets that match the signatures, and then raise alerts to security administrators.Answer: a
Explanation: Both HDLC and PPP both are Data link layer protocol. HDLC stands for High level Data Link Control and PPP stands for Point to Point Protocol.

2. Which protocol does the PPP protocol provide for handling the capabilities of the connection/link on the network?
a) LCP
b) NCP
c) Both LCP and NCP
d) TCP

Answer: c
Explanation: LCP stands for Link Control Protocol and NCP stands for Network Control Protocol. LCP and NCP are the PPP protocols which provide interface for handling the capabilities of the connection/link on the network.

3. The PPP protocol _________
a) Is designed for simple links which transport packets between two peers
b) Is one of the protocols for making an Internet connection over a phone line
c) Is designed for simple links which transport packets between two peers and making an Internet connection over a phone line
d) Is used for sharing bandwidth

Answer: c
Explanation: The PPP protocol is designed for handling simple links which transport packets between two peers. It is a standard protocol that is used to make an Internet connection over phone lines.

4. PPP provides the _______ layer in the TCP/IP suite.
a) Link
b) Network
c) Transport
d) Application

Answer: a
Explanation: PPP provides function of the link layer in the TCP/IP suite. It focuses on the link between two nodes that is going to be used by the users to communicate. It can use pre-installed phone line for the purpose.

5. PPP consists of ________components
a) Three (encapsulating, the Domain Name system)
b) Three (encapsulating, a link control protocol, NCP)
c) Two (a link control protocol, Simple Network Control protocol)
d) One (Simple Network Control protocol)

Answer: b
Explanation: PPP consists of three components namely Link Control Protocol (LCP), Network Control Protocol (NCP), and Encapsulation. LCP and NCP are the PPP protocols which provide interface for handling the capabilities of the connection/link on the network and encapsulation provides for multiplexing of different network-layer protocols.

6. The PPP encapsulation ____________
a) Provides for multiplexing of different network-layer protocols
b) Requires framing to indicate the beginning and end of the encapsulation
c) Establishing, configuring and testing the data-link connection
d) Provides interface for handling the capabilities of the connection/link on the network

Answer: a
Explanation: Encapsulation is a part of PPP which provides means for multiplexing of different network-layer protocols. The other two parts of PPP are Link Control Protocol and Network Control Protocol.

7. A Link Control Protocol (LCP) is used for ____________
a) Establishing, configuring and testing the data-link connection
b) Establishing and configuring different network-layer protocols
c) Testing the different network-layer protocols
d) Provides for multiplexing of different network-layer protocols

Answer: a
Explanation: The Link Control Protocol (LCP) is the part of PPP that is used for establishing, configuring and testing the data-link connection. The other two components are Network Control Protocol and Encapsulation.

8. A family of network control protocols (NCPs) ____________
a) Are a series of independently defined protocols that provide a dynamic
b) Are a series of independently-defined protocols that encapsulate
c) Are a series of independently defined protocols that provide transparent
d) The same as NFS

Answer: b
Explanation: The family of network control protocols (NCPs) is a series of independently-defined protocols that encapsulate the data flowing between the two nodes. It provides means for the network nodes to control the link traffic.

9. Choose the correct statement from the following.
a) PPP can terminate the link at any time
b) PPP can terminate the link only during the link establishment phase

c) PPP can terminate the link during the authentication phase
d) PPP can terminate the link during the callback control phase

Answer: a
Explanation: PPP allows termination of the link at any time in any phase because it works on the data link layer which is the layer in control of the link of the communication.

10. The link necessarily begins and ends with this phase. During the ______ phase, the LCP automata will be in INITIAL or STARTING states.
a) Link-termination phase
b) Link establishment phase
c) Authentication phase
d) Link dead phase

Answer: d
Explanation: The link necessarily begins and ends with the link dead phase. During this phase, the LCP automata will be in the initial or its final state. The link is non-functioning or inactive during the link dead phase.Answer: a
Explanation: EIGRP stands for Enhanced Interior Gateway Routing Protocol is a routing protocol designed by Cisco. It is available only on Cisco routers.

2. EIGRP metric is ________
a) K-values
b) Bandwidth only
c) Hop Count
d) Delay only

Answer: a
Explanation: EIGRP metric is K-values which are integers from 0 to 128. They are used to calculate the overall EIGRP cost with bandwidth and delay metrics.

3. EIGRP can support ____________
a) VLSM/subnetting
b) Auto summary
c) Unequal cast load balancing
d) All of the mentioned

Answer: d
Explanation: EIGRP supports variable and fixed length subnetting, Auto summary, and Unequal cast load balancing to provide efficient routing functionality on Cisco routers.

4. EIGRP sends a hello message after every ___________ seconds.
a) 5 seconds (LAN), 60 seconds (WAN)
b) 5 seconds (LAN), 5 seconds (WAN)
c) 15s
d) 180s

Answer: a
Explanation: EIGRP routers broadcast the hello packets frequently to familiarize with the neighbors. EIGRP routers send the hello message after every 5 seconds on LAN, and every 60 seconds on WAN.

5. Administrative distance for internal EIGRP is ______
a) 90
b) 170
c) 110
d) 91

Answer: a
Explanation: Routers use the metric of administrative distance to select the best path when there are different routes to

the same destination from two different routing protocols as it is a measure of reliability of routing protocols. Administrative distance for internal EIGRP is 90.

6. The EIGRP metric values include:
a) Delay
b) Bandwidth
c) MTU
d) All of the mentioned

Answer: d
Explanation: The EIGRP metric values are Delay, Bandwidth, and MTU. MTU stands for Maximum Transmission Unit. They are combined together to give the overall EIGRP cost in K-values.

7. For default gateway, which of following commands will you use on a Cisco router?
a) IP default network
b) IP default gateway
c) IP default route
d) Default network

Answer: a
Explanation: IP default network command is used to find the default gateway in Cisco router. If the router finds routes to the node, it considers the routes to that node for installation as the gateway to it.

8. Administrative distance for external EIGRP route is _______
a) 90
b) 170
c) 110
d) 100

Answer: b
Explanation: Routers use the metric of administrative distance to select the best path when there are different routes to the same destination from two different routing protocols as it is a measure of reliability of routing protocols. Administrative distance for external EIGRP is 170.

9. EIGRP uses the ____________ algorithm for finding shortest path.
a) SPF
b) DUAL
c) Linkstat
d) Djikstra's

Answer: b
Explanation: EIGRP uses the DUAL algorithm for finding shortest path. DUAL stands for diffusing update algorithm and it is used to prevent routing loops by recalculating routes globally.

10. In EIGRP best path is known as the successor, where as backup path is known as __________
a) Feasible successor
b) Back-up route
c) Default route
d) There is no backup route in EIGRP

Answer: a
Explanation: Feasible successor is the backup path. The backup path is used alternatively used whenever the best path fails. It is not used primarily because it is comparatively expensive than the best path.