Q1. What are the primary purposes of computer networks?

- Sharing cat photos
- Facilitating data sharing
- Sending handwritten letters
- Playing video games

Correct Answer: B

Q2. How do computer networks support communication?

- By delivering pizzas
- By enabling data and resource sharing
- By predicting the weather
- By composing music

Correct Answer: B

Q3. What is a common use of computer networks?

- Baking cookies
- Remote access and mobility
- Gardening
- Skydiving

Correct Answer: B

Q4. What is the role of computer networks in collaboration?

- Sharing secret recipes
- Enabling users to work together from different locations
- Solving crossword puzzles
- Creating origami art

Correct Answer: B

Q5. What is a star topology known for?

- Redundancy
- Circular shape
- Mesh connections
- High collision rates

Correct Answer: A

Q6. Which topology forms a closed-loop structure?

- Bus
- Ring
- Star
- Mesh

Correct Answer: B

Q7. What topology offers high fault tolerance and redundancy?

- Bus
- Ring
- Star
- Mesh

Correct Answer: D

Q8. In which topology do all devices share the same communication medium?

- Star
- Ring
- Bus
- Mesh

Correct Answer: C

Q9. What is a collision domain in networking?

- A group of devices sharing the same MAC address
- A network segment where collisions can occur
- A domain for scheduling network tasks
- A domain for storing network data

Correct Answer: B

Q10. How does the collision domain size affect network performance?

- It has no impact on performance
- Larger collision domains lead to better performance
- Smaller collision domains lead to better performance
- It determines the color of network cables

Correct Answer: C

Q11. What mechanism helps prevent collisions in Ethernet networks?

- Collision detection

- Collision avoidance
- Collision celebration
- Collision prediction

Correct Answer: B

Q12. What can be done to reduce collisions within a collision domain?

- Increase the collision domain size
- Add more devices to the domain
- Implement collision detection algorithms
- Segment the network into smaller collision domains

Correct Answer: D

Q13. What is the role of a broadcast domain in network communication?

- It ensures secure communication
- It limits the size of network traffic
- It enables devices to communicate with each other
- It defines the area where broadcasts are heard

Correct Answer: D

Q14. How does a switch reduce the size of a broadcast domain compared to a hub?

- By making coffee
- By forwarding broadcasts to all ports
- By isolating devices into separate domains
- By broadcasting louder

Correct Answer: C

Q15. What do VLANs (Virtual LANs) do in terms of broadcast domains?

- Increase the broadcast domain size
- Reduce the broadcast domain size
- Convert broadcasts into unicasts
- Broadcast to all devices in a network

Correct Answer: B

Q16. What are the implications of a large broadcast domain on network traffic?

- Faster data transfer
- Reduced network congestion

- Increased network traffic
- Improved network security

Correct Answer: C

Q17. What is the OSI model, and how many layers does it consist of?

- 4 layers
- 5 layers
- 6 layers
- 7 layers

Correct Answer: D

Q18. In the OSI model, which layer is responsible for data encryption and decryption?

- Physical Layer
- Data Link Layer
- Presentation Layer
- Transport Layer

Correct Answer: C

Q19. Which layer of the OSI model is primarily responsible for routing and logical addressing?

- Network Layer
- Transport Layer
- Session Layer
- Data Link Layer

Correct Answer: A

Q20. What is the primary function of the Transport Layer in the OSI model?

- Ensuring data integrity
- Physical data transmission
- Logical addressing
- Establishing and managing connections

Correct Answer: D

Q21. Which layer of the OSI model deals with error detection and correction at the bit level?

- Data Link Layer
- Physical Layer
- Transport Layer

- Network Layer

Correct Answer: A

Q22. What is the purpose of the OSI model's Session Layer?

- Data encryption
- Managing user sessions
- Error detection
- Data compression

Correct Answer: B

Q23. How many layers does the TCP/IP model consist of?

- 4 layers
- 5 layers
- 6 layers
- 7 layers

Correct Answer: A

Q24. Which layer of the TCP/IP model corresponds to the OSI model's Transport Layer?

- Internet Layer
- Link Layer
- Transport Layer
- Application Layer

Correct Answer: C

Q25. What is the primary advantage of the TCP/IP model over the OSI model?

- Simplicity and widespread adoption
- Enhanced security features
- Improved physical layer standards
- Greater flexibility in data presentation

Correct Answer: A

Q26. In the TCP/IP model, which layer is responsible for addressing and routing data packets?

- Internet Layer
- Link Layer
- Transport Layer
- Application Layer

Correct Answer: A

Q27. How does the OSI model compare to the TCP/IP model in terms of layer definitions?

- The layers have different names and numbers
- The layers have the same names but different numbers
- The layers have the same names and numbers
- The OSI model has more layers than the TCP/IP model

Correct Answer: A

Q28. Which model, OSI or TCP/IP, is more commonly used in practical network implementations today?

- OSI model
- TCP/IP model
- Both are equally popular
- Neither is used anymore

Correct Answer: B

Q29. What are the primary functions of the Physical Layer in a network?

- Routing and addressing
- Data link control
- Bit-level transmission
- Logical addressing

Correct Answer: C

Q30. What is the main advantage of using fiber optic cables over copper cables for data transmission?

- Lower cost
- Faster transmission speeds
- Greater flexibility
- Easier installation

Correct Answer: B

Q31. Which of the following is an example of guided transmission media?

- Wireless
- Optical fiber
- Infrared

- Microwave

Correct Answer: B

Q32. In wireless communication, what is the purpose of modulation and demodulation (modem)?

- To convert digital data into analog signals for transmission
- To encrypt and decrypt data packets
- To route data packets between networks
- To establish Wi-Fi connections

Correct Answer: A

Q33. What type of wireless transmission is used in cellular telephone networks?

- Infrared
- Microwave
- Radio waves
- Bluetooth

Correct Answer: C

Q34. Which of the following wireless technologies is commonly used for satellite-based internet connections?

- 4G LTE
- Wi-Fi
- VSAT (Very Small Aperture Terminal)
- NFC (Near Field Communication)

Correct Answer: C

Q35. What are the advantages of using microwave transmission for long-distance communication?

- Low cost and ease of installation
- High data rates and low latency
- Immunity to interference and wide coverage
- Secure and encrypted communication

Correct Answer: B

Q36. What is the role of a transceiver in wireless communication?

- Data encryption
- Signal amplification
- Transmitting and receiving signals

- Routing data packets

Correct Answer: C

Q37. What is latency in network communication, and how does it relate to the Physical Layer?

- Latency is the delay in data transmission, affected by the transmission medium.
- Latency is the data rate of a communication channel.
- Latency is the protocol used to establish connections.
- Latency is the distance between network devices.

Correct Answer: A

Q38. What is the key difference between half-duplex and full-duplex communication?

- Half-duplex can transmit data in both directions simultaneously, while full-duplex cannot.
- Half-duplex can only transmit data in one direction at a time, while full-duplex can transmit in both directions simultaneously.
- Half-duplex uses optical fibers, while full-duplex uses copper cables.
- Half-duplex is used in wireless communication, while full-duplex is used in wired communication.

Correct Answer: B

Q39. 1. What are the common types of errors that can occur in data transmission over a network?

- Bit errors
- Link errors
- Frame errors
- All of the above

Correct Answer: D

Q40. 2. What is redundancy in the context of error detection and correction?

- The process of reducing data size for faster transmission
- The inclusion of extra information to detect and correct errors
- The removal of duplicate data from a message
- None of the above

Correct Answer: B

Q41. 3. Which error detection technique uses a polynomial division to calculate a remainder that is added to the data for error checking?

- CRC (Cyclic Redundancy Check)

- Checksum
- Parity bit
- Hamming code

Correct Answer: A

Q42. 4. What is the purpose of a checksum in error detection?

- To count the number of bits in a message
- To check for errors in the data by comparing the sum of bits to a predefined value
- To encrypt the data for secure transmission
- None of the above

Correct Answer: B

Q43. 5. Which error correction technique can correct single-bit errors and detect double-bit errors in data?

- CRC
- Checksum
- Hamming code
- Parity bit

Correct Answer: C

Q44. 6. What is the Hamming distance between two binary words of equal length?

- The number of bits that differ between the two words
- The total number of bits in the words
- The number of bits set to 1 in the words
- None of the above

Correct Answer: A

Q45. 7. Which error detection method involves adding an extra bit to the data so that the total number of 1s is always even (or odd)?

- CRC
- Checksum
- Parity bit
- Hamming code

Correct Answer: C

Q46. 8. What is the purpose of error detection and correction at the Data Link Layer?

- To ensure data confidentiality
- To prevent unauthorized access to the network
- To detect and correct errors in data transmission
- To establish network connections

Correct Answer: C

Q47. 9. Which error detection technique is commonly used in Ethernet networks to detect errors in frames?

- CRC
- Checksum
- Parity bit
- Hamming code

Correct Answer: A

Q48. 10. In error detection, what is the purpose of the receiver's acknowledgment (ACK) to the sender?

- To request retransmission of the entire data
- To confirm successful receipt of data
- To notify the sender of an error in the data
- To terminate the data transmission

Correct Answer: B

Q49. 1. What is the ALOHA protocol used for in computer networks?

- Error correction
- Multiple access control
- Data encryption
- Packet routing

Correct Answer: B

Q50. 2. In ALOHA, how is the transmission time divided into slots?

- Equally sized slots for all stations
- Unequally sized slots based on station priority
- Dynamically sized slots based on traffic load
- There are no slots in ALOHA

Correct Answer: A

Q51. 3. What is the key disadvantage of the pure ALOHA protocol?

- High collision rate
- Low throughput
- Complex synchronization requirements
- Limited scalability

Correct Answer: A

Q52. 4. What does CSMA stand for in CSMA/CA and CSMA/CD?

- Centralized Synchronization Media Access
- Carrier Sense Multiple Access
- Collision-Free Media Allocation
- Controlled Synchronization Medium Allocation

Correct Answer: B

Q53. 5. In CSMA, what is the purpose of "carrier sense"?

- To detect collisions
- To sense the presence of a carrier signal
- To encrypt data packets
- To regulate access to the medium

Correct Answer: B

Q54. 6. How does CSMA/CD (Carrier Sense Multiple Access with Collision Detection) handle collisions?

- Stations always transmit, and collisions are resolved by the central controller.
- Stations sense the collision and retransmit after a random backoff time.
- Collisions are prevented through strict time-slot allocation.
- Collisions are ignored, and the sender keeps transmitting.

Correct Answer: B

Q55. 7. In CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), how are collisions avoided?

- Stations transmit simultaneously to reduce the chance of collision.
- Stations request permission before transmitting.
- Collisions are resolved by the central controller.
- Collisions are detected and corrected in real-time.

Correct Answer: B

Q56. 8. What is the primary advantage of CSMA/CA over CSMA/CD in wireless networks?

- Lower latency
- Higher throughput
- Reduced collisions
- Simplicity of implementation

Correct Answer: C

Q57. 9. Which protocol is commonly used in Ethernet LANs and employs CSMA/CD?

- ALOHA
- Token Ring
- Wi-Fi
- Ethernet

Correct Answer: D

Q58. 10. What is the primary purpose of the contention window in CSMA/CA?

- To set the maximum data rate
- To specify the channel frequency
- To control the backoff time before retransmission
- To define the maximum frame size

Correct Answer: C

Q59. 1. What does FDMA stand for in the context of channelization protocols?

- Frequency Division Multiple Access
- Frequency Data Management Algorithm
- Fast Digital Modulation Analysis
- Frequency Data Modulation Array

Correct Answer: A

Q60. 2. In FDMA, how are multiple users allocated channels for communication?

- Users share the same frequency channel simultaneously.
- Each user is assigned a unique frequency channel.
- Users take turns transmitting on the same frequency.
- Channels are dynamically assigned based on deman

Correct Answer: B

Q61. 3. What is the primary advantage of FDMA in terms of channel allocation?

- High flexibility and adaptability
- Low susceptibility to interference
- Efficient use of available bandwidth
- Simple implementation and low cost

Correct Answer: C

Q62. 4. What does TDMA stand for in the context of channelization protocols?

- Time Division Media Allocation
- Time Division Multiple Access
- Transmission Data Management Algorithm
- Telecommunication Data Modulation Array

Correct Answer: B

Q63. 5. In TDMA, how is the transmission time divided among multiple users sharing the same channel?

- Users transmit simultaneously on different time slots.
- Users transmit sequentially one after another.
- Users transmit in random order to minimize collisions.
- Users transmit on separate frequency channels.

Correct Answer: A

Q64. 6. What is the key benefit of TDMA in terms of spectrum efficiency?

- High resistance to interference
- Lower latency in data transmission
- Efficient use of available bandwidth
- Reduced complexity of synchronization

Correct Answer: C

Q65. 1. What is the primary goal of the reservation protocol in controlled access?

- Minimize latency
- Maximize throughput
- Ensure fairness
- Reduce collision probability

Correct Answer: A

Q66. 2. In reservation-based protocols, how are time slots allocated to devices for transmission?

- Devices compete for slots in real-time.
- Slots are pre-allocated based on a reservation phase.
- Slots are allocated randomly to devices.
- Slots are assigned permanently to devices.

Correct Answer: B

Q67. 3. What is a potential drawback of reservation-based protocols in dynamic networks?

- Inefficient use of bandwidth
- High collision rates
- Excessive overhead for slot allocation
- Limited scalability

Correct Answer: C

Q68. 1. In polling-based protocols, who controls the communication and polling process?

- Devices independently poll each other.
- A central controller polls devices sequentially.
- Devices send messages whenever they want.
- Devices poll each other randomly.

Correct Answer: B

Q69. 2. What is the advantage of using polling in controlled access networks?

- Low latency due to simultaneous transmission
- High throughput for all devices
- Predictable access to the shared medium
- Minimal overhead in the communication process

Correct Answer: C

Q70. 3. What is a potential drawback of polling-based protocols in large networks with many devices?

- High collision rates
- Long waiting times for polling
- Difficulty in synchronization
- Inefficient use of bandwidth

Correct Answer: B

Q71. 1. What is the fundamental concept behind token passing protocols in controlled access?

- Devices compete for access to the medium.
- Devices transmit when they have a token.
- Devices use polling to access the medium.
- Devices reserve time slots for transmission.

Correct Answer: B

Q72. 2. In token passing, how is access to the shared medium controlled?

- Devices send requests for transmission.
- A token is passed sequentially among devices.
- Devices transmit data simultaneously.
- A central controller allocates time slots.

Correct Answer: B

Q73. 3. What is a significant advantage of token passing protocols in controlled access networks?

- High flexibility in medium access
- Minimal collision probability
- Reduced overhead in communication
- Low latency due to parallel transmission

Correct Answer: B

Q74. Which of the following is a valid IPv4 address format?

- 256.1.1
- 10.10.300
- 31.256.0
- 168.1.1000

Correct Answer: D

Q75. Which network class is primarily used for large-scale organizations and provides over 16 million host addresses?

- g., 10.0.0.0)
- g., 172.16.0.0)
- g., 192.168.0.0)
- g., 224.0.0.0)

Correct Answer: A

Q76. What is the default subnet mask for a Class B network?

- 0.0.0
- 255.0.0
- 255.255.0
- 255.255.255

Correct Answer: B

Q77. Which subnet mask does RIP v1 assume by default when sending route updates?

- 255.255.255)
- 255.255.0)
- 255.0.0)
- 0.0.0)

Correct Answer: C

Q78. What is the multicast address used by RIP v2 for sending route updates?

- 0.0.5
- 0.0.9
- 255.255.255
- 0.0.1

Correct Answer: B

Q79. Which type of protocol does UDP (User Datagram Protocol) represent: connectionless or connection-oriented?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: A

Q80. TCP (Transmission Control Protocol) is an example of which type of protocol: connectionless or connection-oriented?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: B

Q81. In a connection-oriented protocol like TCP, what is the purpose of the three-way handshake during connection establishment?

- To confirm data delivery
- To exchange encryption keys
- To synchronize sequence numbers
- To establish a reliable connection

Correct Answer: C

Q82. In a connection-oriented protocol like TCP, if a segment is not acknowledged by the receiver, what action does the sender take?

- Retransmits the segment
- Drops the segment and continues
- Reduces the transmission speed
- Sends an error message to the receiver

Correct Answer: A

Q83. UDP is often used for real-time applications like streaming and online gaming. What advantage does UDP offer for these applications?

- Reliable data delivery is not required
- Lower latency and reduced overhead
- Greater error checking and correction
- Enhanced security and encryption

Correct Answer: B

Q84. What is the primary role of the Transport Layer protocols such as TCP and UDP?

- To transmit data between devices
- To establish network connections
- To encrypt data for secure transmission
- To manage the physical network

Correct Answer: A

Q85. Which Transport Layer protocol is commonly used for secure, encrypted data transmission on the web?

- FTP
- HTTPs
- SNMP

- ICMP

Correct Answer: B

Q86. Which Transport Layer protocol is designed for email communication and is responsible for sending and receiving emails?

- HTTP
- SMTP
- SNMP
- DNS

Correct Answer: B

Q87. Which Transport Layer protocol is often used for file transfer and allows for efficient, bulk data transfer?

- FTP
- SNMP
- HTTP
- SMTP

Correct Answer: A

Q88. What is the purpose of port numbers in the Transport Layer protocols?

- To identify the physical interface of a device
- To specify the device's IP address
- To identify the application or service
- To determine the device's location

Correct Answer: C

Q89. What does TCP stand for in the context of networking?

- Transmission Control Protocol
- Textual Communication Protocol
- Transport Control Protocol
- Telecommunication Connection Protocol

Correct Answer: A

Q90. Which TCP flag is used to initiate the connection setup in the TCP three-way handshake?

- ACK (Acknowledgment)
- SYN (Synchronize)

- RST (Reset)
- FIN (Finish)

Correct Answer: B

Q91. In TCP, what term refers to the process of ensuring that data segments are received by the destination and in the correct order?

- Segmentation
- Flow control
- Error correction
- Sequence control

Correct Answer: D

Q92. In a TCP connection, which side, the sender or receiver, acknowledges the successful receipt of data segments?

- Only the sender
- Only the receiver
- Both the sender and receiver
- Neither the sender nor receiver

Correct Answer: B

Q93. What is the purpose of the TCP FIN (Finish) flag during the connection termination process?

- To acknowledge data receipt and continue communication
- To reset the connection
- To initiate the connection termination
- To establish a new connection

Correct Answer: C

Q94. What does the term "handshaking" refer to in the context of the TCP three-way handshake?

- A process of physical handshakes between devices
- An agreement to establish a connection
- An authentication method
- A security protocol

Correct Answer: B

Q95. In the TCP three-way handshake, what does the SYN (Synchronize) segment indicate to the receiving device?

- The sender is ready to receive data
- The sender is terminating the connection
- The sender is synchronizing sequence numbers
- The sender is requesting encryption

Correct Answer: C

Q96. In the TCP three-way handshake, after the client sends a SYN segment, what action does the server take?

- The server responds with a SYN-ACK segment
- The server sends data
- The server acknowledges the client's request
- The server terminates the connection

Correct Answer: A

Q97. Which transport layer protocol uses a message format with no header checksum, providing minimal overhead?

- TCP
- UDP
- IP
- HTTP

Correct Answer: B

Q98. What is the maximum length, in bytes, of the UDP message payload (data) that can be accommodated in a single packet?

- 512 bytes
- 1,500 bytes
- 65,535 bytes
- 4,096 bytes

Correct Answer: C

Q99. Which field in the TCP message header indicates the number of 32-bit words in the TCP header itself?

- Window size
- Data offset
- Checksum
- Acknowledgment number

Correct Answer: B

Q100. What field in the TCP message format specifies the maximum number of bytes the sender is willing to accept in one message?

- Checksum
- Sequence number
- Window size
- Acknowledgment number

Correct Answer: C

Q101. In the TCP message format, what is the purpose of the Urgent Pointer field?

- To indicate the start of a new message
- To specify the sender's IP address
- To identify the data sequence number
- To indicate the end of the message

Correct Answer: D

Q102. In congestion control, what does "window-based" congestion control refer to?

- Controlling congestion by limiting the number of packets sent
- Controlling congestion based on network latency
- Controlling congestion by adjusting window size
- Controlling congestion using traffic shaping

Correct Answer: C

Q103. In QoS, what is "jitter," and why is it important to control in real-time communication?

- Jitter refers to network congestion
- Jitter is the variation in packet arrival times
- Jitter indicates the number of lost packets
- Jitter measures data throughput

Correct Answer: B

Q104. What is the primary purpose of a token bucket in traffic shaping for QoS?

- To store packets temporarily
- To prioritize voice traffic
- To control the rate of packet transmission
- To increase network capacity

Correct Answer: C

Q105. Which QoS mechanism involves marking packets with different priority levels based on their importance or type of traffic?

- Packet switching
- Quality of Service (QoS)
- Traffic shaping
- Packet loss prevention

Correct Answer: B

Q106. What is the primary function of the Domain Name System (DNS) in computer networks?

- To encrypt data transmissions
- To resolve human-readable domain names to IP addresses
- To manage email communication
- To perform network monitoring

Correct Answer: B

Q107. What is the significance of a DNS cache in speeding up domain name resolution?

- It stores encrypted DNS records
- It stores frequently accessed DNS records
- It encrypts DNS traffic
- It manages email servers

Correct Answer: B

Q108. What is a top-level domain (TLD) in the context of DNS?

- The highest level of the DNS hierarchy
- A domain that exclusively uses numeric characters
- The domain name of a web server
- A domain used for email addressing

Correct Answer: A

Q109. Which DNS record type is used to specify the mail servers responsible for receiving email for a domain?

- A (Address)
- PTR (Pointer)
- MX (Mail Exchanger)
- CNAME (Canonical Name)

Correct Answer: C

Q110. In remote logging, what is the role of a log collector?

- To encrypt log data
- To centralize and store log data from various sources
- To manage email servers
- To generate network traffic logs

Correct Answer: B

Q111. Who is credited with inventing email, and when was it first introduced?

- Bill Gates in 1995
- Ray Tomlinson in the early 1970s
- Mark Zuckerberg in 2004
- Tim Berners-Lee in 1989

Correct Answer: B

Q112. How does the Simple Mail Transfer Protocol (SMTP) play a role in email transmission?

- It encrypts email messages
- It defines the rules for routing and sending email
- It manages email storage
- It controls email access

Correct Answer: B

Q113. How does email address formatting adhere to the username@domain.com structure?

- It uses IP addresses for email
- It separates username and domain with a period
- It encrypts email data
- It encrypts email headers

Correct Answer: B

Q114. What is the purpose of email aliases and distribution lists in email communication?

- To encrypt email headers
- To manage email attachments
- To route email traffic
- To simplify sending emails to groups

Correct Answer: D

Q115. How does email support the concept of folders and organizational structures?

- By encrypting email contents
- By allowing users to categorize and store emails
- By compressing email headers
- By securing email attachments

Correct Answer: B

Q116. What are the basic components of an FTP connection?

- Username, password, and email client
- Server, client, and encryption key
- Sender, receiver, and IP address
- Header, footer, and routing table

Correct Answer: B

Q117. How does FTP handle file transfers between different operating systems?

- It converts email attachments
- It uses a universal format for all files
- It encrypts email messages
- It encrypts email headers

Correct Answer: B

Q118. What are some common security risks associated with FTP, and how can they be mitigated?

- Lack of email encryption
- Unauthorized access and data interception
- Excessive email logs storage
- Slow email delivery due to FTP use

Correct Answer: B

Q119. What are web servers, and how do they serve web content?

- Servers for secure email delivery
- Computers that store and distribute web pages
- Devices for email encryption
- Routers for FTP file transfers

Correct Answer: B

Q120. What is the purpose of HTML (Hypertext Markup Language) in web development?

- It encrypts email contents
- It defines the structure and content of web pages
- It manages email attachments
- It optimizes email routing

Correct Answer: B

Q121. What is HTTP (Hypertext Transfer Protocol), and what is its primary purpose?

- A protocol for secure email delivery
- A protocol for transferring files
- A protocol for web communication
- A method of email encryption

Correct Answer: C

Q122. What is the purpose of cookies in HTTP, and how are they used?

- They are email attachments for web pages
- They store session information
- They encrypt email data
- They optimize email routing

Correct Answer: B

Q123. What is the role of HTTP headers in web communication, and what types of information do they convey?

- They are email headers for web pages
- They indicate the content type and length
- They manage email routing
- They encrypt email attachments

Correct Answer: B

Q124. How does SMTP facilitate email transmission between email clients and email servers?

- It encrypts email headers
- It uses email attachments for transmission
- It relays email messages
- It optimizes email routing

Correct Answer: C

Q125. Explain the roles of SMTP clients (MUAs) and their interactions with SMTP servers in sending emails.

- Clients compose email content
- Clients store email attachments
- Clients encrypt email headers
- Clients optimize email delivery

Correct Answer: A

Q126. How does SMTP ensure the reliability of email delivery, and what mechanisms are in place for handling failed deliveries?

- It uses email encryption methods
- It tracks email logs for errors
- It implements retries and queuing
- It optimizes email routing

Correct Answer: C

Q127. What are SNMP agents and managers, and how do they interact in network management?

- They are encryption methods for emails
- Agents collect and report data, managers
- They manage email routing
- They compress email attachments

Correct Answer: B

Q128. What are SNMP community strings, and how do they control access to SNMP-managed devices?

- They are email attachments for web pages
- They are authentication keys for SNMP
- They are used to encrypt email data
- They specify SNMP server addresses

Correct Answer: B

Q129. What types of information can SNMP provide about network devices and resources?

- It tracks email logs for errors
- Configuration settings, performance metrics
- It encrypts email headers
- It manages email logs

Correct Answer: B

Q130. What is the purpose of SNMP MIBs (Management Information Bases), and how are they organized?

- They are email logs for SNMP messages
- They store SNMP data and are organized hierarchically
- They encrypt email contents
- They manage email routing

Correct Answer: B

Q131. How does network segmentation contribute to security services, and what are some common segmentation methods?

- It encrypts network traffic
- It improves network performance
- It isolates network segments
- It manages network authentication

Correct Answer: C

Q132. What is the role of disaster recovery planning in network security, and how does it ensure business continuity?

- It ensures data confidentiality
- It verifies user identities
- It restricts unauthorized access
- It prepares for unforeseen disruptions

Correct Answer: D

Q133. How does encryption contribute to data security, and what are common encryption algorithms used in network security?

- It ensures data confidentiality
- It verifies user identities
- It restricts unauthorized access
- It optimizes network performance

Correct Answer: A

Q134. What is the purpose of digital signatures in network security, and how do they verify the authenticity of data?

- They encrypt network traffic
- They improve user authentication

- They authenticate the sender's identity
- They optimize network routing

Correct Answer: C

Q135. Explain the significance of end-to-end encryption in securing data transmission across networks.

- It ensures data confidentiality
- It optimizes network routing
- It restricts unauthorized access
- It detects and responds to incidents

Correct Answer: A

Q136. What is the primary purpose of a digital signature in network security?

- To encrypt network traffic
- To restrict unauthorized access
- To verify the authenticity and integrity of data
- To optimize network routing

Correct Answer: C

Q137. What cryptographic key is typically used for generating a digital signature?

- Public key
- Private key
- Symmetric key
- Session key

Correct Answer: B

Q138. Explain the concept of a revocation list (CRL) in digital certificate management.

- It ensures data confidentiality
- It verifies user identities
- It restricts unauthorized access
- It lists revoked or expired digital certificates

Correct Answer: D

Q139. What is the OSI Model, and how does it work?

- A protocol for wireless communication.
- A conceptual framework with seven layers that standardizes networking functions.

- A type of firewall used in enterprise networks.
- A software for network configuration.

Correct Answer: B

Q140. What is redundancy in the context of error detection and correction?

- The process of reducing data size for faster transmission
- The inclusion of extra information to detect and correct errors
- The removal of duplicate data from a message
- None of the above

Correct Answer: B

Q141. What is the purpose of a checksum in error detection?

- To count the number of bits in a message
- To check for errors in the data by comparing the sum of bits to a predefined value
- To encrypt the data for secure transmission
- None of the above

Correct Answer: B

Q142. In ALOHA, how is the transmission time divided into slots?

- Equally sized slots for all stations
- Unequally sized slots based on station priority
- Dynamically sized slots based on traffic load
- There are no slots in ALOHA

Correct Answer: A

Q143. What does CSMA stand for in CSMA/CA and CSMA/CD?

- Centralized Synchronization Media Access
- Carrier Sense Multiple Access
- Collision-Free Media Allocation
- Controlled Synchronization Medium Allocation

Correct Answer: B

Q144. In CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance), how are collisions avoided?

- Stations transmit simultaneously to reduce the chance of collision.
- Stations request permission before transmitting.

- Collisions are resolved by the central controller.
- Collisions are detected and corrected in real-time.

Correct Answer: B

Q145. What does TDMA stand for in the context of channelization protocols?

- Time Division Media Allocation
- Time Division Multiple Access
- Transmission Data Management Algorithm
- Telecommunication Data Modulation Array

Correct Answer: B

Q146. What is the primary goal of the reservation protocol in controlled access?

- Minimize latency
- Maximize throughput
- Ensure fairness
- Reduce collision probability

Correct Answer: A

Q147. What is a potential drawback of reservation-based protocols in dynamic networks?

- Inefficient use of bandwidth
- High collision rates
- Excessive overhead for slot allocation
- Limited scalability

Correct Answer: C

Q148. What is a potential drawback of polling-based protocols in large networks with many devices?

- High collision rates
- Long waiting times for polling
- Difficulty in synchronization
- Inefficient use of bandwidth

Correct Answer: B

Q149. What is a significant advantage of token passing protocols in controlled access networks?

- High flexibility in medium access
- Minimal collision probability
- Reduced overhead in communication

- Low latency due to parallel transmission

Correct Answer: B

Q150. In the Stop and Wait protocol, what is the role of the sender after sending a data frame?

- Continue sending data frames
- Wait for an acknowledgment (ACK) from the receiver
- Send the next data frame immediately
- Request retransmission of the data frame

Correct Answer: B

Q151. What is the major drawback of the Stop and Wait protocol in terms of efficiency?

- High throughput
- Low latency
- Inefficient use of bandwidth
- Minimal overhead

Correct Answer: C

Q152. In the context of the Stop and Wait protocol, what is the significance of using timers?

- To synchronize sender and receiver
- To measure transmission speed
- To manage network congestion
- To handle timeouts and retransmissions

Correct Answer: D

Q153. Which factor makes the Stop and Wait protocol less suitable for high-speed networks and long-distance communication?

- Reliability
- Simplicity
- Low overhead
- Efficiency

Correct Answer: D

Q154. Which data link layer protocol is known for its simplicity and involves the sender waiting for an acknowledgment before sending the next frame?

- Go-Back-N
- Selective Repeat

- Stop and Wait
- Automatic Repeat Request (ARQ)

Correct Answer: C

Q155. Which data link layer protocol uses a sliding window approach, allowing the sender to transmit multiple frames before waiting for acknowledgments?

- Go-Back-N
- Selective Repeat
- Stop and Wait
- Automatic Repeat Request (ARQ)

Correct Answer: A

Q156. Which ARQ protocol provides more efficient error recovery by retransmitting only the frames with errors, rather than the entire window?

- Go-Back-N
- Selective Repeat
- Stop and Wait
- Automatic Repeat Request (ARQ)

Correct Answer: B

Q157. In the Selective Repeat ARQ protocol, what is the key advantage over Go-Back-N in terms of efficiency and retransmissions?

- It retransmits only frames with errors
- It has a smaller window size
- It offers lower throughput
- It requires fewer acknowledgments

Correct Answer: A

Q158. What is the primary disadvantage of Selective Repeat ARQ compared to Go-Back-N in terms of complexity and implementation?

- Increased complexity of sender and receiver
- Smaller window size
- Lower efficiency
- Higher overhead for acknowledgment

Correct Answer: A

Q159. Which of the following best describes an IP packet in the context of the Network Layer?

- A logical group of data bytes
- A physical network cable
- A data frame within a switch
- A wireless access point

Correct Answer: A

Q160. In IPv4, how many bits are used to represent an IP address?

- 8 bits
- 16 bits
- 32 bits
- 64 bits

Correct Answer: C

Q161. Which part of an IPv4 address designates the network portion?

- The first two octets
- The last two octets
- The third octet
- The fourth octet

Correct Answer: A

Q162. What is the maximum number of IPv4 addresses that can exist within a single subnet?

- 255
- 256
- 2^32 - 1
- 2^32 - 2

Correct Answer: C

Q163. Which routing algorithm updates routing tables based on the number of hops to a destination and shares this information with neighboring routers?

- Distance Vector Routing (DVR)
- Link State Routing (LSR)
- Static Routing
- Default Routing (DR)

Correct Answer: A

Q164. What is a routing metric in the context of routing algorithms?

- The number of routers in the network
- A value used to determine the best path
- The physical distance between routers
- The number of hops to the destination

Correct Answer: B

Q165. What is the key advantage of Link State Routing (LSR) over Distance Vector Routing (DVR)?

- Simplicity and ease of implementation
- Faster convergence
- Lower bandwidth consumption
- Resistance to routing loops and more accurate routing

Correct Answer: D

Q166. ICMP (Internet Control Message Protocol) is primarily used for what purpose in IP networks?

- Network address translation (NAT)
- Error reporting and diagnostics
- Secure data transmission
- IP address allocation and management

Correct Answer: B

Q167. What is the purpose of IPv6 (Internet Protocol version 6) in comparison to IPv4?

- To reduce the number of available IP addresses
- To improve network security and encryption
- To enhance support for multimedia and IoT applications
- To provide backward compatibility with IPv4

Correct Answer: C

Q168. What is the maximum number of unique IP addresses that can be represented by IPv6?

- 2^64 (approximately 18.4 quintillion addresses)
- 2^16 (approximately 65,536 addresses)
- 2^32 (approximately 4.3 billion addresses)
- 2^128 (approximately 340 undecillion addresses)

Correct Answer: D

Q169. In IPv6, what type of address is used to identify a group of devices that may belong to different networks?

- Unicast address
- Anycast address
- Multicast address
- Broadcast address

Correct Answer: C

Q170. What is the primary reason for the transition from IPv4 to IPv6 in modern networking?

- To improve network performance and speed
- To reduce the complexity of routing tables
- To increase backward compatibility with legacy systems
- To accommodate the growing number of internet-connected devices

Correct Answer: D

Q171. In a Class C network, how many bits are assigned to the host portion of the IP address?

- 8 bits
- 16 bits
- 24 bits
- 32 bits

Correct Answer: C

Q172. What is the maximum number of host addresses that can be assigned in a Class C network with a subnet mask of 255.255.255.224?

- 8
- 16
- 32
- 64

Correct Answer: C

Q173. What is the primary purpose of a subnet mask in IP networking?

- To indicate the default gateway for the network
- To identify the network and host portions
- To encrypt data during transmission
- To assign unique hostnames to devices in the network

Correct Answer: B

Q174. What is the term for borrowing bits from the host portion of an IP address to create subnets?

- Subnet borrowing
- Network slicing
- Bit masking
- Subnetting

Correct Answer: D

Q175. What is the primary characteristic of a static routing algorithm?

- It dynamically adjusts routes based on traffic
- It requires manual configuration
- It uses metrics like hop count for routing
- It adapts to network changes automatically

Correct Answer: B

Q176. In a network topology where link costs represent delay, which routing algorithm is suitable for minimizing latency?

- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- OSPF (Open Shortest Path First)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Correct Answer: C

Q177. Which routing protocol typically uses the Bellman-Ford algorithm for path selection?

- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Correct Answer: B

Q178. In dynamic routing, what does the term "metric" refer to?

- The maximum hop count to a destination
- A unique identifier for each route
- A measurement used to determine route preference
- The number of routers in the network

Correct Answer: C

Q179. Which type of routing algorithm adjusts routes based on real-time network conditions?

- Dynamic routing algorithms
- Static routing algorithms
- Shortest Path Routing algorithms
- Link-State routing algorithms

Correct Answer: A

Q180. What does RIP stand for in the context of routing protocols?

- Routing Information Protocol
- Reliable Internet Protocol
- Routing Internet Protocol
- Remote Information Protocol

Correct Answer: A

Q181. What is the maximum hop count allowed in RIP v1 for a valid route?

- 10 hops
- 15 hops
- 16 hops
- 100 hops

Correct Answer: C

Q182. Which metric does RIP use to measure the distance to a destination network?

- Hop count
- Bandwidth
- Delay
- Reliability

Correct Answer: A

Q183. What is the purpose of the RIP "split horizon" rule?

- To prevent routing loops
- To optimize network traffic
- To split route updates into segments
- To ensure equal distribution of routes

Correct Answer: A

Q184. What does OSPF stand for in the context of routing protocols?

- Open Shortest Path Forwarding

- Open System Path Finder
- Open Source Path Forwarding
- Open Shortest Path First

Correct Answer: D

Q185. OSPF uses a link-state routing algorithm. What type of information is stored in OSPF's link-state database?

- The routing tables of all routers
- A list of all network IDs
- Information about the routers in the AS
- The number of hops to reach each router

Correct Answer: C

Q186. What is the purpose of OSPF's Designated Router (DR) and Backup Designated Router (BDR) in a multi-access network?

- To reduce OSPF routing overhead
- To maintain network stability
- To optimize the use of OSPF areas
- To increase OSPF's compatibility with RIP

Correct Answer: B

Q187. What OSPF packet type is used by routers to discover neighbors and establish adjacencies?

- Link-state advertisements (LSAs)
- OSPF Hello packets
- OSPF Database Description (DBD) packets
- OSPF Link State Update (LSU) packets

Correct Answer: B

Q188. In OSPF, what is an ASBR (Autonomous System Border Router)?

- A router that connects to the internet
- A router that connects to an OSPF area
- A router that connects to a different AS
- A router that connects to the backbone area

Correct Answer: C

Q189. What does EIGRP stand for in the context of routing protocols?

- Enhanced Internet Gateway Routing Protocol
- Enhanced Interior Gateway Routing Protocol
- Efficient Internet Gateway Routing Protocol
- Enhanced Interior Gateway Routing Process

Correct Answer: B

Q190. In EIGRP, what is a feasible successor?

- A backup route with a higher metric
- A loop-free backup route
- A route advertised by an ASBR
- A virtual link to a remote router

Correct Answer: B

Q191. EIGRP uses a composite metric to calculate the best path to a destination. What is this metric called?

- Cost metric
- Bandwidth-delay product
- EIGRP metric
- Successor metric

Correct Answer: C

Q192. What is the administrative distance of EIGRP?

- 90
- 100
- 110
- 120

Correct Answer: A

Q193. What is the primary reason for using EIGRP in a Cisco network environment?

- Compatibility with other vendors' routers
- Scalability
- Support for classless routing
- Support for open-standard routing protocols

Correct Answer: C

Q194. What does BGP stand for in the context of routing protocols?

- Border Gateway Protocol
- Best Gateway Protocol
- Border Gateway Process
- Basic Gateway Protocol

Correct Answer: A

Q195. BGP is classified into two main categories based on its role in routing. What are these categories?

- Internal BGP (iBGP) and External BGP (eBGP)
- Border BGP and Core BGP
- Simple BGP and Complex BGP
- Basic BGP and Advanced BGP

Correct Answer: A

Q196. What is the administrative distance of BGP?

- 90
- 100
- 110
- 120

Correct Answer: B

Q197. In the Transport Layer, what service ensures that data units are delivered error-free and in the correct order?

- Segmentation and reassembly
- Error detection and correction
- Flow control
- Multiplexing

Correct Answer: C

Q198. What is the primary purpose of segmentation in the Transport Layer?

- Data encryption
- Breaking large messages into smaller segments
- Error detection and correction
- End-to-end communication

Correct Answer: B

Q199. What type of communication does the Transport Layer provide: connectionless or connection-oriented?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: C

Q200. Which Transport Layer service allows the receiver to detect and correct errors in the data?

- Flow control
- Error detection and correction
- Multiplexing
- Segmentation and reassembly

Correct Answer: B

Q201. Which Transport Layer service provides a means of multiplexing, demultiplexing, and identifying different data streams?

- Flow control
- Multiplexing
- Error detection and correction
- Segmentation and reassembly

Correct Answer: B

Q202. In a connectionless protocol like UDP, are acknowledgments sent to confirm successful data transmission?

- Yes
- No
- It depends on the application
- Acknowledgments are optional

Correct Answer: B

Q203. Which type of protocol provides reliable, error-checked, and ordered data delivery: connectionless or connection-oriented?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: B

Q204. Which type of protocol is more suitable for applications that require low-latency communication?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: A

Q205. Which type of protocol is less complex in terms of overhead and resource usage: connectionless or connection-oriented?

- Connectionless
- Connection-oriented
- Both connectionless and connection-oriented
- Neither connectionless nor connection-oriented

Correct Answer: A

Q206. In a connection-oriented protocol like TCP, how are data segments organized and identified for proper sequencing at the receiver?

- Using sequence numbers
- Using port numbers and IP addresses
- Using timestamps and checksums
- Using packet identifiers

Correct Answer: A

Q207. Which Transport Layer protocol provides a connectionless, unreliable, and low-overhead data transfer service?

- TCP
- SMTP
- UDP
- HTTP

Correct Answer: C

Q208. In the Transport Layer, which protocol is responsible for reliable, error-checked data delivery with flow control?

- UDP

- ICMP
- HTTP
- TCP

Correct Answer: D

Q209. What is the primary difference between TCP (Transmission Control Protocol) and UDP (User Datagram Protocol)?

- TCP provides reliable, ordered data delivery, while UDP offers connectionless, unreliable delivery.
- TCP is faster than UDP.
- UDP provides encryption, while TCP does not.
- TCP is used for video streaming, while UDP is used for web browsing.

Correct Answer: A

Q210. In a Transport Layer protocol like TCP, how is data sequencing achieved to ensure that packets are delivered in the correct order?

- Using sequence numbers
- Using timestamps
- Using encryption keys
- Using checksums

Correct Answer: A

Q211. Which Transport Layer protocol is associated with the World Wide Web and is used for fetching web pages and data?

- FTP
- SMTP
- HTTP
- SNMP

Correct Answer: C

Q212. What is the purpose of the TCP three-way handshake during the establishment of a connection?

- To synchronize sequence numbers
- To encrypt the data
- To establish a secure tunnel
- To transmit data

Correct Answer: A

Q213. During the TCP three-way handshake, what happens after the client sends a SYN (Synchronize) segment to the server?

- The server responds with a SYN-ACK segment
- The client sends data
- The server acknowledges the client's request
- The client acknowledges the server's response

Correct Answer: A

Q214. What is the primary advantage of TCP's reliable data delivery mechanism over UDP's connectionless approach?

- Lower latency and reduced overhead
- Enhanced security
- Reliable and ordered data delivery
- Greater scalability and efficiency

Correct Answer: C

Q215. Which TCP flag is used to indicate the end of data transmission and to initiate connection termination?

- ACK (Acknowledgment)
- SYN (Synchronize)
- RST (Reset)
- FIN (Finish)

Correct Answer: D

Q216. In TCP, what is the purpose of the ACK (Acknowledgment) flag?

- To acknowledge successful data receipt
- To request data retransmission
- To reset the connection
- To synchronize sequence numbers

Correct Answer: A

Q217. During the TCP three-way handshake, which side initiates the process by sending a SYN (Synchronize) segment?

- The server
- The client
- Both the server and client

- Neither the server nor client

Correct Answer: B

Q218. What is the purpose of the SYN-ACK (Synchronize-Acknowledgment) segment sent by the receiving device in the TCP three-way handshake?

- To acknowledge the receipt of data and continue communication
- To reset the connection
- To initiate the connection termination
- To request data retransmission

Correct Answer: A

Q219. What is the final step in the TCP three-way handshake process after both sides have exchanged SYN and ACK segments?

- Data transmission can begin
- The connection is terminated
- Data segmentation is performed
- An acknowledgment is sent

Correct Answer: A

Q220. In the UDP message format, what is the purpose of the source port number field?

- To identify the destination host
- To identify the source host
- To track the sequence number
- To specify the data length

Correct Answer: B

Q221. In TCP, what is the purpose of the Sequence Number field in the message header?

- To identify the destination port
- To track the number of packets received
- To keep track of the order of sent data
- To provide error detection

Correct Answer: C

Q222. In the TCP message format, what is the role of the Acknowledgment (ACK) flag?

- To acknowledge the receipt of data
- To reset the connection

- To indicate the end of the message
- To request data retransmission

Correct Answer: A

Q223. Which field in the UDP message format is used to perform error checking on the message header and data?

- Source port
- Destination port
- Checksum
- Length

Correct Answer: C

Q224. What is the primary goal of congestion control mechanisms in computer networks?

- To maximize network throughput
- To minimize packet loss and delays
- To increase the network's physical capacity
- To prioritize multimedia traffic

Correct Answer: B

Q225. Which QoS technique allows network administrators to assign higher or lower priorities to different types of traffic?

- Traffic shaping
- Packet switching
- Quality of Service (QoS)
- Error correction

Correct Answer: C

Q226. What is the primary metric used to measure the quality of voice and video communication in QoS evaluations?

- Packet loss rate
- Round-trip time (RTT)
- Jitter
- Mean Opinion Score (MOS)

Correct Answer: D

Q227. What is a common technique for mitigating network congestion by temporarily holding packets before transmission?

- Quality of Service (QoS)
- Traffic shaping
- Congestion control
- Jitter control

Correct Answer: B

Q228. Which DNS record type is used to associate an IP address with a domain name?

- MX (Mail Exchanger)
- PTR (Pointer)
- A (Address)
- CNAME (Canonical Name)

Correct Answer: C

Q229. What is the purpose of a DNS recursive query?

- To obtain a DNS cache entry
- To query the root DNS server
- To resolve the entire DNS hierarchy
- To secure email communications

Correct Answer: C

Q230. In DNS, what does an authoritative DNS server do?

- It provides DNS caching services
- It has the final say on the DNS resolution for a domain
- It encrypts DNS queries
- It manages email traffic

Correct Answer: B

Q231. What does the term "DNS propagation" refer to in DNS management?

- The process of encrypting DNS records
- The delay in DNS record updates propagating across the Internet
- The speed of DNS query resolution
- The process of securing email communication

Correct Answer: B

Q232. How does remote logging contribute to security incident detection and response?

- By encrypting log entries

- By providing real-time access to log data
- By managing email communication
- By routing network traffic

Correct Answer: B

Q233. What are the basic components of an email message?

- Subject, recipient, and attachment
- Sender, message body, and attachment
- Encryption key, header, and footer
- DNS server, firewall, and router

Correct Answer: B

Q234. What is the significance of email encryption in ensuring message confidentiality?

- It compresses email attachments
- It protects email contents from unauthorized access
- It manages email routing
- It provides secure email storage

Correct Answer: B

Q235. What is the concept of email forwarding, and how is it used?

- It sends email to multiple recipients
- It redirects received emails to another address
- It encrypts email contents
- It optimizes email routing

Correct Answer: B

Q236. What is spam email, and how do email providers combat spam?

- Unwanted email messages
- Encrypted email messages
- Email encryption keys
- Email server logs

Correct Answer: A

Q237. What is FTP (File Transfer Protocol), and what is its primary purpose?

- A text encryption protocol
- A network protocol for transferring files

- A method of email delivery
- A data compression technique

Correct Answer: B

Q238. What role do passive and active modes play in FTP connections?

- They manage FTP encryption keys
- They define how data connections are established
- They compress email headers
- They optimize email routing

Correct Answer: B

Q239. What is FTPS, and how does it enhance FTP security?

- It encrypts FTP traffic
- It optimizes email delivery
- It manages email logs
- It encrypts email headers

Correct Answer: A

Q240. What is the World Wide Web (WWW), and how does it function in modern communication?

- A system of encrypted emails
- A global network of interconnected web pages
- A method of email delivery
- A file storage protocol

Correct Answer: B

Q241. How are web addresses (URLs) structured, and what do they represent?

- They use IP addresses for encryption
- They indicate the email server's location
- They specify web page content
- They define FTP server addresses

Correct Answer: C

Q242. What is the significance of HTTP (Hypertext Transfer Protocol) in web communication?

- It encrypts email headers
- It facilitates the transfer of web page data
- It compresses email attachments

- It manages email logs

Correct Answer: B

Q243. What is a URL (Uniform Resource Locator), and how does it relate to HTTP?

- It is an email attachment format
- It defines the structure of web pages
- It specifies web page addresses
- It encrypts email headers

Correct Answer: C

Q244. How does caching work in HTTP, and what benefits does it offer in web browsing?

- It optimizes email delivery
- It improves web page loading times
- It encrypts email contents
- It manages email attachments

Correct Answer: B

Q245. What is SMTP (Simple Mail Transfer Protocol), and what is its primary purpose?

- A protocol for secure email delivery
- A protocol for transferring files
- A protocol for web communication
- A method of email encryption

Correct Answer: A

Q246. What are SMTP servers (MTAs), and how do they handle email routing and delivery?

- They are web servers for email storage
- They manage email logs
- They relay email messages
- They compress email headers

Correct Answer: C

Q247. What are the SMTP port numbers (e.g., 25, 587), and how are they used in email transmission?

- They are email attachment formats
- They are used to encrypt email data
- They indicate email destinations

- They specify email server addresses

Correct Answer: C

Q248. How does SNMP enable the monitoring and management of network devices and resources?

- It encrypts email contents
- It uses email attachments to control devices
- It retrieves and configures data
- It optimizes email routing

Correct Answer: C

Q249. Explain the roles of SNMP traps and informs in network management and alerting.

- They are email headers for web pages
- Traps are unsolicited alerts, informs
- They are email headers for SNMP messages
- They encrypt email attachments

Correct Answer: B

Q250. How does SNMP version 3 enhance security and authentication in network management compared to earlier versions?

- It encrypts SNMP messages
- It optimizes email delivery
- It uses email headers for authentication
- It compresses email headers

Correct Answer: A

Q251. How does SNMP contribute to proactive network management and troubleshooting?

- It uses email encryption methods
- It provides real-time monitoring and alerts
- It compresses email attachments
- It optimizes email routing

Correct Answer: B

Q252. What role do firewalls play in network security, and how do they filter network traffic?

- They ensure data confidentiality
- They optimize network performance
- They prevent unauthorized access

- They track network logs for errors

Correct Answer: C

Q253. Explain the concept of incident response in network security and its importance in mitigating security breaches.

- It enhances user authentication
- It minimizes network performance impact
- It detects and responds to incidents
- It optimizes network routing

Correct Answer: C

Q254. What is the primary goal of cryptography in network security?

- To minimize network performance impact
- To ensure data confidentiality
- To optimize network routing
- To restrict unauthorized access

Correct Answer: B

Q255. Explain the difference between symmetric and asymmetric encryption, and when is each used in network security?

- Symmetric encryption uses one key
- Asymmetric encryption uses one key pair
- Symmetric encryption uses two keys
- Asymmetric encryption uses two keys

Correct Answer: C

Q256. What is a cryptographic hash function, and how is it used in data integrity verification and password storage?

- It ensures data confidentiality
- It improves network performance
- It verifies data integrity
- It restricts unauthorized access

Correct Answer: C

Q257. What are some common challenges in implementing cryptography in network security, and how can they be mitigated?

- Lack of encryption algorithms
- Key management issues
- Slow network performance
- Lack of user authentication

Correct Answer: B

Q258. Explain the concept of a digital signature algorithm and how it works.

- It encrypts the entire message
- It verifies the sender's identity
- It creates a unique hash of the message
- It improves network performance

Correct Answer: B

Q259. How does the recipient of a digitally signed message verify the signature's authenticity and integrity?

- By comparing it to a public key
- By decrypting the message using a private key
- By hashing the message and comparing hashes
- By optimizing network routing

Correct Answer: B

Q260. What challenges can arise in implementing digital signatures, and how can they be mitigated for secure data transmission?

- Lack of key management practices
- Slow network performance
- Insufficient user authentication
- Inadequate encryption algorithms

Correct Answer: A

Q261. What is the difference between TCP and UDP?

- They are two different versions of the same protocol.
- Both are connectionless protocols.
- TCP is connection-oriented and provides reliable data delivery, while UDP is connectionless and offers lower overhea
- TCP and UDP are the same and can be used interchangeably.

Correct Answer: c

Q262. What is the primary purpose of the Stop and Wait protocol in data link layer communication?

- Minimize latency
- Maximize throughput
- Ensure error detection
- Achieve reliable data transfer

Correct Answer: D

Q263. What does the receiver do upon successfully receiving a data frame in the Stop and Wait protocol?

- Sends a negative acknowledgment (NAK)
- Waits for the next data frame
- Sends an acknowledgment (ACK) to the sender
- Requests retransmission of the data frame

Correct Answer: C

Q264. In the Stop and Wait protocol, what happens if the sender does not receive an acknowledgment (ACK) within a certain time frame?

- It continues sending data frames
- It sends a negative acknowledgment (NAK)
- It waits indefinitely for the ACK
- It retransmits the same data frame

Correct Answer: D

Q265. In the Stop and Wait protocol, what is the purpose of sequence numbers attached to data frames?

- To identify the sender
- To ensure frame integrity
- To avoid duplicate frames
- To enable parallel transmission

Correct Answer: C

Q266. What is the Stop and Wait protocol's impact on the effective data transmission rate compared to the overall channel capacity?

- It achieves 100% efficiency
- It achieves nearly 100% efficiency
- It achieves 50% efficiency
- It achieves less than 50% efficiency

Correct Answer: D

Q267. What is the main advantage of the Stop and Wait protocol in noiseless channels?

- Minimal latency
- High throughput
- Simple implementation
- Support for parallel transmission

Correct Answer: C

Q268. In a noisy channel, what is the primary challenge that data link layer protocols like ARQ aim to address?

- Minimizing latency
- Ensuring error-free data transmission
- Maximizing throughput
- Reducing the number of frames transmitted

Correct Answer: B

Q269. What action does the sender take in the Stop and Wait protocol upon receiving a negative acknowledgment (NAK) from the receiver?

- Resends the current frame
- Advances to the next frame
- Pauses transmission
- Requests retransmission of the frame

Correct Answer: A

Q270. In Go-Back-N ARQ, if the receiver detects an error in a frame, what action is taken regarding subsequent frames in the window?

- All subsequent frames are discarded
- Only the erroneous frame is discarded
- All frames from the current frame onward are discarded
- The receiver continues accepting frames in the window

Correct Answer: A

Q271. What happens if a frame is lost or corrupted in the Go-Back-N protocol, and the receiver acknowledges subsequent frames?

- The sender resends only the lost or corrupted frame
- All frames following the lost or corrupted frame are discarded

- The sender waits for a timeout and retransmits the entire window
- The receiver retransmits the acknowledgment

Correct Answer: A

Q272. What characteristic of Selective Repeat ARQ allows it to recover from errors in any frame within the window without affecting the rest?

- Independent acknowledgment for each frame
- Sliding window approach
- Simplicity
- Reduced acknowledgment overhead

Correct Answer: A

Q273. What is the primary function of the Network Layer in the OSI model?

- Ensuring error-free data transmission
- Packet forwarding and routing
- Data link establishment and management
- Session establishment and termination

Correct Answer: B

Q274. What is the purpose of an IP address in computer networking?

- Identifying the location of a device
- Encrypting data for secure transmission
- Controlling access to the internet
- Determining the speed of data transmission

Correct Answer: A

Q275. What does the subnet mask in an IPv4 address indicate?

- The host portion of the IP address
- The network portion of the IP address
- The number of available IP addresses
- The broadcast address of the network

Correct Answer: B

Q276. What is the purpose of Network Address Translation (NAT) in IPv4?

- Encrypting data for secure transmission
- Converting private IP addresses to public addresses

- Determining the speed of data transmission
- Resolving domain names to IP addresses

Correct Answer: B

Q277. What is the function of the default gateway in a network configuration?

- Assigning IP addresses to devices
- Providing access to external networks
- Filtering incoming network traffic
- Managing DNS resolution requests

Correct Answer: B

Q278. In IPv4 addressing, what is the purpose of the subnetting process?

- Increasing the number of available IP addresses
- Improving network security by hiding IP addresses
- Grouping IP addresses by geographic location
- Enhancing the speed of data transmission

Correct Answer: A

Q279. Which field in the IPv4 header is used to indicate the time-to-live (TTL) of a packet?

- Protocol
- Destination IP Address
- Source IP Address
- Time-to-Live (TTL)

Correct Answer: D

Q280. In Distance Vector Routing (DVR), what is the primary drawback known as the "count-to-infinity" problem?

- Slow convergence
- Routing loops
- Limited scalability
- Inefficient bandwidth utilization

Correct Answer: B

Q281. Which routing algorithm employs a "link state advertisement" (LSA) flooding mechanism to share routing information with all routers in a network?

- Distance Vector Routing (DVR)

- Link State Routing (LSR)
- Static Routing
- Default Routing (DR)

Correct Answer: B

Q282. In Link State Routing (LSR), what information is included in the link state advertisement (LSA) packets?

- Routing tables and hop counts of neighboring routers
- Network topology and link status
- Encryption keys and access permissions
- IP addresses of all devices in the network

Correct Answer: B

Q283. In the context of routing algorithms, what is the purpose of a routing table?

- To store information about the network topology
- To list all available IP addresses
- To determine the physical distance between routers
- To provide encryption for data in transit

Correct Answer: A

Q284. Which routing algorithm is commonly used in interior routing within autonomous systems and relies on routers broadcasting routing tables to neighbors?

- Distance Vector Routing (DVR)
- Link State Routing (LSR)
- Static Routing
- Default Routing (DR)

Correct Answer: A

Q285. What is the main function of IGMP (Internet Group Management Protocol) in network communications?

- Managing router access control lists (ACLs)
- Allowing devices to join or leave multicast groups
- Providing secure remote access
- Assigning unique IP addresses to devices within a network

Correct Answer: B

Q286. Which of the following is a key advantage of IPv6 over IPv4?

- Longer addresses with fewer address bits
- More efficient header format
- Less security and encryption options
- Incompatibility with older networking equipment

Correct Answer: B

Q287. How does IPv6 address the limitation of IPv4's address exhaustion issue?

- By increasing the length of IP addresses
- By reducing the number of devices per network
- By using NAT (Network Address Translation)
- By implementing IP address sharing between devices

Correct Answer: A

Q288. Which transition mechanism facilitates the coexistence of IPv4 and IPv6 in a network by encapsulating IPv6 packets within IPv4 packets?

- Dual-stack
- Tunneling
- IPv6 over IPv4 (6over4)
- Network Address Translation (NAT)

Correct Answer: B

Q289. Which of the following IPv6 address formats represents a loopback address used for testing on the local device?

- 2001:db8::/32
- ::1/128
- ff00::/8
- fe80::/10

Correct Answer: B

Q290. How many bits are reserved for the network portion in a Class A IP address?

- 8 bits
- 16 bits
- 24 bits
- 32 bits

Correct Answer: A

Q291. What does subnetting allow network administrators to do?

- Assign multiple IP addresses to a single host
- Create smaller, more manageable networks
- Increase the size of the IP address pool
- Eliminate the need for routers in the network

Correct Answer: B

Q292. In a subnetted network, what is the role of a broadcast address?

- To identify the default gateway for the network
- To represent all hosts within a subnet
- To forward data between subnets
- To encrypt data during transmission

Correct Answer: B

Q293. What is the CIDR notation for a subnet mask of 255.255.255.240?

- /24
- /26
- /28
- /30

Correct Answer: C

Q294. Which routing algorithm is commonly used for finding the shortest path in a network?

- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Correct Answer: A

Q295. What is the primary advantage of dynamic routing algorithms over static routing?

- Reduced administrative overhead
- Simplicity and ease of configuration
- High security due to manual updates
- Lower network scalability

Correct Answer: A

Q296. Which routing algorithm calculates the shortest path based on the cumulative link costs?

- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Correct Answer: A

Q297. Which dynamic routing protocol uses a distance-vector algorithm and broadcasts routing updates?

- OSPF (Open Shortest Path First)
- RIP (Routing Information Protocol)
- BGP (Border Gateway Protocol)
- EIGRP (Enhanced Interior Gateway Routing Protocol)

Correct Answer: B

Q298. What is the primary disadvantage of static routing in a large and complex network?

- High computational overhead
- Difficulty in initial configuration
- Inability to adapt to network changes
- High resource utilization

Correct Answer: C

Q299. Which version of RIP sends routing updates using broadcast messages?

- RIP v1
- RIP v2
- Both RIP v1 and v2
- Neither RIP v1 nor v2

Correct Answer: A

Q300. In RIP v2, what is the primary enhancement over RIP v1?

- Support for classless routing
- Faster convergence
- Compatibility with IPv6
- Increased hop count limit

Correct Answer: A

Q301. What action does a RIP router take if it receives a route update with a higher metric than its own?

- It discards the route update
- It updates its routing table
- It compares the source IP address
- It sends an acknowledgment back to the sender

Correct Answer: B

Q302. What is the administrative distance of RIP?

- 90
- 100
- 110
- 120

Correct Answer: C

Q303. In OSPF, what is an Autonomous System (AS)?

- A group of routers using OSPF
- A collection of routers
- A network with a single administrator
- A type of routing algorithm

Correct Answer: C

Q304. Which OSPF area type connects to the backbone area (Area 0)?

- Stub area
- Backbone area
- Transit area
- Virtual link area

Correct Answer: C

Q305. Which OSPF area is typically used to connect multiple OSPF areas together?

- Backbone area
- Transit area
- Stub area
- Virtual link area

Correct Answer: A

Q306. OSPF uses a cost metric to determine the best path to a destination. What does this metric represent?

- Bandwidth
- Delay
- Hop count
- Reliability

Correct Answer: A

Q307. What is OSPF's default administrative distance?

- 90
- 100
- 110
- 120

Correct Answer: A

Q308. EIGRP is a Cisco-proprietary routing protocol. What feature of EIGRP allows it to converge quickly after topology changes?

- DUAL (Diffusing Update Algorithm)
- Hello protocol
- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)

Correct Answer: A

Q309. What is the primary advantage of EIGRP over distance-vector routing protocols like RIP?

- Fast convergence
- Simplicity
- Compatibility with other routing protocols
- Support for large-scale networks

Correct Answer: A

Q310. In EIGRP, what type of packets are used to establish and maintain neighbor adjacencies?

- Update packets
- Hello packets
- Query packets
- Acknowledgment packets

Correct Answer: B

Q311. EIGRP supports both IPv4 and IPv6. Which protocol does EIGRP use for IPv4 routing?

- EIGRPv4
- EIGRP-NG (Next Generation)
- EIGRPv6
- EIGRP-IPv4

Correct Answer: A

Q312. What is the maximum hop count allowed in EIGRP for a valid route?

- 10 hops
- 15 hops
- 16 hops
- 100 hops

Correct Answer: B

Q313. In BGP, what is the primary function of the Autonomous System (AS) number?

- To identify the router's manufacturer
- To specify the router's location
- To uniquely identify the router in the AS
- To determine the router's cost to reach a destination

Correct Answer: C

Q314. What is the primary difference between iBGP and eBGP in BGP routing?

- iBGP is used within an AS, and eBGP is used between different ASes
- iBGP uses a simpler metric than eBGP
- eBGP is used for internal routing, while iBGP is used for external routing
- iBGP uses a different protocol stack than eBGP

Correct Answer: A

Q315. What is the purpose of the BGP "path attribute"?

- To specify the AS path that a route has traversed
- To indicate the route's cost
- To determine the route's administrative distance
- To encrypt BGP routing updates

Correct Answer: A

Q316. In BGP, what is a prefix or network prefix?

- The identifier of a BGP session
- A unique identifier for a router
- A summary of IP addresses within an AS
- A route to a destination network

Correct Answer: D

Q317. BGP is commonly used at the edge of the Internet to exchange routing information between ISPs. What is this type of BGP deployment called?

- Core BGP
- Border BGP
- Edge BGP
- Intermediate BGP

Correct Answer: B

Q318. Which BGP message type is used to establish and maintain BGP neighbor relationships?

- OPEN message
- UPDATE message
- KEEPALIVE message
- NOTIFICATION message

Correct Answer: A

Q319. What is the primary benefit of BGP's path vector routing algorithm over distance-vector or link-state algorithms?

- Loop prevention
- Faster convergence
- Support for classless routing
- Simplicity

Correct Answer: A

Q320. Which Transport Layer service allows multiple applications on the same device to share the network connection simultaneously?

- Segmentation
- Error correction
- Multiplexing
- Flow control

Correct Answer: C

Q321. Which Transport Layer service is responsible for controlling the rate of data exchange between sender and receiver to prevent congestion?

- Segmentation
- Multiplexing
- Flow control
- Error correction

Correct Answer: C

Q322. In the context of Transport Layer services, what is flow control?

- Controlling data flow between devices
- Ensuring error-free data transfer
- Multiplexing data streams
- Encrypting data for security

Correct Answer: A

Q323. When using the Transport Layer, what is the purpose of error detection and correction?

- Ensuring timely delivery of data
- Providing end-to-end encryption
- Detecting and correcting errors
- Managing network resources

Correct Answer: C

Q324. In a TCP connection, what role does the ACK (Acknowledgment) flag play during normal data transmission?

- It acknowledges successful data receipt
- It resets the connection
- It synchronizes sequence numbers
- It requests data retransmission

Correct Answer: A

Q325. During the TCP three-way handshake, if the SYN-ACK segment sent by the server is lost or not received by the client, what happens?

- The client retransmits the SYN segment
- The server sends a RST segment
- The server initiates the connection termination
- The connection remains in an undefined state

Correct Answer: A

Q326. What is the purpose of Quality of Service (QoS) mechanisms in network communication?

- To ensure all traffic is treated equally
- To prioritize traffic based on its importance
- To reduce network latency and jitter
- To increase the network's physical capacity

Correct Answer: B

Q327. What is the purpose of admission control in Quality of Service (QoS) management?

- To admit all incoming traffic
- To prioritize high-bandwidth applications
- To block all incoming traffic
- To ensure network resources are not overcommitted

Correct Answer: D

Q328. How does DNS contribute to load balancing for websites with multiple servers?

- By encrypting user data
- By redirecting DNS queries to the closest server
- By assigning the same IP to all servers
- By managing email routing

Correct Answer: B

Q329. What is the role of DNSSEC (DNS Security Extensions) in DNS?

- To encrypt DNS traffic
- To authenticate and secure DNS data
- To control DNS cache size
- To optimize email delivery

Correct Answer: B

Q330. What is remote logging, and why is it important in network management?

- It's a type of encryption
- It allows monitoring of network events from a remote location
- It is a file storage protocol
- It manages email logs

Correct Answer: B

Q331. What are some common challenges associated with remote logging in distributed environments?

- Inadequate encryption of logs
- Difficulty in accessing logs remotely
- Inefficient handling of email logs
- Limited log storage capacity

Correct Answer: B

Q332. What is log rotation in the context of remote logging, and why is it important?

- A technique for encrypting logs
- A process of periodically archiving and replacing log files
- A method for prioritizing email logs
- A mechanism for load balancing

Correct Answer: B

Q333. What is the syslog protocol, and how is it used for remote logging?

- A file storage protocol
- A network protocol for sending log messages
- An encryption method for logs
- A tool for managing email logs

Correct Answer: B

Q334. How does remote logging facilitate troubleshooting network issues?

- By providing encryption keys
- By storing detailed logs of network events
- By optimizing email routing
- By securing log files

Correct Answer: B

Q335. What is the significance of log correlation in remote logging analysis?

- It ensures email privacy
- It links related log entries to reveal a complete event
- It improves network performance
- It encrypts log data

Correct Answer: B

Q336. How can remote logging be used to monitor user activity and access control?

- By monitoring email attachments
- By tracking logins and access patterns
- By encrypting log data
- By routing network traffic

Correct Answer: B

Q337. Describe the role of log compression in optimizing remote log storage.

- It manages network bandwidth
- It reduces the size of log files for efficient storage
- It encrypts log entries
- It enhances email delivery

Correct Answer: B

Q338. What is electronic mail (email), and how does it function in modern communication?

- A method of network encryption
- A system for sending text messages electronically
- A file storage protocol
- A communication method using digital envelopes

Correct Answer: B

Q339. How does passive FTP differ from active FTP in terms of data transfer?

- Passive FTP uses email for transfers
- Active FTP requires manual intervention
- Passive FTP is slower
- Active FTP requires encryption

Correct Answer: C

Q340. Explain the concept of FTP authentication.

- It encrypts file transfers
- It verifies the identity of users
- It compresses email attachments
- It optimizes email routing

Correct Answer: B

Q341. What is anonymous FTP, and why is it used?

- An encryption method for FTP
- A type of FTP server for secure transfers
- FTP access without user authentication
- A method of email forwarding

Correct Answer: C

Q342. How do FTP clients and FTP servers interact in a typical FTP session?

- Clients send email attachments
- Clients initiate file transfers to servers
- Servers send email logs
- Servers access user email folders

Correct Answer: B

Q343. Who is credited with inventing the World Wide Web, and when was it first introduced?

- Bill Gates in 1995
- Tim Berners-Lee in 1989
- Ray Tomlinson in the 1970s
- Mark Zuckerberg in 2004

Correct Answer: B

Q344. What are web browsers, and how do they work?

- Software for encrypting emails
- Applications for accessing and displaying web pages
- Servers for email routing
- Devices for FTP file transfers

Correct Answer: B

Q345. Explain the difference between a website and a web page.

- A website is a single web address
- A website is a collection of web pages
- A web page is an encrypted file
- A web page is a DNS server

Correct Answer: B

Q346. What is the role of CSS (Cascading Style Sheets) in web design?

- To secure email attachments
- To define the layout and appearance of web pages
- To optimize email delivery
- To encrypt email data

Correct Answer: B

Q347. How does JavaScript enhance web interactivity and functionality?

- It manages email routing
- It provides secure email access
- It allows dynamic web content
- It compresses email headers

Correct Answer: C

Q348. What role does HTTP play in web browsing and accessing web pages?

- It encrypts email contents
- It manages email logs
- It facilitates web page retrieval
- It optimizes email routing

Correct Answer: C

Q349. How does HTTP handle hyperlinks and navigation between web pages?

- It encrypts email headers
- It uses email attachments to navigate
- It uses hyperlinks and URLs
- It encrypts email data

Correct Answer: C

Q350. Explain the concept of HTTP methods (GET, POST, PUT, DELETE, et) and their purposes.

- They are encryption algorithms for emails
- They define actions to perform on resources
- They manage email routing
- They compress email attachments

Correct Answer: B

Q351. What is the significance of HTTP status codes (e.g., 200, 404, 500) in web communication?

- They manage email attachments

- They facilitate email encryption
- They indicate the outcome of requests
- They optimize email delivery

Correct Answer: C

Q352. How does HTTPS (HTTP Secure) enhance web security compared to HTTP?

- It encrypts web page contents
- It optimizes email routing
- It manages email logs
- It uses email headers for navigation

Correct Answer: A

Q353. What is SMTP authentication, and why is it important for email security?

- It encrypts email contents
- It verifies the identity of email clients
- It manages email headers
- It compresses email attachments

Correct Answer: B

Q354. What is the purpose of SMTP relaying, and how does it work in email routing?

- It optimizes email delivery
- It forwards email messages
- It compresses email attachments
- It manages email logs

Correct Answer: B

Q355. How does SMTP handle email attachments, and what formats are commonly used for email attachments?

- It optimizes email routing
- It encrypts email data
- It uses various formats for attachments
- It manages email logs

Correct Answer: C

Q356. What are some common security challenges and solutions in SMTP email communication?

- Lack of email encryption

- Spam filtering and email authentication
- Excessive email attachment sizes
- Slow email delivery due to encryption

Correct Answer: B

Q357. What is SNMP (Simple Network Management Protocol), and what is its primary purpose?

- A protocol for secure email delivery
- A protocol for managing network devices
- A protocol for web communication
- A method of email encryption

Correct Answer: B

Q358. What are some common use cases for SNMP in network management, and how does it benefit IT professionals?

- Lack of email encryption
- Network monitoring, device configuration
- Excessive email attachment sizes
- Slow email delivery due to encryption

Correct Answer: B

Q359. What are the primary goals of network security services?

- Ensuring data confidentiality
- Minimizing network performance impact
- Reducing device costs
- Enhancing user authentication

Correct Answer: A

Q360. Which network security service is responsible for verifying the identity of users and devices?

- Data integrity
- Authentication
- Data encryption
- Intrusion detection systems (IDS)

Correct Answer: B

Q361. How does access control contribute to network security, and what types of access control are commonly used?

- It optimizes network routing
- It restricts unauthorized access
- It encrypts network traffic
- It compresses network logs

Correct Answer: B

Q362. What is the role of intrusion detection and prevention systems (IDS/IPS) in network security?

- They ensure data confidentiality
- They verify user identities
- They detect and respond to threats
- They optimize network performance

Correct Answer: C

Q363. How does network monitoring enhance security services, and what are some common tools used for monitoring?

- It improves user authentication
- It detects security incidents
- It encrypts network logs
- It minimizes network performance impact

Correct Answer: B

Q364. What is the significance of security policy enforcement in network security, and how is it implemented?

- It optimizes network routing
- It verifies user identities
- It restricts unauthorized access
- It ensures compliance with security policies

Correct Answer: D

Q365. How do cryptographic keys enhance the security of encrypted data, and what key management practices are important?

- Keys improve user authentication
- Keys are used to encrypt network traffic
- Keys verify the sender's identity
- Keys are stored securely

Correct Answer: B

Q366. What is the concept of a digital certificate, and how does it relate to public key infrastructure (PKI) in network security?

- Certificates improve user authentication
- Certificates encrypt network traffic
- Certificates verify data integrity
- Certificates optimize network routing

Correct Answer: A

Q367. What is the purpose of secure sockets layer (SSL) and transport layer security (TLS) protocols in network encryption?

- They ensure data confidentiality
- They restrict unauthorized access
- They optimize network performance
- They verify user identities

Correct Answer: A

Q368. What is the significance of a digital certificate in the context of digital signatures?

- It encrypts network traffic
- It verifies the sender's identity
- It optimizes network performance
- It restricts unauthorized access

Correct Answer: B

Q369. What is the difference between a digital signature and a digital certificate in network security?

- Digital signatures verify sender authenticity
- Digital certificates verify data integrity
- Digital signatures use symmetric keys
- Digital certificates encrypt network traffic

Correct Answer: A

Q370. How does a timestamp enhance the security of a digital signature?

- It improves user authentication
- It restricts unauthorized access
- It verifies the message's creation time
- It optimizes network routing

Correct Answer: C

Q371. What is the purpose of the Certificate Authority (CA) in digital signature validation, and how does it work?

- To encrypt the message
- To verify user identities
- To issue and manage digital certificates
- To optimize network performance

Correct Answer: C

Q372. In the TCP header, what field is used to specify the maximum segment size that a sender can handle?

- Acknowledgment Number
- Sequence Number
- Window Size
- Maximum Segment Size (MSS)

Correct Answer: D

Q373. Which field in the UDP header is optional and used for error checking when set to a non-zero value?

- Source Port
- Checksum
- Destination Port
- Length

Correct Answer: B

Q374. What is the purpose of the Urgent Pointer field in the TCP header?

- It specifies the source port number.
- It indicates the length of the header and dat
- It points to the urgent data in the TCP segment.
- It identifies the destination IP address.

Correct Answer: C

Q375. Which field in the TCP header is used to acknowledge the receipt of data and indicate the next expected sequence number?

- Sequence Number
- Acknowledgment Number
- Window Size

- Urgent Pointer

Correct Answer: B

Q376. In the UDP header, what is the purpose of the Length field?

- It stores the source port number.
- It specifies the acknowledgment number.
- It indicates the length of the UDP header and dat
- It identifies the destination IP address.

Correct Answer: C

Q377. What is the primary goal of congestion control in network communication?

- To maximize network throughput at all times.
- To minimize latency for all network traffi
- To maintain network stability and prevent congestion.
- To prioritize certain types of traffic over others.

Correct Answer: C

Q378. Which QoS technique allows network administrators to assign different priority levels to different types of network traffic?

- Traffic Shaping
- Traffic Policing
- Traffic Classification
- Traffic Engineering

Correct Answer: C

Q379. Which congestion control mechanism in TCP reduces the sender's transmission rate when congestion is detected?

- Slow Start
- Congestion Avoidance
- Fast Retransmit
- Selective Acknowledgment

Correct Answer: B

Q380. What is the primary purpose of Quality of Service (QoS) in networking?

- To provide network security and encryption.
- To minimize network latency and jitter.

- To manage and prioritize network traffi
- To determine the physical layout of network components.

Correct Answer: C

Q381. Which QoS parameter measures the variation in packet arrival times in a network?

- Latency
- Throughput
- Jitter
- Bandwidth

Correct Answer: C

Q382. Which Application Layer protocol is primarily responsible for translating human-readable domain names into IP addresses?

- HTTP
- DNS
- SMTP
- POP3

Correct Answer: B

Q383. What is the primary purpose of the FTP (File Transfer Protocol) in the Application Layer?

- Transferring files between client and server
- Resolving domain names to IP addresses
- Sending and receiving email messages
- Remote login and command execution

Correct Answer: A

Q384. Which protocol is used for retrieving email messages from a mail server to a client device, allowing users to read their emails?

- SMTP
- HTTP
- POP3
- DNS

Correct Answer: C

Q385. Which Application Layer protocol is responsible for the delivery of web pages from web servers to web browsers?

- SMTP
- FTP
- HTTP
- Telnet

Correct Answer: C

Q386. What is the primary purpose of the IMAP (Internet Message Access Protocol) in the Application Layer?

- To transfer files between clients and servers
- To retrieve email messages from a server while keeping them on the server
- To resolve domain names to IP addresses
- To secure web communication

Correct Answer: B

Q387. Which Application Layer protocol is commonly used for remote login and terminal emulation on remote systems?

- SMTP
- Telnet
- FTP
- POP3

Correct Answer: B

Q388. What does the SNMP (Simple Network Management Protocol) in the Application Layer primarily enable?

- File transfers between devices on a network
- Secure web communication
- Management and monitoring of network devices
- Real-time communication, including voice and video calls

Correct Answer: C

Q389. Which Application Layer protocol is used for the exchange of email messages between mail servers?

- SMTP
- HTTP
- SIP
- SNMP

Correct Answer: A

Q390. What is the primary function of the SSH (Secure Shell) protocol in the Application Layer?

- File transfer between client and server
- Email communication
- Secure remote login and command execution
- Resolving domain names to IP addresses

Correct Answer: C

Q391. Which Application Layer protocol is used for the retrieval and management of directory information in a network?

- LDAP (Lightweight Directory Access Protocol)
- HTTP
- SIP
- SNMP

Correct Answer: A

Q392. Which security service ensures that data is not altered during transmission and can be relied upon as genuine?

- Authentication
- Integrity
- Confidentiality
- Availability

Correct Answer: B

Q393. Which cryptographic key is used for encrypting data in symmetric-key cryptography?

- Public Key
- Private Key
- Session Key
- Digital Signature

Correct Answer: C

Q394. Which cryptographic technique involves the use of a pair of keys, one for encryption and one for decryption, and is commonly used in asymmetric encryption?

- Hashing
- Digital Signatures
- Public Key Cryptography
- Symmetric Key Cryptography

Correct Answer: C

Q395. What security service ensures that only authorized users or systems have access to data and network resources?

- Confidentiality
- Data Integrity
- Authentication
- Non-repudiation

Correct Answer: C

Q396. What is the maximum number of bytes in the TCP header

- 16 bytes
- 20 bytes
- 24 bytes
- 28 bytes

Correct Answer: B

Q397. Which field in the TCP header is used for flow control and specifies the number of bytes the sender can transmit before receiving an acknowledgment?

- Acknowledgment Number
- Sequence Number
- Window Size
- Urgent Pointer

Correct Answer: C

Q398. In the UDP header, what is the purpose of the Checksum field?

- It stores the source port number.
- It provides error-checking for the entire UDP datagram.
- It indicates the length of the UDP header and dat
- It identifies the destination IP address.

Correct Answer: B

Q399. Which field in the TCP header is used to ensure the integrity of the header and data?

- Source Port
- Checksum
- Acknowledgment Number

- Urgent Pointer

Correct Answer: B

Q400. What is the purpose of the Sequence Number field in the TCP header?

- It identifies the source port.
- It specifies the acknowledgment number.
- It provides error-checking for the header and dat
- It helps in reordering and reassembling segments at the receiver.

Correct Answer: D

Q401. What is the primary goal of congestion control in computer networking?

- To maximize network throughput at all times.
- To minimize the delay and latency in the network.
- To prevent network congestion and maintain network stability.
- To prioritize certain types of traffic over others.

Correct Answer: C

Q402. Which congestion control algorithm is commonly used in TCP to detect and respond to network congestion?

- Leaky Bucket
- Token Bucket
- Slow Start
- Quality of Service (QoS)

Correct Answer: C

Q403. What is Quality of Service (QoS) in networking?

- A protocol used for routing data packets.
- A technique for compressing data to reduce congestion.
- A set of techniques and mechanisms to manage and prioritize network traffi
- A method for error checking and correction in data transmission.

Correct Answer: C

Q404. In QoS, what does the term "Traffic Shaping" refer to?

- The process of detecting and reacting to network congestion.
- The process of allocating bandwidth to different types of traffi
- The process of controlling the flow of traffic to conform to a specified profile.

- The process of encrypting network traffic for security.

Correct Answer: C

Q405. Which of the following is NOT a commonly used QoS parameter for traffic classification and prioritization?

- Delay
- Packet Size
- Throughput
- Jitter

Correct Answer: B

Q406. Which layer of the OSI model is responsible for providing network services directly to end-users or applications?

- Physical Layer
- Data Link Layer
- Transport Layer
- Application LAyer

Correct Answer: D

Q407. What is the primary function of the Application Layer in the OSI model?

- Data encapsulation and framing
- Error detection and correction
- User interface and data access
- Routing and path determination

Correct Answer: C

Q408. Which protocol is commonly used for sending and receiving email messages over the Internet?

- SMTP
- HTTP
- FTP
- DNS

Correct Answer: A

Q409. What is the primary purpose of the HTTP protocol?

- File transfer

- Email communication
- Web page retrieval
- Remote login

Correct Answer: C

Q410. Which protocol is used for secure data transmission over the web, ensuring confidentiality and data integrity?

- HTTP
- FTP
- SMTP
- HTTPS

Correct Answer: D

Q411. Which Application Layer protocol is used for transferring files between a client and a server over a network?

- SMTP
- Telnet
- FTP
- POP3

Correct Answer: C

Q412. Which Application Layer protocol is commonly used for remote login and command execution on remote servers?

- HTTP
- Telnet
- SMTP
- FTP

Correct Answer: B

Q413. What is the primary purpose of the DNS (Domain Name System) protocol in the Application Layer?

- Transferring files between clients and servers
- Resolving human-readable domain names to IP addresses
- Sending and receiving email messages
- Secure web communication

Correct Answer: B

Q414. Which Application Layer protocol is responsible for the retrieval of email messages from a mail server to a client device?

- FTP
- HTTP
- POP3
- IMAP

Correct Answer: C

Q415. Which Application Layer protocol is used for real-time communication, including voice and video calls, over the Internet?

- SMTP
- HTTP
- SIP
- SNMP

Correct Answer: C

Q416. Which network security service ensures that data is not disclosed to unauthorized users?

- Authentication
- Integrity
- Confidentiality
- Availability

Correct Answer: C

Q417. What is the primary purpose of cryptography in network security?

- To prevent unauthorized access to a network
- To protect data from being altered during transmission
- To authenticate users and devices
- To detect and respond to network intrusions

Correct Answer: B

Q418. Which cryptographic key is used for both encryption and decryption in symmetric-key cryptography?

- Public Key
- Private Key
- Session Key
- Digital Signature

Correct Answer: C

Q419. What is a digital signature primarily used for in network security?

- Encrypting data for secure transmission
- Verifying the identity of the sender and ensuring data integrity
- Protecting data from unauthorized access
- Scanning for malware and viruses

Correct Answer: B

Q420. Which cryptographic technique involves the use of two keys, one for encryption and one for decryption, and is commonly used in asymmetric encryption?

- Hashing
- Digital Signatures
- Public Key Cryptography
- Symmetric Key Cryptography

Correct Answer: C

Q421. Which field in the IP header is used for ensuring the integrity of the packet during transmission?

- DES (Data Encryption Standard)
- AES (Advanced Encryption Standard)
- RSA (Rivest-Shamir-Adleman)
- MD5 (Message Digest 5)

Correct Answer: C

Q422. In DNS, what is the purpose of a CNAME (Canonical Name) record?

- To map an alias or nickname to a canonical (true) domain name
- To specify the mail server responsible for receiving email messages
- To indicate the authoritative DNS server for a domain
- To define the start of a zone of authority in the DNS hierarchy

Correct Answer: A

Q423. In email terminology, what is a "mail relay" or "SMTP relay"?

- A system that automatically sends email responses
- An email client application
- A mail server that forwards email messages to their destinations
- A type of email attachment

Correct Answer: C

Q424. In HTTP, what is the purpose of the "Referer" header field in an HTTP request?

- To specify the URL of the current web page
- To indicate the encoding used for the request body
- To identify the previous web page from which the request was initiated
- To define the content type of the response

Correct Answer: C

Q425. In SMTP, what role does the "MX record" play in the email delivery process?

- It specifies the sender's email address
- It defines the email server's IP address
- It identifies the recipient's mail server for a given domain
- It indicates the type of encryption used for email transmission

Correct Answer: C

Q426. In SNMP, what does the term "OID" (Object Identifier) refer to?

- A network device's IP address
- A unique identifier for a managed object in the MIB
- The SNMP version number used for communication
- A specific SNMP security credential

Correct Answer: B

Q427. In the context of network security, what does the term "access control" refer to?

- Controlling the physical access to network devices
- Controlling user privileges and permissions to network resources
- Monitoring network traffic for suspicious activities
- Encrypting sensitive data during transmission

Correct Answer: B

Q428. In the context of network security, what is the primary purpose of an Intrusion Prevention System (IPS)?

- To monitor network traffic for security incidents
- To identify and respond to security incidents
- To prevent security incidents from occurring
- To encrypt data for secure transmission

Correct Answer: C

Q429. What does Quality of Service (QoS) in computer networks refer to?

- The speed of data transmission in a network
- The reliability of network connections
- The ability to prioritize and control network traffic to meet specific service requirements
- The physical security of network infrastructure

Correct Answer: C

Q430. What does the term "digital signature" refer to in cryptography?

- A code that hides the original message
- A method for encrypting data
- A unique identifier for a network device
- A cryptographic technique to verify the authenticity and integrity of a message

Correct Answer: D

Q431. What is the primary benefit of centralizing log management through remote logging?

- It reduces the need for network security measures.
- It simplifies log analysis and troubleshooting.
- It eliminates the need for network monitoring.
- It increases network performance.

Correct Answer: B

Q432. What is the primary purpose of an email "alias" or "nickname"?

- To specify the email recipient's location on the internet
- To provide an alternative email address for the same recipient
- To categorize emails into folders
- To indicate the importance level of an email

Correct Answer: B

Q433. What is the primary purpose of HTTP in computer networks?

- To transfer files between a client and a server
- To exchange emails and messages
- To browse websites and retrieve web pages
- To manage network security

Correct Answer: C

Q434. What is the primary purpose of S/MIME (Secure/Multipurpose Internet Mail Extensions) in email communication?

- To filter spam emails
- To provide end-to-end encryption and digital signatures for email messages
- To compress email attachments
- To improve email server performance

Correct Answer: B

Q435. What is the primary role of SMTP in computer networks?

- To transfer files between client and server
- To manage network security
- To exchange email messages between clients and servers
- To browse websites and retrieve web pages

Correct Answer: C

Q436. What is the purpose of a web browser's "cookie" in the context of the World Wide Web?

- To store passwords for websites
- To encrypt web traffic
- To remember user preferences and track user sessions
- To block unwanted advertisements

Correct Answer: C

Q437. What is the purpose of the "Cache-Control" header field in HTTP responses?

- To specify the maximum file size for caching
- To indicate whether the response can be cached and for how long
- To request the server to send a compressed response
- To define the character encoding for the response content

Correct Answer: B

Q438. Faster data transmission

- To specify the character encoding of the response content
- To indicate whether the response is compressed
- To define the maximum file size for caching
- To identify the type of content being sent

Correct Answer: D

Q439. What is the purpose of the HTML (Hypertext Markup Language) in the World Wide Web?

- To encrypt web pages for security
- To define the structure and content of web pages
- To manage domain name registrations
- To establish secure connections between web servers

Correct Answer: B

Q440. What is the role of a firewall in network security?

- To encrypt data for secure transmission
- To prevent unauthorized access to a network by filtering incoming and outgoing traffic
- To detect and respond to security incidents
- To provide real-time monitoring of network traffic

Correct Answer: B

Q441. Which cryptographic protocol is commonly used for securing web traffic by encrypting data between a web browser and a web server?

- SNMP (Simple Network Management Protocol)
- SSL/TLS (Secure Sockets Layer/Transport Layer Security)
- SMTP (Simple Mail Transfer Protocol)
- HTTP (Hypertext Transfer Protocol)

Correct Answer: B

Q442. Which email authentication mechanism helps prevent email spoofing and phishing by verifying the sender's domain in the email headers?

- SMTPS (SMTP Secure)
- SPF (Sender Policy Framework)
- POP3S (POP3 Secure)
- DMARC (Domain-based Message Authentication, Reporting, and Conformance)

Correct Answer: B

Q443. Which protocol is commonly used for remote logging in Unix and Linux systems?

- RDP (Remote Desktop Protocol)
- SSH (Secure Shell)
- SNMP (Simple Network Management Protocol)
- Syslog

Correct Answer: D

Q444. Which QoS approach involves reserving network resources in advance to guarantee a certain level of service for specific traffic flows?

- Integrated Services (IntServ)
- Differentiated Services (DiffServ)
- Best-Effort Service
- Flow-Based QoS

Correct Answer: A

Q445. Which type of attack in cryptography involves attempting every possible key until the correct one is found?

- Brute-force attack
- Man-in-the-middle attack
- Denial-of-Service (DoS) attack
- Phishing attack

Correct Answer: A

Q446. Which of the following is a connection-oriented protocol?

- TCP
- UDP
- ICMP
- ARP

Correct Answer: A

Q447. Which of the following fields is present in the TCP header but not in the UDP header?

- Sequence number
- Acknowledgement number
- Both sequence number and acknowledgement number
- None of the above

Correct Answer: C

Q448. What are the two main types of congestion control algorithms?

- Open-loop
- Closed-loop
- Both open-loop and closed-loop

- None of the above

Correct Answer: C

Q449. Which of the following is an example of a closed-loop congestion control algorithm?

- TCP slow start
- TCP congestion avoidance
- TCP fast recovery
- All of the above

Correct Answer: D

Q450. Which of the following is an example of an open-loop congestion control algorithm?

- Random early detection (RED)
- Weighted fair queuing (WFQ)
- TCP congestion avoidance
- None of the above

Correct Answer: A

Q451. What is the Domain Name System (DNS) used for?

- To translate domain names into IP addresses
- To provide a directory service for email servers
- To provide a way to log into remote systems
- All of the above

Correct Answer: D

Q452. What is the Simple Mail Transfer Protocol (SMTP) used for?

- To send email messages
- To receive email messages
- To store email messages
- All of the above

Correct Answer: C

Q453. What is the Post Office Protocol (POP3) used for?

- To receive email messages
- To store email messages
- To send email messages
- None of the above

Correct Answer: A

Q454. What is the Internet Mail Access Protocol (IMAP) used for?

- To access email messages that are stored on a remote server
- To send email messages
- To receive email messages
- None of the above

Correct Answer: A

Q455. Which of the following protocols is used for remote logging?

- SSH
- Telnet
- Both SSH and Telnet
- None of the above

Correct Answer: C

Q456. What is FTP used for?

- To transfer files between computers
- To browse the web
- To send email
- None of the above

Correct Answer: A

Q457. What is the WWW used for?

- To browse the web
- To transfer files between computers
- To send email
- None of the above

Correct Answer: A

Q458. What is the difference between FTP and the WWW?

- FTP is used to transfer files between computers, while the WWW is used to browse the we
- FTP is a file transfer protocol, while the WWW is a hypertext transfer protocol.
- FTP uses TCP, while the WWW uses HTTP.
- All of the above

Correct Answer: D

Q459. Which of the following protocols is used by email servers?

- SMTP
- HTTP
- SNMP
- None of the above

Correct Answer: A

Q460. Which of the following protocols is used to monitor network devices?

- SNMP
- HTTP
- SMTP
- None of the above

Correct Answer: A

Q461. What is the main goal of network security?

- To protect networks and their data from unauthorized access, use, disclosure, disruption, modification, or destruction.
- To improve the performance of networks.
- To reduce the cost of network operations.
- All of the above.

Correct Answer: D

Q462. What are the five main security services?

- Confidentiality, integrity, authentication, non-repudiation, and access control.
- Confidentiality, integrity, and availability.
- Confidentiality, integrity, and authentication.
- Confidentiality and integrity.

Correct Answer: A

Q463. What are the two main types of cryptography?

- Symmetric-key cryptography and asymmetric-key cryptography.
- Public key cryptography and private key cryptography.
- Strong cryptography and weak cryptography.
- None of the above.

Correct Answer: A

Q464. What is the difference between symmetric-key cryptography and asymmetric-key cryptography?

- Symmetric-key cryptography uses the same key to encrypt and decrypt data, while asymmetric-key cryptography uses two different keys: a public key and a private key.
- Public key cryptography is more secure than symmetric-key cryptography.
- Symmetric-key cryptography is faster than asymmetric-key cryptography.
- All of the above.

Correct Answer: D

Q465. Which of the following are examples of digital signature algorithms?

- RSA, DSA, and ECDSA
- AES, DES, and 3DES
- SHA-1, SHA-2, and MD5
- None of the above

Correct Answer: A

Q466. What are the benefits of using digital signatures?

- Digital signatures can help to protect against data tampering, forgery, and impersonation.
- Digital signatures can help to improve the efficiency of electronic transactions.
- Digital signatures can help to reduce the cost of doing business electronically.
- All of the above.

Correct Answer: D

Q467. In a connection-oriented protocol, what is the purpose of the "Three-Way Handshake" process?

- To establish a reliable connection before data transmission
- To exchange routing information with neighboring routers
- To ensure the confidentiality of data being transmitted
- To negotiate the encryption settings for the communication

Correct Answer: A

Q468. Which protocol is an example of a connection-oriented protocol used for secure data transmission over the internet?

- HTTP (Hypertext Transfer Protocol)

- FTP (File Transfer Protocol)
- UDP (User Datagram Protocol)
- TLS (Transport Layer Security)

Correct Answer: D

Q469. What is the primary benefit of a connectionless protocol's approach to data transmission?

- Guaranteed delivery of data packets
- Minimal delay due to lack of connection establishment
- Reliable delivery and error correction mechanisms
- Improved congestion control mechanisms

Correct Answer: B

Q470. In a connectionless protocol, how are data packets delivered to the destination?

- With guaranteed delivery and sequencing
- Without any addressing information
- Using virtual circuit switching
- Individually, without establishing a formal connection

Correct Answer: D

Q471. In the TCP header, which field indicates the length of the TCP header and any optional data that follows it?

- Sequence Number
- Acknowledgment Number
- Header Length
- Window Size

Correct Answer: C

Q472. What does the term "Sequence Number" refer to in the context of TCP communication?

- The position of a packet in the transmission order
- The number of packets in the sender's queue
- The maximum amount of data a receiver can handle
- The checksum value calculated for the data

Correct Answer: A

Q473. In the TCP/UDP message format, what is the purpose of the "Source Port" field?

- Identifies the application layer protocol being used

- Identifies the port number of the sender's device
- Specifies the destination port of the receiver
- Provides information about the type of data being transmitted

Correct Answer: B

Q474. Which network security protocol provides secure communication over the web by encrypting data between a web browser and a web server?

- SSH (Secure Shell)
- HTTPS (Hypertext Transfer Protocol Secure)
- SNMP (Simple Network Management Protocol)
- FTP (File Transfer Protocol)

Correct Answer: B

Q475. Which cryptographic technique is used to verify the integrity and authenticity of a message by generating a fixed-length hash?

- Digital signature
- Symmetric encryption
- Asymmetric encryption
- Hashing

Correct Answer: D

Q476. What is the primary purpose of a firewall in network security?

- To encrypt data transmissions
- To authenticate users
- To protect against unauthorized access and threats
- To load balance network traffic

Correct Answer: C

Q477. Which key is used for encryption in asymmetric encryption?

- Private key
- Secret key
- Public key
- Symmetric key

Correct Answer: C

Q478. Which security service ensures that data is not disclosed to unauthorized users?

- Authentication
- Data Integrity
- Confidentiality
- Availability

Correct Answer: C

Q479. Which FTP mode allows for data to flow in both directions but not simultaneously, with the client initiating the data connection?

- Active mode
- Passive mode
- Extended Passive mode
- Passive-active mode

Correct Answer: A

Q480. SNMP is primarily used for:

- Transferring files between computers.
- Managing and monitoring network devices.
- Browsing the World Wide We
- Sending emails securely.

Correct Answer: B

Q481. Which HTTP method is idempotent, meaning that making multiple identical requests will produce the same result as a single request?

- GET
- POST
- PUT
- DELETE

Correct Answer: A

Q482. Which HTTP status code indicates a successful request, and the server has fulfilled it?

- 200 OK
- 302 Found
- 404 Not Found
- 500 Internal Server Error

Correct Answer: A

Q483. In FTP, which mode is used for transferring files where data flows independently of control and may be sent on separate connections?

- Active mode
- Passive mode
- Extended Passive mode
- Stream mode

Correct Answer: B

Q484. What is the primary function of the SNMP Trap message?

- To request information from the SNMP agent.
- To acknowledge the receipt of SNMP messages.
- To inform the SNMP manager of significant events or alarms.
- To encrypt SNMP data for security.

Correct Answer: C

Q485. In HTTP, which request method is typically used to make changes to the server's state or create new resources?

- GET
- POST
- PUT
- HEAD

Correct Answer: C

Q486. Which of the following is NOT a primary security service provided by network security protocols?

- Authentication
- Access Control
- Data Integrity
- Load Balancing

Correct Answer: D

Q487. Which cryptographic algorithm is widely used for securing email communications?

- RSA
- AES
- SHA-256
- HMAC

Correct Answer: A

Q488. Which DiffServ (Differentiated Services) field in an IP header is used to specify the priority level of a packet?

- TOS (Type of Service) field
- TTL (Time-to-Live) field
- Payload Length field
- Identification field

Correct Answer: A

Q489. What does the term "Traffic Policing" refer to in QoS?

- Prioritizing high-priority traffic over low-priority traffic
- Controlling traffic by dropping excess packets
- Measuring network bandwidth
- Encrypting all network traffic

Correct Answer: B

Q490. In a network with QoS, what does the term "DSCP" stand for?

- Delayed Service Control Packet
- Data Sequence Control Protocol
- Differentiated Services Code Point
- Dynamic Source and Channel Protocol

Correct Answer: C

Q491. Identify the field that is NOT present in the TCP header

- Sequence number
- Source port number
- Destination port number
- Time to live (TTL)

Correct Answer: D

Q492. Identify the connectionless protocol

- TCP
- UDP
- Both TCP and UDP
- Neither TCP nor UDP

Correct Answer: B

Q493. Identify the congestion control mechanism that is NOT used by TCP

- Slow start
- Congestion avoidance
- Fast recovery
- Forward error correction (FEC)

Correct Answer: D

Q494. Identify the algorithm that is used by TCP to avoid congestion

- Additive increase, multiplicative decrease
- Round robin
- Weighted fair queuing
- None of the above

Correct Answer: A

Q495. Identify the QoS parameter that is used to measure the delay of a packet

- Latency
- Jitter
- Packet loss rate
- Bandwidth

Correct Answer: A

Q496. Identify the type of DNS record that is NOT valid

- A record
- CNAME record
- MX record
- ARP record

Correct Answer: D

Q497. Identify the protocol that is used for remote logging

- Syslog
- SNMP
- Both Syslog and SNMP
- Neither Syslog nor SNMP

Correct Answer: A

Q498. Identify the component of an email message that is NOT mandatory

- Message header
- Message body
- Message envelope
- Message signature

Correct Answer: D

Q499. Identify the protocol that is used to transfer files over a network

- FTP
- HTTP
- Both FTP and HTTP
- Neither FTP nor HTTP

Correct Answer: A

Q500. Identify the protocol that is used to access web pages

- FTP
- HTTP
- Both FTP and HTTP
- Neither FTP nor HTTP

Correct Answer: B

Q501. Which of the following is NOT a benefit of using additive increase, multiplicative decrease (AIMD) for congestion control?

- It is efficient in avoiding congestion.
- It is fair to all flows.
- It is simple to implement.
- It is robust to changes in network conditions.

Correct Answer: B

Q502. Which of the following QoS mechanisms can be used to guarantee bandwidth to a particular flow?

- Token bucket
- Leaky bucket
- Weighted fair queuing
- All of the above

Correct Answer: D

Q503. Which of the following DNS records is used to map a domain name to an IP address?

- A record
- CNAME record
- MX record
- NS record

Correct Answer: A

Q504. Which of the following is NOT a type of firewall?

- Packet filtering firewall
- Stateful inspection firewall
- Application-level firewall
- Proxy firewall

Correct Answer: C

Q505. Which of the following routing algorithms is used to find the shortest path between two nodes in a network?

- Dijkstra's algorithm
- Bellman-Ford algorithm
- Link state routing
- Distance vector routing

Correct Answer: A

Q506. Which of the following is NOT a disadvantage of UDP?

- It is unreliable.
- It is connectionless.
- It is inefficient for large data transfers.
- It is complex to implement.

Correct Answer: D

Q507. Which of the following factors can affect the performance of TCP congestion control?

- The size of the network
- The type of traffic
- The bandwidth of the links
- All of the above

Correct Answer: D

Q508. Which of the following QoS mechanisms can be used to reduce jitter?

- Packet buffering
- Traffic shaping
- Priority queuing
- All of the above

Correct Answer: D

Q509. Which of the following DNS records is used to map a domain name to a mail server?

- A record
- CNAME record
- MX record
- NS record

Correct Answer: C

Q510. Which of the following security threats can be mitigated by using a firewall?

- Denial-of-service attacks
- Man-in-the-middle attacks
- Malware infections
- All of the above

Correct Answer: D

Q511. Which of the following routing protocols is used in the Internet?

- Open Shortest Path First (OSPF)
- Border Gateway Protocol (BGP)
- Routing Information Protocol (RIP)
- All of the above

Correct Answer: D

Q512. Which of the following wireless networking standards is used for high-speed data transfers?

- 802.11a
- 802.11b
- 802.11g
- 802.11n

Correct Answer: D

Q513. Which of the following tools can be used to measure network performance?

- Ping
- Traceroute
- Wireshark
- All of the above

Correct Answer: D

Q514. Which of the following troubleshooting steps can be used to resolve a connectivity issue?

- Check the cables
- Restart the devices
- Update the firmware
- All of the above

Correct Answer: D

Q515. Which of the following factors should be considered when designing a network?

- The size of the network
- The type of traffic
- The budget
- All of the above

Correct Answer: D