**NETWORK ADMINISTRATOR**

**PAPER 1**

1. Which of the following protocols is used for sending emails?

(a)TCP

(b)UDP

(c)SMTP

(d)HTTP

Answer: (c)SMTP

2. What is the default subnet mask for a Class C IP address?

(a) 255.0.0.0

(b) 255.255.0.0

(c) 255.255.255.0

(d) 255.255.255.255

Answer: (c) 255.255.255.0

3. Which device operates at the Data Link layer of the OSI model?

(a) Router

(b) Bridge

(c) Switch

(d) Hub

Answer: (c) Switch

4. What is the maximum transmission speed of a standard Ethernet connection?

(a) 10 Mbps

(b) 100 Mbps

(c) 1 Gbps

(d) 10 Gbps

Answer: (c) 1 Gbps

5. Which protocol is used for secure transfer of files over a network?

(a) FTP

(b) TFTP

(c) SNMP

(d) SFTP

Answer: (d) SFTP

6. What is the purpose of a DHCP server in a network?

(a) Assign IP addresses dynamically

(b) Translate domain names to IP addresses

(c) Provide secure remote access

(d) Control network traffic flow

Answer: (a) Assign IP addresses dynamically

7. Which network topology requires a central node?

(a) Bus

(b) Ring

(c) Star

(d) Mesh

Answer: (c) Star

8. Which protocol is used for resolving IP addresses to MAC addresses?

(a) ARP

(b) RARP

(c) ICMP

(d) DHCP

Answer: (a) ARP

9. What is the maximum number of devices that can be connected to a single USB port using a USB hub?

(a) 2

(b) 4

(c) 6

(d) 8

Answer: (d) 8

10. Which network device works at the Physical layer of the OSI model?

(a) Repeater

(b) Firewall

(c) Load Balancer

(d) Proxy Server

Answer: (a) Repeater

11. When a packet exceeds the maximum transmission unit (MTU) of a network, it needs to be:

(a) Dropped

(b) Fragmented

(c) Discarded

(d) Reassembled

Answer: (b) Fragmented

12. The purpose of fragmentation in networking is to:

(a) Improve network performance

(b) Increase the packet size

(c) Ensure reliable delivery of packets

(d) Enable packet transmission across networks with different MTUs

Answer: (d) Enable packet transmission across networks with different MTUs

13. The checksum in a packet header is used to detect errors in the:

(a) Data payload

(b) Source IP address

(c) Destination IP address

(d) Entire packet

Answer: (d) Entire packet

14. The extension headers in IPv6 packets are used for:

(a) Fragmentation

(b) Error detection

(c) QoS (Quality of Service)

(d) Optional features and enhancements

Answer: (d) Optional features and enhancements

15. Which transmission medium is characterized by low cost, high flexibility, and is commonly used in Ethernet networks?

(a) Twisted-pair cable

(b) Coaxial cable

(c) Fiber-optic cable

(d) Radio waves

Answer: (a) Twisted-pair cable

16. Which architectural design separates the functionality of a system into distinct layers?

(a) Peer-to-peer process

(b) Encapsulation

(c) Layered architecture

(d) Model hierarchy

Answer: (c) Layered architecture

17. Which layer in the OSI model is responsible for converting data into a format suitable for transmission over a network?

(a) Presentation layer

(b) Transport layer

(c) Physical layer

(d) Data Link layer

Answer: (a) Presentation layer

18. Which layer in the OSI model provides services for file transfers, e-mail, and web browsing?

(a) Network layer

(b) Data Link layer

(c) Application layer

(d) Physical layer

Answer: (c) Application layer

19. Which layer in the TCP/IP suite is responsible for routing and forwarding of packets between networks?

(a) Network layer

(b) Transport layer

(c) Data Link layer

(d) Physical layer

Answer: (a) Network layer

20. Which protocol in the TCP/IP suite provides connectionless, unreliable service for data transmission?

(a) UDP

(b) TCP

(c) SCTP

(d) IP

Answer: (a) UDP

21. Which layer in the TCP/IP suite is responsible for converting data into a format suitable for transmission over a network?

(a) Application layer

(b) Transport layer

(c) Network layer

(d) Physical layer

Answer: (a) Application layer

22. Which layer in the TCP/IP suite handles the logical addressing and routing of data packets?

(a) Network layer

(b) Transport layer

(c) Application layer

(d) Data Link

Answer: (a) Network layer

23. Which protocol in the TCP/IP suite provides multi-homing support and reliable, ordered delivery of data?

(a) UDP

(b) TCP

(c) SCTP

(d) IP

Answer: (c) SCTP

24. Which protocol in the TCP/IP suite provides fragmentation and reassembly of packets?

(a) UDP

(b) TCP

(c) SCTP

(d) IP

Answer: (d) IP

25. Which layer in the TCP/IP suite handles the interface between applications and the network services?

(a) Network layer

(b) Transport layer

(c) Application layer

(d) Data Link layer

Answer: (b) Transport layer

26. Which protocol in the TCP/IP suite provides flow control and congestion control mechanisms?

(a) UDP

(b) TCP

(c) SCTP

(d) IP

Answer: (b) TCP

27. Which layer in the TCP/IP suite handles the physical transmission of data over the network medium?

(a) Network layer

(b) Transport layer

(c) Application layer

(d) Physical layer

Answer: (d) Physical layer

28. Which of the following is a valid IPv4 address in the dotted decimal notation?

(a) 2001:0db8:85a3:0000:0000:8a2e:0370:7334

(b) 192.168.0.1

(c) 2001:0db8::1

(d) fe80::1

Answer: (b) 192.168.0.1

29. Which class of IP address is reserved for multicast addresses?

(a) Class A

(b) Class B

(c) Class C

(d) Class D

Answer: (d) Class D

30. Which subnet mask corresponds to a Class C IP address?

(a) 255.255.255.0

(b) 255.0.0.0

(c) 255.255.0.0

(d) 255.255.255.128

Answer: (a) 255.255.255.0

31. Which of the following is a valid Class B IP address?

(a) 10.0.0.1

(b) 172.16.0.1

(c) 192.168.0.1

(d) 169.254.0.1

Answer: (b) 172.16.0.1

32. Which addressing scheme allows for the division of IP addresses into variable-length subnet masks (VLSM)?

(a) Classful addressing

(b) Classless addressing

(c) IPv4 addressing

(d) IPv6 addressing

Answer: (b) Classless addressing

33. Which notation is used to represent IPv6 addresses?

(a) Dotted decimal notation

(b) Binary notation

(c) Hexadecimal notation

(d) Octal notation

Answer: (c) Hexadecimal notation

34. Which of the following is an example of an IPv6 loopback address?

(a) ::1

(b) 127.0.0.1

(c) 192.168.1.1

(d) fe80::1

Answer: (a) ::1

35. Which type of IPv6 address is used for communication within the same link?

(a) Unicast address

(b) Multicast address

(c) Anycast address

(d) Link-local address

Answer: (d) Link-local address

36. What is the total address space of IPv6?

(a) 32 bits

(b) 64 bits

(c) 128 bits

(d) 256 bits

Answer: (c) 128 bits

37. Which protocol is used to map an IP address to a MAC address?

(a) ARP

(b) RARP

(c) BootP

(d) DHCP

Answer: (a) ARP

38. Which protocol is used to map a MAC address to an IP address?

(a) ARP

(b) RARP

(c) BootP

(d) DHCP

Answer: (b) RARP

39. Which protocol is used to automatically assign IP addresses to hosts on a network?

(a) ARP

(b) RARP

(c) BootP

(d) DHCP

Answer: (d) DHCP

40. Which device operates at the physical layer of the OSI model and amplifies and regenerates signals?

(a) Passive hub

(b) Repeater

(c) Active hub

(d) Bridge

Answer: (a) Passive hub

41. Which device operates at the data link layer of the OSI model and forwards frames based on their MAC addresses?

(a) Passive hub

(b) Repeater

(c) Active hub

(d) Bridge

Answer: (d) Bridge

42. Which device operates at the data link layer of the OSI model and provides signal regeneration and multiple port connectivity?

(a) Passive hub

(b) Repeater

(c) Active hub

(d) Bridge

Answer: (c) Active hub

43. Which network topology uses a central device, such as a switch or hub, to connect multiple LANs?

(a) Bus backbone

(b) Star backbone

(c) Ring backbone

(d) Mesh backbone

Answer: (a) Bus backbone

44. What is the purpose of a router in connecting remote LANs?

(a) To amplify and regenerate signals between LANs.

(b) To provide a central device for LAN connectivity.

(c) To route packets between different networks.

(d) To connect LANs using a shared medium.

Answer: (c) To route packets between different networks.

45. Which layer of the OSI model do routers primarily operate at?

(a) Physical layer

(b) Data link layer

(c) Network layer

(d) Transport layer

Answer: (c) Network layer

46. Which protocol is commonly used for connecting remote LANs over the Internet?

(a) Ethernet

(b) TCP/IP

(c) UDP

(d) IPX/SPX

Answer: (b) TCP/IP

47. Which protocol is commonly used for VLAN configuration and management?

(a) IPX/SPX

(b) ARP

(c) VTP

(d) DNS

Answer: (c) VTP

48. What is the maximum number of VLANs that can be created using the IEEE 802.1Q standard?

(a) 64

(b) 128

(c) 256

(d) 1024

Answer: (d) 1024

49. Which VLAN configuration method allows VLAN information to be dynamically learned from a central server?

(a) Static VLAN configuration

(b) Dynamic VLAN configuration

(c) VLAN Trunking Protocol (VTP)

(d) VLAN tagging

Answer: (c) VLAN Trunking Protocol (VTP)

50. Which layer of the OSI model is responsible for the transmission of raw bits over a communication channel?

(a) Data Link Layer

(b) Physical Layer

(c) Network Layer

(d) Transport Layer

Answer: (b) Physical Layer

51. Which layer of the OSI model is responsible for the error detection and correction in data transmission?

(a) Data Link Layer

(b) Physical Layer

(c) Network Layer

(d) Transport Layer

Answer: (a) Data Link Layer

52. Which Ethernet technology allows for the interconnection of multiple LAN segments using a bridge?

(a) Gigabit Ethernet

(b) Bridged Ethernet

(c) Switched Ethernet

(d) Fast Ethernet

Answer: (b) Bridged Ethernet

53. Which Ethernet technology improves network performance by enabling simultaneous transmission and reception of data?

(a) Standard Ethernet

(b) Bridged Ethernet

(c) Switched Ethernet

(d) Full-Duplex Ethernet

Answer: (d) Full-Duplex Ethernet

54. Which Ethernet standard operates at a data rate of 100 Mbps?

(a) Standard Ethernet

(b) Bridged Ethernet

(c) Switched Ethernet

(d) Fast Ethernet

Answer: (d) Fast Ethernet

55. Which standard defines the architecture and protocols for wireless LANs?

(a) 802.3

(b) 802.5

(c) 802.11

(d) 802.15

Answer: (c) 802.11

56. Which addressing mechanism is used in wireless networks to uniquely identify devices?

(a) MAC addresses

(b) IP addresses

(c) Port numbers

(d) Domain names

Answer: (a) MAC addresses

57. Which physical layer technology is commonly used in 802.11 wireless networks?

(a) Ethernet

(b) Bluetooth

(c) Wi-Fi

(d) Token Ring

Answer: (c) Wi-Fi

58. Which layer of the Bluetooth architecture handles the segmentation and reassembly of data packets?

(a) Radio layer

(b) Baseband layer

(c) Link manager layer

(d) L2CAP layer

Answer: (d) L2CAP layer

59. Which layer of the Bluetooth architecture is responsible for managing the physical transmission of data?

(a) Radio layer

(b) Baseband layer

(c) Link manager layer

(d) L2CAP layer

Answer: (b) Baseband layer

60. Which statement is true regarding VLAN communication between switches?

(a) VLANs cannot communicate with each other.

(b) VLANs can communicate through layer 2 broadcasts.

(c) VLANs can communicate through layer 3 routing.

(d) VLANs can communicate through VLAN trunking protocols only.

Answer: (c) VLANs can communicate through layer 3 routing.

61. In a scenario where multiple cookies are exchanged between a client and a server, which component is responsible for managing the hierarchical structure and dependencies among the cookies?

(a) Client

(b) Server

(c) Web application framework

(d) Cookie management system

Answer: (c) Web application framework

62. When a client sends a request to a server, which component is responsible for handling URL redirection and maintaining the continuity of the client's session?

(a) Client

(b) Server

(c) Proxy server

(d) URL routing system

Answer: (c) Proxy server

63. A client wants to retrieve a webpage from a server using HTTP. The webpage contains 10 embedded images, and each image has an average size of 150 KB. The client is using a persistent connection to retrieve the webpage. If the round trip time (RTT) between the client and server is 80 ms and the server's transmission rate is 2 Mbps, what is the total time required to download the webpage?

(a) 0.4 seconds

(b) 0.6 seconds

(c) 0.8 seconds

(d) 1.0 second

Answer: (a) 0.4 seconds

64. Which statement accurately describes the security vulnerabilities in standard FTP (unencrypted FTP)?

(a) Standard FTP is immune to any security vulnerabilities.

(b) Standard FTP is vulnerable to eavesdropping and unauthorized access to credentials.

(c) Standard FTP is susceptible to malware attacks but not unauthorized access.

(d) Standard FTP is only vulnerable when used over public networks, not private networks.

Answer: B) Standard FTP is vulnerable to eavesdropping and unauthorized access to credentials.

65. What is the primary advantage of a hierarchical name space over a flat name space?

(a) Improved name resolution efficiency

(b) Flexibility in naming conventions

(c) Reduced naming conflicts

(d) Simplified administration and management

Answer: (c) Reduced naming conflicts

66. Consider a domain name system (DNS) hierarchy with a root domain, top-level domains (TLDs), and second-level domains (SLDs). Each label in a domain name can have a maximum length of 63 characters. If a domain name consists of three labels, and the TLD and SLD each have five characters, how many characters are available for the third label?

(a) 58

(b) 59

(c) 60

(d) 61

Answer: (a) 58

67. Suppose a domain name consists of four labels: www, example, com, and net. Each label contains an average of 8 bytes. If the domain name is fully expanded, including the dot separators, what is the total length of the domain name in bytes?

(a) 29 bytes

(b) 30 bytes

(c) 31 bytes

(d) 32 bytes

Answer: (c) 31 bytes

68. Which statement accurately describes a zone in the context of DNS?

(a) A zone refers to the space between the root server and the top-level domain (TLD) server.

(b) A zone represents a specific administrative boundary within the DNS hierarchy and is managed by a primary DNS server.

(c) A zone is a type of DNS server that acts as a proxy for resolving queries from client devices.

(d) A zone is a subset of a domain that corresponds to a specific geographical region.

Answer: (b) A zone represents a specific administrative boundary within the DNS hierarchy and is managed by a primary DNS server.

69. What is the purpose of an inverse domain?

(a) An inverse domain maps IP addresses to corresponding domain names.

(b) An inverse domain provides a reverse lookup for email addresses.

(c) An inverse domain is used to validate the authenticity of SSL/TLS certificates.

(d) An inverse domain is a specific type of top-level domain used exclusively for IP address allocation.

Answer: (a) An inverse domain maps IP addresses to corresponding domain names.

70. Which statement accurately describes the registration process for country code top-level domains (ccTLDs)?

(a) Registration for ccTLDs is only available to citizens or residents of the respective country.

(b) ccTLDs require a more extensive verification process compared to generic top-level domains (gTLDs).

(c) The registration policies for ccTLDs are determined solely by ICANN.

(d) ccTLDs are subject to more stringent legal requirements compared to gTLDs.

Answer: C) The registration policies for ccTLDs are determined solely by ICANN.

71. In the context of DNS, what is the role of a resolver?

(a) Resolvers are responsible for mapping IP addresses to corresponding domain names.

(b) Resolvers act as intermediary servers between the client and authoritative DNS servers.

(c) Resolvers translate fully qualified domain names (FQDNs) into IP addresses for client devices.

(d) Resolvers manage the registration and allocation of domain names within a specific top-level domain (TLD).

Answer: (b) Resolvers act as intermediary servers between the client and authoritative DNS servers.

72. Which process is responsible for mapping names to IP addresses in DNS resolution?

(a) Forward lookup

(b) Reverse lookup

(c) Recursive resolution

(d) Iterative resolution

Answer: (a) Forward lookup

73. What is the significance of Dynamic DNS (DDNS) in the context of remote access and hosting services?

(a) DDNS allows users to access their home network remotely using a domain name, even if their IP address changes.

(b) DDNS provides additional security measures to protect against DNS-based attacks.

(c) DDNS enables load balancing and high availability for hosting services by dynamically redirecting traffic.

(d) DDNS simplifies the process of DNS record management by automating the registration and updating of records.

Answer: (a) DDNS allows users to access their home network remotely using a domain name, even if their IP address changes.

74. Which statement accurately describes the role of encapsulation in the OSI model?

(a) Encapsulation occurs at the Physical layer and is responsible for converting data into bits for transmission.

(b) Encapsulation takes place at the Transport layer and involves breaking down large data packets into smaller segments.

(c) Encapsulation occurs at the Network layer and involves adding IP headers to data packets for routing purposes.

(d) Encapsulation occurs at multiple layers of the OSI model and involves adding headers and trailers specific to each layer.

Answer: (d) Encapsulation occurs at multiple layers of the OSI model and involves adding headers and trailers specific to each layer.

75. What are the benefits of encapsulation in networking?

(a) Encapsulation enhances network security by encrypting data during transmission.

(b) Encapsulation enables the mixing of different types of data and protocols within a single transmission.

(c) Encapsulation allows for efficient routing and delivery of data packets across networks.

(d) Encapsulation simplifies the network architecture by eliminating the need for multiple protocol layers.

Answer: (b) Encapsulation enables the mixing of different types of data and protocols within a single transmission.

76. Which approach is commonly used for network configuration management in large-scale environments?

(a) Manual configuration management through command-line interfaces.

(b) Centralized configuration management using network automation tools.

(c) Distributed configuration management with individual device management interfaces.

(d) Hybrid approach combining manual and automated configuration management.

Answer: (b) Centralized configuration management using network automation tools.

77. Which statement accurately describes the purpose of fault management in network operations?

(a) Fault management focuses on identifying and preventing potential faults before they occur in the network.

(b) Fault management involves quickly detecting and resolving network issues to minimize service downtime.

(c) Fault management primarily deals with analyzing network performance data to optimize resource allocation.

(d) Fault management is responsible for ensuring compliance with regulatory standards and industry best practices.

Answer: (b) Fault management involves quickly detecting and resolving network issues to minimize service downtime.

78. Which of the following metrics is commonly used in performance management to measure network latency?

(a) Round Trip Time (RTT)

(b) Packet Loss Rate (PLR)

(c) Bandwidth Utilization

(d) Quality of Service (QoS)

Answer: (a) Round Trip Time (RTT)

79. What is the primary goal of security management in network operations?

(a) Ensuring confidentiality, integrity, and availability of network resources.

(b) Preventing unauthorized access and protecting against security threats.

(c) Monitoring network activities and detecting potential security breaches.

(d) All of the above.

Answer: (d) All of the above.

80. In the context of accounting management, what is the purpose of network usage monitoring?

(a) Tracking and recording network activities for billing and charging purposes.

(b) Analyzing network performance and resource utilization to optimize efficiency.

(c) Detecting and identifying anomalous network behavior or security incidents.

(d) Generating reports and statistics for compliance and auditing requirements.

Answer: (a) Tracking and recording network activities for billing and charging purposes.

81. What is lexicographic ordering in SNMP?

(a) Lexicographic ordering is the process of arranging SNMP managers in a hierarchical structure.

(b) Lexicographic ordering refers to the alphabetical arrangement of SNMP traps and notifications.

(c) Lexicographic ordering is used to sort and retrieve SNMP variable bindings based on their names.

(d) Lexicographic ordering is a security mechanism that prevents unauthorized access to SNMP devices.

Answer: C) Lexicographic ordering is used to sort and retrieve SNMP variable bindings based on their names.

82. In SNMP, what is the purpose of the Management Information Base (MIB)?

(a) The MIB provides a standardized framework for managing network devices and collecting data.

(b) The MIB is a database that stores network performance metrics for historical analysis.

(c) The MIB is responsible for secure communication between SNMP managers and agents.

(d) The MIB defines the structure and organization of SNMP traps and notifications.

Answer: (a) The MIB provides a standardized framework for managing network devices and collecting data.

83. Which SNMP component is responsible for collecting and storing management information on network devices?

(a) SNMP Manager

(b) SNMP Agent

(c) SNMP Proxy

(d) SNMP Trap

Answer: (b) SNMP Agent

84. Which SNMP message is used by the SNMP manager to inform an SNMP agent about a specific event or condition?

(a) GetRequest

(b) SetRequest

(c) Trap

(d) Inform

Answer: (a) GetRequest

85. Which UDP port number is typically used by SNMP agents to listen for incoming SNMP requests?

(a) 53

(b) 69

(c) 161

(d) 162

Answer: (c) 161

86. Which cryptographic technique is commonly used for entity authentication in network protocols?

(a) Password-based authentication

(b) Biometric authentication

(c) Digital certificates

(d) Challenge-response authentication

Answer: C) Digital certificates

87. Which algorithm is commonly used for symmetric-key encryption in modern cryptographic systems?

(a) RSA

(b) Diffie-Hellman

(c) AES

(d) ElGamal

Answer: (c) AES

88. In asymmetric-key cryptography, how does the confidentiality of data transmission work?

(a) The sender encrypts the data with their private key, and the receiver decrypts it with the sender's public key.

1. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their private key.
2. The sender encrypts the data with their private key, and the receiver decrypts it with their private key as well.
3. The sender encrypts the data with the receiver's public key, and the receiver decrypts it with the same public key.

Answer: (b) The sender encrypts the data with the receiver's public key, and the receiver decrypts it with their private key.

89. Which step is involved in creating a message digest?

(a) Encrypting the message with a private key.

(b)Decrypting the message with a public key.

(c) Applying a hash function to the message.

(d) Splitting the message into multiple fragments.

Answer: (c) Applying a hash function to the message.

90. Which key is used for both generating and verifying the Message Authentication Code (MAC)?

(a) Private key

(b) Public key

(c) Shared secret key

(d) Session key

Answer: (c) Shared secret key

91. In a MAC algorithm, what is the role of the initialization vector (IV)?

(a) To encrypt the message before computing the MAC.

(b) To randomize the encryption process for better security.

(c) To ensure unique MAC values for each message.

(d) To protect the MAC key from unauthorized access.

Answer: (c) To ensure unique MAC values for each message.

92. In a challenge-response protocol, the server generates a random challenge string of 16 bytes and sends it to the client. The client uses a symmetric key algorithm to compute the response, which is 128 bits in length. What is the size of the challenge in bits?

(a) 16 bits

(b) 64 bits

(c) 128 bits

(d) 256 bits

Answer: (b) 64 bits

93. In a public-key distribution system, the public keys are stored in a central repository accessible to all users. If there are 1000 users in the system, how many unique public-private key pairs are needed?

(a) 1000 pairs

(b) 2000 pairs

(c) 500,000 pairs

(d) 1,000,000 pairs

Answer: (a) 1000 pairs

94. In a VPN implementation, two sites are connected using IPsec in tunnel mode. The payload of each packet is 1400 bytes, and the overhead added by IPsec is 100 bytes. If the throughput of the underlying network link is 10 Mbps, what is the maximum achievable throughput of the VPN?

(a) 9.524 Mbps

(b) 9.6 Mbps

(c) 10 Mbps

(d) 10.1 Mbps

Answer: (a) 9.524 Mbps

95. In SSL/TLS, which of the following protocols provides secure key exchange and negotiation of the encryption algorithms?

(a) SSL Handshake Protocol

(b) SSL Record Protocol

(c) SSL Alert Protocol

(d) SSL Change Cipher Spec Protocol

Answer: (a) SSL Handshake Protocol

96. In the context of TLS, which version of SSL was the predecessor to TLS?

(a) SSL 1.0

(b) SSL 2.0

(c) SSL 3.0

(d) SSL 4.0

Answer: (c) SSL 3.0

97. Which of the following statements accurately describes a packet-filter firewall?

(a) It operates at the application layer of the OSI model.

(b) It examines individual packets based on specified criteria.

(c) It uses a proxy server to filter network traffic.

(d) It provides deep packet inspection for advanced threat detection.

Answer: (b) It examines individual packets based on specified criteria.

98. Which of the following is true regarding extended access lists?

(a) They are configured using numbers 1-99.

(b) They can filter traffic based on source and destination IP addresses.

(c) They can only be applied to inbound traffic.

(d) They are suitable for filtering traffic within a LAN.

Answer: (b) They can filter traffic based on source and destination IP addresses.

99. Which detection method used by IDS relies on establishing a baseline of normal behavior and detecting deviations from this baseline?

(a) Signature-based detection

(b) Anomaly-based detection

(c) Statistical-based detection

(d) Rule-based detection

Answer: (b) Anomaly-based detection

100. Suppose an IDS is configured to generate an alert when it detects more than 10 failed login attempts from a single IP address within a 5-minute interval. If the IDS logs show the following failed login attempts from an IP address:

1st attempt: 12:05:10

2nd attempt: 12:06:20

3rd attempt: 12:06:40

4th attempt: 12:07:15

5th attempt: 12:07:30

6th attempt: 12:07:45

Will the IDS generate an alert based on the configured threshold?

1. Yes
2. No

Answer: (a) Yes