Assignment - #1(Types, Transmission media&mode,OSI Model/Protocols)
Computer Networks

1. Which type of network is typically confined to a single building or campus?
   A. WAN
   B. MAN
   C. LAN
   D. More than one of the above
   E. None of the above

2. Which network spans a city or a large campus?
   A. PAN
   B. MAN
   C. LAN
   D. More than one of the above
   E. None of the above

3. Which protocol is used to translate domain names into IP addresses?
   A. ARP
   B. DNS
   C. DHCP
   D. More than one of the above
   E. None of the above

4. Which network type is primarily used for personal devices within a range of a few meters?
   A. LAN
   B. PAN
   C. WAN
   D. More than one of the above
   E. None of the above

5. Which type of network is designed for educational institutions or corporate campuses?
   A. CAN
   B. MAN
   C. WAN
   D. More than one of the above
   E. None of the above

6. What does SAN stand for in networking?
   A. System Area Network
   B. Storage Area Network
   C. Secure Area Network
   D. More than one of the above
   E. None of the above

7. Which network type is best suited for home automation systems?
   A. PAN
   B. HAN
   C. CAN
   D. More than one of the above
   E. None of the above

8. Which network type provides secure connectivity over a public network?
   A. VPN
   B. EPN
   C. WLAN
   D. More than one of the above
   E. None of the above

9. What does WLAN stand for?
   A. Wide Local Area Network
   B. Wireless Local Area Network
   C. Wide Logical Area Network
   D. More than one of the above
   E. None of the above

10. Which network is designed for secure communication within an organization?
    A. Intranet
    B. Extranet
    C. Internet
    D. More than one of the above
    E. None of the above

11. What is the primary difference between an Extranet and an Intranet?
    A. Extranet is publicly accessible
    B. Extranet allows limited external access
    C. Intranet uses wireless technology
    D. More than one of the above
    E. None of the above

12. Which topology connects all devices in a circular arrangement?
    A. Star
    B. Ring
    C. Mesh
    D. More than one of the above
    E. None of the above

13. Which of the following protocols is used for file transfer?
A. FTP
B. TFTP
C. SCP
D. More than one of the above
E. None of the above

14. Which topology provides multiple paths for data transmission?
A. Mesh
B. Star
C. Ring
D. More than one of the above
E. None of the above

15. Which protocol is used for sending emails?
A. HTTP
B. SMTP
C. FTP
D. More than one of the above
E. None of the above

16. Which network topology is most cost-effective for small networks?
A. Star
B. Bus
C. Mesh
D. More than one of the above
E. None of the above

17. Which of the following protocols is primarily used for web browsing?
A. HTTP
B. FTP
C. Telnet
D. More than one of the above
E. None of the above

18. What is a key characteristic of a Mesh topology?
A. All devices are connected to a central hub
B. Devices are connected in a linear sequence
C. Devices have multiple connections to other devices
D. More than one of the above
E. None of the above

19. Which network is used to connect storage devices in a dedicated manner?
A. SAN
B. CAN
C. VPN
D. More than one of the above
E. None of the above

20. What is the main purpose of a VPN?
A. To connect storage devices
B. To secure communication over public networks
C. To connect devices within a home
D. More than one of the above
E. None of the above

21. Which topology requires a terminator at both ends of the communication line?
A. Bus
B. Ring
C. Star
D. More than one of the above
E. None of the above

22. Which protocol is used for secure communication on the web?
A. HTTPS
B. SSH
C. TLS
D. More than one of the above
E. None of the above

23. Which network type is commonly used for connecting IoT devices in a home?
A. HAN
B. PAN
C. WLAN
D. More than one of the above
E. None of the above

24. What is the primary purpose of an Extranet?
A. To provide public access to resources
B. To allow external users limited access to an organization's network
C. To connect personal devices within a short range
D. More than one of the above
E. None of the above

25. Which topology combines the characteristics of Star and Bus topologies?
A. Mesh
B. Hybrid
C. Ring
D. More than one of the above
E. None of the above

26. Which protocol is used for real-time voice communication?
A. RTP
B. SIP
C. VoIP
D. More than one of the above
E. None of the above

27. What does EPN stand for?
A. Enterprise Private Network
B. Extended Public Network
C. Encrypted Private Network
D. More than one of the above
E. None of the above

28. Which topology is most resilient to node failures?
A. Ring
B. Mesh
C. Star
D. More than one of the above
E. None of the above

29. Which type of network is specifically designed for high-performance computing clusters?
A. Storage area Network
B. System Area Network
C. CAN
D. More than one of the above
E. None of the above

30. Which protocol is commonly used for retrieving emails from a server?
A. SMTP
B. IMAP
C. POP3
D. More than one of the above
E. None of the above

31. Which of the following is a transmission mode where data flows in both directions, but only one direction at a time?
A. Simplex
B. Half-duplex
C. Full-duplex
D. More than one of the above
E. None of the above

32. Which of the following is NOT an example of guided transmission media?
A. Coaxial cable
B. Fiber-optic cable
C. Twisted-pair cable
D. Radio waves
E. None of the above

33. What type of signal is used in traditional telephony systems?
A. Analog signal
B. Digital signal
C. Both A and B
D. More than one of the above
E. None of the above

34. Which of the following devices operates at the Data Link layer of the OSI model?
A. Router
B. Switch
C. Hub
D. More than one of the above
E. None of the above

35. Which of the following switching techniques uses a dedicated communication path between sender and receiver?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

36. Which transmission mode is most suitable for video conferencing?
A. Simplex
B. Half-duplex
C. Full-duplex
D. More than one of the above
E. None of the above

37. Which of the following is NOT true about fiber-optic cables?
A. Immune to electromagnetic interference
B. High bandwidth
C. Susceptible to crosstalk
D. Made of glass or plastic
E. None of the above

38. Which protocol is used for network management and monitoring?
A. SNMP
B. ICMP
C. Telnet
D. More than one of the above
E. None of the above

39. Which of the following is a key difference between analog and digital signals?
A. Analog signals are discrete, while digital signals are continuous.
B. Digital signals are discrete, while analog signals are continuous.
C. Analog signals are immune to noise, while digital signals are not.
D. More than one of the above
E. None of the above

40. Which switching technique is most commonly used in the Internet?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

41. Which device is used to regenerate and amplify signals in a network?
A. Hub
B. Repeater
C. Bridge
D. More than one of the above
E. None of the above

42. Which transmission medium is most suitable for long-distance communication with minimal signal loss?
A. Twisted-pair cable
B. Coaxial cable
C. Fiber-optic cable
D. More than one of the above
E. None of the above

43. Which of the following transmission media is most susceptible to electromagnetic interference?
A. Twisted-pair cable
B. Coaxial cable
C. Fiber-optic cable
D. More than one of the above
E. None of the above

44. Which device connects two LAN segments and filters traffic based on MAC addresses?
A. Repeater
B. Bridge
C. Hub
D. More than one of the above
E. None of the above

45. Which of the following best describes frequency-division multiplexing (FDM)?
A. Multiple signals are combined based on time slots.
B. Multiple signals are transmitted on different frequency bands.
C. Signals are transmitted sequentially in a round-robin manner.
D. More than one of the abov.
E. None of the above

46. Which switching technique stores the entire message before forwarding it to the destination?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

47. What is the primary disadvantage of circuit switching?
A. High latency for real-time communication
B. Inefficient use of bandwidth
C. Data loss during transmission
D. More than one of the above
E. None of the above

48. Which of the following is a disadvantage of unguided transmission media?
A. High susceptibility to interference
B. Limited mobility
C. High installation cost
D. More than one of the above
E. None of the above

49. Which of the following is NOT a characteristic of digital signals?
A. Noise resistance
B. Continuous waveform
C. Represented by binary values
D. More than one of the above
E. None of the above

50. Which network device is responsible for dividing a network into multiple collision domains?
A. Hub
B. Switch
C. Router
D. More than one of the above
E. None of the above

51. Which switching technique delivers data packets independently without maintaining a dedicated path?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

52. Which transmission mode is ideal for broadcasting a TV signal?
A. Simplex
B. Half-duplex
C. Full-duplex
D. More than one of the above
E. None of the above

53. Which of the following devices operates at the Network layer of the OSI model?
A. Router
B. Switch
C. Bridge
D. More than one of the above
E. None of the above

54. Which switching technique is best suited for real-time voice and video communication?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

55. Which type of multiplexing is commonly used in optical fiber communication?
A. Time-division multiplexing (TDM)
B. Frequency-division multiplexing (FDM)
C. Wavelength-division multiplexing (WDM)
D. More than one of the above
E. None of the above

56. Which of the following devices works as a central connection point in a star topology?
A. Hub
B. Switch
C. Router
D. More than one of the above
E. None of the above

57. Which property of digital signals makes them preferable for long-distance communication?
A. Continuous waveform
B. Noise resistance
C. High signal attenuation
D. More than one of the above
E. None of the above

58. Which of the following is true about analog signals?
A. They use discrete values.
B. They are less affected by noise.
C. They are continuous waveforms.
D. More than one of the above
E. None of the above

59. Which switching technique is most efficient for transmitting large files?
A. Circuit switching
B. Packet switching
C. Message switching
D. More than one of the above
E. None of the above

60. Which of the following is a characteristic of packet switching?
A. Dedicated communication path
B. Data divided into packets
C. High latency for real-time applications
D. More than one of the above
E. None of the above

61. Which layer of the OSI model is responsible for error detection and correction?
A. Network Layer
B. Data Link Layer
C. Transport Layer
D. More than one of the above
E. None of the above

62. Which OSI layer is responsible for establishing, managing, and terminating communication sessions?
A. Transport Layer
B. Session Layer
C. Presentation Layer
D. More than one of the above
E. None of the above

63. Which device connects multiple networks and directs data packets based on IP addresses?
A. Switch
B. Router
C. Gateway
D. More than one of the above
E. None of the above

64. Which OSI layer is responsible for converting data into a format suitable for transmission?
A. Application Layer
B. Presentation Layer
C. Transport Layer
D. More than one of the above
E. None of the above

65. Which of the following devices can provide network security by filtering incoming and outgoing traffic?
A. Firewall
B. Modem
C. NIC
D. More than one of the above
E. None of the above

66. Which OSI layer is responsible for routing and forwarding data packets?
A. Transport Layer
B. Network Layer
C. Data Link Layer
D. More than one of the above
E. None of the above

67. What is the primary function of a gateway in a network?
A. Connect devices within a LAN
B. Connect networks using different protocols
C. Filter network traffic
D. More than one of the above
E. None of the above

68. Which OSI layer handles flow control and segmentation of data?
A. Transport Layer
B. Data Link Layer
C. Network Layer
D. More than one of the above
E. None of the above

69. Which device operates at the Physical Layer of the OSI model?
A. Repeater
B. Router
C. Firewall
D. More than one of the above
E. None of the above

70. Which OSI layer is responsible for ensuring data integrity and reliable communication?
A. Transport Layer
B. Network Layer
C. Session Layer
D. More than one of the above
E. None of the above

71. Which of the following protocols operate at the Application Layer of the OSI model?
A. HTTP
B. FTP
C. SMTP
D. More than one of the above
E. None of the above

72. What is the primary function of the Network Interface Card (NIC)?
A. Data encryption
B. Network connectivity
C. Routing
D. More than one of the above
E. None of the above

73. Which OSI layer is responsible for data compression and encryption?
A. Session Layer
B. Presentation Layer
C. Application Layer
D. More than one of the above
E. None of the above

74. Which OSI layer converts data into signals suitable for transmission over the physical medium?
A. Network Layer
B. Physical Layer
C. Data Link Layer
D. More than one of the above
E. None of the above

75. Which of the following devices operates at multiple OSI layers?
A. Gateway
B. Repeater
C. Hub
D. More than one of the above
E. None of the above

76. Which layer of the OSI model is responsible for packet forwarding, including routing?
A. Transport Layer
B. Network Layer
C. Data Link Layer
D. More than one of the above
E. None of the above

77. What is the role of the Session Layer in the OSI model?
A. Data segmentation
B. Synchronization of communication
C. Address resolution
D. More than one of the above
E. None of the above

78. Which OSI layer is responsible for framing and physical addressing?
A. Data Link Layer
B. Network Layer
C. Transport Layer
D. More than one of the above
E. None of the above

79. Which layer of the OSI model ensures end-to-end delivery of data?
A. Network Layer
B. Transport Layer
C. Data Link Layer
D. More than one of the above
E. None of the above

80. Which of the following devices works at the Application Layer of the OSI model?
A. Gateway
B. Firewall
C. Modem
D. More than one of the above
E. None of the above

81. Which OSI layer is responsible for managing hardware transmission errors?
A. Physical Layer
B. Data Link Layer
C. Network Layer
D. More than one of the above
E. None of the above

82. What is the primary role of a firewall in a network?
A. Data encryption
B. Packet filtering
C. Signal amplification
D. More than one of the above
E. None of the above

83. Which OSI layer defines the electrical and mechanical characteristics of the network?
A. Data Link Layer
B. Physical Layer
C. Network Layer
D. More than one of the above
E. None of the above

84. Which OSI layer provides services like email, file transfer, and remote login?
A. Application Layer
B. Presentation Layer
C. Session Layer
D. More than one of the above
E. None of the above

85. At which OSI layer does a modem primarily operate?
A. Physical Layer
B. Data Link Layer
C. Network Layer
D. More than one of the above
E. None of the above

86. Which OSI layer is responsible for logical addressing and path determination?
A. Data Link Layer
B. Network Layer
C. Transport Layer
D. More than one of the above
E. None of the above

87. Which device acts as a central point for wireless devices to connect to a network?
A. Firewall
B. Access Point
C. Switch
D. More than one of the above
E. None of the above

88. Which OSI layer is responsible for breaking data into smaller segments for transmission?
A. Data Link Layer
B. Transport Layer
C. Network Layer
D. More than one of the above
E. None of the above

89. What is the primary function of a Network Interface Card (NIC)?
A. Enables network connectivity
B. Provides data encryption
C. Manages error correction
D. More than one of the above
E. None of the above

90. Which of the following is a function of a firewall in a network?
A. Packet filtering
B. Signal amplification
C. Data compression
D. More than one of the above
E. None of the above

91. Which error detection technique uses parity bits to identify errors?
A. CRC
B. Checksum
C. Parity Check
D. More than one of the above
E. None of the above

92. Which error correction technique uses redundant bits to fix errors?
A. Hamming Code
B. Parity Check
C. Cyclic Redundancy Check (CRC)
D. More than one of the above
E. None of the above

93. What is the primary purpose of Access Control Lists (ACLs)?
A. Manage user authentication
B. Define permissions for resources
C. Encrypt sensitive data
D. More than one of the above
E. None of the above

94. Which of the following techniques is used for error detection?
A. CRC
B. Checksum
C. Hamming Code
D. More than one of the above
E. None of the above

95. What is a characteristic of firewalls?
A. Operates only at the Physical Layer
B. Blocks unauthorized access
C. Amplifies network signals
D. More than one of the above
E. None of the above

96. Which error correction technique is suitable for correcting burst errors?
A. Hamming Code
B. Reed-Solomon Code
C. Parity Check
D. More than one of the above
E. None of the above

97. What is the primary function of a checksum?
A. Error detection
B. Error correction
C. Data encryption
D. More than one of the above
E. None of the above

98. Which error detection technique is most suitable for detecting burst errors?
A. Parity Check
B. CRC
C. Checksum
D. More than one of the above
E. None of the above

99. What is a key advantage of using firewalls?
A. Enhanced data compression
B. Prevention of unauthorized access
C. Amplification of network signals
D. More than one of the above
E. None of the above

100. Which of the following is NOT an error detection technique?
A. CRC
B. Checksum
C. Hamming Code
D. More than one of the above
E. None of the above

101. Which protocol is responsible for logical addressing in the network layer?
A. IP
B. ARP
C. ICMP
D. More than one of the above
E. None of the above

102. Which protocol is used to map IP addresses to MAC addresses?
A. ICMP
B. ARP
C. RARP
D. More than one of the above
E. None of the above

103. Which protocol provides error reporting and diagnostics at the network layer?
A. IP
B. ICMP
C. OSPF
D. More than one of the above
E. None of the above

104. Which protocol is used for routing within an autonomous system?
A. RIP
B. OSPF
C. BGP
D. More than one of the above
E. None of the above

105. Which protocol is used to route multicast traffic?
A. IGMP
B. PIM
C. RIP
D. More than one of the above
E. None of the above

106. Which protocol provides reliable communication at the transport layer?
A. UDP
B. TCP
C. ICMP
D. More than one of the above
E. None of the above

107. Which protocol is used for real-time communication at the transport layer?
A. TCP
B. UDP
C. SCTP
D. More than one of the above
E. None of the above

108. Which sublayer handles access to the physical medium?
A. LLC
B. MAC
C. Transport
D. More than one of the above
E. None of the above

109. Which protocol is used for connectionless communication at the transport layer?
A. TCP
B. UDP
C. SCTP
D. More than one of the above
E. None of the above

110. Which sublayer of the data link layer is responsible for error detection?
A. LLC
B. MAC
C. Network
D. More than one of the above
E. None of the above

111. Which protocol is responsible for logical addressing in the network layer?
A. IP
B. ARP
C. ICMP
D. More than one of the above
E. None of the above

112. Which protocol is used to map IP addresses to MAC addresses?
A. ICMP
B. ARP
C. RARP
D. More than one of the above
E. None of the above

113. Which protocol provides error reporting and diagnostics at the network layer?
- **A. IP**
- **B. ICMP**
- **C. OSPF**
- **D. More than one of the above**
- **E. None of the above**

114. Which protocol is used for downloading emails from a mail server to a local client?
- **A. SMTP**
- **B. POP3**
- **C. IMAP**
- **D. More than one of the above**
- **E. None of the above**

115. Which protocol is used to route multicast traffic?
- **A. IGMP**
- **B. PIM**
- **C. RIP**
- **D. More than one of the above**
- **E. None of the above**

Answer With Explanation

1. Answer: C. LAN
Explanation: A Local Area Network (LAN) is designed for small geographical areas, such as a building or campus. It enables high-speed communication and resource sharing within a limited space. Unlike WANs and MANs, LANs are typically privately owned and operated.

2. Answer: B. MAN
Explanation: A Metropolitan Area Network (MAN) covers a city or large campus, providing connectivity over a larger area than LAN but smaller than WAN. MANs often use high-speed technologies like fiber optics to interconnect various LANs within a metropolitan region.

3. Answer: B. DNS
Explanation: The Domain Name System (DNS) is responsible for converting human-readable domain names (e.g., www.example.com) into machine-readable IP addresses. ARP maps IP addresses to MAC addresses, and DHCP assigns IP addresses dynamically. DNS is critical for the functioning of the Internet, enabling user-friendly addressing.

4. Answer: B. PAN
Explanation: A Personal Area Network (PAN) is a small network used for connecting personal devices like smartphones, tablets, and laptops within a short range, typically up to 10 meters. Bluetooth and Infrared technologies are common in PANs.

5. Answer: A. CAN
Explanation: A Campus Area Network (CAN) interconnects multiple LANs within a specific campus, such as a university or corporate office. It is smaller than a MAN and typically uses high-speed connections to provide efficient communication.

6. Answer: D. More than one of the above
Explanation: SAN can refer to both Storage Area Network and System Area Network. A Storage Area Network is used for block-level data storage, while a System Area Network connects high-performance computing resources.

7. Answer: B. HAN
Explanation: A Home Area Network (HAN) connects devices within a home, such as smart appliances, security systems, and personal computers. It enables centralized control and communication among these devices.

8. Answer: A. VPN
Explanation: A Virtual Private Network (VPN) creates a secure, encrypted connection over a public network like the internet. It is commonly used for remote access and protecting sensitive data during transmission.

9. Answer: B. Wireless Local Area Network
Explanation: A WLAN is a type of LAN that uses wireless communication technology, such as Wi-Fi, to connect devices. It provides the flexibility of mobility within a limited area while maintaining network connectivity.

10. Answer: A. Intranet
Explanation: An Intranet is a private network used within an organization to share information and resources securely. It is typically isolated from external access, unlike the Internet.

11. Answer: B. Extranet allows limited external access
Explanation: An Extranet is an extension of an Intranet that provides secure access to external users, such as business partners or clients. It is designed to facilitate collaboration while maintaining security protocols.

12. Answer: B. Ring
Explanation: In a Ring topology, each device is connected to exactly two other devices, forming a circular data path. Data travels in one direction, reducing collisions but making the network vulnerable to a single point of failure.

13. Answer: D. More than one of the above
Explanation: FTP (File Transfer Protocol) is widely used for transferring files over a network. TFTP (Trivial File Transfer Protocol) is a simplified version of FTP that does not require authentication. SCP (Secure Copy Protocol) is used for secure file transfers using SSH. All these protocols are designed for file transfer but differ in complexity and security.

14. Answer: A. Mesh
Explanation: A Mesh topology connects devices in such a way that multiple paths exist for data transmission. This ensures high reliability and fault tolerance, as data can take alternate routes if one path fails.

15. Answer: B. SMTP
Explanation: The Simple Mail Transfer Protocol (SMTP) is used for sending emails. It operates at the application layer and facilitates the transmission of messages between email servers. SMTP uses a client-server model and often works alongside POP3 or IMAP for retrieving emails. HTTP is for web browsing, and FTP is for file transfer. SMTP ensures reliable delivery of emails through a series of commands and responses between mail servers.

16. Answer: B. Bus
Explanation: In a Bus topology, all devices are connected to a single communication line or cable. This topology is cost-effective due to minimal cabling and is suitable for small networks. However, it may face performance issues as the network grows.

17. Answer: A. HTTP
Explanation: Hypertext Transfer Protocol (HTTP) is the foundation of data communication for the World Wide Web. It is used to load web pages using hypertext links. HTTP defines how messages are formatted and transmitted, and how web servers and browsers should respond to requests. FTP is used for file transfers, and Telnet is used for terminal emulation.

18. Answer: C. Devices have multiple connections to other devices
Explanation: In a Mesh topology, each device is connected to multiple other devices, ensuring high redundancy and reliability. This topology is ideal for critical networks where downtime is unacceptable.

19. Answer: A. SAN
Explanation: A Storage Area Network (SAN) is designed for block-level data storage. It connects storage devices like disk arrays and tape libraries to servers, ensuring high-speed and reliable access to data.

20. Answer: B. To secure communication over public networks
Explanation: A Virtual Private Network (VPN) creates an encrypted connection over a public network like the Internet. It ensures data privacy and security, often used for remote work and accessing restricted resources.

21. Answer: A. Bus
Explanation: In a Bus topology, a single communication line connects all devices, and terminators are required at both ends to prevent signal reflection. Without terminators, data transmission would be disrupted.

22. Answer: D. More than one of the above
Explanation: HTTPS (Hypertext Transfer Protocol Secure) is HTTP combined with encryption provided by TLS (Transport Layer Security). TLS ensures data integrity and confidentiality over the network. SSH (Secure Shell) is not for web communication but provides secure remote access. Both HTTPS and TLS contribute to secure communication in web applications.

23. Answer: D. More than one of the above
Explanation: Both HAN (Home Area Network) and WLAN (Wireless Local Area Network) are used to connect IoT devices in homes. HAN focuses on smart appliances and automation, while WLAN provides wireless connectivity.

24. Answer: B. To allow external users limited access to an organization's network
Explanation: An Extranet extends an organization's Intranet to external users, such as clients or partners, providing controlled access to specific resources while maintaining security.

25. Answer: B. Hybrid
Explanation: A Hybrid topology integrates features of multiple topologies, such as Star and Bus. It offers flexibility and scalability, making it suitable for complex networks.

26. Answer: D. More than one of the above
Explanation: RTP (Real-Time Protocol) and SIP (Session Initiation Protocol) are critical for voice and video communication over IP networks. RTP handles the transport of audio and video streams, while SIP manages the signaling for establishing, maintaining, and terminating communication sessions. VoIP (Voice over IP) is an application of these protocols.

27. Answer: A. Enterprise Private Network
Explanation: An Enterprise Private Network (EPN) is a private network used by organizations to securely connect various branches and offices. It ensures efficient and secure communication across the enterprise.

28. Answer: B. Mesh
Explanation: Mesh topology is highly resilient because it provides multiple paths for data transmission. If one node or connection fails, data can still be transmitted through alternate paths.

29. Answer: B. System Area Network
Explanation: A System Area Network (SAN) connects high-performance computing nodes in a cluster, providing low-latency and high-bandwidth communication. It is commonly used in supercomputing environments.

30. Answer: D. More than one of the above
Explanation: IMAP (Internet Message Access Protocol) and POP3 (Post Office Protocol) are both used for retrieving emails from a server. IMAP allows users to manage emails directly on the server, enabling access from multiple devices. POP3 downloads emails to the local device and typically deletes them from the server. SMTP, on the other hand, is used for sending emails.

31. Answer: B. Half-duplex
Explanation: Half-duplex transmission allows data to flow in both directions, but only one direction at a time. For example, a walkie-talkie works in half-duplex mode, where one person speaks while the other listens. Simplex allows data flow in one direction only, while full-duplex enables simultaneous two-way communication.

32. Answer: D. Radio waves
Explanation: Guided transmission media involves physical pathways like cables (e.g., coaxial, twisted-pair, and fiber-optic). Radio waves are part of unguided media, where signals travel through the air without a physical conductor.

33. Answer: A. Analog signal
Explanation: Traditional telephony systems rely on analog signals to transmit voice data. Analog signals vary continuously over time. Modern telephony, however, often uses digital signals for enhanced quality and reliability.

34. Answer: B. Switch
Explanation: Switches operate at the Data Link layer (Layer 2) of the OSI model, forwarding data based on MAC addresses. Routers operate at the Network layer (Layer 3), and hubs are physical layer devices

35. Answer: A. Circuit switching
Explanation: Circuit switching establishes a dedicated communication path for the duration of a session, ensuring consistent bandwidth and latency. Packet switching divides data into packets, while message switching sends the entire message without a dedicated path.

36. Answer: C. Full-duplex
Explanation: Full-duplex transmission allows simultaneous two-way communication, which is essential for applications like video conferencing. It ensures real-time interaction without delays caused by switching directions.

37. Answer: C. Susceptible to crosstalk
Explanation: Fiber-optic cables are immune to crosstalk and electromagnetic interference because they use light to transmit data. They offer high bandwidth and are made of glass or plastic, making them ideal for high-speed communication.

38. Answer: A. SNMP
Explanation: A widely used protocol for managing and monitoring network devices on a (LAN) or (WAN). ICMP is used for error handling and network diagnostics. The Teletype Network Protocol is used to provide a command line interface for communication with a remote device or server.

39. Answer: B. Digital signals are discrete, while analog signals are continuous.
Explanation: Analog signals represent data with continuous waveforms, while digital signals use discrete binary values (0s and 1s). Digital signals are more immune to noise compared to analog signals.

40. Answer: B. Packet switching
Explanation: The Internet relies on packet switching, where data is divided into packets and transmitted independently. This technique is efficient and robust, allowing multiple devices to share the network simultaneously.

41. Answer: B. Repeater
Explanation: Repeaters regenerate and amplify signals to extend the range of a network. They operate at the Physical layer of the OSI model. Hubs do not amplify signals but act as basic connection points.

42. Answer: C. Fiber-optic cable
Explanation: Fiber-optic cables are ideal for long-distance communication due to their low signal attenuation and immunity to electromagnetic interference. Twisted-pair and coaxial cables are more prone to signal loss over long distances.

43. Answer: A. Twisted-pair cable
Explanation: Twisted-pair cables, commonly used in local area networks (LANs), are more susceptible to electromagnetic interference compared to coaxial and fiber-optic cables. Shielded twisted-pair (STP) reduces this vulnerability but not completely.

44. Answer: B. Bridge
Explanation: A bridge connects two LAN segments and uses MAC addresses to filter and forward traffic. It operates at the Data Link layer (Layer 2) of the OSI model. Repeaters and hubs operate at the Physical layer.

45. Answer: B. Multiple signals are transmitted on different frequency bands.
Explanation: FDM allows multiple signals to be transmitted simultaneously by allocating separate frequency bands to each signal. It is commonly used in radio and television broadcasting. Time-division multiplexing (TDM) uses time slots instead of frequency bands.

46. Answer: C. Message switching
Explanation: In message switching, the entire message is stored at intermediate nodes before being forwarded to the next node. This technique can cause delays but ensures reliable delivery. Circuit switching and packet switching do not use this approach.

47. Answer: B. Inefficient use of bandwidth
Explanation: Circuit switching establishes a dedicated path between sender and receiver for the entire session, even if no data is being transmitted. This leads to inefficient bandwidth utilization. However, it ensures a consistent connection with low latency, making it suitable for real-time applications like voice calls.

48. Answer: A. High susceptibility to interference
Explanation: Unguided transmission media, such as radio waves, are prone to electromagnetic interference and weather conditions. Despite offering mobility and ease of installation, interference can degrade signal quality and reliability.

49. Answer: B. Continuous waveform
Explanation: Digital signals are represented by discrete binary values (0s and 1s) and are resistant to noise. Continuous waveforms are a characteristic of analog signals, which vary smoothly over time.

50. Answer: B. Switch
Explanation: A switch divides a network into multiple collision domains, reducing the likelihood of data collisions. Each port on a switch represents a separate collision domain. Routers divide networks into separate broadcast domains, while hubs do not segment collision domains.

51. Answer: B. Packet switching
Explanation: Packet switching divides data into packets, which are transmitted independently and may take different routes to the destination. This technique is efficient and fault-tolerant, as it does not rely on a dedicated path like circuit switching.

52. Answer: A. Simplex
Explanation: Broadcasting a TV signal is a one-way communication process, making simplex mode the most suitable. The signal flows from the broadcaster to viewers without requiring a return path.

53. Answer: A. Router
Explanation: Routers operate at the Network layer (Layer 3) of the OSI model, making routing decisions based on IP addresses. Switches and bridges operate at the Data Link layer (Layer 2).

54. Answer: A. Circuit switching
Explanation: Circuit switching provides a dedicated path for the duration of the communication session, ensuring consistent bandwidth and low latency, which are essential for real-time voice and video communication.

55. Answer: C. Wavelength-division multiplexing (WDM)
Explanation: WDM is a type of multiplexing used in optical fiber communication, where multiple signals are transmitted simultaneously on different wavelengths of light. This technique maximizes the utilization of fiber-optic cables.

56. Answer: D. More than one of the above
Explanation: Both hubs and switches can serve as central connection points in a star topology. Hubs are simpler devices that broadcast data to all ports, while switches intelligently forward data to the intended recipient.

57. Answer: B. Noise resistance
Explanation: Digital signals are less susceptible to noise and can be easily regenerated using repeaters, making them suitable for long-distance communication. Analog signals, on the other hand, degrade more significantly over distance.

58. Answer: C. They are continuous waveforms.
Explanation: Analog signals are represented by continuous waveforms that vary over time. They are more affected by noise compared to digital signals, which use discrete binary values.

59. Answer: C. Message switching
Explanation: Message switching stores and forwards the entire message at intermediate nodes, ensuring reliable delivery of large files. However, this technique may introduce delays, making it less suitable for real-time communication.

60. Answer: D. More than one of the above
Explanation: Packet switching divides data into packets, which are transmitted independently. While it is efficient and fault-tolerant, it may introduce latency, making it less ideal for real-time applications compared to circuit switching.

61. Answer: B. Data Link Layer
Explanation: The Data Link Layer handles error detection and correction through mechanisms like checksums and CRC (Cyclic Redundancy Check). It ensures reliable data transfer between adjacent nodes. The Transport Layer handles end-to-end error control but does not perform physical error correction.

62. Answer: B. Session Layer
Explanation: The Session Layer (Layer 5) establishes, manages, and terminates communication sessions between applications. It synchronizes data streams and ensures proper session handling in case of interruptions. The Transport Layer deals with data delivery, and the Presentation Layer focuses on data formatting.

63. Answer: B. Router
Explanation: Routers operate at the Network Layer (Layer 3) and connect multiple networks. They determine the best path for data packets using routing tables and protocols. Switches connect devices within the same network, while gateways can translate between different network protocols.

64. Answer: B. Presentation Layer
Explanation: The Presentation Layer (Layer 6) ensures that data is in a compatible format for transmission. It handles encryption, compression, and translation of data. The Application Layer focuses on user interaction, while the Transport Layer manages data delivery.

65. Answer: A. Firewall
Explanation: Firewalls filter network traffic based on predefined security rules, operating at multiple OSI layers, including the Transport and Application Layers. NICs (Network Interface Cards) facilitate network connectivity, and modems convert signals for internet access but do not provide traffic filtering.

66. Answer: B. Network Layer
Explanation: The Network Layer (Layer 3) is responsible for routing and forwarding data packets between devices across different networks. It uses logical addressing (IP addresses) and routing protocols like OSPF and BGP. The Transport Layer ensures reliable data delivery, while the Data Link Layer handles local network data transfer.

67. Answer: B. Connect networks using different protocols
Explanation: Gateways operate at multiple OSI layers and connect networks using different communication protocols. They perform protocol conversion, allowing devices on dissimilar networks to communicate. Switches connect devices within a LAN, and firewalls filter traffic.

68. Answer: A. Transport Layer
Explanation: The Transport Layer (Layer 4) manages flow control, segmentation, and reassembly of data for reliable communication. It uses protocols like TCP and UDP. The Data Link Layer handles flow control for local links, but segmentation is not its responsibility.

69. Answer: A. Repeater
Explanation: Repeaters operate at the Physical Layer (Layer 1) by amplifying and retransmitting signals to extend the range of a network. They do not interpret data. Routers operate at the Network Layer, and firewalls operate at higher layers.

70. Answer: A. Transport Layer
Explanation: The Transport Layer (Layer 4) ensures data integrity and reliable communication through error detection, retransmission, and acknowledgment mechanisms. Protocols like TCP provide reliable data delivery, while UDP offers faster but less reliable communication.

71. Answer: D. More than one of the above
Explanation: Protocols like HTTP (for web communication), FTP (for file transfer), and SMTP (for email) operate at the Application Layer (Layer 7). This layer provides services directly to end-users and applications.

72. Answer: B. Network connectivity
Explanation: NICs enable devices to connect to a network by providing a physical and logical interface. They operate at both the Physical Layer (Layer 1) and the Data Link Layer (Layer 2). NICs handle MAC addressing and enable communication over wired or wireless media.

73. Answer: B. Presentation Layer
Explanation: The Presentation Layer (Layer 6) handles data compression and encryption to ensure secure and efficient data transmission. It transforms data into a format suitable for the Application Layer, facilitating compatibility between different systems.

74. Answer: B. Physical Layer
Explanation: The Physical Layer (Layer 1) converts data into electrical, optical, or radio signals for transmission over physical media. It defines hardware specifications, such as cables, connectors, and transmission rates.

75. Answer: A. Gateway
Explanation: Gateways operate at multiple OSI layers, often from the Application Layer down to the Network Layer. They translate communication protocols, data formats, or address schemes to enable communication between dissimilar networks.

76. Answer: B. Network Layer
Explanation: The Network Layer (Layer 3) is responsible for packet forwarding and routing. It determines the best path for data packets using protocols like IP, OSPF, and BGP. It also handles logical addressing through IP addresses.

77. Answer: B. Synchronization of communication
Explanation: The Session Layer (Layer 5) manages sessions between applications. It establishes, maintains, and terminates communication sessions and synchronizes data streams to ensure a smooth flow of information.

78. Answer: A. Data Link Layer
Explanation: The Data Link Layer (Layer 2) is responsible for framing, physical addressing (MAC addresses), and error detection. It ensures reliable data transfer between nodes on the same network segment.

79. Answer: B. Transport Layer
Explanation: The Transport Layer (Layer 4) ensures end-to-end delivery of data by managing error detection, flow control, and retransmissions. It uses protocols like TCP for reliable communication and UDP for faster, connectionless communication.

80. Answer: A. Gateway
Explanation: Gateways can operate at the Application Layer (Layer 7) by translating protocols and data formats between networks. Firewalls operate at higher layers for traffic filtering, while modems work at the Physical Layer.

81. Answer: B. Data Link Layer
Explanation: The Data Link Layer (Layer 2) detects and corrects transmission errors using techniques like CRC. It ensures reliable communication over physical links, while the Physical Layer handles raw data transmission.

82. Answer: B. Packet filtering
Explanation: Firewalls filter packets based on predefined security rules, preventing unauthorized access. They operate at multiple OSI layers, including the Network and Transport Layers, to ensure secure data communication.

83. Answer: B. Physical Layer
Explanation: The Physical Layer (Layer 1) defines the hardware specifications, such as cables, connectors, and voltage levels, for transmitting raw bits over the network medium.

84. Answer: A. Application Layer
Explanation: The Application Layer (Layer 7) provides network services directly to the end-user. Protocols like HTTP, FTP, SMTP, and Telnet enable tasks such as email communication, file transfer, and remote system access. The Presentation Layer handles data formatting, and the Session Layer manages sessions.

85. Answer: A. Physical Layer
Explanation: A modem operates at the Physical Layer (Layer 1), converting digital signals into analog signals (and vice versa) for transmission over telephone lines or other media. It does not interpret or route data, which is handled by higher layers.

86. Answer: B. Network Layer
Explanation: The Network Layer (Layer 3) uses logical addressing (IP addresses) to identify devices and determine the best path for data transmission. Routing protocols like OSPF and BGP enable efficient packet forwarding across interconnected networks.

87. Answer: B. Access Point
Explanation: An Access Point (AP) acts as a central hub for wireless devices, enabling them to connect to a wired network. It operates at the Data Link Layer (Layer 2) and uses Wi-Fi protocols to facilitate communication between wireless and wired devices.

88. Answer: B. Transport Layer
Explanation: The Transport Layer (Layer 4) breaks data into smaller segments for transmission. It ensures reliable delivery through error detection and retransmission mechanisms. The Network Layer handles routing, while the Data Link Layer focuses on framing and local data transfer.

89. Answer: A. Enables network connectivity
Explanation: A NIC is a hardware component that connects a device to a network. It operates at the Physical and Data Link layers of the OSI model, handling MAC addressing and enabling communication over wired or wireless networks. NICs do not perform encryption or error correction directly, as these functions are handled by higher layers or other components.

90. Answer: A. Packet filtering
Explanation: A firewall acts as a security barrier, filtering incoming and outgoing network traffic based on predefined rules. It operates at the Network and Transport layers, inspecting packets for malicious content or unauthorized access. Signal amplification and data compression are not firewall functions.

91. Answer: C. Parity Check
Explanation: Parity Check is a simple error detection method where a parity bit is added to the data. It ensures the total number of 1s in the data is either even (even parity) or odd (odd parity). While effective for single-bit errors, it cannot detect multiple-bit errors.

92. Answer: A. Hamming Code
Explanation: Hamming Code is an error correction technique that adds redundant bits to data, enabling the detection and correction of single-bit errors. It uses parity bits at specific positions to determine the location of the error and correct it.

93. Answer: B. Define permissions for resources
Explanation: ACLs specify which users or devices have access to specific resources, such as files or network segments. They are a key component of access control systems, ensuring only authorized entities can access or modify data. Authentication and encryption are separate processes.

94. Answer: D. More than one of the above
Explanation: Both CRC (Cyclic Redundancy Check) and Checksum are error detection techniques. CRC uses polynomial division to detect errors, while Checksum calculates the sum of data segments. Hamming Code, on the other hand, is an error correction technique.

95. Answer: B. Blocks unauthorized access
Explanation: Firewalls block unauthorized access to a network by filtering traffic based on predefined rules. They operate at multiple layers, primarily the Network and Transport layers. They do not amplify signals or operate at the Physical Layer.

96. Answer: B. Reed-Solomon Code
Explanation: Reed-Solomon Code is an error correction technique designed to correct burst errors, commonly used in CDs, DVDs, and QR codes. It works by adding redundant data to ensure the recovery of original data even if a part is corrupted.

97. Answer: A. Error detection
Explanation: A checksum is used for error detection by calculating the sum of data segments and appending it to the data. The receiver recalculates the checksum and compares it with the transmitted one to detect errors.

98. Answer: B. CRC
Explanation: CRC is highly effective for detecting burst errors due to its polynomial division method. It can detect multiple bit errors within a block of data, making it more robust than parity checks or checksums.

99. Answer: B. Prevention of unauthorized access
Explanation: Firewalls enhance network security by blocking unauthorized access and filtering traffic based on predefined rules. They do not compress data or amplify signals, as these are unrelated functions.

100. Answer: C. Hamming Code
Explanation: Hamming Code is an error correction technique, not an error detection method. CRC and Checksum are used for detecting errors during data transmission.

101. Answer: A. IP
Explanation: The Internet Protocol (IP) is the primary protocol at the network layer, responsible for logical addressing and routing packets between devices. It ensures that data packets are delivered to the correct destination using IP addresses. ARP resolves MAC addresses, and ICMP handles error reporting and diagnostics.

102. Answer: B. ARP
Explanation:The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses in a local network. It ensures that packets sent at the network layer reach the correct device at the data link layer. RARP performs the reverse operation, mapping MAC addresses to IP addresses.

103. Answer: B. ICMP
Explanation: The Internet Control Message Protocol (ICMP) is used for error reporting and network diagnostics. For example, it is used in the "ping" command to check connectivity. OSPF is a routing protocol, and IP is used for addressing and routing but does not handle diagnostics.

104. Answer: D. More than one of the above
Explanation: Both RIP (Routing Information Protocol) and OSPF (Open Shortest Path First) are used for routing within an autonomous system. RIP uses distance-vector routing, while OSPF uses link-state routing. BGP (Border Gateway Protocol) is used for routing between autonomous systems.

105. Answer: D. More than one of the above
Explanation: IGMP (Internet Group Management Protocol) manages multicast group memberships, while PIM (Protocol Independent Multicast) routes multicast traffic efficiently. RIP is unrelated to multicast, as it is used for unicast routing.

106 Answer: B. TCP
Explanation: The Transmission Control Protocol (TCP) ensures reliable communication through mechanisms like acknowledgment, retransmission, and flow control. UDP (User Datagram Protocol) is connectionless and does not guarantee reliability. ICMP operates at the network layer for error reporting.

107. Answer: D. More than one of the above
Explanation: UDP and SCTP (Stream Control Transmission Protocol) are used for real-time communication. UDP is lightweight and suitable for latency-sensitive applications like VoIP. SCTP combines features of TCP and UDP, providing reliability for multimedia and signaling.

108. Answer: B. MAC
Explanation: The MAC sublayer manages access to the physical medium, ensuring that multiple devices can share the same channel without collisions. LLC operates above MAC, handling logical connections. Transport is a higher-layer function.

109. Answer: B. UDP
Explanation: UDP (User Datagram Protocol) is a connectionless protocol that sends data without establishing a connection. It is lightweight and suitable for applications like DNS queries and video streaming. TCP and SCTP are connection-oriented.

110. Answer: B. LLC
Explanation: The LLC (Logical Link Control) sublayer handles error detection and correction through techniques like CRC (Cyclic Redundancy Check), flow control and logical addressing. Network is not a data link sublayer.

111. Answer: A. IP
Explanation:The Internet Protocol (IP) is the primary protocol at the network layer, responsible for logical addressing and routing packets between devices. It ensures that data packets are delivered to the correct destination using IP addresses. ARP resolves MAC addresses, and ICMP handles error reporting and diagnostics.

112. Answer: B. ARP
Explanation: The Address Resolution Protocol (ARP) maps IP addresses to MAC addresses in a local network. It ensures that packets sent at the network layer reach the correct device at the data link layer. RARP performs the reverse operation, mapping MAC addresses to IP addresses.

113. Answer: B. ICMP
Explanation: The Internet Control Message Protocol (ICMP) is used for error reporting and network diagnostics. For example, it is used in the "ping" command to check connectivity. OSPF is a routing protocol, and IP is used for addressing and routing but does not handle diagnostics.

114. Answer: B. POP3
Explanation: POP3 (Post Office Protocol) used for downloading emails. POP3 downloads emails to the client and deletes them from the server, while IMAP synchronizes emails across devices. SMTP is used for sending emails.

115. Answer: b. PIM
Explanation: IGMP (Internet Group Management Protocol) manages multicast group memberships, while PIM (Protocol Independent Multicast) routes multicast traffic efficiently. RIP is unrelated to multicast, as it is used for unicast routing.