CN ORAL QUESTION BANK TE COMPUTER

(CN QUESTION BANK FROM ORAL EXAMINATION POINT OF VIEW)

Answers by: BHAKTI THAKUR

1. What are different types of cables used in networking? Also list name of connectors for eachone.

A: 1. Coaxial Cable
    Connector: BNC, F-type
  2. Twisted Pair Cable
    Types:
    Unshielded Twisted Pair (UTP)
    Shielded Twisted Pair (STP)
    Connector: RJ45
  3. Fiber Optic Cable
    Types:
    Single-mode
    Multi-mode
    Connector: SC, LC, ST

2. What is the maximum segment size for twisted pair, fiber optic cable?

A: 1. Twisted Pair Cable: Max segment size - 100 meters (for Ethernet)
  2. Fiber Optic Cable: Max segment size - Up to 2 kilometers (multi-mode), 100+ kilometers (single-mode)

3. How many wires and twist are their in UTP?

A: Wires: 8 wires (4 pairs)
  Twists: Varies; typically 2-3 twists per inch

4. Which cable is used in our LAN?

A: Cable Used: Unshielded Twisted Pair (UTP), usually Cat5e or Cat6

5. What is the use of firewall?

A: Monitors and controls network traffic; blocks unauthorized access; protects against cyber threats.

6. What are different topologies also give adv and disadv of each? Which will you prefer to designa LAN and why?

A: Bus Topology
  Advantages: Simple, low cost
  Disadvantages: Single point of failure, limited cable length

  Ring Topology
  Advantages: Easy to install, consistent data transfer
  Disadvantages: Failure of one device affects the entire network

  Star Topology
  Advantages: Easy to manage, failure of one device doesn’t affect others
  Disadvantages: Central hub failure affects entire network

  Mesh Topology
  Advantages: Redundant paths, high reliability
  Disadvantages: Expensive, complex installation

  Tree Topology
  Advantages: Hierarchical structure, scalable
  Disadvantages: Central node failure can affect subnets

Preferred for LAN Design:
Star Topology: Easy to manage, fault tolerance, and scalability.

7. What are different IEEE standards for Ethernet LAN?

A: IEEE 802.3: Standard for Ethernet
IEEE 802.3u: Fast Ethernet (100 Mbps)
IEEE 802.3z: Gigabit Ethernet (1000 Mbps)
IEEE 802.3ae: 10 Gigabit Ethernet
IEEE 802.3an: 10 Gigabit over Copper (10GBASE-T)

8. If you want to design a network for 10 pcs what things you have to consider that time?

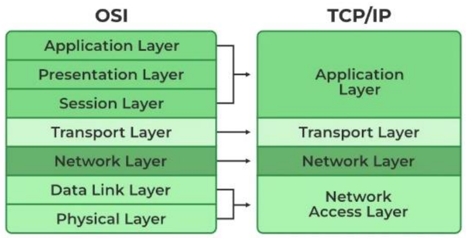
A: Network Topology: Choose suitable topology (Star recommended)
Cable Type: UTP Cat5e or Cat6
Switch/Hub: Select based on number of ports (at least 10 ports)
IP Addressing: Decide on static or dynamic IP allocation (use DHCP if dynamic)
Router: For internet access (if needed)
Network Security: Firewalls, encryption, and access control
Power Supply: Ensure reliable power for devices (UPS for backup)
Devices: Ensure network adapters for PCs and proper drivers

9. What are 7 layers of OSI model?
10. Explain working of each layer?

A: Physical Layer: Transmission of raw data bits
Data Link Layer: Frames data for transmission, error detection
Network Layer: Routing and forwarding of data (e.g., IP)
Transport Layer: End-to-end communication, flow control (e.g., TCP, UDP)
Session Layer: Manages sessions between applications
Presentation Layer: Data translation, encryption, compression
Application Layer: Interfaces with end-user applications

11. Draw dig of OSI and TCP/IP reference model?

A:



12. Difference between OSI and TCP/IP?

A:

Feature	**OSI Model**	**TCP/IP Model**
Layers	7 layers	4 layers
Layers (OSI)	1. Physical 2. Data Link 3. Network 4. Transport 5. Session 6. Presentation 7. Application	1. Link 2. Internet 3. Transport 4. Application
Development	Theoretical model	Practical model for the Internet
Standardization	Developed by ISO	Developed by ARPANET

Feature	OSI Model	TCP/IP Model
Layer Functions	Specific functions for each layer	Combines multiple OSI layers (e.g., Application layer combines OSI's Session, Presentation, and Application layers)
Protocol Dependency	Protocol-independent	Protocol-specific (TCP, IP, etc.)

13. List name of protocols work at each layer of OSI model.

A: Layer 1 (Physical): Ethernet, DSL, fiber optics
Layer 2 (Data Link): ARP (Address Resolution Protocol), PPP (Point-to-Point Protocol), Ethernet
Layer 3 (Network): IP (Internet Protocol), ICMP (Internet Control Message Protocol)
Layer 4 (Transport): TCP (Transmission Control Protocol), UDP (User Datagram Protocol)
Layer 5 (Session): SMB (Server Message Block), RPC (Remote Procedure Call)
Layer 6 (Presentation): SSL (Secure Sockets Layer), TLS (Transport Layer Security)
Layer 7 (Application): HTTP (HyperText Transfer Protocol), FTP (File Transfer Protocol), SMTP (Simple Mail Transfer Protocol)

14. List name of networking devices working at each layer of TCP/IP?

A: Layer 1 (Physical): Hub, Repeater
Layer 2 (Data Link): Switch, Bridge
Layer 3 (Network): Router
Layer 4 (Transport): Firewall, Load Balancer

15. What is ATM?

A: ATM (Asynchronous Transfer Mode) is a high-speed networking technology designed for transmitting voice, video, and data. It uses fixed-size cells (53 bytes) for data transfer, ensuring constant data rate and low latency, making it suitable for real-time applications.

16. What is meant by tunneling?

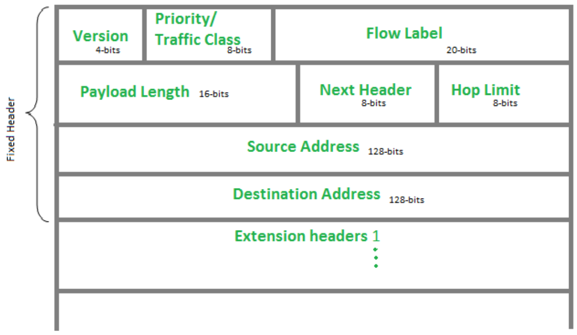
A: Tunneling refers to encapsulating data packets from one protocol within another, allowing them to pass securely through an intermediate network. It’s commonly used in VPNs (Virtual Private Networks) to securely transmit data over the internet.

17. What is meant by fragmentation?

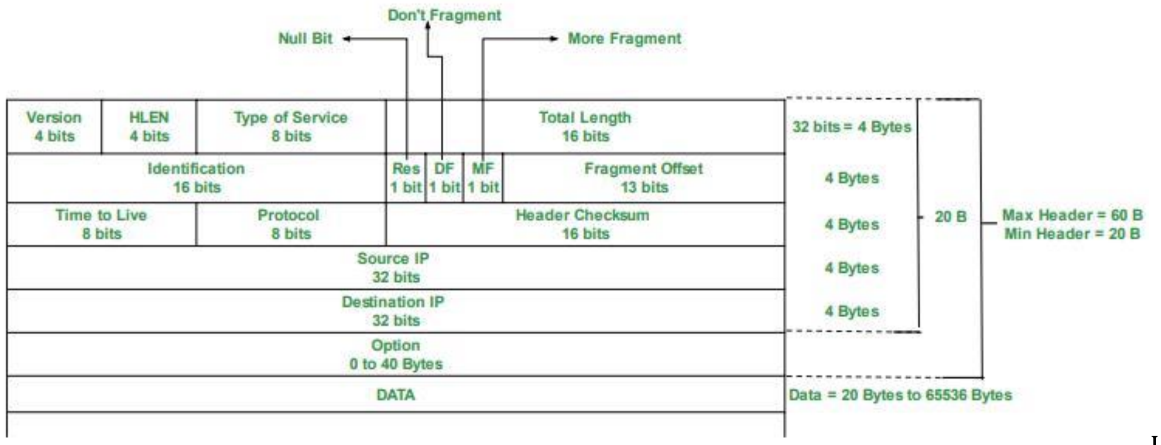
A: Fragmentation is the process of breaking a large data packet into smaller pieces to ensure it can be transmitted over a network with size limitations. Reassembly happens at the destination.

18. Draw IPV4 and IPV6 header format.

A:

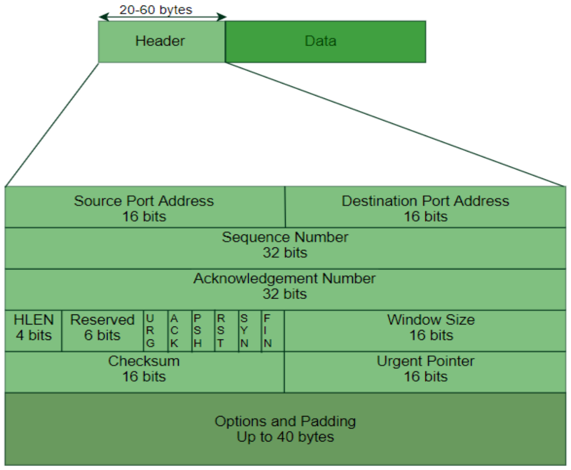


IPv6

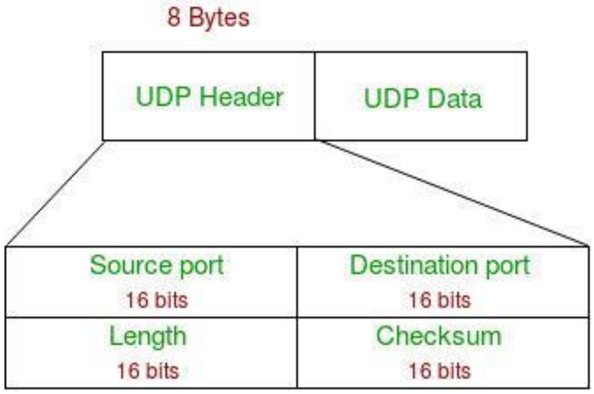


IPv4

19. Draw TCP, UDP header format?

A: 

TCP



UDP

20. What are the two types of transmission technology available?

A: Circuit-Switched: A dedicated communication path is established between the sender and receiver for the entire duration of the communication. It's used in traditional telephone networks.

Packet-Switched: Data is divided into packets and each packet is sent independently across the network. It's used in modern networking, such as the internet.

21. What is subnetting? When to use it.

A: Subnetting is the process of dividing an IP network into smaller subnetworks (subnets) to improve efficiency and security. It involves borrowing bits from the host portion of the IP address and using them for network identification.

22. Difference between the communication and transmission.

A: Communication: The exchange of information between devices or systems. It involves the transfer of data in a manner that both sender and receiver understand.

Transmission: The actual sending of data over a physical medium (e.g., cables, radio waves).

23. What is router?

A: A router is a network device that forwards data packets between different networks. It uses routing tables to determine the best path for each packet. Routers operate at the Network Layer (Layer 3) of the OSI model.

24. What is point-to-point protocol

A: PPP is a data link layer protocol used to establish a direct connection between two network nodes. It is commonly used for dial-up connections and enables multiple network layer protocols, such as IP, to run over the same physical link. PPP provides features like authentication (PAP/CHAP), encryption, and error detection.

25. What is MAC address? How many bits of it and in which format?

A: A MAC (Media Access Control) address is a unique identifier assigned to network interfaces for communications at the data link layer of the OSI model.

It is a 48-bit address, typically written in hexadecimal format.

Example: 00:14:22:01:23:45. The address is made up of six pairs of hexadecimal digits, each representing 8 bits.

26. IP address works at which layer? How many bits of it is ? give one example

A: An IP address works at the Network Layer (Layer 3) of the OSI model.

It is used to uniquely identify devices on a network and to route data packets.

IPv4 is a 32-bit address (e.g., 192.168.1.1), while IPv6 is a 128-bit address.

Example (IPv4): 192.168.1.1 (32-bit address), and

Example (IPv6): 2001:0db8:85a3:0000:0000:8a2e:0370:7334 (128-bit address).

27. How many classes are their in IPV4? Also give range of each.

A: There are five main classes in IPv4:

Class A: 0.0.0.0 to 127.255.255.255

Class B: 128.0.0.0 to 191.255.255.255

Class C: 192.0.0.0 to 223.255.255.255

Class D (Multicast): 224.0.0.0 to 239.255.255.255

Class E (Reserved): 240.0.0.0 to 255.255.255.255

28. For each class show the no of networks and host?

A: Class A:

Networks: 128

Hosts: 16,777,214 per network

Class B:

Networks: 16,384

Hosts: 65,534 per network

Class C:

Networks: 2,097,152

Hosts: 254 per network

Class D (Multicast): Reserved for multicast, not used for normal host addressing.

Class E (Reserved): Reserved for future use or research, not assigned for hosts.

29. What is the default subnet mask for class A, B, C?

A: Class A: 255.0.0.0 (or /8)

Class B: 255.255.0.0 (or /16)

Class C: 255.255.255.0 (or /24)

The subnet mask determines the boundary between the network and host portions of the IP address.

30. What is Physical & Logical address?

A: Physical Address: Also known as the MAC address, it is a hardware address used to uniquely identify devices on a network at the data link layer. It is assigned by the manufacturer and is embedded into the network interface card (NIC).

Logical Address: This refers to IP addresses, which are used to identify devices on a network at the network layer. IP addresses can be changed and are assigned dynamically.

31. What are the types of Transmission media?

A: Transmission media refer to the physical paths through which data is transmitted in a network.
The types include:
Guided Media:
Twisted Pair Cable: Common for Ethernet networks; used in telephones and LANs.
Coaxial Cable: Used for cable TV, internet connections, and older LANs.
Fiber Optic Cable: Transmits data as light; very high speed and long-distance.
Unguided Media:
Radio Waves: Used in wireless communication, including Wi-Fi and cellular networks.
Microwaves: Used for long-distance communication via satellite.
Infrared: Used for short-range communication, e.g., remote controls and short-range wireless devices.

32. What is Repeater?/
33. What is Bridges?/
34. What is Routers?/
35. What is Gateways?/
36. What is Switches?/
37. Difference between Hub and Switch?/
38. Difference between switch and router?/

A:

Device	Definition	Function	OSI Layer	Types	Use	Example
Repeater	A device that amplifies or regenerates a signal to extend the distance it can travel.	Extends the range of a network signal.	Physical (Layer 1)	Active, Passive	Used in long-distance networks to overcome signal loss.	Ethernet repeaters, wireless repeaters
Bridge	A device that connects two or more network segments and filters traffic based on MAC addresses.	Divides traffic between network segments to reduce congestion.	Data Link (Layer 2)	Transparent, Source Routing	Used to create larger networks or reduce collision domains.	Network bridges in LANs

Device	Definition	Function	OSI Layer	Types	Use	Example
Gateway	A device that connects two different networks and translates data between different protocols.	Allows communication between different types of networks (e.g., between LAN and WAN).	All Layers (Layer 1-7)	Protocol Gateway, Default Gateway	Used to connect different network protocols or different network types.	Email servers, router/firewall between LAN and the internet
Switch	A device that connects multiple devices on a LAN, forwarding data based on MAC addresses.	Directs data to the correct device within the same network.	Data Link (Layer 2)	Managed, Unmanaged, Layer 2, Layer 3 (Multilayer Switch)	Used to build network infrastructure and reduce collisions.	Managed switches, Layer 2 switches
Hub	A basic networking device that connects multiple devices, broadcasting data to all connected ports.	Forwards data to all devices in the network (no filtering).	Physical (Layer 1)	Active, Passive	Often replaced by switches due to inefficiency.	Simple network hubs used in home networks
Router	A device that forwards data packets between networks, using IP addresses to determine the best path.	Directs data from one network to another (e.g., LAN to the internet).	Network (Layer 3)	Wireless Router, Wired Router, Core Router, Edge Router	Used to connect different networks and direct internet traffic.	Home routers, enterprise routers
Modem	A device that converts digital data from a computer into analog signals for transmission over a phone line.	Modulates and demodulates signals for internet access.	Physical (Layer 1)	Cable Modem, DSL Modem	Used for broadband or dial-up internet connections.	Cable modem, DSL modem
NIC (Network Interface Card)	A hardware device that allows computers to connect to	Converts data from the computer into electrical signals for	Data Link (Layer 2)	Wired NIC, Wireless NIC	Used in every computer to connect to networks.	Ethernet NIC, Wi-Fi NIC

Device	Definition	Function	OSI Layer	Types	Use	Example
	a network.	transmission.				
Access Point	A device that allows wireless devices to connect to a wired network via Wi-Fi.	Provides wireless connectivity to a network.	Data Link (Layer 2)	Indoor, Outdoor, Managed, Unmanaged	Used in Wi-Fi networks to extend wireless coverage.	Wi-Fi routers and dedicated access points

39. What is cutoff switch and store and forward switch?

A: Cutoff Switch: A switch that immediately drops or rejects a corrupted packet without checking the rest of the data.

Store and Forward Switch: A switch that receives the entire packet, stores it, checks for errors, and then forwards it if it's error-free.

40. What is manageable and unmanageable switch?

A: Manageable Switch: A switch that can be configured, monitored, and controlled via a web interface, CLI, or SNMP.

Unmanageable Switch: A basic switch with no configuration capabilities, it operates out-of-the-box without any adjustments.

41. What is the need of web server?

A: A server that hosts web pages and responds to client requests over HTTP/HTTPS. It stores, processes, and delivers web content to browsers.

42. What is meant by Broadcast, Multicast and Unicast?

A: Broadcast: Data sent to all devices on the network (e.g., ARP requests).

Multicast: Data sent to a specific group of devices (e.g., video conferencing).

Unicast: Data sent from one device to another specific device (e.g., sending an email).

43. What is FDDI?

A: (Fiber Distributed Data Interface): A high-speed network protocol that uses fiber-optic cables for data transmission. It is typically used for LANs.

44. What is Token ring and token bus?

A: Token Ring: A LAN protocol where data is passed around the network in a circular manner, with a token granting permission to send data.

Token Bus: Similar to Token Ring, but uses a bus (linear) topology for data transmission.

45. Give all IEEE standards from 802.2 to 802.16 .

A: 802.2: Logical Link Control (LLC) – Provides error control and flow control.
802.3: Ethernet – Standard for wired LANs.
802.4: Token Bus – LAN using a bus topology and token passing.
802.5: Token Ring – LAN using a ring topology and token passing.
802.6: Metropolitan Area Network (MAN) – Standard for metropolitan networks.
802.11: Wi-Fi – Wireless LAN standards.
802.15: Wireless Personal Area Networks (WPAN) – Bluetooth.
802.16: WiMAX – Broadband wireless access standard.

46. What the IP address of our server?

A: **CHECK**

47. What are two line used in our organization for internet connection?

A: **CHECK**

48. What is difference between leased line and dial up connection?

A: Leased Line: A dedicated, always-on, high-speed internet connection with guaranteed bandwidth and stable performance.

Dial-up Connection: A slower, temporary internet connection using a telephone line, requiring dialing to establish the connection.

49. What is meant by ISP?

A: (Internet Service Provider): A company or organization that provides internet access to users or businesses.

50. What is ICMP?

A: (Internet Control Message Protocol): A protocol used for network diagnostics and error reporting (e.g., ping and traceroute).

51. What are the data units at different layers of the TCP / IP protocol suite?

A: Application Layer: Data
Transport Layer: Segments (TCP) / Datagrams (UDP)
Internet Layer: Packets
Network Access Layer: Frames

52. What is difference between ARP and RARP?

A: ARP (Address Resolution Protocol): Resolves an IP address to a MAC address (used to find hardware address from IP).

RARP (Reverse Address Resolution Protocol): Resolves a MAC address to an IP address (used by devices to find their IP address from a known MAC).

53. What is the minimum and maximum length of the header in the TCP segment and IPdatagram?

A: TCP Header: Minimum 20 bytes, Maximum 60 bytes.
IP Datagram: Minimum 20 bytes, Maximum 60 bytes (IPv4).

54. What is the difference between TFTP and FTP application layer protocols?

A: TFTP (Trivial File Transfer Protocol): A simple, connectionless protocol for transferring files, no authentication, no error recovery.

FTP (File Transfer Protocol): A more robust, connection-oriented protocol that supports authentication, error handling, and directory operations.

55. What are major types of networks and explain?

A: LAN (Local Area Network): A network covering a small geographical area, like a home or office.
WAN (Wide Area Network): A network that spans a large geographic area, connecting multiple LANs.
MAN (Metropolitan Area Network): A network that covers a city or large campus.
PAN (Personal Area Network): A network for personal devices within a small range, like Bluetooth.
WLAN (Wireless LAN): A LAN using wireless technology.

56. What are the important topologies for networks?

A: Bus Topology: Single central cable connects all devices.
Star Topology: Devices connected to a central hub/switch.
Ring Topology: Devices connected in a circular manner.
Mesh Topology: Every device is connected to every other device.
Hybrid Topology: A combination of two or more topologies.

57. What is mesh network?

A: A Mesh Network is a type of network where every device is connected to every other device, ensuring multiple paths for data transmission and providing redundancy.

58. Why should you care about the OSI Reference Model?
A: The OSI Reference Model helps standardize and understand how different network protocols interact, guiding troubleshooting, network design, and system interoperability.

59. What is VPN?
A: VPN (Virtual Private Network): A technology that creates a secure and encrypted connection over a less secure network (such as the internet), enabling private communication between devices

60. What is Virtual Lan?
A: Virtual LAN (VLAN): A logical grouping of devices within a physical LAN, segmenting networks into smaller, isolated networks for better traffic management and security.

61. What is packet filter?
A: A firewall function that inspects packets of data and allows or blocks them based on predefined rules like IP address, port number, and protocol type.

62. What is traffic shaping?
A: A technique used to control the amount and rate of traffic sent into a network, optimizing performance by reducing congestion and ensuring fair bandwidth allocation.

63. What is meant by flow control?
A: A mechanism to control the rate of data transmission between two devices, preventing the sender from overwhelming the receiver with too much data at once.

64. What is meant by congestion control?
A: A set of techniques used to prevent or control network congestion by adjusting the transmission rate, ensuring that the network can handle the volume of traffic.

65. What is IGP (Interior Gateway Protocol)?
A: A protocol used to exchange routing information within a single autonomous system (AS). Examples include RIP, OSPF, and EIGRP.

66. What is EGP (Exterior Gateway Protocol)?
A: A protocol used to exchange routing information between different autonomous systems. The most common example is BGP.

67. What is autonomous system?
A: (AS): A collection of IP networks and routers under the control of a single organization or entity, which presents a common routing policy to the internet.

68. What is BGP (Border Gateway Protocol)?
A: A path vector protocol used to exchange routing information between different autonomous systems, forming the backbone of internet routing.

69. What is OSPF?
A: (Open Shortest Path First): A link-state routing protocol used within an autonomous system, which calculates the shortest path based on the Dijkstra algorithm.

70. What is RIP (Routing Information Protocol)?
A: A distance-vector routing protocol used within an autonomous system that uses hop count as the metric to determine the best path for routing.

71. What is PPP?

A: (Point-to-Point Protocol): A data link layer protocol used to establish a direct connection between two network nodes, typically over a serial link.

72. DHCP (Dynamic Host Configuration Protocol)

A: A network protocol used to dynamically assign IP addresses and other network configuration parameters to devices on a network.

73. SNMP (Simple Network Management Protocol)

A: A protocol used for monitoring and managing devices in a network (e.g., routers, switches) by exchanging management information.

74. How are current IPv4 addresses allocated?

A: IPv4 addresses are allocated by IANA (Internet Assigned Numbers Authority) and distributed through regional internet registries (RIRs), which assign blocks to ISPs and organizations.

75. How do IPv6 addresses differ from addresses used in current IP version?

A: Uses 128-bit addresses (e.g., 2001:0db8:85a3:0000:0000:8a2e:0370:7334), allowing a vastly larger address space compared to the 32-bit IPv4 addresses (e.g., 192.168.1.1).

76. How does IPv6 address allocation differ from address allocation used with IPv4?

A: IPv6 addresses are allocated hierarchically with a larger address space and subnetting to support more devices. IPv6 uses a more flexible allocation mechanism compared to IPv4's reliance on NAT (Network Address Translation) and limited address space.

77. IPv6 is supposed to solve address allocation problems with IPv4. How is it supposed to dothat?

A: IPv6 Expands the address space from 32 bits to 128 bits, allowing for a virtually unlimited number of unique IP addresses. This eliminates the need for techniques like NAT and resolves the exhaustion of IPv4 addresses.

78. How are addresses belonging to different types differentiated from each other?

A: IPv4: Differentiated by the first few bits (e.g., Class A starts with 0, Class B with 10, etc.).
IPv6: Differentiated by the first bits of the address (e.g., Global Unicast addresses start with 001).

79. What is supernetting and subnetting?

A: Subnetting: Dividing a larger network into smaller sub-networks, improving network management and security.
Supernetting: Combining smaller networks into a larger network, typically for more efficient routing.

80. Write in decimal form the IP-address C22F1582. To which address class it belongs to? Writethe address also in binary form

A: Decimal Form: 194.47.21.130
Binary Form: 11000010.00101111.00010101.10000010
Class: Class C (Address range 192.0.0.0 to 223.255.255.255)

81. What is the network part in the address 172.16.10.50/27? What is the host part?

A: Network Part: 172.16.10.32
Host Part: .50 (within the subnet 172.16.10.32/27)

82. How many subnets are available in the network mentioned above? How many hosts can be inone subnet?

A: Number of Subnets: 8 subnets (using a /27 subnet mask).
Number of Hosts per Subnet: 30 hosts (since 2 IPs are reserved for network address and broadcast).

83. What does the notation 211.22.23.0,3 mean? What addresses belong to this definition

A: Notation: Refers to a subnet with a network address of 211.22.23.0 and a subnet mask /30, indicating 4 IP addresses in total.

Addresses: 211.22.23.0 (network), 211.22.23.1 (usable host), 211.22.23.2 (usable host), 211.22.23.3 (broadcast).

84. What are networking commands? Explain each one?

A: ipconfig: Displays and configures network settings like IP address, subnet mask, and gateway.
ping: Sends an ICMP echo request to test connectivity to a destination.
tracert: Traces the route packets take to reach a destination.
nslookup: Queries DNS to find domain name details.
netstat: Displays active network connections and listening ports.
ifconfig: (Linux) Configures and displays network interface settings.
route: Displays or modifies the routing table.
arp: Displays or modifies the ARP (Address Resolution Protocol) table.
telnet: Connects to a remote host using the Telnet protocol.

85. When you give ping command what is the output after that and also tell meaning of each term?

A: Output:
Reply from [IP Address]: The destination device is reachable.
Request Timed Out: No reply received from the destination.
TTL expired in transit: The time-to-live value of the packet expired before it reached the destination.
Meaning of terms:
TTL: Time to live, specifies the maximum hops a packet can make.
Packet Loss: The number of lost packets.
Round-trip time (RTT): Time taken for the packet to travel from the source to the destination and back.

86. What is TFTP and how it differs from FTP?

A: TFTP (Trivial File Transfer Protocol): A simple protocol for transferring files, no authentication, used for small file transfers.

FTP (File Transfer Protocol): A more robust file transfer protocol, supports authentication, and allows both file upload and download.

87. What are the common transmission rates for Ethernet?

A: 10 Mbps (10Base-T)
100 Mbps (Fast Ethernet or 100Base-T)
1 Gbps (Gigabit Ethernet or 1000Base-T)
10 Gbps (10 Gigabit Ethernet or 10GBase-T)

88. What is the difference between half and full duplex mode in Ethernet?

A: Half-Duplex: Data can flow in only one direction at a time.
Full-Duplex: Data can flow in both directions simultaneously.

89. What are the transmission speed for Cat 5, Cat 5e, Cat 6 network cable?

A: Cat 5: Up to 100 Mbps.
Cat 5e: Up to 1 Gbps (Gigabit Ethernet).
Cat 6: Up to 10 Gbps (for short distances).

90. What is the maximum connection length for Cat 5, Cat 5e, Cat6 network cable

A: Cat 5: 100 meters (for 100 Mbps).
Cat 5e: 100 meters (for 1 Gbps).
Cat 6: 55 meters (for 10 Gbps).

91. What do you mean by 10base2,10base5,10baseT and 10baseF?

A: 10Base2: 10 Mbps over coaxial cable (also known as Thin Ethernet, with a maximum cable length of 185 meters).

10Base5: 10 Mbps over coaxial cable (also known as Thick Ethernet, with a maximum cable length of 500 meters).
10BaseT: 10 Mbps over twisted pair cable (used in Ethernet networks, maximum cable length 100 meters).
10BaseF: 10 Mbps over fiber optic cable.

92. What is 192.168.1.1 IP address?
A: 192.168.1.1: Common private IP address used by home routers and modems as the default gateway.

93. What is 192.168.0.1 IP address?
A: 192.168.0.1: Another private IP address often used as a default gateway for routers and modems.

94. What is 192.168.2.1 IP address?
A: 192.168.2.1: A private IP address often used as a default gateway by some router brands.

95. How to see IP address of your PC?
A: Command: Use ipconfig (Windows) or ifconfig (Linux/macOS) in the command prompt or terminal.

96. What is meant by default gateway?
A: The IP address of a device (usually a router) that serves as the access point for devices in a local network to communicate with devices on external networks.

97. Why IP address is important in networking?
A: It uniquely identifies devices on a network and enables communication between them across different networks.

98. What is the usage of ipconfig command?
A: Displays the IP configuration details of the network interfaces on a Windows device (e.g., IP address, subnet mask, default gateway).

99. How to solve limited or no connectivity problem?
A: Check physical connections (cables, Wi-Fi).
Reboot the router and device.
Run ipconfig /release and ipconfig /renew.
Check if the correct network settings (IP, DNS) are configured.

100. What is the difference between IPv4 and IPv6?
A: IPv4: 32-bit address, provides approximately 4 billion unique addresses.
IPv6: 128-bit address, provides a virtually unlimited number of unique addresses.

101. What is IP routing?
A: The process of forwarding data packets from one network to another based on IP address information.

102. What is routing table?
A: A data structure used by routers to store information about network destinations and the paths to reach them.

103. What is basic behind Distance Vector Routing?
A: Routing protocol where routers send information about the distance to various destinations to their neighbors, which helps them update their routing tables.

104. How Link state routing works?
A: Routers share the state of their direct connections (links) with all other routers, enabling each router to independently calculate the best path to all destinations in the network.

105. How to connect 2 computers directly without router/switch?

A: Use a crossover Ethernet cable to directly connect the two computers' network ports.

106. How does proxy server work?
A: Acts as an intermediary between client devices and the internet, forwarding client requests and responses, often used for security, caching, or filtering.

107. What is client/server networking?
A: A network model where client devices request services or resources from a centralized server.

108. What is QoS (Quality of Service)?
A: Refers to the techniques used to manage network traffic to ensure the performance of critical applications, prioritize traffic, and minimize delays.

109. What is protocol?
A: A set of rules or standards that defines how devices on a network communicate with each other.

110. What is port?
A: A communication endpoint in a network used to identify specific services or applications (e.g., HTTP uses port 80).

111. What is the usage of TCP (Transmission Control Protocol)?
A: A connection-oriented protocol that ensures reliable communication by establishing a connection and guaranteeing the delivery of packets in the correct order.

112. What is the usage of UDP (User Datagram Protocol)?
A: A connectionless protocol used for fast, low-latency communication where reliability is not a priority (e.g., video streaming, VoIP).

113. What does FTP stand for?
A: File Transfer Protocol, used for transferring files between computers over a network.

114. Why do we need DNS (Domain Name Server)?
A: Resolves human-readable domain names (e.g., www.example.com) into IP addresses, enabling devices to locate websites on the internet.

115. What is Voice over IP (VoIP)?
A: Technology that allows voice communication over the internet or other IP-based networks instead of traditional phone lines.

116. What is encryption?
A: The process of converting data into a secure format to prevent unauthorized access during transmission or storage.

118. What is the wireless speed for 802.11a, 802.11b, 802.11g and 802.11n wireless standard?
A: 802.11a: Up to 54 Mbps.
802.11b: Up to 11 Mbps.
802.11g: Up to 54 Mbps.
802.11n: Up to 600 Mbps.

119. What is WiMAX?
A: Worldwide Interoperability for Microwave Access; a wireless communication standard designed for

broadband internet access over large areas.

120. Can we connect 2 computers directly and wirelessly?
A: Yes: You can use Wi-Fi Direct or Bluetooth to connect two computers directly without a router.

121. What is null modem?
A: A method of connecting two computers directly via a serial cable (usually a DB9 or DB25) without a modem, using a special cable.

122. Can we configure wireless router as an access point only?
A: Yes: Many wireless routers have an option to be configured as an access point (AP) to extend the network range.

123. Which wireless standard should I use?
A: Choice depends on requirements:
802.11a/b/g: Older standards, suitable for low-speed or legacy devices.
802.11n: Offers good speed and range, widely used.
802.11ac: Better performance, higher speed (for high-demand environments).
802.11ax (Wi-Fi 6): Latest standard with improved speed, efficiency, and range.

124. What is the difference between wireless router and access point?
A: Wireless Router: Provides routing functionality, creates a network, and often has a built-in firewall.
Access Point: Extends the existing network by providing wireless access but does not perform routing.

125. What is the difference between Wi-Fi and Bluetooth?
A: Wi-Fi: Designed for high-speed internet access over longer distances (e.g., 100 meters).
Bluetooth: Designed for short-range, low-power communication between devices (e.g., under 100 meters).

126. What is socket?
A: An endpoint for sending or receiving data across a network, often used in client-server communication.

127. What is PORT? Explain types of port number.
A: Port: A logical endpoint used for communication between network devices.
Well-known ports (0–1023): Used by widely used protocols (e.g., HTTP – port 80).
Registered ports (1024–49151): Used by software applications.
Dynamic/Private ports (49152–65535): Used for ephemeral connections.

128. What is meant by subnet mask? What is subnet mask for class A,B and C?
A: Subnet Mask: Defines the portion of an IP address that identifies the network and the portion that identifies the host.
Class A: 255.0.0.0
Class B: 255.255.0.0
Class C: 255.255.255.0

129. Explain different classes of IPV4 and also give its range?
A: Class A: 1.0.0.0 – 127.255.255.255 (16 million hosts per network)
Class B: 128.0.0.0 – 191.255.255.255 (65,000 hosts per network)
Class C: 192.0.0.0 – 223.255.255.255 (254 hosts per network)
Class D: 224.0.0.0 – 239.255.255.255 (Multicast addresses)
Class E: 240.0.0.0 – 255.255.255.255 (Reserved for future use)

130. What is NAT?
A: Network Address Translation; a method of remapping an IP address to another by modifying the IP

header in packets, commonly used for private networks to access the public internet.

131. For what purpose Class D and E is used?

A: Class D: Used for multicast addressing.
Class E: Reserved for experimental or future use.

132. What is meant by broadcast, Multicast and Unicast?

A: Broadcast: Sending data to all devices in a network (e.g., ARP request).
Multicast: Sending data to a specific group of devices (e.g., streaming).
Unicast: Sending data to a single destination device (point-to-point communication).