Core Concepts & Protocols

1.1 Differentiate between TCP and UDP.

TCP: Connection-oriented (sets up connection), reliable (error checking, retransmission, acknowledgements, flow control), slower, stream-oriented.

UDP: Connectionless, unreliable (no error checking beyond optional checksum, no retransmission, no ACKs, no flow control), faster, packet-oriented. Both are bidirectional.

1.2 What is TCP/IP?

The fundamental protocol suite for the internet. TCP provides reliable data stream delivery, while IP handles packet addressing and routing.

1.3 What is UDP?

User Datagram Protocol: A simpler, faster, connectionless alternative to TCP. Good for speed but doesn't guarantee delivery (used for DNS, VoIP, streaming).

1.4 Define Network?

A collection of interconnected devices (nodes) linked by media, allowing communication.

2. What is a Link?

The physical medium (e.g., cable, wireless signal) connecting network devices.

3. What is a node?

Any active device connected to a network (e.g., computer, router, switch).

4. What is a gateway or Router?

A device connecting different networks and directing traffic (packets) between them based on addresses.

5. What is point-point link?

A direct link connecting only two nodes.

6. What is Multiple Access?

A link shared by more than two nodes.

12. What is Protocol?

A set of rules governing how data is exchanged over a network.

13. What are the key elements of protocols?

Syntax: Data format and structure.

Semantics: Meaning of the data bits.

Timing: When and how fast data is sent.

77. What is SAP?

Service Access Point: An identifier specifying which protocol or service within a layer should handle incoming data.

100. Difference between ARP and RARP?

ARP (Address Resolution Protocol): Finds a device's MAC (hardware) address from its known IP address.

RARP (Reverse ARP): Finds a device's IP address from its known MAC address (less common now, DHCP is used).

98. What is ICMP?

Internet Control Message Protocol: Used for network error reporting and diagnostics (like ping).

Network Performance & Design

7. Advantages of Distributed Processing?

Security, distributed databases, faster problem solving, redundancy, collaboration.

8. Criteria necessary for an effective and efficient network?

Performance: Speed (throughput) and delay (latency).

Reliability: Frequency of failures and recovery time.

Security: Protection against unauthorized access and threats.

9. Factors that affect the performance of the network?

Number of users, medium type, hardware capabilities, software efficiency.

10. Factors that affect the reliability of the network?

Frequency of failures, time to recover from failures.

11. Factors that affect the security of the network?

Unauthorized access, viruses/malware.

14. Key design issues of a computer Network?

Connectivity, cost-effective resource sharing, common service support, performance.

15. Define Bandwidth and Latency?

Bandwidth: Data carrying capacity, measured in bits per second (bps). Often called throughput.

Latency: Delay for data to travel from source to destination, measured in time.

16. Define Routing?

The process of selecting paths across networks for data packets to travel.

20. What is Round Trip Time (RTT)?

The time it takes for a signal/packet to travel from source to destination and back again.

18. When a switch is said to be congested?

When it receives data faster than it can forward, causing its internal buffers to fill up and potentially drop packets.

19. What is semantic gap?

The difference between what applications need and what the underlying network technology can actually provide.

90. What is attenuation?

The weakening of signal strength as it travels over a distance.

92. Difference between bit rate and baud rate.

Bit rate: Number of bits transmitted per second.

Baud rate: Number of signal changes (symbols) per second. One symbol can represent multiple bits.

93. What is Bandwidth?

The data carrying capacity of a network link, typically measured in bits per second (bps). (Can also refer to frequency range).

155. What is Network Throughput?

The actual measured rate of successful data transfer over a network (often less than bandwidth).

OSI Model & Layers

28. List the layers of OSI.

Application, 6. Presentation, 5. Session, 4. Transport, 3. Network, 2. Data Link, 1. Physical. (Mnemonic: All People Seem To Need Data Processing)

29. Which layers are network support layers?

Physical, Data Link, Network (Layers 1-3).

30. Which layers are user support layers?

Session, Presentation, Application (Layers 5-7).

31. Which layer links the network support layers and user support layers?

Transport Layer (Layer 4).

32. Concerns of the Physical Layer?

Transmitting raw bits: voltage levels, connectors, cables, data rates, synchronization.

33. Responsibilities of Data Link Layer?

Reliable node-to-node delivery: Framing, physical addressing (MAC), error control, flow control, medium access.

34. Responsibilities of Network Layer?

Source-to-destination delivery across multiple networks: Logical addressing (IP), routing.

35. Responsibilities of Transport Layer?

End-to-end message delivery and reliability: Segmentation/reassembly, service-point addressing (ports), connection control, flow control, error control (TCP).

36. Responsibilities of Session Layer?

Managing communication sessions: Dialog control, synchronization.

37. Responsibilities of Presentation Layer?

Data format translation: Syntax/semantics, encryption, compression. Ensures data is usable by applications.

38. Responsibilities of Application Layer?

Provides network services directly to user applications (e.g., HTTP, FTP, SMTP, DNS).

111. Why should you care about the OSI Reference Model?

It provides a standard framework to understand, design, and troubleshoot network functions layer by layer.

137. Functions of different layers?

L1 (Physical): Signals & media.

L2 (Data Link): Frames, MAC addresses, local delivery.

L3 (Network): Packets, IP addresses, routing.

L4 (Transport): Segments/Datagrams, Ports, end-to-end reliability/flow control.

L5 (Session): Manages sessions.

L6 (Presentation): Data formatting, encryption.

L7 (Application): User network services.

99. Data units at different TCP/IP layers?

Application: Message

Transport: Segment (TCP) / Datagram (UDP)

Network: Datagram (or Packet)

Data Link: Frame

Physical: Bit

138. What is encapsulation?

Wrapping data from a higher layer with header/trailer information from a lower layer as it passes down the protocol stack.

Data Link Layer Details (Framing, Error/Flow Control)

60. What is Framing?

Dividing the bitstream into discrete units (frames) for transmission, often adding addresses and control info.

61. What is Fixed Size Framing?

Using frames of a constant, predefined length.

62. Define Character Stuffing?

Inserting a special "escape" character before a data character that mimics a control character (like a flag), to avoid confusion. (Also called Byte Stuffing).

63. What is Bit Stuffing?

Inserting an extra bit (usually 0) into the data stream whenever a pattern matching the flag sequence occurs naturally in the data.

64. What is Flow Control?

Mechanisms preventing a fast sender from overwhelming a slow receiver.

65. What is Error Control?

Mechanisms for detecting and correcting errors that occur during transmission.

43. What is Error Detection? What are its methods?

Identifying if data has been corrupted during transmission using redundant bits. Methods: Parity (VRC), LRC, CRC, Checksum.

51. Compare Error Detection and Error Correction:

Detection: Finds if an error exists.

Correction: Finds where the error is and fixes it (or allows fixing).

44. What is Redundancy?

Adding extra bits to data specifically for error detection or correction.

45. What is VRC?

Vertical Redundancy Check (Parity): Adds one bit per data unit to make the total number of '1's even or odd. Detects single-bit errors.

46. What is LRC?

Longitudinal Redundancy Check: Calculates parity across corresponding bits of multiple data units. Better at detecting burst errors than VRC.

47. What is CRC?

Cyclic Redundancy Check: A powerful error detection method using polynomial division.

48. What is Checksum?

Error detection where data segments are summed up; the result (or its complement) is sent with the data. Common in TCP/IP.

49. List the steps involved in creating the checksum.

Divide data into fixed-size segments. 2. Add segments using 1's complement arithmetic. 3. Complement the final sum to get the checksum.

52. What is Forward Error Correction (FEC)?

The receiver corrects errors using redundant bits, without needing retransmission from the sender.

53. Define Retransmission?

The sender resending data after the receiver detects an error or the sender doesn't receive an acknowledgement.

66. What Automatic Repeat Request (ARQ)?

Error control mechanisms using ACKs and timeouts to trigger retransmissions (e.g., Stop-and-Wait ARQ, Go-Back-N ARQ, Selective Repeat ARQ).

67. What is Stop-and-Wait Protocol?

Sender sends one frame and waits for an acknowledgement (ACK) before sending the next. Simple but inefficient.

68. What is Stop-and-Wait ARQ?

Stop-and-Wait combined with sequence numbers and timers for error detection and retransmission.

69. What is usage of Sequence Number in Reliable Transmission?

To identify frames uniquely, allowing detection of lost or duplicate frames.

70. What is Pipelining?

Allowing multiple frames to be "in flight" (sent but not yet acknowledged), improving efficiency over Stop-and-Wait.

71. What is Sliding Window?

A flow control technique allowing sender/receiver to manage a range (window) of sequence numbers for frames that can be in transit or processed.

72. What is Piggybacking?

Combining a data frame with an acknowledgement for a received frame in the reverse direction to save bandwidth.

50. What are the Data link protocols?

Specifications for implementing the Data Link Layer (e.g., Ethernet, PPP, HDLC). Categorized by sync (Async/Sync) or framing (Character/Bit oriented).

112. What is logical link control (LLC)?

An IEEE 802 standard defining the upper sublayer of the Data Link Layer; handles multiplexing, flow control, and error control independent of the specific MAC sublayer below it.

Coding & Encryption

54. What are Data Words?

In block coding, the original k-bit blocks of message data before adding redundancy.

55. What are Code Words?

The n-bit blocks created by adding r redundant bits to k-bit data words (n = k + r).

56. What is a Linear Block Code?

A block code where the XOR of any two valid codewords results in another valid codeword.

57. What are Cyclic Codes?

Linear block codes where cyclically shifting a codeword produces another valid codeword (used in CRCs).

58. Define Encoder?

A device/program that converts data into a specific coded format (e.g., for transmission, compression, error control).

59. Define Decoder?

A device/program that converts coded data back into its original format.

151. What are the other error detection & correction algorithms?

Hamming codes, Reed-Solomon codes, BCH codes, Turbo codes, LDPC codes.

152. What are key, ciphertext and plaintext?

Plaintext: Original readable message.

Ciphertext: Encrypted, unreadable message.

Key: Secret information used with an algorithm (cipher) to encrypt/decrypt.

121. Expand IDEA.

International Data Encryption Algorithm.

131. What is Kerberos?

A network authentication protocol using tickets from a trusted Key Distribution Center (KDC) for secure access.

122. What is wide-mouth frog?

An early, simple key distribution protocol using a trusted third party (KDC).

Addressing & Routing

91. What is MAC address? (Same as Q146)

Media Access Control address: A unique, hardware-based address assigned to a Network Interface Card (NIC) for Layer 2 identification.

145. What is an IP address?

Internet Protocol address: A unique logical address assigned to devices on a network for identification and routing (Layer 3).

101. What is the minimum and maximum length of the header in the TCP segment and IP datagram?

Both TCP and IPv4 headers are typically 20 bytes minimum, up to 60 bytes maximum (with options).

102. What is the range of addresses in the classes of internet addresses? (Historical)

Class A: 1.0.0.0 to 126.255.255.255

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 (Experimental): 240.0.0.0 to 255.255.255.255

(Note: Classful addressing is largely replaced by CIDR)

74. What is subnet? (Same as Q143)

A logical subdivision of a larger IP network, created via subnetting.

117. What is multicast routing?

Routing algorithms designed to efficiently deliver packets from one source to multiple specific destinations (a multicast group).

21. Define the terms Unicasting, Multiccasting and Broadcasting?

Unicast: One-to-one transmission.

Multicast: One-to-many (specific group) transmission.

Broadcast: One-to-all transmission within a network segment.

118. What is region?

In hierarchical routing, a group of routers where each router knows detailed paths within the region but only summary paths to other regions.

124. What is IGP (Interior Gateway Protocol)?

A routing protocol used within a single Autonomous System (e.g., OSPF, RIP, EIGRP).

125. What is EGP (Exterior Gateway Protocol)?

A routing protocol used between different Autonomous Systems (BGP is the standard EGP).

126. What is autonomous system (AS)?

A collection of networks under a single administrative control with common routing policies.

127. What is BGP (Border Gateway Protocol)?

The standard EGP used to exchange routing information between Autonomous Systems on the Internet.

132. What is OSPF?

Open Shortest Path First: A common link-state IGP known for efficiency and scalability.

135. What is RIP (Routing Information Protocol)?

Routing Information Protocol: An older, simpler distance-vector IGP using hop count as its metric.

136. What is source route?

An IP option allowing the sender to specify the path (sequence of routers) a packet must take.

133. What is Proxy ARP?

A router answering ARP requests on behalf of another host, making remote hosts appear local.

Network Devices & Hardware

39. What are the two classes of hardware building blocks?

Nodes (devices like computers, routers) and Links (media connecting nodes).

40. What are the different link types used to build a computer network?

Cables (Twisted Pair, Coax, Fiber), Leased Lines, Last-Mile Links (DSL, Cable Modem), Wireless Links.

41. Categories of Transmission media? (Same as Q94)

Guided: Twisted-Pair, Coaxial Cable, Fiber-Optic Cable.

Unguided (Wireless): Radio waves, Microwaves, Satellite.

87. What is cladding?
* The layer surrounding the core in a fiber-optic cable, which reflects light back into the core.

97. What are the different type of networking / internetworking devices?
* Repeater (L1): Regenerates signals.
* Hub (L1): Multi-port repeater (shared bandwidth).
* Bridge (L2): Connects LAN segments, filters traffic by MAC address.
* Switch (L2): Multi-port bridge (dedicated bandwidth per port).
* Router (L3): Connects networks, routes packets by IP address.
* Gateway (L3+): Connects dissimilar networks, often performs protocol translation.

* NIC (Network Interface Card): Hardware connecting a node to the network medium.

86. What is Brouter?
* A hybrid device that can function as both a bridge (Layer 2) and a router (Layer 3).

89. How Gateway is different from Routers?
* Router: Connects similar networks using Layer 3 (IP) addressing.
* Gateway: Broader term, often connects dissimilar networks and can translate protocols, potentially operating up to Layer 7. Routers can act as gateways.

144. What is meant by Gateway?
* A node that serves as an entry/exit point between networks, often handling routing, firewalling, or protocol translation.

109. What MAU?
* Multistation Access Unit: The central hub device used in Token Ring networks.

Network Topologies & Types

104. What are major types of networks and explain?
* Server-based: Centralized servers manage resources and security.
* Peer-to-peer: Devices share resources directly without dedicated servers.

105. What are the important topologies for networks?
* Bus: All nodes share a single cable.
* Star: All nodes connect to a central device (hub/switch).
* Ring: Nodes connect in a closed loop.
* Mesh: Nodes have multiple interconnections for redundancy.

106. What is mesh network?
* A topology where devices are interconnected with many redundant paths, increasing reliability.

85. What is passive topology?
* A topology where nodes only listen/receive the signal without regenerating or amplifying it (e.g., classic Ethernet bus).

Multiplexing & Transmission

22. What is Multiplexing?
* Combining multiple signals or data streams onto a single communication channel.

23. Name the categories of Multiplexing?
* FDM: Frequency Division Multiplexing.
* TDM: Time Division Multiplexing (Synchronous & Asynchronous/Statistical).

* WDM: Wave Division Multiplexing (used in fiber optics).

24. What is FDM?
* Dividing the link's frequency spectrum into multiple smaller channels for simultaneous analog signals.

25. What is WDM?
* Similar to FDM but uses different wavelengths (colors) of light in fiber optic cables.

26. What is TDM?
* Sharing a digital link by assigning time slots to different signals.

27. What is Synchronous TDM?
* Each device gets a fixed, dedicated time slot in every cycle, even if it has no data to send.

73. What are the two types of transmission technology available?
* Broadcast: Shared medium where transmission is received by all nodes.
* Point-to-point: Dedicated link between two nodes.

76. What are the possible ways of data exchange?
* Simplex: One direction only.
* Half-duplex: Both directions, but only one way at a time.
* Full-duplex: Both directions simultaneously.

107. Difference between baseband and broadband transmission?
* Baseband: Uses the entire channel bandwidth for a single digital signal.
* Broadband: Divides the channel into multiple frequency bands, allowing simultaneous analog or digital signals.

WAN & Specific Protocols

78. What do you meant by "triple X" in Networks?
* The set of ITU-T standards (X.3, X.28, X.29) defining terminal-to-PAD and PAD-to-network communication in X.25 networks.

79. What is frame relay, in which layer it comes?
* A fast, packet-switched WAN technology operating primarily at the Data Link Layer.

88. What is point-to-point protocol (PPP)?
* A Data Link layer protocol for establishing direct connections, common for dial-up/DSL.

134. What is SLIP (Serial Line Interface Protocol)?
* An older, simple protocol for transmitting IP datagrams over serial lines (mostly replaced by PPP).

113. What is virtual channel?
* A logical connection pathway between endpoints in packet-switched networks like ATM; acts like a dedicated circuit.

114. What is virtual path?
* In ATM, a bundle of virtual channels grouped together for management.

Traffic Management & QoS

115. What is packet filter?
* A firewall technique that inspects packet headers (IP addresses, ports) and forwards or drops them based on rules.

116. What is traffic shaping?
* Controlling the rate and pattern of network traffic flow (e.g., smoothing bursts) to achieve predictable performance or meet service agreements.

148. How do you implement Leaky bucket?
* Use a finite queue (bucket) that outputs data at a fixed rate. Incoming data fills the queue; if it overflows, data is discarded. Smooths traffic flow.

149. Differentiate between Leaky bucket and Token bucket.
* Leaky Bucket: Enforces a strict average output rate, smooths traffic, drops excess. Cannot save "credits" for future bursts.
* Token Bucket: Allows bursts up to the number of available tokens. Tokens regenerate at a fixed rate. More flexible for bursty traffic while still limiting the long-term average rate.

150. How do you generate bursty traffic?
* Create traffic patterns with high data rates for short periods, followed by periods of low or no data transmission.

119. What is silly window syndrome?
* A TCP problem where sender and receiver exchange very small data segments and ACKs, wasting bandwidth and reducing efficiency.

Application Layer & Miscellaneous

80. What is terminal emulation, in which layer it comes?
* Allows one computer to act like a terminal connected to another (e.g., Telnet, SSH). Application Layer.

129. What is NVT (Network Virtual Terminal)?
* A standard, simple terminal definition used by Telnet to ensure basic interoperability.

103. What is the difference between TFTP and FTP application layer protocols?
* FTP (File Transfer Protocol): Uses TCP for reliable, connection-oriented file transfer (separate control/data connections).
* TFTP (Trivial File Transfer Protocol): Uses UDP for simple, unreliable, connectionless file transfer.

83. What is NETBIOS and NETBEUI?
* NETBIOS: An API (programming interface) for network communication, often used on LANs (Session Layer functions).
* NETBEUI: A small, efficient, non-routable transport protocol based on NetBIOS, suitable only for small LANs.

82. What is redirector?
* Software that intercepts local requests (like file/print access) and directs them to network resources. (Related to Presentation/Application layers).

123. What is Mail Gateway?
* A server that translates between different email system protocols (e.g., SMTP to X.400).

81. What is Beaconing?
* In Token Ring/FDDI, a process where stations signal serious network failures by sending continuous "beacon" frames.

95. What is Project 802?
* An IEEE project defining standards for LANs and MANs, covering Physical and Data Link layers (e.g., 802.3 Ethernet, 802.11 Wi-Fi, 802.15 Bluetooth).

108. Explain 5-4-3 rule?
* A design rule for older, shared-medium Ethernet: Max 5 segments, 4 repeaters, and only 3 populated (host-connected) segments between any two nodes.

110. What is difference between routable and non- routable protocols?
* Routable: Contain Layer 3 network addresses that routers can use (e.g., IP).
* Non-Routable: Lack Layer 3 addressing, cannot pass through routers (e.g., NetBEUI).

120. What are Digrams and Trigrams?
* Common two-letter (digram) and three-letter (trigram) combinations in a language.

84. What is RAID?
* Redundant Array of Independent Disks: Using multiple hard drives together for performance and/or fault tolerance.

130. What is a Multi-homed Host?

* A host connected to more than one network simultaneously (has multiple NICs/IP addresses).

147. What is IPC? Name three techniques.
* Inter-Process Communication: Methods for processes to exchange data. Techniques: Message Passing (pipes, sockets), Shared Memory, Remote Procedure Calls (RPC).

153. What is simulation?
* Using a computer model to imitate the behavior of a real-world system or process.

154. Differentiate between Simulation and Emulation.
* Simulation: Models the behavior or results of a system.
* Emulation: Replicates the exact function or internal workings of a system, allowing it to substitute for the original.

139. Why fragmentation required?
* To break down large packets into smaller pieces when they need to cross a network segment with a smaller Maximum Transmission Unit (MTU).

140. What is MTU?
* Maximum Transmission Unit: The largest packet size (in bytes) that can be transmitted over a specific network link without fragmentation.

141. Which layer imposes MTU?
* The Data Link Layer (Layer 2), based on the specific technology (e.g., Ethernet's MTU is typically 1500 bytes).

142. Differentiate between Point-to-Point Connection and End-to-End connections.
* Point-to-Point: A direct link or protocol operation between two adjacent nodes (e.g., PPP link, Data Link layer focus).
* End-to-End: A connection or principle spanning the entire path between the original source and final destination hosts (e.g., TCP connection, Transport layer focus).

96. What is Protocol Data Unit (PDU)?
* The general term for a unit of data at a specific protocol layer (e.g., segment at L4, packet at L3, frame at L2).

75. Difference between the communication and transmission.
* Transmission: Physical movement of signals/bits.
* Communication: Meaningful exchange of information.