COMPUTER NETWORKS
QUESTION BANK

PART A – 2 Mark Questions with Answers | PART B – 16 Mark Questions

UNIT I – INTRODUCTION AND PHYSICAL LAYER

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is a Computer Network?	A computer network is a collection of interconnected devices (computers, servers, routers) that share resources and communicate using common protocols.
2	What are the types of networks?	Network types based on coverage: LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network), and PAN (Personal Area Network).
3	What is Protocol Layering?	Protocol layering organizes network functions into hierarchical layers, where each layer provides services to the layer above it and uses services from below. Examples: OSI, TCP/IP.
4	What is the TCP/IP Protocol Suite?	TCP/IP is a set of communication protocols organized in four layers: Application, Transport, Internet, and Network Access (Link) layer.
5	What are the layers of the OSI Model?	The OSI model has 7 layers: Physical, Data Link, Network, Transport, Session, Presentation, and Application.
6	What is the Physical Layer?	The Physical layer (Layer 1) is responsible for the transmission of raw bits over a physical medium such as cables, fiber, or wireless signals.
7	What is Bandwidth?	Bandwidth is the maximum rate of data transfer across a network path, measured in bits per second (bps).
8	What is Throughput?	Throughput is the actual rate of successful data transfer over a network, which may be less than bandwidth due to congestion and overhead.
9	What is Circuit Switching?	Circuit switching establishes a dedicated communication path between sender and receiver for the entire duration of the session. Example: traditional telephone networks.
10	What is Packet Switching?	Packet switching divides data into packets that are independently routed through the network and reassembled at the destination. Example: internet.

11	What are Transmission Media?	Transmission media carry data signals. Guided media: twisted pair, coaxial cable, fiber optic. Unguided media: radio waves, microwaves, infrared.
12	Differentiate Circuit Switching and Packet Switching.	Circuit switching reserves a dedicated path (fixed bandwidth, low delay). Packet switching shares network resources dynamically (efficient, variable delay).

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain the OSI Reference Model in detail. Describe the functions of each of the seven layers with examples.
2	Explain the TCP/IP Protocol Suite. Compare it with the OSI model, highlighting similarities and differences.
3	Explain the various types of Transmission Media: guided (twisted pair, coaxial, fiber optic) and unguided (radio, microwave, infrared) with their characteristics.
4	Explain Circuit Switching and Packet Switching in detail. Compare their performance, advantages, and disadvantages.
5	Explain the Physical Layer: performance metrics (bandwidth, throughput, latency), transmission impairments, and switching techniques.

UNIT II – DATA LINK LAYER & MEDIA ACCESS

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is the Data Link Layer?	The Data Link Layer (Layer 2) provides node-to-node data transfer, handles framing, error detection/correction, and MAC addressing.
2	What is a MAC Address?	A MAC (Media Access Control) address is a unique 48-bit hardware identifier assigned to a network interface card for communication within a local network.
3	What are DLC Services?	DLC (Data Link Control) services include framing (packaging bits into frames), flow control, and error control between adjacent nodes.
4	What is HDLC?	HDLC (High-level Data Link Control) is a bit-oriented data link protocol providing error detection, flow control, and framing for point-to-point and multipoint links.
5	What is PPP?	PPP (Point-to-Point Protocol) is a data link protocol used to establish a direct connection between two nodes, commonly used for dial-up and DSL connections.
6	What is Media Access Control (MAC)?	MAC is a sublayer of the Data Link layer that controls how devices on a shared medium access the channel, using protocols like CSMA/CD and CSMA/CA.
7	What is Ethernet?	Ethernet is the most widely used wired LAN technology (IEEE 802.3) that uses CSMA/CD for media access and supports speeds from 10 Mbps to 100 Gbps.
8	What is CSMA/CD?	CSMA/CD (Carrier Sense Multiple Access with Collision Detection) is the MAC protocol used in wired Ethernet where devices detect and recover from collisions.
9	What is IEEE 802.11?	IEEE 802.11 is the standard for wireless LANs (Wi-Fi) defining the protocols for wireless communication in the 2.4 GHz and 5 GHz frequency bands.
10	What is Bluetooth?	Bluetooth (IEEE 802.15) is a short-range wireless technology for connecting devices over 2.4 GHz within about 10 meters, used for PANs.
11	What is CSMA/CA?	CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance) is the MAC protocol used in wireless LANs (Wi-Fi) to avoid collisions before transmission.

12	What are Connecting Devices?	Connecting devices link network segments: Repeaters (Layer 1), Bridges/Switches (Layer 2), Routers (Layer 3), and Gateways (all layers).

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain Data Link Layer services: framing, flow control, and error control. Describe Go-Back-N and Selective Repeat ARQ protocols.
2	Explain HDLC protocol in detail: frame structure, frame types, and modes of operation with diagrams.
3	Explain PPP (Point-to-Point Protocol): frame structure, phases of a PPP session, and services provided.
4	Explain Ethernet (IEEE 802.3): frame format, CSMA/CD protocol, and evolution from 10 Mbps to Gigabit Ethernet.
5	Explain Wireless LANs: IEEE 802.11 architecture, CSMA/CA, frame format, and Bluetooth technology for PANs.

UNIT III – NETWORK LAYER

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is the Network Layer?	The Network Layer (Layer 3) is responsible for logical addressing, routing packets across multiple networks, and delivering them from source to destination.
2	What is an IPv4 Address?	An IPv4 address is a 32-bit logical address written in dotted decimal notation (e.g., 192.168.1.1) that uniquely identifies a device on a network.
3	What is IP?	IP (Internet Protocol) is the primary network layer protocol responsible for addressing and routing packets from source to destination across interconnected networks.
4	What is ICMP?	ICMP (Internet Control Message Protocol) is used by network devices to send error messages and operational information (e.g., ping uses ICMP Echo request/reply).
5	What is ARP?	ARP (Address Resolution Protocol) maps a known IPv4 address to its corresponding MAC address within a local network.
6	What is RARP?	RARP (Reverse ARP) maps a known MAC address to an IP address, historically used by diskless workstations to obtain their IP at boot time.
7	What is DHCP?	DHCP (Dynamic Host Configuration Protocol) automatically assigns IP addresses, subnet masks, gateways, and DNS server addresses to hosts on a network.
8	What is Routing?	Routing is the process of selecting the best path for packets to travel from source to destination across an internetwork using routing algorithms and tables.
9	What is IPv6?	IPv6 is the 128-bit successor to IPv4, providing a vastly larger address space, improved security, auto-configuration, and simplified headers.
10	What is Unicast Routing?	Unicast routing delivers packets from one source to one specific destination using routing protocols like RIP, OSPF, or BGP.
11	What is Multicasting?	Multicasting delivers packets from one source to a group of interested receivers simultaneously, more efficient than sending individual unicast copies.
12	What is the difference between IPv4 and IPv6?	IPv4 uses 32-bit addresses (4.3 billion). IPv6 uses 128-bit addresses (virtually unlimited), adds built-in IPsec, stateless auto-configuration, and no broadcast.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain IPv4 addressing: classful addressing, subnetting, CIDR, and special addresses with examples.
2	Explain IP protocol: IPv4 datagram format, fragmentation, options, and forwarding with diagrams.
3	Explain Unicast Routing Algorithms: Distance Vector Routing (RIP) and Link State Routing (OSPF) with examples.
4	Explain IPv6: addressing format, IPv6 datagram structure, advantages over IPv4, and transition mechanisms from IPv4 to IPv6.
5	Explain ARP, RARP, and DHCP protocols: their purpose, working mechanism, and message formats with examples.

UNIT IV – TRANSPORT LAYER

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is the Transport Layer?	The Transport Layer (Layer 4) provides end-to-end communication, error recovery, flow control, and multiplexing between processes on different hosts.
2	What is a Port Number?	A port number is a 16-bit identifier that distinguishes different applications/processes on the same host. Well-known ports: 80 (HTTP), 443 (HTTPS), 21 (FTP).
3	What is UDP?	UDP (User Datagram Protocol) is a connectionless, unreliable transport protocol that provides fast, low-overhead data transmission without error recovery.
4	What is TCP?	TCP (Transmission Control Protocol) is a connection-oriented, reliable transport protocol providing ordered delivery, error recovery, and flow/congestion control.
5	What is the TCP Three-Way Handshake?	TCP establishes connections using three steps: SYN (client to server), SYN-ACK (server to client), ACK (client to server).
6	What is Flow Control in TCP?	TCP flow control uses a sliding window mechanism where the receiver advertises its buffer size (window size) to prevent the sender from overwhelming it.
7	What is Congestion Control?	TCP congestion control prevents network overload using algorithms like Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery.
8	What is SCTP?	SCTP (Stream Control Transmission Protocol) is a transport protocol that combines features of TCP and UDP, supporting multi-streaming and multi-homing.
9	What is Multiplexing in Transport Layer?	Multiplexing allows multiple application processes to use the network simultaneously by assigning each a unique port number for identification.
10	Differentiate TCP and UDP.	TCP: connection-oriented, reliable, ordered, slower. UDP: connectionless, unreliable, unordered, faster. TCP for file transfer; UDP for streaming/DNS.
11	What is a Socket?	A socket is the combination of an IP address and a port number (e.g., 192.168.1.1:80) that uniquely identifies a communication endpoint.
12	What is Slow Start in TCP?	Slow Start is a TCP congestion control algorithm that begins with a small congestion window and doubles it each RTT until a threshold is reached.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain UDP protocol: segment format, services provided, applications that use UDP, and why UDP is preferred over TCP in some cases.
2	Explain TCP protocol in detail: segment format, connection establishment (three-way handshake), data transfer, and connection termination.
3	Explain TCP Flow Control and Congestion Control: sliding window protocol, Slow Start, Congestion Avoidance, Fast Retransmit, and Fast Recovery.
4	Explain SCTP (Stream Control Transmission Protocol): features, packet format, association establishment, multi-streaming, and multi-homing.
5	Explain Transport Layer services: connection-oriented vs connectionless, multiplexing/demultiplexing, port numbers, and error control mechanisms.

UNIT V – APPLICATION LAYER

PART A – 2 Mark Questions with Answers

Q.No	Question	Answer
1	What is the Application Layer?	The Application Layer (Layer 7) provides network services directly to end-user applications such as web browsing, email, and file transfer.
2	What is HTTP?	HTTP (HyperText Transfer Protocol) is the stateless application-layer protocol used to transfer web pages between a web server and client browser.
3	What is the World Wide Web (WWW)?	The WWW is a system of interlinked hypertext documents accessed via the internet using HTTP, identified by URLs and rendered by web browsers.
4	What is FTP?	FTP (File Transfer Protocol) is an application-layer protocol used to transfer files between a client and server over a TCP connection using ports 20 and 21.
5	What is Email?	Email (Electronic Mail) uses protocols SMTP (for sending), POP3/IMAP (for receiving) to send and receive messages across networks.
6	What is SMTP?	SMTP (Simple Mail Transfer Protocol) is the standard protocol for sending email from a client to a mail server and between mail servers, using port 25.
7	What is Telnet?	Telnet is an application-layer protocol that provides a command-line interface for remote login to another computer over a TCP/IP network using port 23.
8	What is SSH?	SSH (Secure Shell) is a cryptographic network protocol for secure remote login and command execution over an unsecured network, replacing Telnet, using port 22.
9	What is DNS?	DNS (Domain Name System) translates human-readable domain names (e.g., www.google.com) into IP addresses using a hierarchical distributed database.
10	What is SNMP?	SNMP (Simple Network Management Protocol) is used to monitor and manage network devices (routers, switches, servers) by collecting and organizing information.
11	What is a DNS Record?	DNS records store information about domains. Common types: A (IPv4 address), AAAA (IPv6), MX (mail server), CNAME (alias), NS (name server).
12	Differentiate HTTP and HTTPS.	HTTP transmits data in plain text (insecure). HTTPS uses SSL/TLS to encrypt HTTP traffic,

		providing security, authentication, and data integrity.

PART B – 16 Mark Questions

Q.No	Question (16 Marks)
1	Explain WWW and HTTP: web architecture, HTTP request/response format, HTTP methods, persistent vs non-persistent connections, and HTTP/2 improvements.
2	Explain FTP protocol: architecture, active vs passive mode, control and data connections, and FTP commands with examples.
3	Explain Email protocols: SMTP (sending), POP3 and IMAP (receiving) — message format, working, and differences between POP3 and IMAP.
4	Explain DNS in detail: domain name hierarchy, resource records, name resolution process (iterative and recursive), and DNS security issues.
5	Explain Telnet, SSH, and SNMP: purpose, working, security comparison between Telnet and SSH, and SNMP architecture with MIB.