CN Question Bank

Computer Network Question Bank Answers

1. What is a computer network? List out Advantages. *(5 Marks)*

Definition (1 Mark):

A computer network is a system where multiple computers and devices are connected to share resources, data, and applications. Networks can be wired or wireless.

Advantages (4 Marks):

1. **Resource Sharing** – Users can share hardware (printers, scanners) and software.
2. **Communication** – Enables emails, chats, and video conferencing.
3. **Centralized Data Management** – Data can be stored on a central server for easy access.
4. **Security & Backup** – Data can be protected with encryption and regular backups.

---

2. What are the different types of computer networks? *(5 Marks)*

Definition (1 Mark):

A computer network can be categorized based on size and purpose.

Types (4 Marks):

1. **Local Area Network (LAN)** – Covers a small area like offices or homes.
2. **Metropolitan Area Network (MAN)** – Covers a city or large campus.
3. **Wide Area Network (WAN)** – Spans large areas, such as different cities or countries.
4. **Personal Area Network (PAN)** – Small-scale network for personal use (e.g., Bluetooth).

3. Difference between LAN, MAN, and WAN (5 Marks)

1. **LAN (Local Area Network)** – Covers a small area like a home, office, or school. It has high speed and low latency. Example: Wi-Fi in a college.
2. **MAN (Metropolitan Area Network)** – Covers a city or large area, often using fiber optics. Example: City-wide broadband network.
3. **WAN (Wide Area Network)** – Covers a large geographical area, connecting multiple LANs and MANs. Example: The Internet.
4. **Speed Comparison** – **LAN > MAN > WAN** in terms of speed.
5. **Ownership** – LAN is privately owned, MAN is often by ISPs, WAN is public or privately owned.

---

4. What is an IP Address? Difference Between IPv4 and IPv6 (5 Marks)

IP Address: A **unique numerical label** assigned to devices for identification and communication over a network.

Difference Between IPv4 and IPv6:

1. **Address Length** – IPv4 is **32-bit**, IPv6 is **128-bit**.
2. **Address Format** – IPv4: **192.168.1.1**, IPv6: **2001:db8::1**.
3. **Address Capacity** – IPv4 supports **~4.3 billion** addresses, IPv6 supports **trillions**.
4. **Security** – IPv6 has **built-in encryption**, IPv4 requires additional security measures.

---

5. What is a Router and How Does It Work? (5 Marks)

Router: A **networking device** that connects multiple networks and directs data packets between them.

Functions of a Router:

1. **Data Forwarding** – Routes data based on **IP addresses**.

2. **Best Path Selection** – Uses algorithms to find the **fastest** and **most efficient** route.
3. **Network Segmentation** – Separates networks for **better security and performance**.
4. **Provides Internet Access** – Connects local networks to the **Internet**.

---

6. What is a Switch? Difference Between Switch and Hub (5 Marks)

Switch: A **networking device** that connects multiple devices in a LAN and forwards data only to the intended recipient.

Difference Between Switch and Hub:

1. **Data Handling** – **Switch** uses **MAC addresses**, **Hub** broadcasts data to all.
2. **Efficiency** – **Switch** reduces **network congestion**, **Hub** increases it.
3. **Speed** – **Switches** are **faster**, **Hubs** cause delays.
4. **Network Type** – **Switches** are used in **modern LANs**, **Hubs** are outdated.

7. Different Layers of the OSI Model (5 Marks)

The **OSI (Open Systems Interconnection) Model** has **7 layers**, each with a specific function:

1. **Physical Layer** – Transmits raw bits over a physical medium (cables, wireless).
2. **Data Link Layer** – Handles MAC addressing and error detection (e.g., Ethernet, switches).
3. **Network Layer** – Manages IP addressing and routing (e.g., routers, IP protocol).
4. **Transport Layer** – Ensures reliable data transmission using **TCP/UDP**.
5. **Session Layer** – Manages and controls sessions between devices.
6. **Presentation Layer** – Formats, encrypts, and compresses data.

7. **Application Layer** – Provides network services to users (e.g., HTTP, FTP, SMTP).

---

8. Function of the Transport Layer in the OSI Model (5 Marks)

The **Transport Layer** is responsible for **end-to-end communication** between devices.

Functions:

1. **Reliable Data Transfer** – Uses **TCP** for error-free communication.
2. **Segmentation and Reassembly** – Breaks data into segments and reassembles at the destination.
3. **Flow Control** – Prevents data overflow using buffering techniques.
4. **Error Control** – Ensures data integrity using acknowledgments and retransmissions.
5. **Multiplexing** – Allows multiple applications to send/receive data simultaneously.

---

9. Purpose of the TCP/IP Model (5 Marks)

The **TCP/IP Model** is a networking framework that enables communication over the internet.

Purpose:

1. **Standardized Communication** – Defines rules for data exchange between devices.
2. **Interconnectivity** – Allows different networks to communicate globally.
3. **Reliability** – Ensures accurate data transfer using **TCP (Transmission Control Protocol)**.
4. **Scalability** – Supports small and large networks (LAN, WAN, Internet).
5. **Efficiency** – Uses **packet switching** for fast data transmission.

---

10. What is a Virtual LAN (VLAN)? Explain with an Example (5 Marks)

A **VLAN (Virtual Local Area Network)** is a **logical segmentation** of a physical network into multiple isolated networks.

Example:

- A company has **HR, IT, and Finance** departments on the same physical network.
- Using **VLANs**, the network is divided so HR cannot access IT data, improving **security** and **performance**.
- VLAN **reduces broadcast traffic** and improves network management.

---

11. What is the difference between TCP and UDP? *(5 Marks)*

Definition (1 Mark):

TCP (Transmission Control Protocol) and UDP (User Datagram Protocol) are transport layer protocols used for communication between devices.

Differences (4 Marks):

1. **TCP – Connection-oriented; UDP – Connectionless.**
2. **TCP – Ensures reliability; UDP – Faster but unreliable.**
3. **TCP – Uses error checking and retransmission; UDP – No retransmission.**
4. **TCP – Suitable for web browsing and emails; UDP – Ideal for gaming and video streaming.**

---

12. What is DNS, and how does it work? *(5 Marks)*

Definition (1 Mark):

DNS (Domain Name System) is a protocol that translates human-readable domain names (e.g., www.google.com) into IP addresses.

Working (4 Marks):

1. **User Request** – The user enters a website URL in a browser.
2. **DNS Query** – The request is sent to a DNS resolver.

3. **IP Resolution** – The resolver queries a DNS server to find the corresponding IP address.
4. **Connection Establishment** – The IP address is returned to the browser, and the connection is established.

---

13. DHCP (Dynamic Host Configuration Protocol) and Its Importance *(5 Marks)*

Definition (1 Mark):

DHCP (Dynamic Host Configuration Protocol) is a network protocol that automatically assigns IP addresses and other network configurations (such as subnet mask, gateway, and DNS) to devices on a network.

Importance (4 Marks):

1. **Automatic IP Assignment** – Reduces manual configuration errors and saves time.
2. **Efficient IP Management** – Prevents IP conflicts by dynamically assigning and reusing addresses.
3. **Scalability** – Ideal for large networks where assigning IPs manually is impractical.
4. **Network Connectivity** – Ensures devices can connect to the network without manual setup.

---

14. What is a router and how does it work? *(5 Marks)*

Definition (1 Mark):

A router is a networking device that directs data between different networks and ensures efficient data transmission.

Working (4 Marks):

1. **Packet Examination** – Examines data packets and determines the best route based on IP addresses.
2. **Routing Decisions** – Uses routing tables and protocols (RIP, OSPF, BGP) to manage network paths.

3. **Network Connectivity** – Connects different types of networks (LAN, WAN, internet) securely.
4. **Data Forwarding** – Filters and forwards packets to the correct destination.

15. What is subnetting, and why is it used? *(5 Marks)*

Definition (1 Mark):

Subnetting is the process of dividing a large network into smaller subnetworks to improve efficiency and security.

Uses (4 Marks):

1. **Efficient IP Address Utilization** – Reduces wastage of IP addresses.
2. **Improved Security** – Isolates network segments to enhance security.
3. **Better Network Performance** – Reduces congestion by limiting broadcast traffic.
4. **Simplifies Management** – Makes troubleshooting and maintenance easier.

---

16. What is a VPN, and how does it improve network security? *(5 Marks)*

Definition (1 Mark):

A VPN (Virtual Private Network) is a secure connection that encrypts data while transmitting over the internet, ensuring privacy.

Security Improvements (4 Marks):

1. **Data Encryption** – Protects sensitive information from hackers.
2. **Anonymity** – Hides the user's IP address to enhance privacy.
3. **Secure Remote Access** – Allows employees to securely access a private network from anywhere.
4. **Prevents ISP Tracking** – Stops internet service providers from monitoring online activity.

---

17. What is a MAC address, and how is it different from an IP address? *(5 Marks)*

Definition (1 Mark):

A MAC (Media Access Control) address is a unique identifier assigned to a network interface card (NIC) of a device.

Differences (4 Marks):

1. **MAC Address – Physical identifier; IP Address – Logical identifier.**
2. **MAC Address – Unique to the device; IP Address – Changes based on network.**
3. **MAC Address – Works at the Data Link Layer; IP Address – Works at the Network Layer.**
4. **MAC Address – Remains constant; IP Address – Can be reassigned dynamically.**

---

18. Explain File Transfer Protocol in detail? *(5 Marks)*

Definition (1 Mark):

File Transfer Protocol (FTP) is a standard network protocol used to transfer files between a client and a server.

Features (4 Marks):

1. **Uses TCP for Reliable Transfer** – Ensures data is delivered without loss.
2. **Supports Authentication** – Users need credentials for secure access.
3. **Allows File Upload & Download** – Enables bidirectional file transfer.
4. **Uses Active & Passive Modes** – Provides flexibility in connection setup.

---

19. Discuss about Simple Network Management Protocol (SNMP)? *(5 Marks)*

Definition (1 Mark):

SNMP (Simple Network Management Protocol) is a protocol used for managing and monitoring network devices such as routers, switches, and servers.

Features (4 Marks):

1. **Monitors Network Performance** – Helps in tracking bandwidth usage and uptime.
2. **Fault Detection** – Identifies and reports network failures.
3. **Remote Device Management** – Allows administrators to control devices remotely.
4. **Uses Management Information Base (MIB)** – Stores network data for easy access.

---

20. What do you mean by InterVLAN Routing? Explain with an example. *(5 Marks)*

Definition (1 Mark):

InterVLAN Routing is a technique used to enable communication between different VLANs within a network using a router or Layer 3 switch.

Example (4 Marks):

1. **Scenario:** A company has two VLANs – VLAN 10 for HR and VLAN 20 for IT.
2. **Without InterVLAN Routing:** Devices in VLAN 10 cannot communicate with devices in VLAN 20.
3. **With InterVLAN Routing:** A Layer 3 switch or router is configured to allow traffic between VLANs.
4. **Implementation:** The router has sub-interfaces for each VLAN and routes traffic accordingly.

---

21. Explain the protocol used to send an email from one machine to another? *(5 Marks)*

Definition (1 Mark):

SMTP (Simple Mail Transfer Protocol) is the standard protocol used for sending emails between mail servers.

Working (4 Marks):

1. **Sender's Email Client** – Uses SMTP to send the email to the mail server.

2. **Mail Server Processing** – The email is stored and forwarded to the recipient's mail server.
3. **Recipient's Mail Server** – Uses SMTP to deliver the email.
4. **Email Retrieval** – The recipient can download the email using POP3 or IMAP.

---

22. Explain Carrier Sense Multiple Access with Collision Detection (CSMA/CD) and Collision Avoidance (CSMA/CA)? *(5 Marks)*

Definition (1 Mark):

CSMA/CD (Collision Detection) and CSMA/CA (Collision Avoidance) are network access methods used in Ethernet and wireless networks to manage data transmission.

Working (4 Marks):

1. **CSMA/CD (Used in Wired Networks):**
   - Detects collisions in Ethernet networks.
   - If a collision occurs, devices stop transmitting and wait before retrying.
   - Used in older Ethernet (half-duplex communication).
2. **CSMA/CA (Used in Wireless Networks):**
   - Avoids collisions by waiting for the channel to be free before transmitting.
   - Uses an acknowledgment (ACK) system to confirm successful transmission.
   - Used in Wi-Fi networks for better efficiency.

23. Write the functionality of the Physical Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Physical Layer is the first layer of the OSI model responsible for transmitting raw data bits over a physical medium.

Functionality (4 Marks):

1. **Bit Transmission** – Converts data into electrical, optical, or radio signals for transmission.
2. **Physical Media Handling** – Defines connectors, cables, and transmission media (e.g., fiber optic, Ethernet).
3. **Data Rate Control** – Manages the speed of data transmission between devices.
4. **Synchronization of Bits** – Ensures sender and receiver are synchronized for accurate data transfer.

---

24. Write the functionality of the Data-Link Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Data-Link Layer is the second layer of the OSI model that ensures reliable data transfer between two directly connected nodes.

Functionality (4 Marks):

1. **Framing** – Divides data into frames for transmission.
2. **Error Detection & Correction** – Uses CRC (Cyclic Redundancy Check) to detect transmission errors.
3. **MAC Addressing** – Assigns unique MAC addresses to devices for identification.
4. **Flow Control** – Regulates data flow to prevent congestion in the network.

---

25. Write the functionality of the Network Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Network Layer is the third layer of the OSI model responsible for routing and forwarding data between different networks.

Functionality (4 Marks):

1. **Logical Addressing** – Uses IP addresses to identify devices in different networks.
2. **Routing** – Determines the best path for data to reach its destination.
3. **Packet Forwarding** – Transfers data packets between source and destination networks.
4. **Fragmentation & Reassembly** – Breaks large data packets into smaller ones for efficient transmission.

---

26. Write the functionality of the Application Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Application Layer is the seventh and topmost layer of the OSI model that provides network services directly to end-users.

Functionality (4 Marks):

1. **User Interface Services** – Provides protocols for email, web browsing, and file transfer (e.g., HTTP, FTP, SMTP).
2. **Data Formatting & Translation** – Ensures compatibility between different devices and applications.
3. **Authentication & Encryption** – Provides security mechanisms such as SSL/TLS.
4. **Session Management** – Manages user sessions and maintains connection integrity.

27. Write the functionality of the Session Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Session Layer is the fifth layer of the OSI model responsible for establishing, managing, and terminating communication sessions between applications.

Functionality (4 Marks):

1. **Session Establishment** – Initiates communication between devices.

2. **Session Maintenance** – Keeps the session active during data exchange.
3. **Synchronization** – Uses checkpoints to resume communication in case of failure.
4. **Session Termination** – Properly closes active sessions after data transfer.

---

28. Write the functionality of the Presentation Layer of the OSI Model. *(5 Marks)*

Definition (1 Mark):

The Presentation Layer is the sixth layer of the OSI model responsible for data formatting, encryption, and compression.

Functionality (4 Marks):

1. **Data Translation** – Converts data formats between sender and receiver.
2. **Encryption & Decryption** – Ensures secure data transmission using protocols like SSL/TLS.
3. **Data Compression** – Reduces data size to optimize bandwidth usage.
4. **Character Encoding** – Converts text formats such as ASCII and Unicode.

---

29. What do you mean by Virtual LAN (VLAN) Concept? *(5 Marks)*

Definition (1 Mark):

A Virtual LAN (VLAN) is a logically segmented network within a physical network, allowing devices to communicate as if they were on the same LAN, even if physically separated.

Features (4 Marks):

1. **Improves Security** – Segregates sensitive data from other traffic.
2. **Enhances Performance** – Reduces network congestion by limiting broadcast domains.
3. **Flexibility** – Devices in different locations can be part of the same VLAN.
4. **Easy Management** – Simplifies network administration without physical reconfiguration.

30. What is the Address Resolution Protocol (ARP)? It works on which layer of the OSI Model? *(5 Marks)*

Definition (1 Mark):

ARP (Address Resolution Protocol) is used to map an IP address to a MAC address in a local network.

Functionality (4 Marks):

1. **IP to MAC Mapping** – Converts logical IP addresses to physical MAC addresses.
2. **Broadcast Request** – Sends a query to all devices asking for the MAC address of a given IP.
3. **Response Handling** – The device with the matching IP address replies with its MAC address.
4. **Works at Data Link Layer (Layer 2)** – Used for communication within a local network.

---

31. What is the Reverse Address Resolution Protocol (RARP)? It works on which layer of the OSI Model? *(5 Marks)*

Definition (1 Mark):

RARP (Reverse Address Resolution Protocol) is used to find an IP address associated with a given MAC address.

Functionality (4 Marks):

1. **MAC to IP Mapping** – Helps diskless devices obtain an IP address.
2. **Request Mechanism** – Sends a request to a RARP server to obtain an IP address.
3. **Server Response** – The RARP server replies with the corresponding IP address.
4. **Works at Data Link Layer (Layer 2)** – Operates within local networks.

---

32. Explain Guided and Unguided Media? Write its advantages and disadvantages. *(5 Marks)*

Definition (1 Mark):

Transmission media in networking can be classified into **Guided Media** (wired) and **Unguided Media** (wireless).

Types & Features (4 Marks):

1. **Guided Media (Wired):**
   - Uses cables like coaxial, fiber optic, and twisted pair.
   - Advantages: High speed, reliable, secure.
   - Disadvantages: Expensive, difficult to install.
2. **Unguided Media (Wireless):**
   - Uses radio waves, microwaves, and infrared.
   - Advantages: Flexible, easy to install.
   - Disadvantages: Prone to interference, security risks.

---

33. What do you mean by Routing Information Protocol? How to make a configuration in Cisco Packet Tracer? *(5 Marks)*

Definition (1 Mark):

Routing Information Protocol (RIP) is a distance-vector routing protocol used to determine the best path for data transmission in small to medium-sized networks.

Configuration in Cisco Packet Tracer (4 Marks):

1. **Enable RIP** – Use the command `router rip` in global configuration mode.
2. **Specify Network Addresses** – Add networks using `network [network address]`.
3. **Enable RIP Version 2** – Use `version 2` for classless routing.
4. **Verify Configuration** – Use `show ip route` to check RIP routes.

---

34. What do you mean by OSPF Protocol? How to make a configuration in Cisco Packet Tracer? *(5 Marks)*

Definition (1 Mark):

OSPF (Open Shortest Path First) is a link-state routing protocol used in large networks for efficient and scalable routing.

Configuration in Cisco Packet Tracer (4 Marks):

1. **Enable OSPF** – Use the command `router ospf [process-id]`.
2. **Specify Network & Wildcard Mask** – Use `network [network] [wildcard] area [area-id]`.
3. **Assign Router IDs** – Use `router-id [id]` for unique identification.
4. **Verify Configuration** – Use `show ip ospf neighbor` and `show ip route`.

---

35. What is the use of get, set commands in File Transfer Protocol? Give an example? *(5 Marks)*

Definition (1 Mark):

The `get` and `set` commands in FTP (File Transfer Protocol) are used for downloading and uploading files between a client and a server.

Example (4 Marks):

1. **GET Command (Download File)** – `get filename.txt` downloads a file from the server.
2. **PUT Command (Upload File)** – `put filename.txt` uploads a file to the server.
3. **LIST Command** – `ls` or `dir` lists available files on the server.
4. **EXIT Command** – `bye` or `quit` terminates the FTP session.

---

36. What do you mean by switching technique? How to do a demonstration in Cisco Packet Tracer? *(5 Marks)*

Definition (1 Mark):

Switching techniques determine how data is transferred between devices in a network. Types include circuit switching, packet switching, and message switching.

Demonstration in Cisco Packet Tracer (4 Marks):

1. **Create a Network Topology** – Add switches, routers, and PCs.
2. **Assign IP Addresses** – Configure devices with proper addressing.

3. **Configure VLANs (If Required)** – Assign VLANs to separate traffic.
4. **Test Communication** – Use `ping` to verify successful data transmission.

---

37. Explain Encryption Technique in detail? *(5 Marks)*

Definition (1 Mark):

Encryption is a technique used to convert plaintext data into unreadable ciphertext to protect it from unauthorized access.

Features (4 Marks):

1. **Symmetric Encryption** – Uses a single key for encryption and decryption (e.g., AES, DES).
2. **Asymmetric Encryption** – Uses a public key for encryption and a private key for decryption (e.g., RSA).
3. **Hashing** – Converts data into a fixed-size hash value (e.g., SHA, MD5).
4. **End-to-End Encryption** – Ensures data remains encrypted throughout transmission.

---

38. Differentiate between Symmetric and Asymmetric Encryption Techniques? *(5 Marks)*

Definition (1 Mark):

Symmetric encryption uses one key for both encryption and decryption, while asymmetric encryption uses a pair of public and private keys.

Differences (4 Marks):

1. **Symmetric – Faster; Asymmetric – Slower due to key complexity.**
2. **Symmetric – Uses one key; Asymmetric – Uses two keys.**
3. **Symmetric – Suitable for large data encryption; Asymmetric – Used in secure key exchanges.**
4. **Examples:** AES, DES (Symmetric); RSA, ECC (Asymmetric).

---

39. What is the difference between Static and Dynamic Routing technique? *(5 Marks)*

Definition (1 Mark):

Static routing uses manually configured routes, while dynamic routing uses protocols to automatically determine paths.

Differences (4 Marks):

1. **Static – Manually configured; Dynamic – Automatically updated.**
2. **Static – No overhead; Dynamic – Uses processing resources.**
3. **Static – Suitable for small networks; Dynamic – Used in large, scalable networks.**
4. **Examples:** RIP, OSPF (Dynamic); Manual IP route (Static).

---

40. What is the difference between Connectionless and Connection-Oriented Transmission technique? *(5 Marks)*

Definition (1 Mark):

Connection-oriented transmission establishes a dedicated connection before data transfer, while connectionless transmission sends data without prior setup.

Differences (4 Marks):

1. **Connection-Oriented – Reliable; Connectionless – Unreliable but faster.**
2. **Connection-Oriented – Uses handshaking (TCP); Connectionless – No handshake (UDP).**
3. **Connection-Oriented – Used for file transfers, emails; Connectionless – Used for video streaming, VoIP.**
4. **Examples:** TCP (Connection-Oriented); UDP (Connectionless).
