

CLASS 9 • COMPUTER SCIENCE & ENTREPRENEURSHIP

CHAPTER 06

Introduction To Computer Networks

Complete Exercise Solutions

10

Solved MCQs

10

Short Questions

9

Long Questions

A

Multiple Choice Questions

Correct answers are ticked & highlighted, each with an explanation

Q1

What is the primary objective of computer networks?

A

Increase computational power

B

Enable resource sharing and data communication



C

Enhance graphic capabilities

D

Improve software development



Correct Answer: (b) Enable resource sharing and data communication

Explanation: The fundamental purpose of connecting computers into a network is to allow them to share hardware, software, and data, as well as to communicate efficiently (e.g., via email or messaging). While networks can facilitate distributed computing (a), the primary, defining objective is resource sharing and communication.

Q2

Which device is used to connect multiple networks and direct data packets between them?

A

Switch

B

Hub

C

Router



D

Modem



Correct Answer: (c) Router

Explanation: A router operates at the Network Layer (Layer 3) of the OSI model. Its primary function is to connect different networks (like connecting a home network to the internet) and determine the best path (routing) for data packets to reach their destination. Hubs and switches connect devices *within* a single network, and modems convert signals for transmission over telephone/cable lines.

Q3

Which layer of the OSI model is responsible for node-to-node data transfer and error detection?

A

Physical Layer

B

Data Link Layer



C

Network Layer

D

Transport Layer



Correct Answer: (b) Data Link Layer

Explanation: The Data Link Layer (Layer 2) is responsible for transferring data between nodes on the same network segment. It packages data into frames, uses MAC addresses for physical addressing, and performs error detection (using techniques like CRC) to ensure data is received correctly.

Q4

What is the function of the Domain Name System (DNS)?

- ☐ A Assign IP addresses dynamically
- ☒ B Translate domain names to IP addresses
- ☐ C Secure data communication
- ☐ D Monitor network traffic

 **Correct Answer: (b) Translate domain names to IP addresses**

Explanation: DNS acts as the “phonebook” of the internet. Humans easily remember names like `www.google.com`, but computers communicate using IP addresses (e.g., `142.250.190.46`). DNS translates the human-readable domain name into the machine-readable IP address. (Option a refers to DHCP.)

Q5

Which method of data transmission uses a dedicated communication path?

A Packet Switching

B Circuit Switching ✓

C Full-Duplex

D Half-Duplex

✓ **Correct Answer: (b) Circuit Switching**

Explanation: In circuit switching (like traditional landline telephones), a dedicated physical communication path is established and reserved for the entire duration of the session. In packet switching, data is broken into packets that share paths with other traffic.

Q6

What is encapsulation in the context of network communication?

- ☐ A Converting data into a secure format
- ☒ B Wrapping data with protocol information
- ☐ C Monitoring network traffic
- ☐ D Translating domain names to IP addresses

☒ **Correct Answer: (b) Wrapping data with protocol information**

Explanation: Encapsulation is the process where data moves down the OSI model layers. At each layer, a header (and sometimes a trailer) containing specific protocol information (like source/destination addresses, error-checking codes) is added to the data. It's like putting a letter in an envelope, then putting that envelope in a shipping box.

Q7

Which protocol is used for reliable data transfer in the TCP/IP model?

(A) HTTP

(B) FTP

(C) TCP



(D) UDP

✓ Correct Answer: (c) TCP

Explanation: Transmission Control Protocol (TCP) is a connection-oriented protocol. It guarantees reliable delivery by using acknowledgments, sequencing, and retransmission of lost packets. UDP (User Datagram Protocol) is faster but connectionless and does not guarantee delivery. HTTP and FTP rely on TCP for transport.

Q8

What is the main purpose of a firewall in network security?

A Convert data into a secure format

B Monitor and control network traffic



C Assign IP addresses

D Translate domain names

Correct Answer: (b) Monitor and control network traffic

Explanation: A firewall acts as a security barrier between a trusted internal network and untrusted external networks (like the internet). It monitors incoming and outgoing traffic and either allows or blocks it based on predetermined security rules.

Q9

Which network topology connects all devices to a central hub?

A Ring

B Mesh

C Bus

D Star



Correct Answer: (d) Star

Explanation: In a star topology, every device (node) is independently connected to a central device, such as a hub or switch. If one cable fails, only that specific device is affected; however, if the central hub fails, the entire network goes down.

Q10

What is a key benefit of using computer networks in businesses?

A Increase computational power

B Enable resource sharing and efficient communication



C Enhance graphic capabilities

D Improve software development

 **Correct Answer: (b) Enable resource sharing and efficient communication**

Explanation: For businesses, the primary benefit of networking is the ability to share expensive resources (like printers, servers, and software licenses) and facilitate rapid, efficient communication (email, VoIP, video conferencing) among employees and with clients.

B

Short Questions

Clear, concise answers for every question

S1

Define data communication and list its key components.

Data communication is the exchange of data between two devices via some form of transmission medium (such as a wire cable or wireless signal).

Its key components are:

1. **Sender:** The device that sends the data message (e.g., a computer, phone).
2. **Receiver:** The device that receives the message.
3. **Message:** The information (data) being communicated (e.g., text, numbers, images).
4. **Transmission Medium:** The physical path through which the message travels (e.g., twisted-pair cable, fiber optics, radio waves).
5. **Protocol:** The set of rules that govern data communication, ensuring the sender and receiver understand each other.

S2

Explain the role of routers in a computer network.

Routers are networking devices that operate at the Network Layer (Layer 3) of the OSI model. Their primary role is to connect multiple networks together (such as connecting a LAN to the Internet) and direct data packets between them.

Routers examine the destination IP address of each packet and use routing tables to determine the best path for the packet to travel across the interconnected networks, ensuring efficient delivery. They also act as a barrier, reducing network traffic by containing broadcast domains.

S3

What are the main functions of the Network Layer in the OSI model?

The Network Layer (Layer 3) is responsible for logical addressing and routing. Its main functions include:

- **Logical Addressing:** Assigning unique IP addresses to devices to identify them globally.
- **Routing:** Determining the optimal path for data packets to travel from the source to the destination across multiple networks.
- **Fragmentation and Reassembly:** Breaking large packets into smaller fragments if the underlying network cannot handle the larger size, and reassembling them at the destination.
- **Packet Forwarding:** Moving packets from the router's input port to the appropriate output port based on routing decisions.

S4

Describe the difference between packet switching and circuit switching.

- **Circuit Switching:** Establishes a dedicated physical communication path between two devices before data transfer begins. This path remains reserved for the entire duration of the communication (e.g., traditional telephone networks). It guarantees bandwidth but wastes resources when no data is being sent.
- **Packet Switching:** Data is broken down into small blocks called packets. These packets are sent independently over shared network paths and may take different routes to reach the destination, where they are reassembled. It is highly efficient as it utilizes network resources dynamically, but it may experience variable delays (e.g., the Internet).

S5

What is the purpose of the Dynamic Host Configuration Protocol (DHCP)?

The purpose of DHCP is to automatically assign IP addresses and other network configuration parameters (such as subnet mask, default gateway, and DNS server addresses) to devices on a network.

Without DHCP, network administrators would have to manually configure IP addresses for every device, which is time-consuming and prone to errors. DHCP allows devices to join a network and obtain a valid IP address dynamically from a pool of available addresses.

S6**How does encapsulation ensure secure communication in a network?**

Encapsulation itself does not inherently ensure *security* (like encryption does), but it enables secure communication by structuring data in a way that security protocols can be applied at different layers.

By wrapping data with protocol headers at each layer (Application, Transport, Network, Data Link), encapsulation allows security mechanisms like TLS/SSL (at the Transport layer) or IPsec (at the Network layer) to encrypt the payload and headers. The receiving device must decapsulate the data layer by layer, meaning it must possess the correct protocols and security keys to unwrap and read the original message, thus preventing unauthorized entities from easily interpreting intercepted traffic.

s7

Differentiate between TCP and UDP in terms of data transfer reliability.

- **TCP (Transmission Control Protocol):** Is a connection-oriented and reliable protocol. It guarantees data delivery through mechanisms like acknowledgments (ACKs), sequence numbers, and retransmission of lost packets. It ensures data arrives in the correct order and without errors, but has higher overhead and latency.
- **UDP (User Datagram Protocol):** Is a connectionless and unreliable protocol. It sends data packets (datagrams) without establishing a connection first and does not wait for acknowledgments. There is no guarantee of delivery, ordering, or error checking. However, it is much faster and has lower overhead, making it ideal for real-time applications like video streaming or online gaming where speed matters more than perfect reliability.

s8

Explain the importance of encryption in network security.

Encryption is the process of converting plain, readable data (plaintext) into an unreadable, scrambled format (ciphertext) using mathematical algorithms and a key. It is crucial for network security because it ensures **confidentiality**.

If an unauthorized user intercepts the data while it is in transit over a network (e.g., via Wi-Fi sniffing or man-in-the-middle attacks), they will only see the scrambled ciphertext, not the sensitive information. Encryption also helps ensure **integrity** (verifying data hasn't been tampered with) and **authentication** (verifying the identity of the sender).

S9

What are the advantages of using a star topology in a network?

- **Easy to install and manage:** Adding or removing devices only requires connecting/disconnecting a single cable to the central hub/switch.
- **Failure isolation:** If one device or its connecting cable fails, it does not affect the rest of the network.
- **Easy troubleshooting:** Faults can be easily isolated by checking individual connections to the central device.
- **Centralized management:** The central hub can monitor and manage all network traffic.

Disadvantage: If the central hub fails, the entire network goes down.

S10

How do firewalls contribute to network security?

Firewalls contribute to network security by acting as a barrier or “gatekeeper” between a trusted internal network and untrusted external networks (like the Internet). They inspect incoming and outgoing data packets and compare them against a set of predefined security rules.

Based on these rules, the firewall decides to allow, deny, or drop the traffic. This prevents unauthorized access, blocks malicious traffic (like hackers or malware), and helps enforce an organization’s security policies.



Long Questions

Detailed step-by-step answers

L1

Discuss the objectives of computer networks and provide examples of how they facilitate resource sharing and data communication.

◆ Objectives of Computer Networks

- **Resource Sharing:** To make all programs, equipment, and data available to anyone on the network without regard to the physical location of the resource or the user.
- **High Reliability:** To provide alternative sources of supply in case of hardware failure (e.g., data replication across multiple servers).
- **Cost Reduction:** To save money by sharing expensive hardware and software. Small computers have a much better price/performance ratio than larger ones.
- **Scalability:** To increase system performance gradually as the workload grows just by adding more processors.
- **Powerful Communication Medium:** To facilitate communication between geographically dispersed individuals (email, video conferencing, instant messaging).

Long Question 1 • continued

◆ Examples of Resource Sharing

- **Hardware:** A single high-volume, high-speed laser printer can be shared by dozens of employees in an office, eliminating the need to buy a printer for every desk.
- **Software:** A company can purchase a single license for a specialized accounting software and install it on a central server, allowing authorized users to access it over the network.
- **Data:** A centralized database on a server can be accessed and updated by multiple departments simultaneously, ensuring everyone works with the latest information.

Long Question 1 • continued

◆ Examples of Data Communication

- **Email and Messaging:** Employees can instantly send documents, messages, and updates to colleagues across the globe.
- **VoIP (Voice over IP):** Using the network to make phone calls, reducing long-distance telephone costs.
- **Video Conferencing:** Enabling face-to-face meetings without the need for travel.

L2

In a Simplex communication system, assume data is transmitted at a rate of 500 bits per second (bps). Compute the time to transmit a message if: (a) it is of 10 kilobits. (b) it is of 10 kilobytes.

◆ Given

Given	Transmission rate = 500 bits per second (bps)
Mode	Simplex communication — data flows in only one direction
Formula	Time = Total Data Size ÷ Transmission Rate

Long Question 2 • continued

◆ (a) Message size = 10 kilobits

Convert	1 kilobit = 1000 bits (standard for networking) Size in bits = $10 \times 1000 = \mathbf{10,000 \text{ bits}}$
Formula	Time = Total Data Size ÷ Transmission Rate
Calculate	Time = $10,000 \text{ bits} \div 500 \text{ bps}$

Time = 20 seconds

Long Question 2 • continued

♦ (b) Message size = 10 kilobytes

Convert	1 byte = 8 bits and 1 kilobyte = 1024 bytes (standard computing) Size in bits = $10 \times 1024 \times 8 = \mathbf{81,920 \text{ bits}}$
Calculate	Time = $81,920 \text{ bits} \div 500 \text{ bps}$

Time = 163.84 seconds (2 min 43.84 s)

Note: If the textbook uses 1 KB = 1000 bytes, then size = $10 \times 1000 \times 8 = 80,000$ bits and Time = $80,000 \div 500 = \mathbf{160 \text{ seconds}}$. Both are correct depending on the convention; 1024 is the standard computer-science definition for storage.

L3

Describe how data is transmitted across computer networks using packet switching and circuit switching.

◆ Circuit Switching

A dedicated physical path is established between the sender and receiver before any data is transmitted.

- **Process:** The network creates a continuous, end-to-end connection (a circuit) by allocating specific bandwidth on each link between the nodes.
- **Transmission:** Data is sent as a continuous stream along this dedicated path. No other traffic can use this path until the connection is terminated.
- **Example:** Traditional telephone networks (PSTN).
- **Pros/Cons:** Guarantees bandwidth and minimal delay once connected, but it is inefficient because idle time on the circuit wastes network resources, and establishing the connection takes time.

Long Question 3 • continued

◆ Packet Switching

There is no dedicated path. Instead, the message is divided into smaller units called packets.

- **Process:** Each packet contains a header with the destination address and a sequence number. The packets are sent independently into the network.
- **Transmission:** Routers along the way examine the destination address and forward each packet individually. Packets from the same message may take different routes based on network congestion and availability. At the destination, the packets are reassembled into the original message based on their sequence numbers.
- **Example:** The Internet (TCP/IP).
- **Pros/Cons:** Highly efficient and resilient (if one path fails, packets can be rerouted). It maximizes network utilization. However, it can suffer from variable delays (jitter) and packets can arrive out of order or be lost, requiring higher-layer protocols to manage reliability.

L4

Discuss the role and importance of protocols in data communication. Explain the functions of key protocols such as TCP/IP, HTTP, DNS, and DHCP.

◆ Role and Importance of Protocols

In data communication, a protocol is a set of rules and conventions that govern how data is exchanged between devices. Without protocols, devices would not be able to understand each other, similar to two people trying to talk where one speaks only English and the other only Japanese. Protocols define:

- **Syntax:** The structure or format of the data (e.g., the order of fields in a header).
- **Semantics:** The meaning of each section of bits (e.g., which bits represent the address).
- **Timing:** When data should be sent and how fast it can be sent.

Protocols are essential for interoperability, error handling, and ensuring reliable communication across diverse hardware and software.

Long Question 4 • continued

◆ Functions of Key Protocols: TCP/IP

This is the foundational suite of protocols for the Internet.

- **IP:** Responsible for logical addressing and routing packets across networks.
- **TCP:** Ensures reliable, ordered, and error-checked delivery of a stream of bytes between applications. It breaks data into segments, acknowledges received data, and retransmits lost packets.

Long Question 4 • continued

◆ HTTP (Hypertext Transfer Protocol)

An application-layer protocol used for transmitting web pages and other resources over the Internet. It defines how web browsers (clients) request information from web servers and how servers respond. It is a request-response protocol.

Long Question 4 • continued

◆ DNS (Domain Name System)

An application-layer protocol that translates human-readable domain names (e.g., `www.example.com`) into numerical IP addresses (e.g., `192.0.2.1`). It acts as the phonebook of the internet, allowing users to access websites without memorizing complex IP addresses.

Long Question 4 • continued

◆ DHCP (Dynamic Host Configuration Protocol)

A network management protocol used to automate the configuration of devices on an IP network. When a device connects to a network, DHCP automatically assigns it a unique IP address, subnet mask, default gateway, and DNS server, eliminating the need for manual configuration by network administrators.

L5

Evaluate different methods of network security, including firewalls, encryption, and antivirus software.

◆ Overview

Network security is a multi-layered defense strategy. Evaluating the key methods:

Long Question 5 • continued

◆ Firewalls

- **Function:** Acts as a barrier between trusted internal networks and untrusted external networks. It filters incoming and outgoing traffic based on security rules (packet filtering, stateful inspection, or application-level gateways).
- **Evaluation:** Highly effective as the first line of defense against external threats (e.g., hackers, worms). However, firewalls cannot protect against internal threats (malicious employees) or attacks that bypass the firewall via authorized channels (e.g., email attachments, infected USB drives).

Long Question 5 • continued

◆ Encryption

- **Function:** Converts data into an unreadable format (ciphertext) using algorithms and keys. Only authorized parties with the correct decryption key can read it (e.g., HTTPS, VPNs).
- **Evaluation:** Crucial for data confidentiality and privacy, especially for data in transit over public networks (like Wi-Fi). It protects against eavesdropping and man-in-the-middle attacks. However, it relies on proper key management; if keys are lost or stolen, security is compromised. It does not prevent malware from entering a system, only protects the data itself.

Long Question 5 • continued

◆ Antivirus Software

- **Function:** Installed on endpoint devices (PCs, servers, phones), it scans files and system memory for known malicious code signatures and suspicious behavior. It detects, quarantines, or removes malware (viruses, Trojans, ransomware).
- **Evaluation:** Essential for protecting end-users and preventing the spread of malware within a network. However, it is signature-based, meaning it struggles with new, zero-day threats until updated. It also consumes system resources and cannot protect against social engineering attacks (like phishing) if the user willingly grants access.

L6

Describe real-world applications of computer networks in business, education, and healthcare.**◆ Business**

- **E-commerce:** Online retail platforms (Amazon, eBay) rely entirely on networks to process transactions, manage inventory, and communicate with customers globally.
- **Enterprise Resource Planning (ERP):** Centralized databases shared across networks allow different departments (HR, Finance, Sales) to access and update information in real-time.
- **VoIP and Video Conferencing:** Tools like Zoom and Microsoft Teams enable remote work and global collaboration, reducing travel costs.
- **Cloud Computing:** Businesses rent computing power and storage (AWS, Azure) over the network instead of maintaining their own physical servers.

Long Question 6 • continued**◆ Education**

- **E-learning Platforms:** Websites like Coursera, Khan Academy, and Moodle provide online courses and resources to students worldwide.
- **Virtual Classrooms:** Video conferencing tools facilitate remote learning, allowing students and teachers to interact from different locations.
- **Digital Libraries:** Students can access vast databases of academic journals, e-books, and research materials via university networks.

Long Question 6 • continued

◆ Healthcare

- **Electronic Health Records (EHR):** Patient medical histories, lab results, and prescriptions are stored digitally and can be securely accessed by authorized doctors and hospitals across a network.
- **Telemedicine:** Patients can consult with specialists via video calls, which is crucial for rural areas or during pandemics.
- **Remote Monitoring:** Wearable devices (like heart monitors) can transmit patient data directly to healthcare providers over a network for continuous monitoring.
- **Hospital Information Systems:** Networks manage scheduling, billing, and medical imaging (PACS) within a hospital.

L7

Compare and contrast the different types of network topologies (star, ring, bus, and mesh).

◆ Star Topology

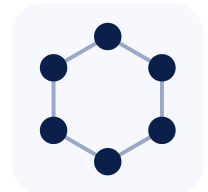
- **Structure:** All devices connect to a central hub/switch.
- **Pros:** Easy to install and manage; failure of one node doesn't affect others; easy fault isolation.
- **Cons:** Single point of failure (if the central hub fails, the whole network fails); requires more cabling than bus topology.



Long Question 7 • continued

◆ Ring Topology

- **Structure:** Devices are connected in a closed loop. Data travels in one direction (or both in dual-ring) from node to node.
- **Pros:** No collisions (in token ring); predictable performance; can span larger distances than bus.
- **Cons:** Failure of one node or cable break can bring down the entire network (unless it's a dual-ring); troubleshooting is difficult; adding/removing nodes disrupts the network.



Long Question 7 • continued

◆ Bus Topology

- **Structure:** All devices connect to a single central backbone cable via drop lines.
- **Pros:** Easy to install for small networks; requires less cable than star.
- **Cons:** Limited cable length and number of nodes; if the main backbone cable breaks, the entire network goes down; performance degrades heavily with high traffic due to collisions.



Long Question 7 • continued

◆ Mesh Topology

- **Structure:** Every device is connected to every other device via dedicated links (Full Mesh) or multiple links (Partial Mesh).
- **Pros:** Highly redundant and fault-tolerant (if one link fails, data can be rerouted); no traffic congestion; highly secure (dedicated links).
- **Cons:** Very expensive and difficult to install due to massive amount of cabling and hardware required; complex configuration.



L8

Consider a shift cipher with a shift amount of 4. (a) Encrypt the message "SECURITY". (b) Decrypt the message "WMYXVYMI".

◆ How a Shift (Caesar) Cipher Works

A shift cipher shifts each letter of the alphabet by a fixed number of places. Here, the shift amount is **+4** for encryption (A→E, B→F, ...) and **-4** for decryption.

Long Question 8 • continued

◆ (a) Encrypt "SECURITY" (Shift +4)

S +4	W	E +4	I	C +4	G	U +4	Y	R +4	V	I +4	M	T +4	X
Y +4	C												

Encrypted Message: WIGYVMXC

Long Question 8 • continued

♦ (b) Decrypt “WMYXVYMI” (Shift -4)

W -4 S

M -4 I

Y -4 U

X -4 T

V -4 R

Y -4 U

M -4 I

I -4 E

Decrypted Message: SIUTRUIE

Note: The working above is correct for the ciphertext exactly as printed (W-4=S, M-4=I, Y-4=U, X-4=T, V-4=R, Y-4=U, M-4=I, I-4=E), although the result does not form an English word.

19

An IPv4 address is a 32-bit number. Calculate the total number of unique IPv4 addresses possible. (a) Show the calculation for the total number of IPv4 addresses. (b) How many addresses are left if 10% of the total addresses are reserved for special purposes?

♦ (a) Total Number of IPv4 Addresses

Idea

An IPv4 address is a 32-bit binary number. Each bit can be either 0 or 1 (2 possibilities).

Formula

Total addresses = 2^{32}

Calculate

$2^{32} = 4,294,967,296$

Total = 4,294,967,296 (≈ 4.29 billion)

Long Question 9 • continued

♦ (b) Addresses Left After Reserving 10%

Reserved	10% of total = $0.10 \times 4,294,967,296 = 429,496,729.6 \approx 429,496,730$
Left	Addresses left = 90% of total = $0.90 \times 4,294,967,296 = 3,865,470,566.4$
Round	Addresses are discrete, so we round to the nearest whole number

$\approx 3,865,470,566$ addresses left

Note: In reality, far fewer than 90% of IPv4 addresses are available because of historical allocations, but mathematically, based on the question, this is the answer.

CHAPTER 06 • COMPLETED

Thank You & Keep Learning!

Introduction To Computer Networks

✓ 10 Solved MCQs with explanations

✓ 10 Short Questions answered

✓ 9 Long Questions step by step

✓ Class 9 Computer Science

scholareye.xyz