

Comprehensive Notes On Networking and Internet (Unit 2)

Class XI - Information Technology

Contents

1	Session 1: Computer Networking Fundamentals	2
1.1	Evolution of Networks and the Internet	2
1.2	Four Elements of Communication & Transmission Modes	2
1.3	Transmission Media: Guided vs. Unguided	3
1.4	Network Hardware Devices	3
1.5	Classification of Networks by Geographical Span	4
1.6	Network Topologies (Physical Layouts)	4
1.7	Identification of Nodes: MAC Address, IP Address & Domain Names	5
2	Session 2: Internet Services and Protocol Architecture	6
2.1	Digital Literacy & Digital India Initiative	6
2.2	Standard Internet Application Services	6
2.3	The TCP/IP 4-Layer Protocol Model	6
3	Session 3: Cyber Threats and Cyber Security	7
3.1	Malware Classification	7
3.2	Network Attacks & Fraudulent Activities	8
3.3	Categorization of Cyber Crimes	8
3.4	Network Security Tools & Protective Measures	8
4	Comprehensive Question Bank	10
4.1	Multiple Choice Questions (MCQs)	10
4.2	Assertion-Reasoning Questions	12
4.3	One-Word / Brief Answer Questions	12
4.4	Differentiate Between Questions	13
4.5	Short Answer Questions	14
4.6	Long Answer Questions	15
4.7	Case-Study / Competency-Based Questions	16

1 Session 1: Computer Networking Fundamentals

1.1 Evolution of Networks and the Internet

Communication has evolved from oral traditions and printing presses (Gutenberg, 1440) to telecommunication systems. The key milestones in computer networking include:

- **Public Switched Telephone Network (PSTN, 1877):** Developed following Alexander Graham Bell's telephone invention (1876). Utilized **Circuit Switching**, establishing a dedicated physical path between caller and receiver.
- **Digital Packet Switching (Late 1950s / Cold War):** Developed by Paul Baran, Donald Davies, and Len Kleinrock for the US Department of Defense (DoD) to create fault-tolerant networks resilient against single-point failure during military conflict. Messages are broken into small units called **packets** shared across dynamic link paths.
- **ARPANET (1969):** The Advanced Research Projects Agency Network connected research computers via digital packet switching, initially for military and academic non-commercial use.
- **TCP/IP (1970) & NSFNET (1984):** The U.S. National Science Foundation established NSFNET. Interconnecting ARPANET and NSFNET via the ****TCP/IP**** (Transmission Control Protocol/Internet Protocol) suite formed the modern **Internet** (network of networks).

Global Internet Governance Bodies

- **IETF (Internet Engineering Task Force):** Standardizes core Internet protocols (IPv4, IPv6).
- **ICANN (Internet Corporation for Assigned Names and Numbers):** Coordinates global assignment of IP addresses, domain names, and protocol parameters.
- **ISP (Internet Service Provider):** Provides physical access and bandwidth connectivity to the Internet.

1.2 Four Elements of Communication & Transmission Modes

A communication system comprises four fundamental components:

1. **Sender:** The originating node transmitting the data.
2. **Receiver:** The target node receiving the data.
3. **Message:** The structured information or payload being communicated.
4. **Channel / Medium:** The physical path through which signals travel.

Transmission Mode	Operational Direction	Real-World Applications
Simplex	Unidirectional (Data flows in one fixed direction only).	Television / Radio broadcasts, satellite video feeds.
Half-Duplex	Bidirectional (Data flows both ways, but only one party transmits at a time).	Walkie-Talkies, low-bandwidth file transfers.
Full-Duplex	Simultaneous Bidirectional (Both parties send and receive at the same time).	Telephone calls, Interactive video conferencing, NIC hardware.

1.3 Transmission Media: Guided vs. Unguided

Transmission channels are categorized into physical conductors (**Guided**) and electromagnetic wireless waves (**Unguided**):

Medium Category	Specific Channel Type	Signal Form & Physical Characteristics
Guided (Bounded)	Twisted Pair Cable	Voltage/Current signals; insulated copper wires twisted to reduce crosstalk.
	Coaxial Cable	Electrical current; central copper conductor with metal shield; used in Cable TV.
	Fiber Optic Cable	Light pulses; total internal reflection through glass fibers; ultra-high bandwidth.
Unguided (Unbounded)	Radio Waves	Omnidirectional electromagnetic waves (3 kHz–1 GHz); penetrates walls.
	Microwaves	Line-of-sight directional waves (1 GHz–300 GHz); parabolic dish antennas.
	Infrared	High-frequency short-range line-of-sight waves; TV remotes, optical wireless mouse.
	Satellite Link	Transponders in geostationary orbit relaying microwave signals across continents.

1.4 Network Hardware Devices

Network infrastructure relies on specialized interconnectivity devices:

Functions of Core Network Devices

- **Repeater (Digital Regenerator):** Placed between long cable segments to amplify and reshape attenuated digital signals, extending total transmission distance.
- **Hub:** Multiport broadcast device. Data arriving on one port is blindly retransmitted to all other ports (no address filtering, single collision domain).
- **Bridge:** Multiport device connecting two LAN segments. Filters and forwards frames based on MAC address tables.
- **Switch:** Multiport unicast device connecting individual nodes within a LAN. Inspects destination MAC addresses to forward frames directly to target ports.
- **Router:** Connects disparate networks (LAN/WAN). Maintains routing tables to determine optimum paths and forward packets based on destination IP addresses.
- **Gateway:** Connects networks operating on completely different protocol architectures by performing protocol conversion.

1.5 Classification of Networks by Geographical Span

Network Type	Geographical Radius	Radius	Typical Speed / Bandwidth	Example Scenario
PAN (Personal Area)	Up to 10 meters		Short range (1–3 Mbps)	Bluetooth connecting smartphone, smartwatch, and wireless headphones.
LAN (Local Area)	Up to 1 km		High speed (10 Mbps–1 Gbps)	Private network inside a school building, office, or lab campus.
MAN (Metropolitan Area)	Up to 50 km		Moderate to High speed	City-wide cable television network or multi-branch bank network within a city.
WAN (Wide Area)	Up to 1000 km+		Variable broad network	Country-wide or global network (e.g., the Internet, ATM banking network).

1.6 Network Topologies (Physical Layouts)

Topology refers to the arrangement or geometric layout of nodes and communication links in a network:

Topology Type	Key Architectural Advantages	Limitations / Disadvantages
Bus Topology	Minimal cabling required; easy to install and extend via T-taps on backbone cable.	Difficult fault isolation; central backbone cable failure crashes entire network.
Ring Topology	Equal access for all nodes; signals travel unidirectionally in closed loop.	Single-node or link failure breaks entire loop; high token delay.
Star Topology	Easy installation and fault isolation; single node failure does not affect others.	High cabling requirement; central Hub/Switch failure crashes whole network.
Mesh Topology	Maximum security, redundancy, and throughput via dedicated point-to-point links $(n(n-1)/2)$.	Extremely expensive; complex cabling installation as node count increases.
Tree Topology	Combination of Bus backbone and Star branches; modular expansion of segments.	Backbone failure disconnects entire branches from communicating with each other.

1.7 Identification of Nodes: MAC Address, IP Address & Domain Names

To ensure accurate data delivery, nodes on a network possess unique physical and logical identifiers:

- **MAC Address (Media Access Control):**

- Permanently burned into Network Interface Card (NIC) by manufacturer.
- 48-bit (12-digit hexadecimal) address written as MM:MM:MM:SS:SS:SS or MM-MM-MM-SS-SS-SS.
- *Manufacturer OUI*: First 6 digits (e.g., 00:A0:C9 = Intel); *Serial Number*: Last 6 digits.

- **IP Address (Internet Protocol):**

- Logical 32-bit (4-byte) numerical address assigned by network administrator or ISP.
- Expressed in dotted decimal notation (0–255), e.g., 59.177.134.72.
- Changes dynamically when moving between different networks.

- **Domain Name & DNS Resolution:**

- Human-readable textual names assigned to IP addresses (e.g., cbse.nic.in).
- **Generic TLDs**: .com (commercial), .edu (education), .gov (government), .org (non-profit).
- **Country-Code TLDs**: .in (India), .au (Australia), .uk (United Kingdom), .us (United States).
- **Domain Name Resolution**: Process performed by Domain Name System (DNS) servers to translate URLs into numerical IP addresses.

2 Session 2: Internet Services and Protocol Architecture

2.1 Digital Literacy & Digital India Initiative

Digital Literacy involves acquiring knowledge, awareness, and skills to efficiently and ethically utilize technology tools (computers, smartphones, web portals) for education, social interaction, e-commerce, and governance.

Digital India Campaign

Launched by Prime Minister Narendra Modi, **Digital India** aims to transform the nation into a digitally empowered society by building robust digital infrastructure, delivering electronic government services to rural regions, and expanding access to **MOOCs** (Massive Open Online Courses).

2.2 Standard Internet Application Services

- **Electronic Mail (E-Mail):** System for transmitting digital messages and multimedia attachments over networks. Managed via Webmail (Gmail, Yahoo) or Desktop Clients (Outlook, Thunderbird).
 - **SMTP (Simple Mail Transfer Protocol):** Used by client/server to *send* outgoing emails.
 - **POP3 (Post Office Protocol v3):** Downloads incoming emails from server to local disk for offline reading.
- **File Transfer Protocol (FTP):** Client-server protocol enabling secure uploading and downloading of files between remote hosts over TCP.
- **Remote Login (TELNET):** *Terminal Network* protocol enabling a client user to log into, manage, and execute commands on a remote server system.
- **World Wide Web (WWW):** A global hyperlinked repository of web pages containing text, images, audio, video, and hyperlinks accessed via **HTTP / HTTPS**.

2.3 The TCP/IP 4-Layer Protocol Model

Communication over the Internet is structured into four functional layers:

TCP/IP Layer	Primary Operational Responsibilities	Protocols Operating at Layer
Application Layer	Provides user application interfaces, message creation, header formatting.	HTTP, HTTPS, FTP, SMTP, POP3, TELNET, DNS.
Transport Layer	Handles end-to-end process delivery, port addressing, segmentation, and sequencing.	TCP (Connection-oriented, reliable) & UDP (Connectionless, streaming).
Internet Layer	Formats data packets and routes them across networks using logical IP addressing.	IP (IPv4, IPv6), ICMP, ARP.
Link Layer (Host-to-Net)	Appends physical MAC address headers/trailers for hardware frame transmission over medium.	Ethernet, Wi-Fi (802.11), PPP.

🔄 Transport Layer Protocols: TCP vs. UDP

- **TCP (Transmission Control Protocol):** Connection-oriented protocol providing reliable, error-checked, ordered packet delivery (used for web pages, file downloads, emails).
- **UDP (User Datagram Protocol):** Connectionless, lightweight protocol optimized for speed without delivery acknowledgements (used for live video streaming, online gaming, DNS).

3 Session 3: Cyber Threats and Cyber Security

3.1 Malware Classification

Malware (Malicious Software) refers to programs designed to disrupt system operations, gain unauthorized access, or destroy data:

Malware Type	Replication & Host Dependency	Harmful Effects & Examples
Computer Virus	Replicates by attaching code to legitimate host executable files or boot sectors.	Corrupts files, overwrites memory, slows boot execution (e.g., Boot sector virus, Macro virus).
Network Worm	Standalone program; self-replicates across networks without needing a host application.	Floods hard disks, consumes network bandwidth, crashes systems (e.g., <i>Code Red Worm</i>).
Trojan Horse	Disguised as desirable software (games, utility apps); does not replicate.	Creates backdoors for hackers to spy, steal files, or gain remote control (e.g., <i>Sub7 Trojan</i>).
Ransomware	Encrypts user files on victim device using complex cryptography.	Extorts monetary ransom payments from victim in exchange for decryption keys.

3.2 Network Attacks & Fraudulent Activities

- **Eavesdropping:** Secretly monitoring or intercepting private communications (phone calls, emails, instant messages) without user consent.
- **Denial of Service (DoS Attack):** Overloading a target web server or network resource with superfluous requests, denying access to legitimate users.
- **Phishing:** Deceptive practice of sending fraudulent emails with fake website links to trick users into revealing sensitive credentials (passwords, bank PINs, credit card numbers).
- **Spamming:** Sending bulk unsolicited commercial or promotional emails containing advertising links or malware.

3.3 Categorization of Cyber Crimes

Cybercrimes are unlawful acts where computers are used as a tool, target, or both:

Major Cyber Crime Types

- **Cyberbullying / Cyberstalking:** Online harassment or repeated unwanted contact via social media/messaging.
- **Vishing & SMSing:** Fraudulent phone calls (Voice Phishing) or SMS text messages seeking OTPs and banking PINs.
- **SIM Swap Scam:** Fraudulently obtaining a duplicate SIM card to intercept bank OTPs and financial transactions.
- **Identity Theft:** Unlawfully misusing another person's digital signature, passwords, or unique identity credentials.
- **Online Job Fraud:** Defrauding job seekers by offering fake employment promises in exchange for upfront fees.

3.4 Network Security Tools & Protective Measures

To protect hardware, networks, and data against intrusion, users must implement multi-layered defense tools and best practices:

Security Tool / Feature	Primary Protective Mechanism	Best Practice Guidelines
Firewall	Hardware router or software barrier inspecting network traffic; blocks unauthorized packet flow.	Enable built-in OS firewall; configure strict inbound/outbound security rules.
Antivirus Software	Scans files against updated malware definition databases to detect and remove threats.	Perform regular full system scans; enable automatic background definition updates.
HTTPS / SSL Padlock	Encrypts data exchanged between web browser and server using SSL digital certificates.	Verify padlock icon and https:// prefix before making online financial transactions.
Browser Patching	Fixes known browser security vulnerabilities.	Update browser regularly (Chrome security dots: Grey = current; Red = 7 days out-dated).
Cookie Management	Deletes tracking text files stored by web servers on client browser storage.	Periodically clear browser cache and cookies to prevent session hijacking.
Cyber Law (IT Act)	Legal framework punishing cyber-crimes (**IT Act 2000** & **IT Amendment Act 2008**).	Report incidents to cyber police or portal cybercrime.gov.in .

4 Comprehensive Question Bank

4.1 Multiple Choice Questions (MCQs)

1. Which early network, developed by the US Department of Defense in 1969, laid the foundation for the modern Internet?

(A) NSFNET
(B) ARPANET
(C) PSTN
(D) ISDN

Answer: (B)

Explanation: ARPANET made use of digital packet switching to interconnect research computers in 1969.

2. What is the reach or geographical span of a Personal Area Network (PAN)?

(A) Up to 10 meters
(B) Up to 1 km
(C) Up to 50 km
(D) Up to 1000 km

Answer: (A)

Explanation: A PAN connects personal devices (Bluetooth, phones, printers) within a small radius of up to 10 meters.

3. Which network device blindly broadcasts incoming data to all connected lines except the line it arrived on?

(A) Switch
(B) Router
(C) Hub
(D) Gateway

Answer: (C)

Explanation: A Hub lacks MAC address filtering intelligence and broadcasts incoming signals to all ports.

4. How many bits are contained in a standard Media Access Control (MAC) address?

(A) 16 bits
(B) 32 bits
(C) 48 bits
(D) 64 bits

Answer: (C)

Explanation: A MAC address is a 12-digit hexadecimal number (6 bytes = 48 bits) permanently assigned to an NIC.

5. Which transport layer protocol provides connection-oriented, reliable, and error-checked data delivery?

(A) UDP
(B) TCP
(C) IP
(D) HTTP

Answer: (B)

Explanation: TCP (Transmission Control Protocol) guarantees reliable, ordered packet delivery with acknowledgements.

6. Which network topology connects every node to a central Hub or Switch?

(A) Bus Topology

(C) Star Topology

(B) Ring Topology

(D) Mesh Topology

Answer: (C)

Explanation: Star topology connects all peripheral nodes to a central controller device (Hub or Switch).

7. What type of malware self-replicates across networks without requiring a host application file?

(A) Trojan Horse

(C) Network Worm

(B) Computer Virus

(D) Macro Virus

Answer: (C)

Explanation: Worms are standalone malicious programs that automatically replicate across network connections.

8. Which protocol is used by email clients to send outgoing emails to a server?

(A) POP3

(C) FTP

(B) SMTP

(D) TELNET

Answer: (B)

Explanation: SMTP (Simple Mail Transfer Protocol) governs the sending and transfer of outgoing email messages.

9. What cyber attack floods a server with superfluous requests to disrupt services for legitimate users?

(A) Phishing

(C) Eavesdropping

(B) Denial of Service (DoS)

(D) SIM Swap

Answer: (B)

Explanation: A DoS attack overloads system resources, preventing legitimate user requests from being fulfilled.

10. Which legal Act in India governs electronic commerce, cybercrimes, and security penalties?

(A) Cyber Security Act 1995

(C) Indian Penal Code 1860

(B) Information Technology Act 2000

(D) Digital India Act 2015

Answer: (B)

Explanation: The Information Technology Act 2000 (and 2008 Amendment) provides the legal framework for cybercrime in India.

4.2 Assertion-Reasoning Questions

- Assertion (A):** MAC addresses are dynamic and change whenever a computer connects to a new network.
Reason (R): MAC addresses are 48-bit physical addresses permanently burned into the Network Interface Card by the manufacturer.
Answer: A is false but R is true.
Explanation: MAC addresses are permanent physical addresses assigned by manufacturers; IP addresses are dynamic logical addresses assigned by network administrators.
- Assertion (A):** Fiber optic cables provide significantly higher data transfer speeds and bandwidth than twisted pair cables.
Reason (R): Fiber optic cables transmit data in the form of light pulses using total internal reflection, unaffected by electrical interference.
Answer: Both A and R are true, and R is the correct explanation of A.
Explanation: Optical light pulse transmission prevents electromagnetic interference, supporting high-speed bandwidth over long distances.
- Assertion (A):** A Trojan Horse self-replicates rapidly across disk storage to flood hard drive space.
Reason (R): A Trojan Horse disguises itself as useful software to open backdoors for unauthorized hacker access.
Answer: A is false but R is true.
Explanation: Trojan Horses do not replicate themselves; they rely on deceiving users into executing them to open backdoors.
- Assertion (A):** HTTPS ensures secure communication between a web browser and a remote web server.
Reason (R): HTTPS encrypts communication traffic using SSL/TLS digital certificates issued by trusted Certificate Authorities.
Answer: Both A and R are true, and R is the correct explanation of A.
Explanation: SSL/TLS encryption under HTTPS protects sensitive user credentials during web transmission.
- Assertion (A):** Star topology networks fail completely if any single peripheral node cable breaks.
Reason (R): In star topology, every node is connected via an independent point-to-point cable to a central Hub or Switch.
Answer: A is false but R is true.
Explanation: Breakage of a single peripheral node line only isolates that node; central Hub failure is required to crash the whole network.

4.3 One-Word / Brief Answer Questions

- Name the global organization responsible for assigning IP addresses and domain names.
Answer: ICANN (Internet Corporation for Assigned Names and Numbers).
- What is the term for the maximum data transfer rate of a network connection?
Answer: Bandwidth.
- Name the transmission mode where both parties can transmit and receive data simultaneously.
Answer: Full-Duplex Mode.

4. Which digital regenerator device amplifies weak signals over long cable lengths?
Answer: Repeater.
5. What is the physical layout or arrangement of nodes in a network called?
Answer: Network Topology.
6. Which protocol is used to log into and manage a remote host computer over a terminal?
Answer: TELNET.
7. Name the malware received via network that flooded systems with 250,000 copies in 9 hours.
Answer: Code Red Worm.
8. What type of cyber attack uses fraudulent phone calls to steal banking PINs and OTPs?
Answer: Vishing (Voice Phishing).
9. Name the security software or hardware device that filters incoming and outgoing network traffic.
Answer: Firewall.
10. What small text files are stored on client browsers by web servers to record user session data?
Answer: Cookies.

4.4 Differentiate Between Questions

1. Differentiate between MAC Address and IP Address.

Feature	MAC Address	IP Address
Addressing Type	Physical Hardware Address.	Logical Network Address.
Assignment	Burned into NIC by Manufacturer.	Assigned by Network Administrator / ISP.
Format & Size	48-bit (12 Hexadecimal digits).	32-bit (4 Dotted Decimal numbers, 0–255).
Permanence	Permanent and unchangeable.	Dynamic; changes when moving between networks.

2. Differentiate between Hub and Switch.

Feature	Hub	Switch
Data Transmission	Broadcasts incoming frames to all ports.	Unicasts frames directly to target port.
Addressing	No address recognition.	Uses MAC address table to forward frames.
Collision Domains	Single shared collision domain.	Separate collision domain per port.

3. Differentiate between Computer Virus and Network Worm.

Feature	Computer Virus	Network Worm
Host Requirement	Requires a host file/program to attach to.	Standalone program; requires no host file.
Replication	Replicates when host program is executed.	Automatically self-replicates across networks.
Primary Harm	Corrupts files, memory, and boot sectors.	Consumes network bandwidth and floods disks.

4. Differentiate between Bus Topology and Star Topology.

Feature	Bus Topology	Star Topology
Central Element	Single long backbone cable.	Central Hub or Switch.
Cabling Cost	Low cabling requirement.	Higher cabling requirement (point-to-point lines).
Fault Impact	Backbone cable break crashes whole network.	Node cable break isolates only that single node.

5. Differentiate between Firewall and Antivirus.

Feature	Firewall	Antivirus
Focus Area	Network traffic and packet filtering.	Internal system file scanning and execution.
Detection Method	Inspects port protocols against security rules.	Compares file code against malware definition databases.
Primary Role	Prevents unauthorized external network intrusions.	Detects, quarantines, and deletes infected files.

4.5 Short Answer Questions

1. Explain packet switching and why it was developed during the Cold War.

Answer: Digital packet switching divides messages into small chunks (packets) routed dynamically across shared network links. Developed by Paul Baran and the US DoD for ARPANET, it replaced rigid circuit switching to create fault-tolerant networks that could survive single-point infrastructure damage during military conflicts.

2. What is Domain Name Resolution? Describe the steps involved.

Answer: Domain Name Resolution is the process of translating human-readable web domain names (e.g., `cbse.nic.in`) into numerical IP addresses (59.177.134.72). When a user types a URL, the web browser checks local cache; if absent, it queries Domain Name Servers (DNS) to retrieve the server's IP address and establish a connection.

3. Describe the role of a Router in computer networking.

Answer: A router is a network device that connects different networks (LANs/WANs) operating on similar or different protocols. It reads destination IP addresses on incoming data packets and

uses internal routing tables to determine the optimum path for forwarding packets toward their destination.

4. **What is a Trojan Horse? How does it infect a system?**

Answer: A Trojan Horse is malicious software disguised as useful, legitimate applications (e.g., free games or utilities). When executed by an unsuspecting user, it installs hidden backdoors that allow hackers to remotely spy on user activity, steal data, or manipulate the infected host.

5. **Differentiate between SMTP and POP3 protocols.**

Answer: SMTP (Simple Mail Transfer Protocol) is an application layer protocol used by email clients to *send* outgoing messages to mail servers. POP3 (Post Office Protocol version 3) is used to *download* incoming email messages from a mail server onto a local host machine for offline reading.

4.6 Long Answer Questions

1. **Explain the 4-Layer TCP/IP Protocol Architecture with the responsibilities and protocols of each layer.**

Answer: The TCP/IP model organizes network communication into four layers:

(1) Application Layer: Interacts with user software. Formats messages and appends protocol headers. Protocols: HTTP, HTTPS, FTP, SMTP, POP3, TELNET, DNS.

(2) Transport Layer: Manages end-to-end process communication and port addressing. Divides data into segments with sequence numbers. Protocols: TCP (connection-oriented, reliable) and UDP (connectionless, fast).

(3) Internet Layer: Handles logical network addressing and packet routing across networks. Protocols: IP (IPv4, IPv6) and ICMP.

(4) Link Layer (Host-to-Network): Adds physical MAC addressing frames and manages hardware signal transmission across copper cables, fiber optics, or wireless media.

2. **Detail the four geographical categories of networks (PAN, LAN, MAN, WAN) with their radius, bandwidth, and applications.**

Answer: Networks are classified by geographical span:

(1) PAN (Personal Area Network): Radius up to 10 meters. Connects personal devices via Bluetooth or USB. Application: Smartwatches, phones, game controllers.

(2) LAN (Local Area Network): Radius up to 1 km. High bandwidth (10 Mbps–1 Gbps). Private networks within a building or school campus for resource sharing.

(3) MAN (Metropolitan Area Network): Radius up to 50 km. Links multiple LANs across a city. Application: Cable television networks, municipal office interconnects.

(4) WAN (Wide Area Network): Radius up to 1000 km+. Spans countries or continents using satellite and fiber links. Application: The global Internet, international banking ATM networks.

3. **Discuss various cyber threats (Virus, Worm, Trojan, Phishing, DoS) and outline five essential protective measures for safe browsing.**

Answer: Cyber threats compromise data safety:

(1) Virus: Corrupts host files and boot sectors.

(2) Worm: Replicates automatically across networks, flooding bandwidth.

(3) Trojan: Disguised malware opening unauthorized backdoors.

(4) Phishing: Fraudulent emails stealing banking credentials.

(5) DoS Attack: Overloads servers to crash web services.

Five Protective Measures:

- Use strong, complex passwords and change them regularly.
- Verify `https://` and SSL Padlock on address bar before online financial transactions.
- Maintain updated Antivirus software and enable Firewall rules.
- Avoid clicking suspicious links or downloading email attachments from unknown senders.
- Clear browser cookies and temporary files periodically to prevent tracking.

4.7 Case-Study / Competency-Based Questions

1. Case Study 1: Designing Campus Network Infrastructure

Scenario: A newly constructed school campus consists of three main blocks: Academic Block, Administrative Block, and Science Lab. The school management wishes to connect 40 computers in the Science Lab using a private network, and connect all three blocks together across the 500 meter campus.

Sub-Questions:

- (a) What type of network (PAN, LAN, MAN, WAN) will be established across the school campus?
- (b) Which topology should be selected for the Science Lab computers to ensure that a single cable failure does not bring down the lab network, and what central device is required?
- (c) What guided transmission medium should be used to connect the three blocks to guarantee maximum bandwidth and immunity to electrical noise over 500 meters?

Answers:

- (a) A **Local Area Network (LAN)** will be established (radius < 1 km).
- (b) **Star Topology** using a central **Switch**.
- (c) **Fiber Optic Cable** for high speed, long distance, and zero electromagnetic interference.

2. Case Study 2: Investigating Financial Cyber Fraud

Scenario: An employee received an urgent email appearing to come from his bank, requesting him to click a link and verify his account password and debit card CVV. After clicking the link and submitting his details on a web page, he received an SMS stating that money had been debited from his account.

Sub-Questions:

- (a) What specific cyber attack technique was used to trick the employee into entering his credentials on a fake website?
- (b) What visual indicators in the web browser address bar should the employee have checked to verify site authenticity?
- (c) Under which Indian Act can the employee lodge a legal cybercrime complaint, and at what official portal?

Answers:

- (a) **Phishing** (Email Phishing).
- (b) Check for the **Padlock Icon** and the `https://` security prefix (indicating SSL certificate encryption) on the browser address bar.
- (c) The **Information Technology Act 2000 (Amendment 2008)**, lodged at `cybercrime.gov.in`.

3. Case Study 3: Network Diagnostics and Protocol Troubleshooting

Scenario: An IT administrator is setting up a new web server. She wants to ensure that users can access web pages reliably over TCP, and also wants to block a specific unauthorized computer permanently from accessing the server.

Sub-Questions:

- (a) Why is TCP chosen over UDP for web page transfer (HTTP)?
- (b) Should the administrator block the unauthorized computer using its IP Address or its MAC Address to make the block permanent? Explain why.
- (c) Which network device should be installed between the external internet and internal web server to inspect incoming data packets and enforce security policies?

Answers:

- (a) TCP provides connection-oriented, reliable, and ordered delivery with error checks, ensuring web pages download completely without missing packets.
- (b) Block the **MAC Address**. IP addresses can change dynamically on reconnecting, whereas MAC addresses are permanent physical identifiers burned into the NIC hardware.
- (c) A **Firewall** (Hardware router firewall or dedicated software firewall).