Question 1(a) [3 marks]

What is the Computer Network? Why it is important?

Answer:
A computer network is a collection of interconnected computing devices that can exchange data and share resources.

Diagram:

- **Resource sharing**: Enables sharing of printers, files, applications
- **Communication**: Facilitates information exchange between users
- **Scalability**: Allows networks to grow as needs increase

Mnemonic: "CSI" - "Connect, Share, Interact"

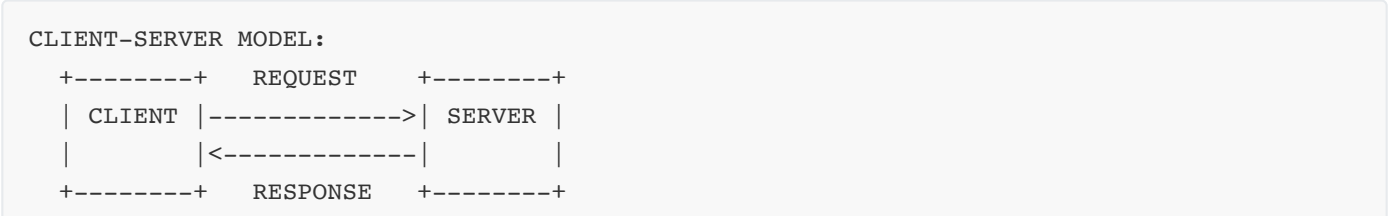
Question 1(b) [4 marks]

Define terms: 1) Web Server, 2)Encrypted data, 3)Hacking, 4)Client-server

Answer:

Term	Definition
Web Server	Software/hardware that serves web content to clients using HTTP/HTTPS
Encrypted Data	Information converted to code to prevent unauthorized access
Hacking	Unauthorized access to computer systems through security vulnerabilities
Client-Server	Network model where centralized servers provide services to client computers

Diagram:



Mnemonic: "WECHS" - "Web servers Encrypt data, Clients and Hackers use Servers"

Question 1(c) [7 marks]

Classify and explain the transmission media in detail.

Answer:
Transmission media are physical pathways that carry data in a network.

Category	Types	Characteristics	Applications
Guided Media			
Twisted Pair	UTP, STP	100m range, 10Mbps-10Gbps	Office LANs
Coaxial Cable	Baseband, Broadband	500m range, 10-100Mbps	Cable TV, Internet
Fiber Optic	Single-mode, Multi-mode	Long distance, 100Mbps-100Gbps	Backbone, WAN
Unguided Media			
Radio Waves	WiFi, Cellular	Omnidirectional, 1-100Mbps	Wireless networks
Microwaves	Terrestrial, Satellite	Line-of-sight, 1-10Gbps	Point-to-point links
Infrared	IrDA	Short-range, 4-16Mbps	Remote controls

Diagram:

- **Guided media**: Physical paths for signal confinement
- **Unguided media**: Wireless transmission through air/space
- **Selection factors**: Cost, bandwidth, distance, environment

Mnemonic: "TCFRIM" - "Twisted pair, Coaxial, Fiber, Radio, Infrared, Microwave"

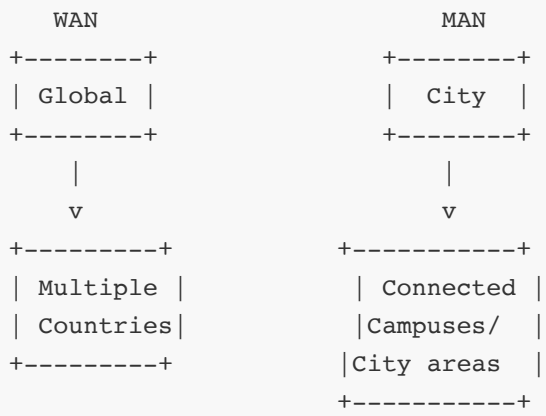
Question 1(c) OR [7 marks]

Explain WAN and MAN type of network.

Answer:
Wide Area Networks (WAN) and Metropolitan Area Networks (MAN) are network types classified by geographic scope.

Feature	MAN (Metropolitan Area Network)	WAN (Wide Area Network)
Coverage	City-wide (5-50 km)	Country/Global (>50 km)
Speed	10 Mbps - 10 Gbps	1.5 Mbps - 1 Gbps
Ownership	Municipal/Telecom	Multiple organizations
Technologies	Ethernet, SONET, WiMAX	Frame Relay, ATM, MPLS
Examples	City networks, Campus networks	Internet, Corporate networks

Diagram:



- **MAN**: Connects LANs within a city/metropolitan area
- **WAN**: Spans large geographical areas across cities/countries
- **Management**: WAN typically requires service providers
- **Infrastructure**: Different transmission media and technologies

Mnemonic: "SWIM" - "Size: WAN Is Massive compared to MAN"

Question 2(a) [3 marks]

Explain in detail: Transmission technology.

Answer:
Transmission technology refers to methods used to transfer data between network devices.

Technology Type	Description	Example
Point-to-Point	Direct connection between two nodes	Leased line
Broadcast	Single communication channel shared by all nodes	Wireless LAN
Multipoint	Multiple devices share single link	Cable networks

- **Analog transmission**: Continuous signal, susceptible to noise

- **Digital transmission**: Discrete signal, more reliable
- **Baseband**: Single signal uses entire bandwidth (Ethernet)
- **Broadband**: Multiple signals share bandwidth (Cable TV)

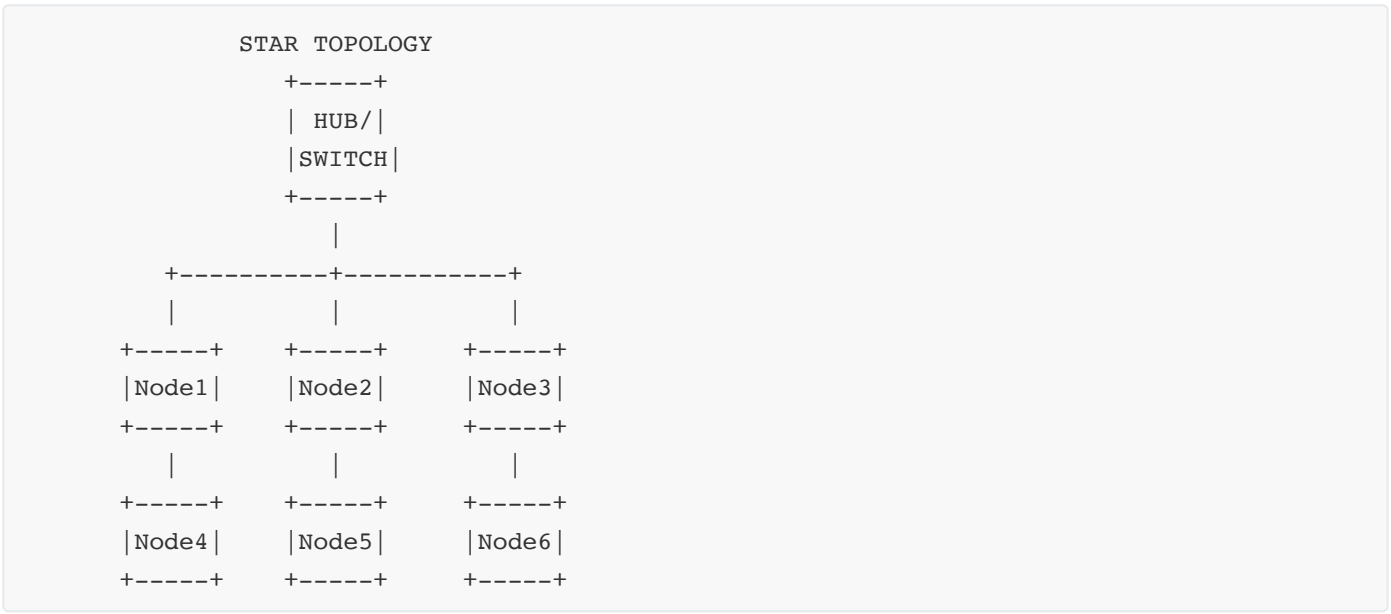
Mnemonic: "ABP-DMB" - "Analog or Baseband, Point-to-point; Digital or Multipoint, Broadcast"

Question 2(b) [4 marks]

Draw and explain Star topology in detail.

Answer:
Star topology is a network configuration where all devices connect to a central hub/switch.

Diagram:



Advantages	Disadvantages
Easy installation	Single point of failure (hub/switch)
Simple troubleshooting	Requires more cable than bus topology
Scalable	Higher cost due to central device
Better performance	Hub/switch limits determine network size

- **Operation**: All data passes through central device
- **Installation**: Easier to manage and expand
- **Fault isolation**: Node failure doesn't affect others

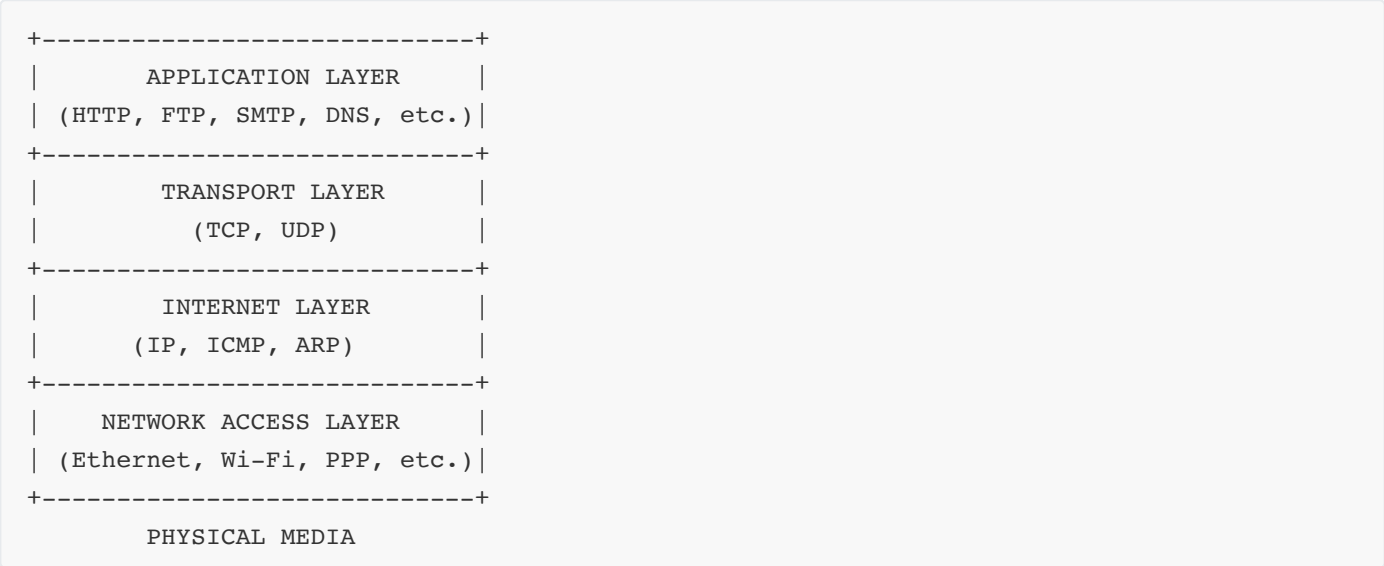
Mnemonic: "CASE" - "Centralized, All connected, Simple expansion, Easy troubleshooting"

Question 2(c) [7 marks]

Draw and explain TCP/IP model.

Answer:
TCP/IP model is a conceptual framework used for network communications, consisting of four layers.

Diagram:



Layer	Main Functions	Protocols
Application	User interfaces, data formatting	HTTP, FTP, SMTP, DNS
Transport	End-to-end communication, reliability	TCP, UDP
Internet	Logical addressing, routing	IP, ICMP, ARP, IGMP
Network Access	Physical addressing, media access	Ethernet, WiFi, PPP

- **Application Layer**: Interface between applications and network
- **Transport Layer**: Reliable data transfer between end systems
- **Internet Layer**: Routing packets across networks
- **Network Access Layer**: Physical connection to network media

Mnemonic: "ATNI" - "Application Talks, Network Internet Interfaces"

Question 2(a) OR [3 marks]

Draw and explain Bus topology in detail

Answer:
Bus topology is a network configuration where all devices connect to a single communication line.

Diagram:

```
        BUS TOPOLOGY
+-----+    +-----+    +-----+    +-----+
|Node1|====|Node2|====|Node3|====|Node4|
+-----+    +-----+    +-----+    +-----+
                |
             +-----+
             |Node5|
             +-----+
```

Advantages	Disadvantages
Simple layout	Single point of failure (main cable)
Less cabling	Limited cable length
Low cost	Performance degrades with more nodes
Easy to extend	Difficult to troubleshoot

- **Operation**: Data travels along the bus in both directions
- **Terminator**: Required at both ends to prevent signal reflection
- **Usage**: Primarily in older networks, small setups

Mnemonic: "SLUE" - "Simple Layout, Uses less cable, Easy installation"

Question 2(b) OR [4 marks]

Explain Network Classification based on its architecture.

Answer:
Networks can be classified based on their architectural models that define how devices interact.

Architecture	Characteristics	Example
Peer-to-Peer	Equal privileges, no dedicated servers	Home networks, small workgroups
Client-Server	Centralized services, dedicated servers	Enterprise networks, web services
Three-Tier	Presentation, application, and data tiers	Modern web applications
N-Tier	Multiple specialized tiers	Large distributed systems

Diagram:

```
PEER-TO-PEER:                CLIENT-SERVER:
  +----+     +----+            +------+
  |Node|-----|Node|            |Client|
  +----+\   /+----+            +------+
        \ /                        |
         X                     +------+
        / \                    |Server|
  +----+/   \+----+            +------+
  |Node|-----|Node|
  +----+     +----+
```

- **Peer-to-Peer**: Direct device communication, distributed resources
- **Client-Server**: Centralized resource management, better security
- **Hybrid**: Combines elements of both architectures

Mnemonic: "PCAN" - "Peer-to-peer, Client-server, Architecture Networks"

Question 2(c) OR [7 marks]

Explain classification of IP address.

Answer:
IP addresses are classified into different categories based on their structure and purpose.

IP Classification	Range	Default Mask	Available Networks	Hosts/Network
Class A	1.0.0.0 - 127.255.255.255	255.0.0.0 (/8)	126	16,777,214
Class B	128.0.0.0 - 191.255.255.255	255.255.0.0 (/16)	16,384	65,534
Class C	192.0.0.0 - 223.255.255.255	255.255.255.0 (/24)	2,097,152	254
Class D (Multicast)	224.0.0.0 - 239.255.255.255	N/A	N/A	N/A
Class E (Reserved)	240.0.0.0 - 255.255.255.255	N/A	N/A	N/A

Special IP Ranges:

- **Private IPs**: 10.0.0.0/8, 172.16.0.0/12, 192.168.0.0/16
- **Loopback**: 127.0.0.0/8 (typically 127.0.0.1)
- **Link-local**: 169.254.0.0/16

Diagram:

```
CLASS A: |0|NETWORK(7 bits)|      HOST(24 bits)       |
CLASS B: |10|  NETWORK(14 bits)   |    HOST(16 bits)   |
CLASS C: |110| NETWORK(21 bits)        |  HOST(8 bits) |
CLASS D: |1110|       MULTICAST ADDRESS(28 bits)       |
CLASS E: |1111|       RESERVED ADDRESS(28 bits)        |
```

- **Classful addressing**: Original IP address classification scheme
- **CIDR (Classless)**: Modern approach that allows flexible subnet masks

- **IPv4 vs IPv6**: IPv4 uses 32-bit addresses, IPv6 uses 128-bit addresses

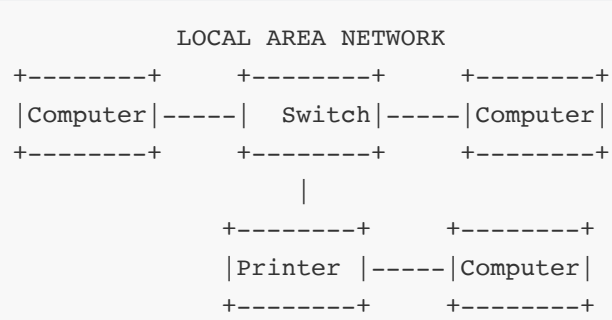
Mnemonic: "ABCDE" - "Address Blocks Categorized by Decreasing End-host counts"

Question 3(a) [3 marks]

What is full name of LAN? Explain it in detail.

Answer:
LAN stands for Local Area Network, a network confined to a limited geographic area.

Diagram:



LAN Characteristics	Description
Geographic Scope	Building, campus, or small area (1-2 km)
Data Rate	High (10 Mbps to 10 Gbps)
Ownership	Single organization or individual
Technology	Ethernet, WiFi, Token Ring
Media	Twisted pair, fiber optic, wireless

- **Purpose**: Connect nearby devices for resource sharing
- **Administration**: Easier management than larger networks
- **Applications**: Office networking, home networking

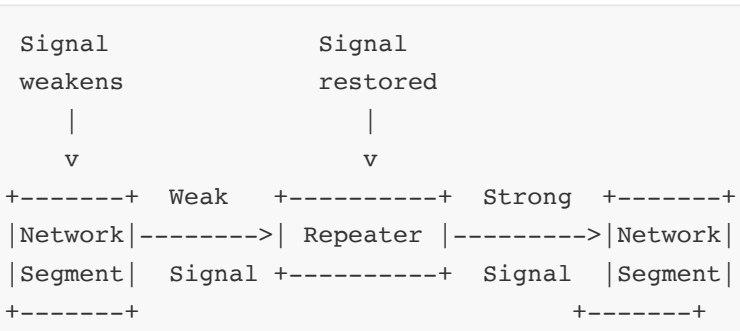
Mnemonic: "LOCAL" - "Limited in range, Owned by one entity, Connected devices, Access control, Low latency"

Question 3(b) [4 marks]

Write a short-note of Repeater.

Answer:
A repeater is a network device that amplifies and regenerates signals to extend network range.

Diagram:



Feature	Description
OSI Layer	Physical Layer (Layer 1)
Function	Signal regeneration and amplification
Purpose	Extend network transmission distance
Limitation	Cannot filter traffic or connect different networks

- **Operation**: Receives, regenerates, and retransmits signals
- **Usage**: Extending cable length beyond normal limits
- **Types**: Traditional repeaters, hubs (multiport repeaters)

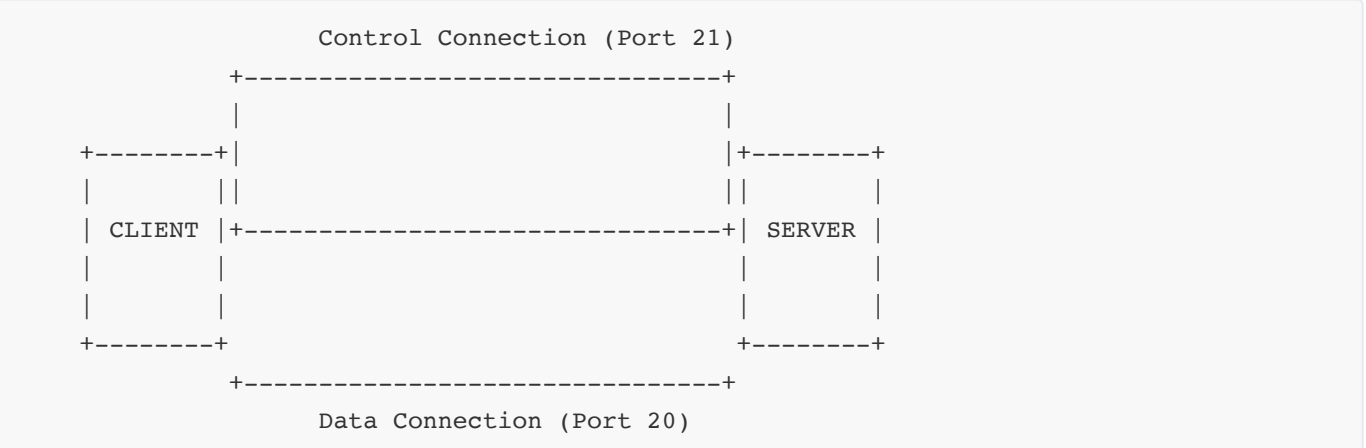
Mnemonic: "RARE" - "Repeaters Amplify and Regenerate Electrical signals"

Question 3(c) [7 marks]

Write short note on FTP.

Answer:
File Transfer Protocol (FTP) is a standard network protocol for transferring files between clients and servers.

Diagram:



Feature	Description
Port	Control: 21, Data: 20
Mode	Active or Passive
Authentication	Username/password (or anonymous)
Transfer Types	ASCII (text) or Binary (raw data)
Security	Basic FTP (unsecured), FTPS, SFTP (secure variants)

- **Dual Channel**: Separate control and data connections
- **Commands**: GET, PUT, LIST, DELETE, RENAME, etc.
- **User Authentication**: Requires login credentials

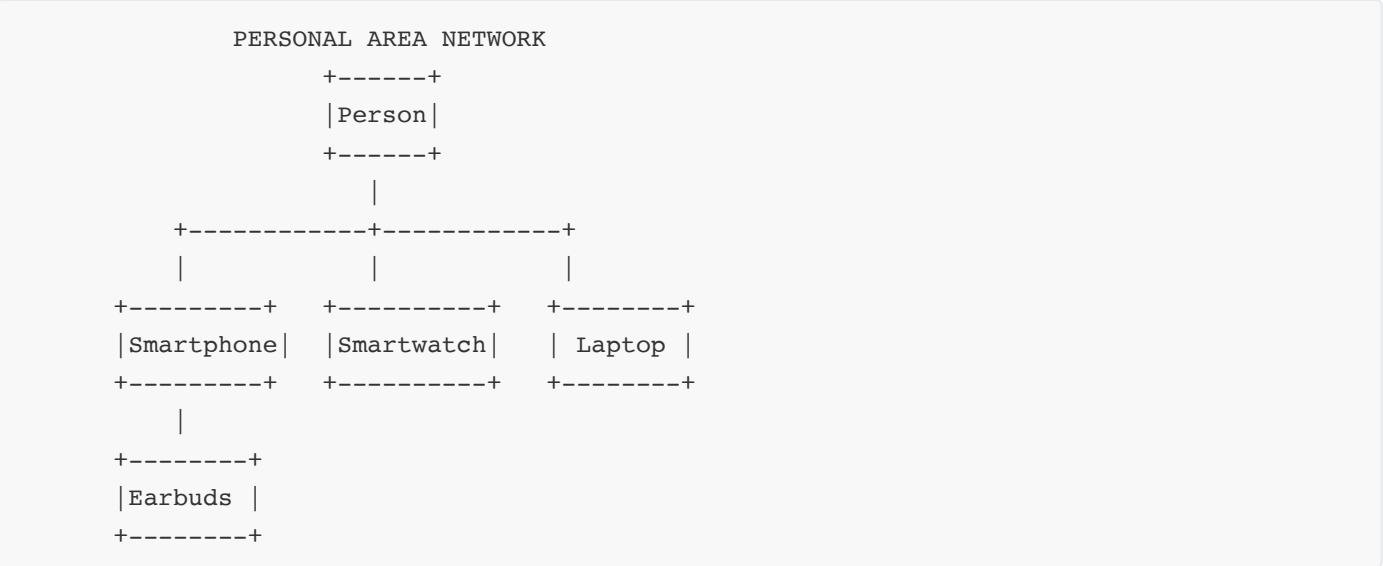
Mnemonic: "CDATA" - "Control channel, Data channel, Active/passive modes, Transfer types, Authentication"

Question 3(a) OR [3 marks]

What is full name of PAN? Explain in detail.

Answer:
PAN stands for Personal Area Network, a network for connecting devices centered around an individual.

Diagram:



PAN Characteristics	Description
Geographic Scope	Very small (1-10 meters)
Data Rate	Low to medium (100 Kbps - 100 Mbps)
Ownership	Individual person
Technology	Bluetooth, Zigbee, NFC, Infrared
Devices	Personal devices (phones, wearables, laptops)

- **Purpose**: Connect personal devices for communication/data sharing
- **Types**: Wired PAN (USB) and Wireless PAN (Bluetooth)
- **Applications**: Data synchronization, audio streaming, health monitoring

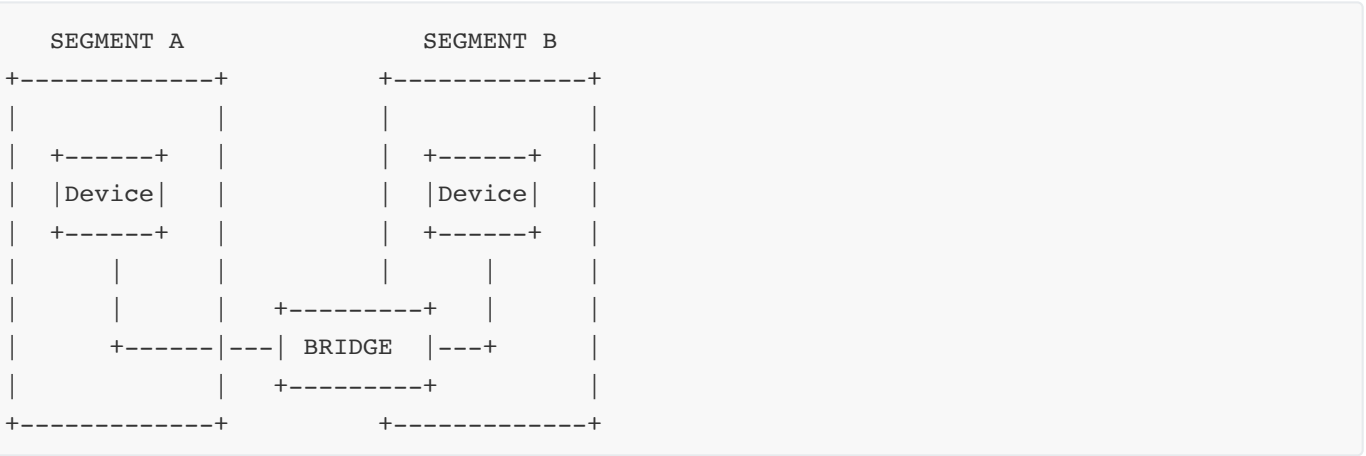
Mnemonic: "PIPER" - "Personal, Individual, Proximity, Easy setup, Reduced range"

Question 3(b) OR [4 marks]

What is the importance of a Bridge? Write short-note on it.

Answer:
A bridge is a network device that connects and filters traffic between network segments.

Diagram:



Feature	Description
OSI Layer	Data Link Layer (Layer 2)
Function	Connect similar network segments
Intelligence	Uses MAC addresses to filter traffic
Advantage	Reduces unnecessary traffic between segments

- **Importance**: Extends network, reduces collision domains

- **Operation**: Learns MAC addresses, forwards frames selectively
- **Types**: Transparent, translational, source-route bridges

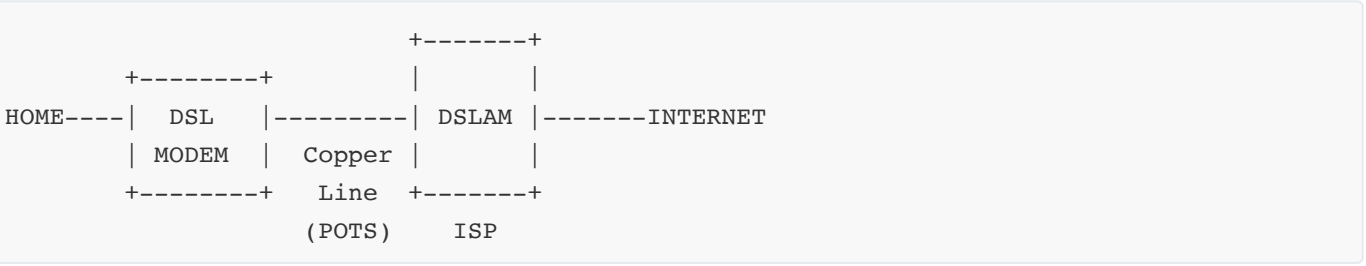
Mnemonic: "SELF" - "Segmentation, Extension, Learning addresses, Filtering traffic"

Question 3(c) OR [7 marks]

What is DSL? Explain its different types.

Answer:
Digital Subscriber Line (DSL) is a family of technologies that provides digital data transmission over telephone lines.

Diagram:



DSL Type	Full Name	Speed (Down/Up)	Distance	Application
ADSL	Asymmetric DSL	8 Mbps/1 Mbps	Up to 5.5 km	Residential internet
SDSL	Symmetric DSL	2 Mbps/2 Mbps	Up to 3 km	Small business
VDSL	Very high-bit-rate DSL	52-85 Mbps/16-85 Mbps	Up to 1.2 km	Video streaming, businesses
HDSL	High-bit-rate DSL	2 Mbps/2 Mbps	Up to 3.6 km	T1/E1 replacement
IDSL	ISDN DSL	144 Kbps/144 Kbps	Up to 5.5 km	ISDN alternative

- **Working Principle**: Uses unused frequency spectrum on phone lines
- **Advantage**: Uses existing telephone infrastructure
- **Always-on**: Continuous connection without dial-up

Mnemonic: "SAVHI" - "Symmetric, Asymmetric, Very high-bit-rate, High-bit-rate, ISDN DSL"

Question 4(a) [3 marks]

Explain an error control and flow control at data link layer.

Answer:
Error and flow control are essential data link layer functions that ensure reliable data transmission.

Mechanism	Purpose	Techniques
Error Control	Detect/correct transmission errors	CRC, Checksums, Parity bits
Flow Control	Prevent sender overwhelming receiver	Stop-and-wait, Sliding window

Diagram:

```
ERROR CONTROL:
  +------+  DATA   +-------+  ACK/NAK +--------+
  |Sender|-------->|Channel|--------->|Receiver|
  +------+         +-------+          +--------+

FLOW CONTROL:
  +------+  DATA   +--------+
  |Sender|-------->|Receiver|
  +------+  STOP   +--------+
         <---------
```

- **Error Detection**: CRC, checksum identify corrupted frames
- **Error Correction**: Forward Error Correction (FEC), retransmission
- **Flow Control**: Prevents buffer overflow at receiver

Mnemonic: "SAFE" - "Stop-and-wait, Acknowledgment, Flow control, Error detection"

Question 4(b) [4 marks]

What is Firewall? Explain it in detail.

Answer:
A firewall is a network security device that monitors and filters incoming and outgoing network traffic.

Diagram:

```
   INTERNAL NETWORK                  INTERNET
+-------------------+             +--------------+
|                   |  FIREWALL   |              |
|  +-----+  +-----+ |  +------+   |  +--------+  |
|  |Host1|  |Host2| |  |      |   |  |External|  |
|  +-----+  +-----+ |--|FILTER|---|  |Server  |  |
|                   |  |      |   |  +--------+  |
|  +-----+  +-----+ |  +------+   |              |
|  |Host3|  |Host4| |             |              |
|  +-----+  +-----+ |             |              |
+-------------------+             +--------------+
```

Firewall Type	Functionality	Example
Packet Filtering	Examines packet headers	Router ACLs
Stateful Inspection	Tracks connection state	Most hardware firewalls
Application Layer	Inspects content	Web application firewalls
Next-Generation	Combines multiple technologies	Palo Alto, Fortinet

- **Purpose**: Protects networks from unauthorized access
- **Implementation**: Hardware, software, or cloud-based
- **Security Policy**: Rules defining allowed/blocked traffic

Mnemonic: "PAPSI" - "Packet filtering, Application layer, Policies, Stateful inspection"

Question 4(c) [7 marks]

Compare IPV4 and IPV6.

Answer:
IPv4 and IPv6 are Internet Protocol versions with significant differences in addressing and capabilities.

Feature	IPv4	IPv6
Address Size	32-bit (4 bytes)	128-bit (16 bytes)
Format	Dotted decimal (192.168.1.1)	Hexadecimal with colons (2001:0db8:85a3::8a2e:0370:7334)
Address Space	~4.3 billion addresses	340 undecillion addresses
Header	Variable length (20-60 bytes)	Fixed length (40 bytes)
Fragmentation	Routers and sending hosts	Only sending hosts
Checksum	Included in header	Removed from header
Security	Not built-in (IPsec optional)	Built-in IPsec support

Diagram:

```
IPv4: |VER|IHL|DSCP|ECN|  TOTAL LENGTH   |
      |  IDENTIFICATION   |FLAGS|FRAGMENT|
      |TTL |PROTOCOL|  HEADER CHECKSUM   |
      |        SOURCE ADDRESS           |
      |      DESTINATION ADDRESS        |
      |          OPTIONS...             |

IPv6: |VER|TRAFFIC CLASS|     FLOW LABEL      |
      |   PAYLOAD LENGTH   |NEXT HDR|HOP LIMIT|
      |                                       |
      |           SOURCE ADDRESS              |
      |                                       |
```

```
      |                                     |
      |                                     |
      |          DESTINATION ADDRESS        |
      |                                     |
```

- **Auto-configuration**: IPv6 has stateless address auto-configuration
- **NAT**: Not required in IPv6 due to larger address space
- **Transition**: Dual-stack, tunneling, translation mechanisms
- **Header efficiency**: IPv6 has streamlined header for better performance

Mnemonic: "SHAPE" - "Size, Header, Addressing, Performance, Extensibility"

Question 4(a) OR [3 marks]

What is an IP address? How it is used in network?

Answer:
An IP address is a numerical identifier assigned to each device connected to a network that uses Internet Protocol.

Diagram:

```
IP ADDRESS: 192.168.1.100
 +---+---+---+---+
 |192|168| 1 |100|  <-- Dotted decimal notation
 +---+---+---+---+
  |   |   |   |
  |   |   |   +---- Host identifier
  |   |   +-------- Subnet identifier
  +---+------------ Network identifier
```

IP Address Usage	Description
Identification	Uniquely identifies devices on a network
Routing	Determines path for data packets
Addressing	Enables sending data to specific destinations
Network Division	Allows subdivision into subnets

- **Structure**: Network portion and host portion
- **Assignment**: Static (manual) or dynamic (DHCP)
- **Versions**: IPv4 (32-bit) and IPv6 (128-bit)

Mnemonic: "IRAN" - "Identification, Routing, Addressing, Network division"

Question 4(b) OR [4 marks]

Compare FDDI and CDDI.

Answer:
FDDI (Fiber Distributed Data Interface) and CDDI (Copper Distributed Data Interface) are high-speed network technologies.

Feature	FDDI	CDDI
Medium	Fiber optic cable	Copper twisted pair
Speed	100 Mbps	100 Mbps
Distance	Up to 200 km total, 2 km between stations	Up to 100 m between stations
Topology	Dual counter-rotating rings	Dual counter-rotating rings
Cost	Higher	Lower
Reliability	Very high	Moderate
Standard	ANSI X3T9.5	Same as FDDI (adapted for copper)

Diagram:

- **Redundancy**: Secondary ring for fault tolerance
- **Access Method**: Token passing with timed token rotation
- **Applications**: FDDI for backbones, CDDI for workstations

Mnemonic: "FDDI Flies, CDDI Crawls" - Fiber for long distance, Copper for shorter runs

Question 4(c) OR [7 marks]

Draw and explain OSI reference model in detail.

Answer:
The OSI (Open Systems Interconnection) model is a conceptual framework that standardizes network functions into seven layers.

Diagram:

```
+----------------------------+
|         APPLICATION (7)    |
|      User interface, apps  |
+----------------------------+
|        PRESENTATION (6)    |
|    Data format, encryption |
+----------------------------+
|          SESSION (5)       |
|    Connection management   |
+----------------------------+
|         TRANSPORT (4)      |
|   End-to-end reliability   |
+----------------------------+
|          NETWORK (3)       |
|   Routing between networks |
+----------------------------+
|         DATA LINK (2)      |
|  Node-to-node reliability  |
+----------------------------+
|          PHYSICAL (1)      |
|   Physical transmission    |
+----------------------------+
```

Layer	Primary Function	Protocols/Standards	Data Unit
Application	User interface, network services	HTTP, FTP, SMTP	Data
Presentation	Data formatting, encryption	SSL/TLS, JPEG, MIME	Data
Session	Connection establishment, management	NetBIOS, RPC	Data
Transport	End-to-end delivery, flow control	TCP, UDP	Segments
Network	Logical addressing, routing	IP, ICMP, OSPF	Packets
Data Link	Physical addressing, media access	Ethernet, PPP, HDLC	Frames
Physical	Bit transmission, cabling, signaling	USB, Ethernet, Bluetooth	Bits

- **Layer Independence**: Each layer performs specific functions
- **Encapsulation**: Data wrapped with headers at each layer
- **Standardization**: Promotes interoperability between systems
- **Troubleshooting**: Isolates problems to specific layers

Mnemonic: "All People Seem To Need Data Processing" (Layers 7 to 1)

Question 5(a) [3 marks]

What is ISO? How it works in information security?

Answer:
ISO (International Organization for Standardization) develops and publishes standards including those for information security.

ISO Security Standards	Purpose
ISO/IEC 27001	Information security management systems
ISO/IEC 27002	Code of practice for security controls
ISO/IEC 27005	Information security risk management
ISO/IEC 27017	Cloud security
ISO/IEC 27018	Protection of personally identifiable information

Working in Information Security:

- **Framework-based**: Provides structured approach to security
- **Risk-based**: Focuses on identification and mitigation of risks
- **Process-oriented**: Establishes continuous improvement cycle
- **Certification**: Organizations can be certified for compliance

Mnemonic: "PRIMP" - "Policies, Risk assessment, Implementation, Monitoring, Process improvement"

Question 5(b) [4 marks]

Explain terms in detail for cryptography: 1) Encryption 2) Decryption

Answer:
Encryption and decryption are fundamental processes in cryptography that secure information.

Term	Definition	Types	Example Algorithms
Encryption	Process of converting plaintext to ciphertext using an algorithm and key	Symmetric, Asymmetric, Hybrid	AES, RSA, ECC
Decryption	Process of converting ciphertext back to plaintext using an algorithm and key	Symmetric, Asymmetric, Hybrid	AES, RSA, ECC

Diagram:

```
ENCRYPTION:
  +-----------+    ENCRYPTION    +------------+
  | PLAINTEXT |----------------->| CIPHERTEXT |
  +-----------+   ALGORITHM &    +------------+
                  KEY

DECRYPTION:
  +------------+    DECRYPTION    +-----------+
  | CIPHERTEXT |----------------->| PLAINTEXT |
  +------------+   ALGORITHM &    +-----------+
                   KEY
```

Encryption:

- **Purpose**: Protects confidentiality of information
- **Methods**: Substitution, transposition, block cipher, stream cipher
- **Key Management**: Critical aspect of secure encryption

Decryption:

- **Purpose**: Retrieves original information from encrypted form
- **Requirements**: Correct algorithm and key
- **Implementation**: Hardware or software-based

Mnemonic: "PACK-DUKE" - "Plaintext Algorithm Cipher Key - Decoding Using Key for Extraction"

Question 5(c) [7 marks]

Write a short-note on 1) E-mail and 2) DNS

Answer:
1) E-mail (Electronic Mail):

E-mail is a method of exchanging digital messages over a communication network.

Diagram:

```
E-MAIL SYSTEM:
   +--------+    SMTP     +---------+    POP3/IMAP   +--------+
   | SENDER |------------>|  MAIL   |--------------->|RECEIVER|
   | CLIENT |             | SERVER  |                | CLIENT |
   +--------+             +---------+                +--------+
                              |
                          +---------+
                          |   DNS   |
                          | SERVER  |
                          +---------+
```

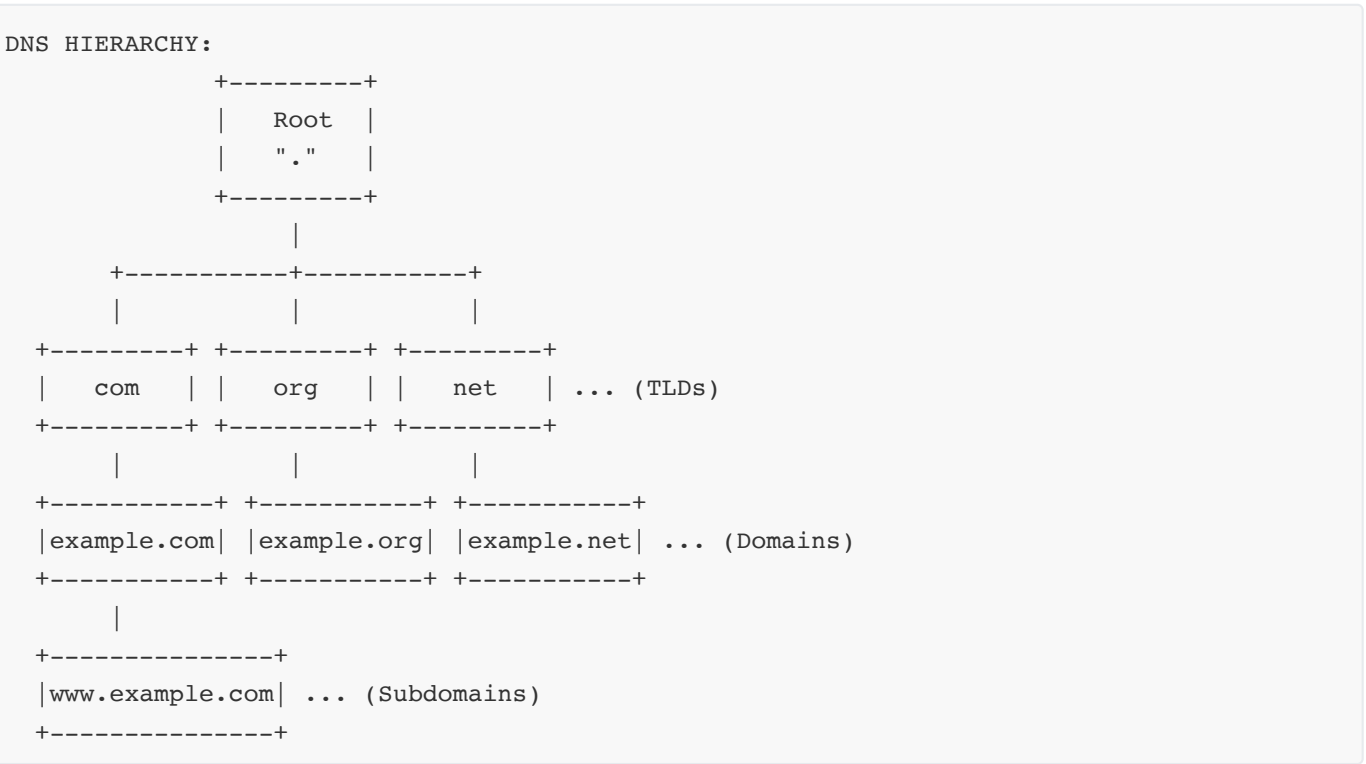
Component	Function
Mail User Agent (MUA)	Email client software used by end-users
Mail Transfer Agent (MTA)	Server software that transfers emails
Mail Delivery Agent (MDA)	Delivers email to recipient's mailbox
Protocols	SMTP (sending), POP3/IMAP (receiving)

- **Structure**: Headers (To, From, Subject) and Body
- **Security**: Features like encryption (TLS), authentication (SPF, DKIM)
- **Attachments**: Binary files encoded for text transmission
- **Features**: Forwarding, filtering, organizing, searching

2) DNS (Domain Name System):

DNS is a hierarchical and decentralized naming system for translating domain names to IP addresses.

Diagram:



DNS Component	Function
Root Servers	Top of DNS hierarchy
TLD Servers	Manage top-level domains (.com, .org)
Authoritative Servers	Store DNS records for specific domains
Recursive Resolvers	Query other servers to resolve domain names
DNS Records	Resource records (A, AAAA, MX, CNAME, etc.)

- **Purpose**: Map human-readable names to machine-readable addresses
- **Resolution Process**: Recursive or iterative queries through hierarchy
- **Caching**: Temporary storage of results to improve performance
- **Security**: DNSSEC provides authentication and integrity

Mnemonic: "MAPS" - "Mail needs Addresses, Protocols, and Servers"
Mnemonic: "HARD" - "Hierarchy, Addressing, Resolution, Distributed system"

Question 5(a) OR [3 marks]

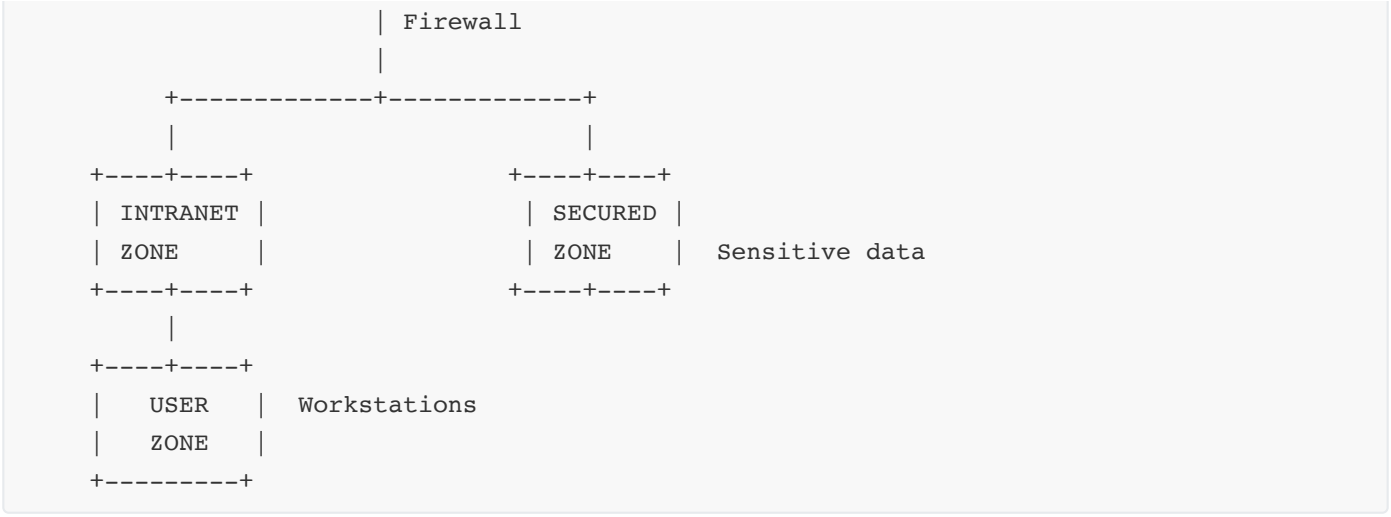
What do you mean by security topology and security zone?

Answer:
Security topology and security zones are network security concepts that organize and protect network resources.

Concept	Definition	Examples
Security Topology	Physical and logical arrangement of security controls	DMZ, Defense-in-depth
Security Zone	Segment of network with specific security requirements	DMZ, Intranet, Extranet

Diagram:

```
SECURITY TOPOLOGY WITH ZONES:
                  +----------+
                  | INTERNET |
                  +----+-----+
                       |
                       | Firewall
                       |
                  +----+-----+
                  |   DMZ    |  Web, Email, DNS servers
                  +----+-----+
                       |
```



- **Security Topology**: Overall security architecture design
- **Security Zones**: Logical boundaries with consistent security policies
- **Defense-in-depth**: Multiple layers of security controls

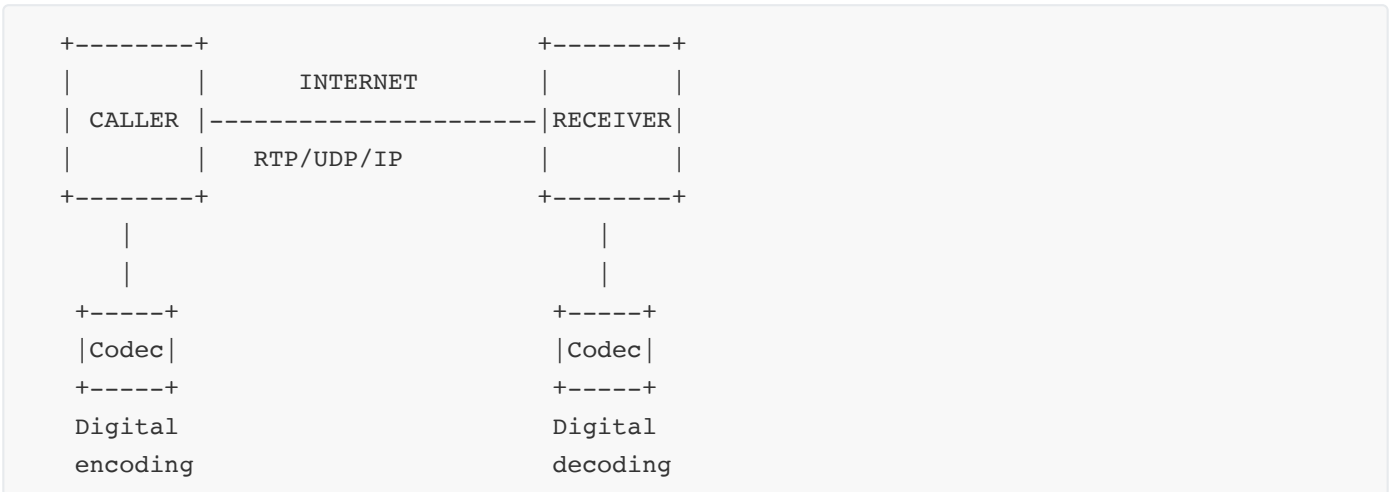
Mnemonic: "TIPS" - "Topology Isolates and Protects Systems"

Question 5(b) OR [4 marks]

Write short-note on Voice and Video IP.

Answer:
Voice and Video over IP (VoIP/Video IP) refers to technologies for transmitting voice and video communications over IP networks.

Diagram:



Component	Function
Codecs	Encode/decode audio and video (G.711, H.264)
Signaling Protocols	Call setup/teardown (SIP, H.323)
Transport Protocol	Real-time media transport (RTP/RTCP)
QoS Mechanisms	Prioritize voice/video traffic

Voice over IP (VoIP):

- **Benefits**: Cost savings, flexibility, integration with apps
- **Challenges**: Latency, jitter, packet loss
- **Applications**: IP phones, softphones, conferencing

Video over IP:

- **Types**: Video conferencing, streaming, surveillance
- **Requirements**: Higher bandwidth, low latency
- **Technologies**: WebRTC, SIP video, RTSP streaming

Mnemonic: "CLEAR" - "Codecs compress, Latency matters, Encodes audio/video, Applications integrate, Real-time transport"

Question 5(c) OR [7 marks]

What is IP security? Explain in detail.

Answer:
IP Security (IPsec) is a suite of protocols designed to secure IP communications by authenticating and encrypting each IP packet.

Diagram:

```
|         | (Key Management)  |        |
|         +-------------------+        |
+--------------------------------------+
|           NETWORK ACCESS             |
+--------------------------------------+
```

IPsec Protocol	Function	Protection
Authentication Header (AH)	Data integrity, authentication	No encryption
Encapsulating Security Payload (ESP)	Confidentiality, integrity, authentication	Encrypts data
Internet Key Exchange (IKE)	Key exchange, SA negotiation	Secure key management

IPsec Modes:

Mode	Description	Use Case
Transport Mode	Protects payload only	Host-to-host communications
Tunnel Mode	Protects entire packet	Site-to-site VPNs, remote access

Security Services:

- **Authentication**: Verifies identity of communicating entities
- **Confidentiality**: Protects data from unauthorized disclosure
- **Data Integrity**: Ensures data hasn't been altered in transit
- **Replay Protection**: Prevents packet replay attacks
- **Access Control**: Limits access to network resources

Applications:

- **VPNs**: Remote access and site-to-site connections
- **Secure Routing**: Protects routing protocols
- **Secure Host-to-Host**: End-to-end security

Mnemonic: "AVID TC" - "Authentication, Verification, Integrity, Datagram protection, Transport mode, Confidentiality"