COMPUTER NETWORKS

STUDY MATERIAL

UNIT I: INTRODUCTION AND PHYSICAL LAYER

UNIT I

INTRODUCTION AND PHYSICAL LAYER

1.1 Introduction to Computer Networks

A **computer network** is a collection of interconnected computing devices (computers, servers, routers, switches) that can communicate and share resources with each other. Networks enable resource sharing, communication, data storage, and distributed processing.

Types of Networks

Network Type	Full Form	Coverage Area	Example
PAN	Personal Area Network	~10 meters	Bluetooth devices
LAN	Local Area Network	Building / Campus	Office network, Ethernet
MAN	Metropolitan Area Network	City / Town	Cable TV network
WAN	Wide Area Network	Country / World	Internet, leased lines

1.2 Protocol Layering

Protocol layering organizes network functions into a **hierarchical stack of layers**. Each layer provides services to the layer above and uses services from the layer below. This modular design simplifies implementation and troubleshooting.

Advantages of Layering

- Modularity – each layer is independent and can be changed without affecting others.
- Interoperability – different vendors implement the same standards.
- Easier troubleshooting – problems can be isolated to a specific layer.
- Reusability – lower layers can serve multiple upper-layer protocols.

1.3 OSI Reference Model

The **OSI (Open Systems Interconnection)** model, developed by ISO, defines seven layers for network communication. It is a conceptual framework; actual protocols follow TCP/IP.

Layer No.	Layer Name	Key Functions	Example Protocols
7	Application	User interface, network services	HTTP, FTP, DNS, SMTP
6	Presentation	Data translation, encryption, compression	SSL/TLS, JPEG, ASCII
5	Session	Session establishment, synchronization	NetBIOS, RPC
4	Transport	End-to-end delivery, error recovery, flow control	TCP, UDP
3	Network	Logical addressing, routing	IP, ICMP, OSPF
2	Data Link	Framing, MAC addressing, error detection	Ethernet, PPP, HDLC
1	Physical	Bit transmission over medium	RS-232, DSL, 802.11

1.4 TCP/IP Protocol Suite

The **TCP/IP model** is the practical implementation model used on the internet. It has four layers that map to OSI layers.

TCP/IP Layer	OSI Equivalent	Protocols
Application	Application + Presentation + Session	HTTP, FTP, DNS, SMTP, SSH
Transport	Transport	TCP, UDP, SCTP
Internet	Network	IP, ICMP, ARP, RARP
Network Access	Data Link + Physical	Ethernet, Wi-Fi, PPP

1.5 Physical Layer

The **Physical Layer** is responsible for transmitting raw bits over a communication channel. It deals with electrical, mechanical, and timing specifications.

Performance Metrics

Metric	Definition	Unit

Bandwidth	Maximum data rate a channel can carry	bps (bits per second)
Throughput	Actual data rate achieved in practice	bps
Latency / Delay	Time for data to travel from source to destination	Milliseconds (ms)
Jitter	Variation in packet delay	ms
BER	Bit Error Rate – fraction of bits received in error	Dimensionless ratio

1.6 Transmission Media

Guided (Wired) Media

Medium	Bandwidth	Distance	Advantages	Disadvantages
Twisted Pair (UTP/STP)	Up to 1 Gbps	100 m	Cheap, easy to install	Susceptible to EMI
Coaxial Cable	Up to 10 Gbps	500 m	Better shielding	Bulky, expensive
Fiber Optic	Up to 100 Tbps	Km range	Very high speed, immune to EMI	Costly, fragile

Unguided (Wireless) Media

Medium	Frequency	Range	Use
Radio Waves	3 kHz – 1 GHz	Long range	AM/FM radio, cellular
Microwaves	1–300 GHz	Line of sight	Satellite, point-to-point links
Infrared	300 GHz – 400 THz	Short range	Remote controls, IR LAN

1.7 Switching Techniques

Circuit Switching

In **circuit switching**, a dedicated physical path is established between sender and receiver before data transfer begins and maintained throughout the session. The path is reserved exclusively.

- Three phases: Circuit establishment → Data transfer → Circuit teardown.
- Example: Traditional PSTN telephone network.
- Advantages: Guaranteed bandwidth, constant delay.
- Disadvantages: Wasteful if link is idle, setup delay.

Packet Switching

In **packet switching**, data is divided into packets. Each packet is independently routed through the network and reassembled at the destination.

- Two types: Datagram (connectionless) and Virtual Circuit (connection-oriented).
- Example: Internet (IP-based networking).
- Advantages: Efficient use of bandwidth, resilient to failures.
- Disadvantages: Variable delay (jitter), packet reordering needed.

Feature	Circuit Switching	Packet Switching
Path	Dedicated fixed path	No fixed path
Setup	Required before data transfer	Not required
Bandwidth	Reserved	Shared dynamically
Delay	Constant	Variable
Efficiency	Low (idle capacity wasted)	High
Example	Telephone network	Internet

COMPUTER NETWORKS

STUDY MATERIAL

UNIT II: DATA LINK LAYER & MEDIA ACCESS

UNIT II

DATA LINK LAYER & MEDIA ACCESS

2.1 Introduction to Data Link Layer

The **Data Link Layer (Layer 2)** provides node-to-node data transfer between directly connected devices. It packages raw bits from the Physical layer into **frames** and handles addressing, error detection, and flow control.

DLC Services (Data Link Control)

Service	Description
Framing	Encapsulates bits into frames with header, data, and trailer
Flow Control	Prevents sender from overwhelming a slow receiver (sliding window)
Error Control	Detects and corrects transmission errors (CRC, ARQ)
Link Management	Establishes, maintains, and releases data link connections

2.2 Link-Layer Addressing (MAC Address)

A **MAC (Media Access Control) address** is a unique 48-bit (6-byte) hardware identifier burned into every NIC. Written in hexadecimal: **00:1A:2B:3C:4D:5E**. Used for communication within the same local network segment.

- First 3 bytes: OUI (Organizationally Unique Identifier) – identifies manufacturer.
- Last 3 bytes: Device-specific identifier.
- Broadcast MAC: FF:FF:FF:FF:FF:FF
- ARP resolves IP address → MAC address within LAN.

2.3 Data Link Layer Protocols

HDLC (High-Level Data Link Control)

HDLC is a bit-oriented, synchronous data link protocol. It is the basis for many other protocols (PPP, X.25). Uses flags (01111110) to delimit frames.

Frame Type	Purpose
I-Frame (Information)	Carries user data with sequence numbers for flow/error control
S-Frame (Supervisory)	Flow and error control (RR, RNR, REJ, SREJ)
U-Frame (Unnumbered)	Link management – setup, disconnect, mode setting

PPP (Point-to-Point Protocol)

PPP is a data link protocol used to establish a direct connection between two nodes. Used in dial-up, DSL, VPN tunnels.

PPP Frame Field	Size	Purpose
Flag	1 byte	Frame delimiter (01111110)
Address	1 byte	Always 11111111 (broadcast)
Control	1 byte	Always 00000011 (unnumbered)
Protocol	2 bytes	Identifies the payload protocol (IP=0x0021)
Data	Variable	Payload (max 1500 bytes default)
FCS	2-4 bytes	Frame Check Sequence (error detection)

2.4 Media Access Control (MAC)

When multiple devices share a single medium, a **MAC protocol** coordinates access to prevent collisions and ensure fair use.

MAC Protocol	Type	Used In
CSMA/CD	Contention-based + collision detection	Wired Ethernet (IEEE 802.3)
CSMA/CA	Contention-based + collision avoidance	Wireless LAN (IEEE 802.11)
TDMA	Scheduled (Time Division)	Cellular networks
Token Ring	Controlled (token passing)	Legacy IBM Token Ring

CSMA/CD (Wired Ethernet)

- Carrier Sense: Device listens before transmitting.
- Multiple Access: Multiple devices share the medium.
- Collision Detection: Detects collision during transmission.
- After collision: Jam signal sent, exponential back-off applied, retransmit.
- Used in half-duplex Ethernet (legacy). Modern switches use full-duplex (no CSMA/CD needed).

CSMA/CA (Wireless LAN)

- Collision cannot be detected in wireless (hidden node problem).
- Collision Avoidance: Device waits random back-off time before transmitting.
- Uses ACK frames to confirm successful reception.
- Optional: RTS/CTS (Request to Send / Clear to Send) to reserve medium.

2.5 Wired LANs – Ethernet (IEEE 802.3)

Ethernet is the dominant wired LAN technology. The Ethernet frame format is:

Field	Size	Description
Preamble	7 bytes	Synchronization pattern (10101010...)
SFD (Start Frame Delimiter)	1 byte	Marks start of frame (10101011)
Destination MAC	6 bytes	Recipient's MAC address
Source MAC	6 bytes	Sender's MAC address
Type/Length	2 bytes	Protocol type (e.g. 0x0800=IPv4) or frame length
Data	46–1500 bytes	Payload (padded if < 46 bytes)
CRC/FCS	4 bytes	Error detection

Ethernet Standard	Speed	Cable
10BASE-T (IEEE 802.3i)	10 Mbps	Cat 3 UTP
100BASE-TX (IEEE 802.3u) Fast Ethernet	100 Mbps	Cat 5 UTP
1000BASE-T (IEEE 802.3ab) Gigabit Ethernet	1 Gbps	Cat 5e/6 UTP
10GBASE-T (IEEE 802.3an)	10 Gbps	Cat 6a UTP

2.6 Wireless LANs (IEEE 802.11 – Wi-Fi)

IEEE 802.11 defines the standard for wireless LANs (Wi-Fi). It operates in the 2.4 GHz and 5 GHz bands.

Standard	Frequency	Max Speed	Notes
802.11b	2.4 GHz	11 Mbps	Legacy Wi-Fi
802.11g	2.4 GHz	54 Mbps	Backward compatible with b
802.11n (Wi-Fi 4)	2.4/5 GHz	600 Mbps	MIMO antennas
802.11ac (Wi-Fi 5)	5 GHz	3.5 Gbps	MU-MIMO, wider channels
802.11ax (Wi-Fi 6)	2.4/5/6 GHz	9.6 Gbps	OFDMA, better in dense environments

Bluetooth (IEEE 802.15.1)

- Short-range wireless for Personal Area Networks (PANs).
- Frequency: 2.4 GHz ISM band. Range: ~10 meters (Class 2).
- Uses Frequency Hopping Spread Spectrum (FHSS) to avoid interference.
- Piconet: up to 8 devices (1 master + 7 slaves).
- Applications: wireless headsets, keyboards, mice, file transfer.

2.7 Connecting Devices

Device	OSI Layer	Function
Repeater / Hub	Layer 1 (Physical)	Regenerates and broadcasts signals; no intelligence
Bridge	Layer 2 (Data Link)	Filters frames using MAC table; connects two LAN segments
Switch	Layer 2 (Data Link)	Multi-port bridge; creates separate collision domains per port
Router	Layer 3 (Network)	Routes packets between different networks using IP addresses
Gateway	All Layers	Protocol conversion between different architectures

COMPUTER NETWORKS

STUDY MATERIAL

UNIT III: NETWORK LAYER

UNIT III

NETWORK LAYER

3.1 Network Layer Overview

The **Network Layer (Layer 3)** is responsible for **logical addressing** and **routing** of packets from source to destination across multiple networks (internetworking). Key protocols: IP, ICMP, ARP, RARP, DHCP.

- Logical addressing: uses IP addresses (not hardware MAC addresses).
- Routing: selects best path through the network.
- Fragmentation: splits large packets to fit MTU of underlying networks.
- Packet forwarding: examines destination IP and forwards accordingly.

3.2 IPv4 Addressing

IPv4 uses 32-bit addresses written in dotted decimal notation (e.g., 192.168.1.10). Originally divided into classful categories:

Class	Leading Bits	Range	Default Subnet Mask	Use
A	0	1.0.0.0 – 126.255.255.255	255.0.0.0 (/8)	Large organisations
B	10	128.0.0.0 – 191.255.255.255	255.255.0.0 (/16)	Medium organisations
C	110	192.0.0.0 – 223.255.255.255	255.255.255.0 (/24)	Small organisations
D	1110	224.0.0.0 – 239.255.255.255	N/A	Multicast
E	1111	240.0.0.0 – 255.255.255.255	N/A	Reserved/Research

Special IPv4 Addresses

- 127.0.0.1 – Loopback address (localhost).
- 0.0.0.0 – 'This host on this network'.
- 255.255.255.255 – Limited broadcast.
- 169.254.x.x – APIPA (Automatic Private IP Addressing).
- 10.x.x.x, 172.16–31.x.x, 192.168.x.x – Private (RFC 1918) addresses.

3.3 IP Protocol (IPv4 Datagram)

The **IPv4 datagram** header is minimum 20 bytes. Key fields:

Field	Size (bits)	Purpose
Version	4	IP version (4 for IPv4)
IHL (Header Length)	4	Length of header in 32-bit words
Type of Service (DSCP)	8	QoS / differentiated services
Total Length	16	Total datagram length in bytes
Identification	16	Fragment identification number
Flags	3	DF (Don't Fragment), MF (More Fragments)
Fragment Offset	13	Position of fragment in original datagram
TTL (Time to Live)	8	Max hops; decremented by each router
Protocol	8	Upper-layer protocol (6=TCP, 17=UDP, 1=ICMP)
Header Checksum	16	Error detection for header only
Source IP	32	Sender's IPv4 address
Destination IP	32	Recipient's IPv4 address

3.4 ICMP (Internet Control Message Protocol)

ICMPv4 is used by routers and hosts to send error messages and operational information about IP packet processing. It is encapsulated within IP datagrams.

ICMP Message Type	Code	Use
Echo Request / Reply	Type 8/0	Ping – test reachability
Destination Unreachable	Type 3	Host/network/port unreachable
Time Exceeded	Type 11	TTL expired (used by traceroute)

Redirect	Type 5	Inform host of better route
Source Quench	Type 4	Request sender to slow down (deprecated)

3.5 ARP, RARP, and DHCP

ARP (Address Resolution Protocol)

ARP resolves an IPv4 address to a MAC address. A host broadcasts an ARP Request; the target replies with its MAC address. Results are cached in the ARP table.

RARP (Reverse ARP)

RARP works in the opposite direction – a diskless machine broadcasts its MAC address to obtain an IP address. Largely replaced by DHCP.

DHCP (Dynamic Host Configuration Protocol)

DHCP automatically configures IP settings for hosts. The four-step DORA process:

- Discover – Client broadcasts a DHCPDISCOVER message.
- Offer – DHCP server responds with an IP address offer (DHCPOFFER).
- Request – Client accepts the offer (DHCPREQUEST broadcast).
- Acknowledge – Server confirms assignment (DHCPACK).

3.6 Unicast Routing Protocols

Distance Vector Routing – RIP

RIP (Routing Information Protocol) is a distance-vector protocol. Each router shares its entire routing table with direct neighbors periodically (every 30 seconds). Metric: hop count (max 15; 16 = infinity/unreachable).

Link-State Routing – OSPF

OSPF (Open Shortest Path First) is a link-state protocol. Each router floods Link-State Advertisements (LSAs) to all routers. Every router builds a complete topology map and uses Dijkstra's algorithm to compute shortest paths.

Feature	RIP	OSPF
Algorithm	Bellman-Ford (Distance Vector)	Dijkstra (Link State)
Metric	Hop count (max 15)	Cost (based on bandwidth)
Convergence	Slow	Fast
Scalability	Small networks	Large enterprise networks
Updates	Periodic (30 sec) full table	Triggered, incremental LSAs
Standard	RFC 1058 / 2453	RFC 2328

3.7 IPv6

IPv6 uses 128-bit addresses (written as 8 groups of 4 hex digits, e.g., **2001:0db8:85a3::8a2e:0370:7334**). It was developed to solve IPv4 address exhaustion.

Feature	IPv4	IPv6
Address Size	32 bits (4 bytes)	128 bits (16 bytes)
Address Space	~4.3 billion	~3.4 × 10^38
Header Size	20–60 bytes (variable)	40 bytes (fixed)
Fragmentation	Routers and hosts	Source host only
Checksum	Yes (header)	No (moved to transport)
IPsec	Optional	Mandatory
Auto-configuration	DHCP required	SLAAC built-in
Broadcast	Yes	No (replaced by multicast/anycast)

COMPUTER NETWORKS

STUDY MATERIAL

UNIT IV: TRANSPORT LAYER

UNIT IV

TRANSPORT LAYER

4.1 Transport Layer Overview

The **Transport Layer (Layer 4)** provides **end-to-end communication** between application processes running on different hosts. It handles multiplexing, error recovery, flow control, and (for TCP) reliable ordered delivery.

Port Numbers

Port numbers (16-bit) identify application processes. Combined with an IP address, they form a **socket** (e.g., 192.168.1.1:80).

Port Range	Category	Examples
0 – 1023	Well-Known Ports	80 HTTP, 443 HTTPS, 21 FTP, 22 SSH, 25 SMTP, 53 DNS
1024 – 49151	Registered Ports	3306 MySQL, 8080 HTTP-alt, 27017 MongoDB
49152 – 65535	Dynamic/Ephemeral	Assigned temporarily by OS for client connections

4.2 UDP (User Datagram Protocol)

UDP is a **connectionless, unreliable** transport protocol. It adds minimal overhead to IP for faster, low-latency transmission.

UDP Segment Format

Field	Size	Purpose
Source Port	16 bits	Sender's port number
Destination Port	16 bits	Receiver's port number
Length	16 bits	Total length of UDP segment (header + data)

Checksum	16 bits	Error detection (optional in IPv4, mandatory in IPv6)
Data	Variable	Application payload

When to Use UDP

- Real-time applications: video streaming, VoIP, online gaming.
- DNS queries – fast single request/response.
- DHCP – broadcast-based discovery.
- SNMP – simple network management.
- Applications that handle their own error recovery.

4.3 TCP (Transmission Control Protocol)

TCP is a **connection-oriented, reliable** protocol providing ordered delivery, error recovery, flow control, and congestion control.

TCP Segment Format

Field	Size	Purpose
Source Port	16 bits	Sender's port
Destination Port	16 bits	Receiver's port
Sequence Number	32 bits	Position of first data byte in stream
Acknowledgment Number	32 bits	Next expected byte from sender
Header Length (HLEN)	4 bits	Header length in 32-bit words
Control Flags	6 bits	SYN, ACK, FIN, RST, PSH, URG
Window Size	16 bits	Receiver's buffer size (flow control)
Checksum	16 bits	Error detection
Urgent Pointer	16 bits	Points to urgent data if URG flag set
Options	Variable	MSS, window scaling, timestamps

TCP Three-Way Handshake (Connection Establishment)

- Step 1 – SYN: Client sends SYN segment (seq=x) to server. Client → SYN_SENT state.
- Step 2 – SYN-ACK: Server replies with SYN+ACK (seq=y, ack=x+1). Server → SYN_RCVD state.
- Step 3 – ACK: Client sends ACK (ack=y+1). Both enter ESTABLISHED state.

- Data transfer begins after handshake completes.

TCP Connection Termination (Four-Way)

- Step 1 – FIN: Active closer sends FIN.
- Step 2 – ACK: Passive closer acknowledges.
- Step 3 – FIN: Passive closer sends its own FIN.
- Step 4 – ACK: Active closer acknowledges. Connection closed after TIME_WAIT.

4.4 Flow Control

Flow control prevents a fast sender from overwhelming a slow receiver. TCP uses the **sliding window mechanism**: the receiver advertises its buffer size (rwnd) in the Window Size field. The sender cannot exceed this window.

- Receiver sends rwnd (receiver window) in ACK segments.
- Sender limits unacknowledged data to min(cwnd, rwnd).
- Zero-window probe: sender probes when window = 0.
- Silly window syndrome: avoid by Nagle's algorithm / Clark's solution.

4.5 Congestion Control

TCP **congestion control** prevents overloading the network. Uses a congestion window (cwnd) maintained by the sender.

Phase	Behaviour	Trigger
Slow Start	cwnd doubles each RTT (exponential growth)	Initial connection or after timeout
Congestion Avoidance	cwnd increases by 1 MSS per RTT (linear growth)	When cwnd ≥ ssthresh
Fast Retransmit	Retransmit lost segment immediately	3 duplicate ACKs received
Fast Recovery	ssthresh = cwnd/2; cwnd = ssthresh + 3	After fast retransmit

4.6 SCTP (Stream Control Transmission Protocol)

SCTP combines features of both TCP and UDP. It provides reliable, ordered delivery while supporting multiple streams within a single association.

Feature	TCP	UDP	SCTP
Connection	Connection-oriented	Connectionless	Association-oriented
Reliability	Yes	No	Yes

Ordering	Single stream	No ordering	Multiple independent streams
Multi-homing	No	No	Yes (multiple IP addresses per endpoint)
Head-of-line blocking	Yes	No	No (streams are independent)
4-Way Handshake	3-way	None	4-way (INIT, INIT-ACK, COOKIE-ECHO, COOKIE-ACK)

SCTP applications: Signaling (SS7 over IP), VoIP signaling, telecom protocols.

COMPUTER NETWORKS

STUDY MATERIAL

UNIT V: APPLICATION LAYER

UNIT V

APPLICATION LAYER

5.1 WWW and HTTP

The **World Wide Web (WWW)** is a system of interlinked hypertext documents accessed via the Internet. It uses **URLs** (Uniform Resource Locators) to identify resources and **HTTP** to transfer them.

HTTP (HyperText Transfer Protocol)

HTTP is a stateless, application-layer request-response protocol. Default port: **80**. HTTPS (HTTP over TLS) uses port **443**.

HTTP Method	Purpose	Request Body?
GET	Retrieve a resource	No
POST	Submit data to server	Yes
PUT	Replace resource at URL	Yes
DELETE	Remove a resource	No
HEAD	GET but returns headers only	No
PATCH	Partial update of resource	Yes

HTTP Response Status Codes

Code Range	Category	Examples
1xx	Informational	100 Continue
2xx	Success	200 OK, 201 Created
3xx	Redirection	301 Moved Permanently, 304 Not Modified
4xx	Client Error	400 Bad Request, 401 Unauthorized, 404 Not Found

5xx	Server Error	500 Internal Server Error, 503 Service Unavailable

Persistent vs Non-Persistent HTTP

Type	Behaviour	HTTP Version
Non-Persistent	New TCP connection per object	HTTP/1.0
Persistent	Multiple objects over same TCP connection	HTTP/1.1+
HTTP/2	Multiplexed streams, header compression, server push	HTTP/2
HTTP/3	QUIC (UDP-based), faster connection setup	HTTP/3

5.2 FTP (File Transfer Protocol)

FTP transfers files between a client and server using **two separate TCP connections**: a **Control Connection** (port 21) for commands and a **Data Connection** (port 20 or dynamic) for actual file transfer.

Mode	Data Connection	How
Active Mode	Server initiates data connection	Server connects from port 20 to client
Passive Mode	Client initiates data connection	Client connects to random high port on server

- Common FTP commands: USER, PASS, LIST, RETR (retrieve), STOR (store), QUIT.
- FTP is insecure (plain text). Alternatives: FTPS (FTP over TLS), SFTP (SSH File Transfer).
- Anonymous FTP: allows public access without credentials.

5.3 Email (Electronic Mail)

Email system uses three main protocols for sending and receiving messages:

Protocol	Full Name	Port	Role
SMTP	Simple Mail Transfer Protocol	25 (587 for secure)	Send mail from client → server, server → server
POP3	Post Office Protocol v3	110 (995 TLS)	Download and optionally delete from server
IMAP	Internet Message Access Protocol	143 (993 TLS)	Access/manage mail on server (keeps mail on server)

Email Message Format (RFC 5322)

- Header: From, To, CC, BCC, Subject, Date, Message-ID.
- Body: Plain text or HTML.
- MIME (Multipurpose Internet Mail Extensions): allows attachments, HTML, non-ASCII characters.
- SMTP uses ASCII only; MIME encodes binary content as Base64 or quoted-printable.

POP3 vs IMAP

Feature	POP3	IMAP
Storage	Downloaded to client; deleted from server	Stored on server
Multiple devices	Poor (one device)	Excellent (sync across devices)
Offline access	Yes (after download)	Requires connection for new mail
Folder management	No server-side folders	Full server-side folder management

5.4 Telnet and SSH

Telnet

Telnet provides remote command-line access to another computer over a TCP connection (port 23). **Major weakness:** all data including passwords is transmitted in plain text — highly insecure and deprecated.

SSH (Secure Shell)

SSH (port 22) is the secure replacement for Telnet. It provides encrypted remote login, command execution, file transfer (SCP, SFTP), and port forwarding.

Feature	Telnet	SSH
Security	No encryption (plain text)	Fully encrypted
Authentication	Password (plain text)	Password + Public Key
Port	23	22
Status	Deprecated (insecure)	Current standard for remote access
File Transfer	No	Yes (SCP, SFTP)

5.5 DNS (Domain Name System)

DNS is a distributed hierarchical database that maps **domain names** to **IP addresses** (and vice versa). Without DNS, users would need to remember IP addresses.

DNS Hierarchy

- Root Servers (.) – Top of hierarchy; 13 root server clusters worldwide.

- Top-Level Domain (TLD) servers – .com, .org, .net, .edu, .in, etc.
- Authoritative Name Servers – Hold actual DNS records for a domain.
- Local DNS Resolver – ISP or organisation resolver; caches results.

DNS Resolution Process

- 1. Client queries Local Resolver for www.example.com.
- 2. Local Resolver checks cache; if miss, queries Root Server.
- 3. Root Server directs to .com TLD server.
- 4. TLD server directs to authoritative server for example.com.
- 5. Authoritative server returns IP address.
- 6. Local Resolver caches and returns IP to client.

Common DNS Record Types

Record	Purpose	Example
A	IPv4 address	www.google.com → 142.250.193.36
AAAA	IPv6 address	www.google.com → 2607:f8b0:...
MX	Mail server for domain	example.com → mail.example.com
CNAME	Alias for another name	www → example.com
NS	Authoritative name server	example.com → ns1.example.com
PTR	Reverse DNS (IP → name)	142.250.193.36 → www.google.com
TXT	Text information (SPF, DKIM)	v=spf1 include:example.com ~all

5.6 SNMP (Simple Network Management Protocol)

SNMP is used to **monitor and manage** network devices (routers, switches, servers, printers) from a central Network Management System (NMS).

SNMP Component	Role
Manager (NMS)	Runs on network management station; polls and configures agents
Agent	Software on managed device; responds to queries and sends traps
MIB (Management Information Base)	Hierarchical database of manageable objects on each device

OID (Object Identifier)	Unique dotted number identifying each MIB object
Community String	Password-like string for access control (SNMPv1/v2c)

SNMP Operations

Operation	Direction	Purpose
GetRequest	Manager → Agent	Retrieve value of a specific MIB object
GetNextRequest	Manager → Agent	Retrieve next object in MIB tree
GetBulkRequest	Manager → Agent	Retrieve large block of data (SNMPv2+)
SetRequest	Manager → Agent	Change value of a MIB object
GetResponse	Agent → Manager	Reply to Get/Set requests
Trap	Agent → Manager	Unsolicited alert from agent (event notification)

SNMP Version	Security	Notes
SNMPv1	Community strings (plain text)	Original, insecure
SNMPv2c	Community strings (plain text)	Improved operations, still insecure
SNMPv3	Authentication + Encryption	Current standard; USM for security