Page No.
Date

How Internet Works

1) Device Connection

Phone / Laptop —(Wifi / Mobile Data)→ ISP (Internet Service Provider)

2) DNS Resolution (Domain Name System)

Name → IP Address (public and private)

www.google.com → 142.250.182.46 (public IP)

3) Protocols

Browser —(TCP (3-step handshake) / HTTPS)→ Google server

4) Routers

Decides which route to use for requests / response

5) HTTP Request & Server Response

Browser —HTTP→ Google Server

Google Server —HTTP (HTML, CSS, JS)→ Browser

Load Balancer decides which server to use

6) Rendering Page

Renders HTML → CSS → JS → Images / videos

Page No.
Date

Network -

It is a collection of interconnected devices, like computers, servers, or IOT devices, that communicate with each other to share resources and data.

Communication happens using TCP/IP protocols

LAN (Local Area Network)
- Small geographical area (office, home), high speed, low latency

MAN (Metropolitan Area Network)
- covers a city or campus, larger than LAN but smaller than WAN

WAN (Wide Area Network)
- Spans large areas (countries, continents), Internet is biggest WAN.

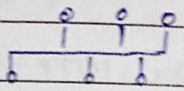
- Hub → Physical layer → device that broadcasts data to all devices in a network
- Switch → Data Link layer → sends data only to the intended device using MAC addresses (Media Access Control Address) → unique, hardware base identifier
- Router → Network layer → connects different networks and routes data based on IP addresses

Page No.
Date

Network Topology -

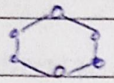
Arrangement of nodes and links in a network.

Bus



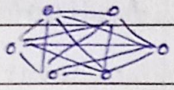
single backbone cable
Simple but prone to failure

Ring



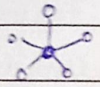
devices connected in loop
data travels in one direction
failure disrupt network

Mesh



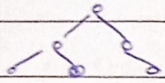
every device connects to every other
reliable, costly

Star



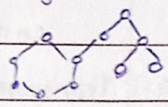
central hub/switch
easy to manage
central point critical

Tree



various secondary hubs connected to central hub
central hub fails entire system fails

Hybrid



combination of topologies
scalable for large networks

Node - any device in a network (computer, router, switch, etc)

Link - communication medium between nodes (wired cable, fiber, wireless)

Page No.
Date

OSI Model (Open Systems Interconnection) —
Conceptual framework that standarizes how data is transmitted across a network.

1. Application Layer
   - closest to user, provides services like HTTP, FTP, SMTP
2. Presentation Layer
   - ensures data is in a usable format (encryption, compression, translation)
3. Session Layer
   - Manages sessions, establishes, maintains, and terminates connections.
4. Transport Layer
   - ensures reliable data delivery, error checking, segmentation (eg. TCP / UDP)
5. Network Layer
   - responsible for logical addressing and routing (IP addresses, routers)
6. Data Link Layer
   - handles MAC addresses, error detection, and frames (switches, ethernet)
7. Physical Layer
   - actual hardware transmission : cables, signals, bits over the medium.

Developed by ISO (International Standards Organization)
Just a conceptual model, doesn't specify protocols.

Page No.
Date

TCP / IP Protocol Suite –

It defines how data should be packaged, addressed, transmitted, routed, and received across networks.

TCP (Transmission Control Protocol) → reliable communication

IP (Internet Protocol) → addressing and routing

1. Application Layer
   - includes protocols like HTTP, FTP, SMTP, DNS (equivalent to Application + Presentation + session of OSI)
2. Transport Layer
   - provides end to end communication, reliability (TCP/UDP)
3. Internet Layer
   - handles logical addressing and routing (IP, ICMP, ARP)
4. Network Access Layer
   - deals with physical transmission (ethernet, wifi, hardware)

Developed by DoD (Department of Defense, USA).
A practical model, defines actual protocols (TCP, IP, HTTP, etc).

Data Transmission –

It is a process of sending digital or analog data from one device to another through a medium.

→ Simplex : one way communication (TV broadcast)

→ Half Duplex : both directions, but one at a time (walkie talkie)

→ Full Duplex : both directions simultaneously (Telephone)

It can be synchronous (timed) or asynchronous (no fixed timing)

Page No.
Date

Bandwidth -
It is maximum rate at which data can be transmitted over a communication channel, usually measured in bits per second (bps).
Higher bandwidth means more data transfer capacity and faster communication.

Transmission Media —
It refers to physical path or channel through which data is transmitted.
Guided (Wired)
- Data travels through physical medium
  - Twisted Pair Cable (ethernet)
  - Coaxial Cable (TV cable)
  - Optical Fiber (long distances)

Unguided (Wireless)
- Data is transmitted through air using electromagnetic waves
  - Radio waves (WiFi, FM, Bluetooth)
  - Microwaves (satellite, mobile signal)
  - Infrared (remote controls)

Wireless is flexible, but prone to security risk

Bandwidth → maximum capacity
Throughput → actual data transmitted.

Page No.
Date

Error Detection = finding errors
It ensures that errors introduced during transmission are caught.
Techniques - Parity bits, Checksums, CRC (Cyclic Redundancy Check)

Error Correction = fixing errors
It detects and automatically fixes errors,
Techniques - Hamming Code, Forward Error Correction

Data Link Protocols -
It control how data is packaged into frames and transmitted reliably between nodes.
- Stop and Wait ARQ
- Go back N ARQ
- Selective Repeat ARQ

It handles flow control, error detection and retransmission

Multiple Access Protocols -
It define how multiple devices, share the same communication channel.
- Random Access
  ALOHA, slotted ALOHA, CSMA/CD (Ethernet)
- Controlled Access
  Polling, Reservation
- Channelization
  FDMA, TDMA, CDMA

They prevent collisions and decide "who gets to talk when" on a shared medium.

MAC Address —
Media Access Control address is a unique hardware address assigned to a network interface card (NIC).
It's 48 bits, written in hexadecimal (00:1A:2B:3C:4D:5E)
It works at the Data Link Layer and identifies devices within the same local network.
IP = logical, can change
MAC = physical, fixed
ARP → maps IP addresses to MAC addresses

Channel Allocation Problem —
It is about dividing the communication medium so multiple users can transmit without interfering.
The problem is balancing efficiency, fairness, and collision avoidance.
Solutions include: static allocation (FDMA/TDMA)
dynamic allocation (ethernet)

Data Link Layer Switching —
It uses switches that forward frames based on MAC addresses. It's faster than routing because it doesn't deal with IPs.
Switches build a MAC address table to decide where

to forward frames, reducing unnecessary traffic compared to hubs.

Ethernet LANs —

It is most widely used LAN technology. It follows IEEE 802.3 standard, uses CSMA/CD for medium access, and supports high data rates (from 10Mbps to 400 Gbps).

It is defined in Data Link + Physical layer.

Routing Algorithms —

It decides the best path for data packets.

- Distance Vector
  Uses hop count, simpler but slower convergence.
  "tell me what you know"
- Link state
  Each router builds a full map of the network, more complex but efficient
  "tell me what you see"
- Hybrid
  Mix of both

Congestion Control Algorithms —

They prevent network overload by controlling traffic flows

- TCP Tahoe, TCP Reno — use slow start and congestion avoidance.
- Leaky Bucket / Token Bucket — traffic shaping at sender

Page No.
Date

It keeps the network stable and fair by adjusting sending rates.

IP Address : A logical identifier for a device in a network
IPv4 = 32 bit , IPv6 = 128 bit

Subnetting : Dividing a large network into smaller, manageable networks using a subnet mask.
It improves efficiency and security.
192.168.1.0/24 → 256 addresses, split into subnets.

IPv4 : 32 bit , ~4.3 billion addresses, written as dotted decimal

IPv6 : 128 bit, virtually unlimited addresses, written in hexadecimal.
It adds features like auto configuration, better security (IPSec mandatory), and simpler headers.

ICMP (Internet Control Messaging Protocol) — used for error reporting and diagnostics.
Examples : Ping (echo request/reply), Traceroute
Works at the Network Layer.

Page No.
Date

Fragmentation –
If a packet is too large for a network's MTU (Maximum Transmission Unit), it's split into smaller fragments.
Each fragment has headers for reassembly at the destination.
IPv4 supports fragmentation, IPv6 avoids it.

Tunneling –
Encapsulation of one protocol's packet inside another.
Example : IPv6 traffic sent over an IPv4 network, or VPNs where private packets are wrapped inside public internet packets.

Subnet –
It is a smaller portion of a network created through subnetting.
Example : 192.168.1.0/24 ⟶ split into 192.168.1.0/26 and 192.168.1.64/26

Router : forwards packets between different networks using IP addresses. Works at Layer 3 Network.

Gateway : A broader term – it connects network using different protocols. Every gateway is a router, but not every router is a gateway.

Page No.
Date

Count to Infinity Problem –
Happens in distance vector routing (eg. RIP). When a link fails, incorrect routing updates cause routers to keep increasing hop counts indefinitely.
Solutions : Split Horizon
Route Poisoning
Hold down times

Elements of Transport Protocol –

- Addressing (Port Numbers)
  Identify which process/app gets the data
- Multiplexing / Demultiplexing
  Combine multiple streams → single channel, then separate at receiver.
- Segmentation & Reassembly
  Break data into segments, reassemble at destination.
- Connection Control
  Establish, maintain, terminate connections.
- Flow Control
  Prevent sender from overwhelming receiver
- Error Control
  Detect and recover lost/corrupted segments.

Transport protocol ensures reliable, ordered delivery between processes, not just machines.

Page No.
Date

Internet Transport Layer Protocol —

→ TCP (Transmission Control Protocol)
- Connection oriented
- Reliable (acknowledgements, retransmission)
- Ordered delivery
- Flow + congestion control
- Used in HTTP, SMTP, FTP

→ UDP (User Datagram Protocol)
- Connectionless
- Unreliable (no ack, no retransmission)
- Faster, lightweight
- Used in DNS, VoIP, video streaming

Flow = receiver side (prevent buffer overflow)
Congestion = network side (prevent overload)
Socket = endpoint of communication between two devices

State Transition Diagram —
This represents TCP connection states during its lifecycle.
Key states: LISTEN, SYN-SENT, SYN-RECEIVED, ESTABLISHED, FIN-WAIT, CLOSE-WAIT, TIME-WAIT, CLOSED.

3-Way Handshaking —
TCP establishes a connection using 3 steps:
1) SYN: client → server (request to start connection)
2) SYN + ACK: server → client (ack + request back)
3) ACK: client → server (final communication).

Page No.
Date

Congestion Control Mechanism –

- Slow start : gradually increase sending rate to probe capacity
- Congestion Avoidance : use algorithms like AIMD (additive increase, multiplicative decrease)
- Fast Retrasmit & Fast Recovery : quickly detect and recover from packet loss.

TCP congestion control balances efficiency and fairness by probing available bandwidth and backing off when congestion is detected.

Session Layer –

Manages sessions (conversation) between applications.
Responsible for establishing, maintaining, synchronizing and terminating communication sessions.
Ex : Login sessions, video conferencing, keep track of multiple browser tabs.

Presentation Layer –

Deals with the syntax and semantics of data.
Ensures data is in a usable, understandle format.
Functions : Translation, Encryption / Decryption, Compression / Decompression.
EX : JPEG, MP3, SSL/TLS encryption.

Page No.
Date

DNS (Domain Name System) –
Translates human readable domain names (like google.com) into IP addresses. Works like the internet's "phonebook".
Ex: Typing www.openai.com → DNS resolves it to its IP.

WWW (World Wide Web) –
A system of interlinked hypertext documents accessible via the internet using browsers. Runs mainly on HTTP / HTTPS.
Ex: Browsing Wikipedia is using the www.

HTTP (Hypertext Transfer Protocol) –
Protocol for transfering web pages on the web. Stateless, text based and works on port 80 (HTTPS→443 with encryption).
Ex: Clicking a link → browser sends an HTTP GET request

FTP (File Transfer Protocol) –
Used to transfer files between client and server. Uses port 20/21 and supports authentication.
Ex: uploading a website to a server.

SMTP (Simple Mail Transfer Protocol) –
Used for sending emails between mail servers. Works on port 25 (or 587 with authentication).
Ex: gmail sending an email to outlook users SMTP.
POP3/IMAP → used for receiving mail

Page No.
Date

DHCP (Dynamic Host Configuration Protocol) —
Automatically assigns IP addresses and network settings to devices. Saves manual configuration effort.
Ex: when you connect your phone to wifi, DHCP gives it an IP.

HTTPS → HTTP + SSL/TLS encryption
DNS → resolves names to IPs
DHCP → assigns IPs to hosts.

Network Security —
It is the practice of protecting data, devices, and services from unauthorized access, misuse, or attacks. It ensures confidentiality, integrity, and availability (CIA triad).

Cryptography —
It is the science of securing communication by converting data into unreadable form (encryption) and back (decryption).
Goal: Protect data from envesdropping or tampering

CSMA/CD : collision detection → Ethernet
CSMA/CA : collision avoidance → WiFi

Page No.
Date

Types of Encryption -

- RSA (Rivest Shamir Adleman)
  Asymmetric encryption (public & private keys). Used in SSL/TLS
- DES (Data Encryption Standard)
  Old symmetric key algorithm (56 bit), now outdated.
- AES (Advanced Encryption Standard)
  Modern symmetric encryption, fast and secure (128/192/256 - bit)
- Diffie Hellman
  Key exchange algorithm, allows two parties to securely share keys over insecure channels

Symmetric = same key
Asymmetric = public / private key

Hash Functions —
It takes input data and produces a fixed size output (hash value).
- One way, irreversible
- Used for data integrity and password storage.

Digital Signatures
It use hashing + asymmetric encryption to prove authenticity and integrity.
- Sender signs data with private key
- Receiver verifies with public key.

Page No.
Date

Network Security Protocols —
SSL / TLS : secure web traffic (HTTPS)
IPSec : secure IP packets (VPNs)
Kerberos : authentication protocols.
PGP : encrypts emails.

Virtual Private Networks (VPNs) —
It creates a secure, encrypted tunnel between a device and a private network over the public internet.

Network Attacks —
DoS / DDoS : overwhelm servers with traffic
Man in the Middle : intercept communications
Phishing : trick users into giving credentials
SQL Injection : insert malicious code into databases
Spoofing : faking identity (IP / MAC)

Ping Command —
It is a simple network utility used to test the reachability of a host over an IP network.
It sends ICMP Echo Request packets to the target host and waits for ICMP Echo Reply.
It is used to :
- Check if a host / server is reachable
- Measure round trip time (RTT) between source and

destination.

- Diagnose network issues like packet loss or high latency.

Ex: ping google.com

shows - no. of packets sent/received
packet loss percentage
average round trip time

Delays -

When data travels through a network, it experiences different kinds of delays.

Total delays = sum of all these.

1) Processing Delays

Time taken by routers/switches to process packet headers. Usually a few microseconds.

2) Queuing Delay

Time a packet waits in a router's/switch's queue before being transmitted. Depends on congestion in the network.

3) Transmission Delay

Time taken to push all bits of packet onto the link.

$$\text{Transmission Delay} = \frac{\text{Packet Size (bits)}}{\text{Link Bandwidth (bps)}}$$

4) Propagation Delay

Time taken for a signal to travel through the physical medium.

$$\text{Propagation Delay} = \frac{\text{Distance}}{\text{Propagation Speed}}$$

Page No.
Date

5) End to End Delay
Total delay from source to destination.
$D_{end\text{-}to\text{-}end} = D_{proc} + D_{queue} + D_{trans} + D_{prop}$

Ping → checks connectivity
Traceroute → shows path taken (all hops)

If two devices are in the same network but can't communicate, what could be wrong?
→ Wrong subnet mask, faulty cable, switch/port issue, ARP failure.

API (Application Programming Interface)
A set of rules and protocols that allows different software applications to communicate.
Acts as a bridge between client and server or between two software components.

SOAP (Simple Object Access Protocol)
- Protocol based API
- Uses XML for data exchange
- Strict, standardized, heavy (lots of overhead)
- Better suited for enterprise level secure transactions (eg. banking)

Page No.
Date

REST (Representation State Transfer)

- Architectural style, not a protocol. [Stateless]
- Works over HTTP using standard methods: GET, POST, PUT, DELETE
- Data formats supported: JSON, XML, etc
- Lightweight, faster, widely used in modern web services.

WebSocket

- Protocol that provides full duplex (two way) communication between client and server over a single TCP connection. [stateful]
- Unlike REST (request-response), websocket keeps the connection open for real time updates
- Used in chat apps, live notifications, gaming, stock market dashboard.

Web API –

General term for any API accessible over the web (HTTP / HTTPs). Both REST and SOAP can be web APIs

REST API –

A specific implementation of REST principles using HTTP methods.

Ex: GET /users → fetch users, POST /users → Add user

Page No.
Date

RESTful API –

An API that strictly follows REST principles (stateless, resource based URLs, uniform interfaces) but implies full compliance.