Internet and Networking Overview

1 Introduction to the Internet

The Internet is a global network connecting billions of devices (e.g., computers, smartphones, servers) to share information using standardized protocols. It serves as a platform for communication, education, entertainment, and commerce, enabling activities like web browsing, email, and streaming.

2 What is a Network?

A network connects two or more devices (e.g., computers, smartphones, routers) to share resources and data via wired (e.g., Ethernet) or wireless (e.g., Wi-Fi) technologies. Networks enable file sharing, Internet access, and device communication.

2.1 Hosts

Hosts are devices with unique IP addresses capable of sending/receiving data over a network. Examples include computers, smartphones, servers, and tablets.

2.2 Networking Devices

- Switch: Connects devices within a local network (LAN), forwarding data to the intended recipient.
- Router: Connects different networks, routing data between them, often linking a LAN to the Internet.

Switches and routers form the backbone of the Internet, ensuring efficient data flow.

3 Communication Links

Communication links are physical or wireless media connecting routers, enabling data packet transmission. Types include:

- Fiber-optic cables: High-speed, long-distance.
- Copper wires: Used in DSL or Ethernet.

- Radio waves: For Wi-Fi and mobile networks.
- Satellite links: For global coverage in remote areas.

4 Bandwidth and Data Rate

Bandwidth is the maximum data transmission capacity of a network link, measured in bits per second (bps, Kbps, Mbps, Gbps). Data rate is the actual amount of data transmitted per second. Higher bandwidth allows faster data rates, improving performance for streaming, downloads, and communication.

5 Network Structure

The Internet is a network of networks, interconnecting millions of smaller networks (e.g., personal, organizational, academic) via standardized protocols. Key components include:

- Access ISPs: Connect end users to the Internet.
- Transit ISPs: Provide backbone connectivity between Access ISPs.
- Tier-1 ISPs: Large networks with global coverage (e.g., AT&T, NTT).
- Content Provider Networks: Private networks for services like Google or Netflix.

6 Network Edge

The network edge is where end devices (hosts) like computers, smartphones, and IoT devices connect to the network. It includes:

- Edge Devices: Smartphones, laptops, routers, IoT devices that generate/consume data.
- Access Network: Connects end devices to the Internet via ISPs.

Edge computing processes data locally to reduce latency and bandwidth usage.

7 Network Core

The network core consists of interconnected routers and high-speed links (e.g., fiber-optic cables) that route data globally. Key functions:

- Routing: Determines the best path for data packets.
- Forwarding: Moves packets from one router to the next.

8 Packet Switching

Data is broken into small units called packets, sent independently across the network, and reassembled at the destination. Key features:

- Store-and-Forward: Routers receive an entire packet before forwarding it.
- Queueing: Packets wait in buffers if arrival rate exceeds link capacity, causing delays or loss.

Packet switching is efficient but can lead to resource contention and congestion when demand exceeds capacity.

8.1 Packet Structure

Packets consist of:

- Payload: Actual data.
- Header: Control information (e.g., source/destination IP addresses, sequence number, checksum).

Segment: A transport-layer unit (e.g., TCP/UDP) containing payload and header (port numbers, sequence number, checksum). Packets include segments plus network-layer headers.

8.2 Maximum Transmission Unit (MTU)

The MTU (e.g., 1500 bytes for Ethernet) is the maximum packet size. Larger data is split into multiple packets.

9 Circuit Switching

In circuit switching, dedicated resources are reserved for a connection (e.g., telephone calls). Types include:

- FDM (Frequency Division Multiplexing): Divides link frequency into bands for simultaneous use.
- TDM (Time Division Multiplexing): Divides time into slots for sequential use.

Unlike packet switching, circuit switching wastes resources if unused but ensures guaranteed performance.

10 Network Protocols

Protocols are rules defining how data is formatted, transmitted, and received. Examples:

- HTTP/HTTPS: Web browsing.

- TCP/IP: Reliable data transmission.
- FTP: File transfers.
- SMTP/IMAP: Email.
- DNS: Domain name to IP address translation.

Protocols ensure interoperability across devices and networks, akin to human communication protocols (e.g., greet, state intent, share information).

10.1 TCP (Transmission Control Protocol)

Defined in RFC 793, TCP is a connection-oriented protocol ensuring reliable data transfer. Key features:

- Three-Way Handshake: SYN, SYN-ACK, ACK to establish a connection.
- Reliable Delivery: Ensures in-order, error-free data via acknowledgments and retransmissions.
- Flow Control: Uses sliding window to match receiver capacity.
- Congestion Control: Adjusts sending rate to avoid network overload (e.g., slow start, congestion avoidance).

10.2 UDP (User Datagram Protocol)

Defined in RFC 768, UDP is a connectionless protocol prioritizing speed over reliability. Features:

- No handshake, flow control, or congestion control.
- Used for real-time applications (e.g., VoIP, gaming, streaming).
- Relies on IP layer for delivery, offering best-effort service.

11 Network Delays

Packets experience four types of delay:

1. Transmission Delay: Time to push packet onto link, $\frac{L}{R}$ (L = packet size in bits, R = link bandwidth in bps).
2. Propagation Delay: Time for a bit to travel, $\frac{d}{s}$ (d = distance, s = propagation speed).
3. Queueing Delay: Time waiting in router buffer, varies with congestion.
4. Nodal Processing Delay: Time for header processing and forwarding decisions (typ-

ically microseconds).

End-to-End Delay: Sum of all delays across n routers:

$$\text{Total Delay} = n \times (\text{Transmission} + \text{Propagation} + \text{Queueing} + \text{Processing})$$

Retransmission Delay: Extra time to resend lost/corrupted packets.

12 Throughput and Goodput

- Throughput: Total data transfer rate (bps), including retransmissions.
- Goodput: Rate of useful data delivered, excluding protocol overhead and retransmissions.

The bottleneck link (slowest link in the path) limits throughput.

13 Network Security

The Internet, originally designed for trusted users, now requires robust security due to malicious actors. Security is implemented across all protocol layers.

13.1 Types of Attacks

- Active Attacks: Modify or disrupt data (e.g., DoS, DDoS, IP spoofing).
- Passive Attacks: Eavesdrop without altering data (e.g., packet sniffing).

13.2 DoS and DDoS Attacks

- DoS (Denial of Service): Overloads a target with traffic to disrupt service.
- DDoS: Uses a botnet for larger-scale attacks.

Protection Methods:

- Traffic filtering, rate limiting, CDNs, firewalls, blackholing.

13.3 Packet Sniffing

A passive attack where attackers intercept packets using tools like Wireshark, capturing unencrypted data (e.g., passwords) on broadcast networks.

13.4 IP Spoofing

An active attack where attackers forge source IP addresses to impersonate trusted devices, used in DoS or man-in-the-middle attacks.

14 Transmission Media

- Guided Media: Copper cables, fiber optics, coaxial cables.
- Unguided Media: Radio waves, microwaves, infrared (e.g., Wi-Fi, Bluetooth, satellite).

Wireless signals face reflection, obstruction, and interference, mitigated by stronger antennas, frequency selection, and error correction.

15 Multihoming

A host/network connects to multiple ISPs for redundancy, load balancing, and improved reliability.

16 Internet Engineering Task Force (IETF)

The IETF develops Internet standards and protocols, publishing RFCs (Request for Comments). Examples:

- RFC 791: Internet Protocol (IP).
- RFC 2616: HTTP/1.1.

The IETF ensures global interoperability through open discussion and consensus.

17 Layered Protocol Stack

The Internet uses a layered architecture (TCP/IP model) to manage complexity:

1. Application Layer: Supports user applications (e.g., HTTP, SMTP).
2. Transport Layer: Ensures process-to-process delivery (TCP/UDP).
3. Network Layer: Routes packets using IP addresses.
4. Link Layer: Handles data transfer between adjacent devices.
5. Physical Layer: Transmits raw bits over media.

Encapsulation: Each layer adds headers to data, removed by the receiving layer during decapsulation.

18 Applications of the Internet

The Internet powers smart systems via the Internet of Things (IoT):

- Smart Utility Management: Monitors water, gas, energy usage.

- Smart Electricity Management: Tracks usage via smart meters/grids.
- Smart Environment Management: Monitors air quality, weather, disasters.