Computer Networks and the Internet

Date	@August 21, 2024
tag	chapter 1 lecture

1.1 What is the Internet?

- The Internet is a public computer network used to discuss computer networks and protocols.
- It can be described as:
    1. **Nuts-and-bolts**: Basic hardware and software components.
    2. **Networking infrastructure**: Provides services to distributed applications.

1.1.1 A Nuts-and-Bolts Description

- The Internet is a network that connects millions of devices worldwide.
- **End systems** (hosts) include:
    - Traditional devices (PCs, servers).
    - Non-traditional devices (laptops, smartphones, TVs, sensors, etc.).
    - Estimated 850 million end systems in 2011, with about 2 billion users globally.
- **Communication Links and Packet Switches**:
    - End systems are connected by communication links (e.g., coaxial cable, copper wire, optical fiber).
    - Data is transmitted in bits/second.

- **Packet switches** (routers and link-layer switches) forward data in **packets**.
- **Routers**: Used in the core network.
- **Link-layer switches**: Used in access networks.
- Packets follow a **route** or **path** through the network.

- **Packet-Switched Networks**:
  - Similar to transportation networks.
  - Data is segmented like cargo in trucks, which travel through a network of highways and roads to their destination.
- **Internet Service Providers (ISPs)**:
  - End systems access the Internet via ISPs (residential, corporate, university ISPs).
  - ISPs offer various access types (broadband, DSL, dial-up).
  - ISPs are interconnected, with lower-tier ISPs connecting through national/international upper-tier ISPs (e.g., AT&T, Sprint).
  - Each ISP network is independently managed and runs the IP protocol.

Protocols and Standards

- The Internet runs on protocols, with **TCP** and **IP** being the most important.
  - **IP protocol**: Defines packet formats between routers and end systems.
  - Collectively called **TCP/IP** protocols.
- **Standards**:
  - Protocols must be standardized for interoperability.
  - Internet standards are developed by the **Internet Engineering Task Force (IETF)**.
  - Standards documents are known as **Requests for Comments (RFCs)**.
  - Over 6,000 RFCs define protocols such as TCP, IP, HTTP, and SMTP.
- **IEEE Standards**:

    - **IEEE 802 LAN/MAN Standards Committee** defines network components like Ethernet and WiFi.

1.1.2 A Services Description

- **Internet Applications**:
    - Examples: Electronic mail, Web surfing, social networks, instant messaging, VoIP, video streaming, distributed games, P2P file sharing, television over the Internet, remote login.
    - Distributed applications involve multiple end systems exchanging data.
- **Applications vs. Packet Switches**:
    - Applications run on end systems, not on packet switches.
    - Packet switches facilitate data exchange but do not handle application data directly.
- **Developing Internet Applications**:
    - Requires programming end systems (e.g., Java, C, Python).
    - Programs on different end systems need to communicate data.
    - End systems use an **Application Programming Interface (API)** to instruct the Internet to deliver data to destination programs.
- **Internet API**:
    - A set of rules for data delivery.
    - Analogy: Like postal service rules for sending a letter (envelope, address, stamp).
- **Internet Services**:
    - Provides multiple services to applications.
    - Developers must choose from these services for their applications.
    - Details on Internet services will be covered in Chapter 2.
- **Further Learning**:

    - The book will explain packet switching, TCP/IP, routers, communication links, distributed applications, and Internet attachment of devices like toasters and weather sensors.

1.1.3 What Is a Protocol?

- **Human Analogy**:
    - **Example 1:** Asking someone for the time:
        - Greeting is essential (e.g., "Hi").
        - Response indicates willingness to communicate.
        - Lack of response or inappropriate responses may end the interaction.
    - **Example 2:** Asking a question in class:
        - Raising a hand to indicate a question.
        - Teacher acknowledges and responds.
- **Network Protocols**:
    - Similar to human protocols but involve hardware or software components.
    - **Examples**:
        - Flow of bits between network interface cards.
        - Congestion control in end systems.
        - Path determination by routers.
- **Key Elements of a Protocol**:
    - Defines **format** and **order** of messages exchanged.
    - Specifies **actions** taken on message transmission and receipt.
- **Internet Protocols**:
    - Examples include Web server communication:
        - Sending a connection request.

        - Receiving a connection reply.
        - Sending a GET request for a Web page.
        - Receiving the Web page.
- **Importance**:
    - Understanding protocols is crucial for mastering computer networking.
    - Protocols can range from simple to complex.

▼ 1.2 The Network Edge

End Systems

- **Definition**: Computers, smartphones, and other devices connected to the Internet.
- **Types**:
    - Desktop computers (PCs, Macs, Linux boxes)
    - Servers (Web, e-mail)
    - Mobile devices (laptops, smartphones, tablets)
- **Hosts**: End systems running application programs (e.g., Web browsers, e-mail clients).

1.2.1 Access Networks

- **Definition**: Network connecting an end system to the first router (edge router).
- **Types**:
    - **Home Access**:
        - **DSL**:
            - Uses existing telephone lines.
            - Transmission rates: 12-24 Mbps downstream, 1.8-2.5 Mbps upstream.
        - **Cable**:

            - Uses cable TV infrastructure.
            - Transmission rates: Up to 42.8 Mbps downstream, 30.7 Mbps upstream.
            - Shared broadcast medium affecting speeds.
        - **FTTH (Fiber to the Home)**:
            - Direct optical fiber path from CO to home.
            - Speed potential: Gigabits per second.
    - **Other Technologies**:
        - **Satellite**: Internet speeds over 1 Mbps.
        - **Dial-Up**: Up to 56 kbps, slow compared to DSL and cable.

Access in the Enterprise and Home

- **Ethernet**:
    - Common in corporate and university settings.
    - Speed: Typically 100 Mbps to 10 Gbps.
- **WiFi**:
    - Wireless LAN technology.
    - Speed: Up to 54 Mbps.
    - Common in homes and public places.

Wide-Area Wireless Access

- **3G**:
    - Provides speeds in excess of 1 Mbps.
- **4G/LTE**:
    - Higher-speed access, potentially over 10 Mbps.
    - LTE speeds: Tens of Mbps reported.

1.2.2 Physical Media

- **Definition and Role**
  - Physical media refer to the physical medium through which data travels from one end system to another.
  - The bit travels through various transmitter-receiver pairs, each using different physical media.
- **Categories of Physical Media**
  - **Guided Media**: Waves are guided along a solid medium.
    - Examples: Fiber-optic cable, twisted-pair copper wire, coaxial cable.
  - **Unguided Media**: Waves propagate in the atmosphere or space.
    - Examples: Wireless LAN, digital satellite channels.
- **Cost Considerations**
  - Material cost is often minor compared to installation labor.
  - Installation of multiple media types in buildings can be cost-effective for future use.

Types of Physical Media

- **Twisted-Pair Copper Wire**
  - Commonly used in telephone networks and LANs.
  - Consists of two insulated copper wires twisted together to reduce interference.
  - Data rates: 10 Mbps to 10 Gbps (modern technology).
  - DSL technology allows Internet access at tens of Mbps.
- **Coaxial Cable**
  - Contains two concentric copper conductors.
  - Used in cable television systems and cable Internet access.

  - Provides high data transmission rates and can be used as a shared medium.
- **Fiber Optics**
  - Uses thin, flexible fibers to conduct light pulses.
  - Supports high bit rates (tens to hundreds of gigabits per second).
  - Immune to electromagnetic interference, low signal attenuation.
  - Common in long-haul and backbone networks.
  - High cost of optical devices limits short-haul applications.
- **Terrestrial Radio Channels**
  - Carry signals via electromagnetic spectrum.
  - No physical wire required; can penetrate walls and provide mobile connectivity.
  - Classified into short-distance, local-area, and wide-area channels.
  - Characteristics affected by path loss, shadow fading, multipath fading, and interference.
- **Satellite Radio Channels**
  - Use communication satellites to link ground stations.
  - Two types:
    - **Geostationary Satellites**: Fixed above one spot on Earth; higher signal propagation delay.
    - **Low-Earth Orbit (LEO) Satellites**: Rotate around Earth; require multiple satellites for coverage.
  - Geostationary satellites used for high-speed links in remote areas; LEO satellites may become more relevant for future Internet access.

▼ 1.3 The Network Core

- The network core consists of packet switches and links connecting end systems.

1.3.1 Packet Switching

- **Function**
  - End systems exchange messages that are broken into packets.
  - Packets travel through communication links and packet switches (routers and link-layer switches).
  - Transmission rate: Packet transmission time = L/R seconds, where L is packet size and R is link rate.

    L/RL / R

    LL

    RR
- **Store-and-Forward Transmission**
  - Packets must be fully received before forwarding begins.
  - Total delay for one packet: 2L/R seconds.
  - For multiple packets, delay accumulates based on transmission and processing at each router.
  - $d_{EndToEnd} = NL/R$
- **Queuing Delays and Packet Loss**
  - Packets wait in output buffers if links are busy.
  - Buffer overflow leads to packet loss.
  - Queuing delays vary with network congestion.

Forwarding Tables and Routing Protocols

- **Forwarding Process**
  - Routers use forwarding tables to direct packets based on destination IP addresses.
  - The router's forwarding table maps addresses to outbound links.
- **Routing Protocols**

- Automated protocols set and update forwarding tables.
- They determine paths and configure routers to optimize packet routing.
- **Practical Example**
  - Use Traceroute to observe end-to-end routing paths in the Internet.

1.3.2 Circuit Switching

- **Overview**:
  - **Definition**: Resources (buffers, link transmission rate) are reserved for the duration of the communication session.
  - **Analogy**: Similar to reserving a table at a restaurant versus waiting for a table.
- **Traditional Use**:
  - **Example**: Telephone networks.
  - **Connection**: Establishes a dedicated end-to-end connection with reserved transmission rate.
- **Mechanism**:
  - **Circuit**: Maintains connection state and reserves a constant transmission rate.
  - **Illustration**: Figure shows circuits on links with dedicated bandwidth.
- **Multiplexing**:
  - **Frequency-Division Multiplexing (FDM)**: Divides frequency spectrum among connections.
  - **Time-Division Multiplexing (TDM)**: Divides time into frames and assigns time slots to connections.
- **Efficiency Issues**:
  - **Resource Wastage**: Idle periods result in underutilization of reserved resources.
  - **Complexity**: Requires complex signaling software.

- **Numerical Example**:
  - **File Transmission**: 640,000 bits file with 1.536 Mbps bit rate and 24 TDM slots takes 10.5 seconds (including circuit establishment).

Packet Switching vs. Circuit Switching

- **Packet Switching**:
  - **Overview**: Sends packets without reserving resources; uses resources on demand.
  - **Efficiency**: More efficient as it allows for higher user numbers and better sharing of transmission capacity.
- **Comparison**:
  - **Real-Time Services**: Circuit switching is preferred for services requiring predictable delays (e.g., voice calls).
  - **Capacity Sharing**: Packet switching allows for dynamic allocation of bandwidth based on demand.
- **Examples**:
  - **Circuit Switching**: Limited to number of simultaneous users due to reserved bandwidth.
  - **Packet Switching**: Can handle more users with minimal delay, even under high demand.
- **Trends**:
  - **Current Use**: Packet switching is increasingly dominant, with many circuit-switched networks migrating to packet switching for efficiency.

1.3.3 A Network of Networks

Overview

- **Access ISPs**: Provide connectivity to end systems (e.g., PCs, smartphones) via wired or wireless technologies (DSL, cable, FTTH, Wi-Fi, cellular).

- **Access ISP Examples**: Universities, companies, telcos, and cable companies.
- **Objective**: Connect billions of end systems through interconnecting access ISPs.

Network Structures

1. **Network Structure 1**
    - **Design**: Access ISPs connect to a single global transit ISP.
    - **Cost**: High for global transit ISP; charges access ISPs based on traffic.
    - **Role**: Global transit ISP acts as a provider to access ISPs.
2. **Network Structure 2**
    - **Design**: Multiple global transit ISPs interconnect with access ISPs.
    - **Benefit**: Access ISPs can choose from multiple providers.
    - **Requirement**: Global transit ISPs must interconnect to enable communication between access ISPs connected to different providers.
3. **Network Structure 3**
    - **Design**: Includes regional ISPs connecting to tier-1 ISPs.
    - **Components**:
        - **Tier-1 ISPs**: Major ISPs with extensive coverage (e.g., Level 3, AT&T, Sprint).
        - **Regional ISPs**: Connect to tier-1 ISPs and other regional ISPs.
        - **Hierarchy**: Access ISPs connect to regional ISPs, which connect to tier-1 ISPs.
4. **Network Structure 4**
    - **Components**:
        - **Points of Presence (PoPs)**: Routers where customer ISPs connect.
        - **Multi-Homing**: ISPs connect to multiple providers for redundancy.

    - **Peering**: ISPs connect directly to avoid intermediary costs; typically settlement-free.
    - **Internet Exchange Points (IXPs)**: Facilitate peering among multiple ISPs.

5. **Network Structure 5**
    - **Design**: Adds content provider networks to the existing hierarchy.
    - **Example**: Google's private network connects its data centers globally and peers with lower-tier ISPs.
    - **Advantage**: Reduces payments to upper-tier ISPs and improves service control.

Key Points

- **Internet Complexity**: Consists of tier-1 ISPs, regional ISPs, and access ISPs.
- **Tier-1 ISPs**: Large, globally connected ISPs.
- **Content Providers**: Establish private networks to reduce costs and enhance control over content delivery.
- **Customer-Provider Relationships**: Access ISPs and content providers pay higher-tier ISPs for connectivity.

▼ 1.4 Delay, Loss, and Throughput in Packet Switched Networks

1.4.1 Overview of Delay in Packet-Switched Networks

Overview

- The Internet provides services to distributed applications on end systems.
- Ideal network performance aims for instantaneous data transfer without loss.

- Real networks face constraints: limited throughput, delays, and packet loss.

Types of Delay

1. **Processing Delay**
   - Time to examine the packet header and check for errors.
   - Typically in microseconds or less.
2. **Queuing Delay**
   - Time spent waiting in the queue before transmission.
   - Depends on the number of packets ahead in the queue.
   - Ranges from microseconds to milliseconds.
3. **Transmission Delay**
   - Time to push all bits of a packet into the link.
   - Calculated as L/R, where L is packet length and R is transmission rate.
   - Typically microseconds to milliseconds.
4. **Propagation Delay**
   - Time for a bit to travel from sender to receiver.
   - Calculated as d/s, where d is distance and s is propagation speed.
   - Ranges from milliseconds in wide-area networks.
     $2.10^8 meters/sec to 3.10^8 meters/sec$

Comparison of Delays

- **Transmission Delay**: Time to push the packet into the link; independent of distance.
- **Propagation Delay**: Time for bits to propagate; dependent on distance.

Practical Considerations

- **Total Nodal Delay**: dnodal=dproc+dqueue+dtrans+dprop

  $$d_{\text{nodal}} = d_{\text{proc}} + d_{\text{queue}} + d_{\text{trans}} + d_{\text{prop}}$$

- **dproc**: Often negligible but impacts maximum throughput.
- **dqueue**: Varies with traffic load.
- **dtrans**: Significant for low-speed links.
- **dprop**: Can dominate in satellite links.

1.4.2 Queuing Delay and Packet Loss

Queuing Delay

- **Definition**: Time a packet spends waiting in the queue before transmission.
- **Characteristics**:
  - Varies from packet to packet.
  - Analyzed using statistical measures: average delay, variance, and probability of exceeding a threshold.
- **Factors Influencing Queuing Delay**:
  - **Traffic Intensity**: Ratio La/R, where La is the packet arrival rate and R is the transmission rate.
    - If $La/R > 1$: Queue length increases indefinitely, causing delay to approach infinity.
    - If $La/R <= 1$: Queuing delay is impacted by traffic patterns (periodic or bursty).

- **Traffic Patterns**:
  - **Periodic Arrivals**: Predictable queuing delays.
  - **Random Arrivals**: More complex; average delay depends on traffic intensity.

Packet Loss

- **Definition**: Occurs when a packet arrives at a full queue and is dropped due to finite queue capacity.

- **Impact**:
  - Packet loss becomes more frequent as traffic intensity exceeds 1.
  - From an end-system perspective, a lost packet never reaches its destination.
  - Performance is assessed based on both delay and packet loss probability.
- **Mitigation**:
  - Lost packets may be retransmitted to ensure complete data transfer.

1.4.3 End-to-End Delay

End-to-End Delay

- **Definition**: Total delay from the source host to the destination host, considering multiple routers.
- **Formula**:

  $d_{end-to-end} = N \times (d_{proc} + d_{trans} + d_{prop})$
  where
  $d_{trans} = \frac{L}{R}$, L is the packet size, and N is the number of routers.

Traceroute

- **Purpose**: Measures end-to-end delay by sending special packets through routers.
- **Process**:
  - Sends multiple packets, each marked with a unique number.
  - Each router responds with a message containing its name and address.
  - The source calculates the round-trip delay for each packet.
- **Output**:
  - Displays router numbers, names, addresses, and round-trip delays.

- Example output includes delays for each router along the route.

- **Usage**: Available at Traceroute.org and graphical tools like PingPlotter.

Additional Delays

- **End System Delays**:
  - Protocol-based delays (e.g., medium access in shared networks).
  - Media packetization delay (e.g., VoIP applications) where time is spent filling packets with data.

1.4.4 Throughput in Computer Networks

Definition

- **Throughput**: The rate at which data is successfully transferred from Host A to Host B, measured in bits per second (bps).

Examples and Analysis

- **Two-Link Network**:
  - **Throughput**: Determined by the bottleneck link.
  - **Formula**: $\text{Throughput} = \min(R_s, R_c)$
  - **Transfer Time**: $\text{Time} = \frac{F}{\min(R_s, R_c)}$, where F is the file size, Rs is the server link rate, and Rc is the client link rate.

- **Network with Multiple Links**:
  - **Throughput**: Determined by the bottleneck link in the path.
  - **Formula**: $\text{Throughput} = \min(R_1, R_2, ..., R_N)$, where Ri are the rates of the links.

- **Core Network with High-Speed Links**:

- **Throughput**: Limited by the access network links.
- **Formula**: $\text{Throughput} = \min(R_s, R_c)$, assuming core links have high capacity.

- **Shared Core Link with Multiple Downloads**:
    - **Throughput**: Can be limited by the shared core link.
    - **Example**: If the common link rate is R and is shared equally among N downloads, throughput per download is $\frac{R}{N}$

Key Points

- **Throughput** is affected by the transmission rates of all links along the data path.
- **Bottleneck Link**: The link with the lowest transmission rate along the path typically determines the overall throughput.
- **Traffic Impact**: Throughput can be reduced if a shared link is heavily used by multiple data flows.

▼ 1.5 Protocol Layers and Their Service Models

1.5.1 Layered Architecture

- **Analogy**: Complex systems, like the airline system, can be described in layers (e.g., ticketing, baggage, gate, takeoff/landing).
- **Layered Functionality**:
    - Each layer performs specific actions and uses services from the layer below.
    - Layers provide modularity and ease of updates without affecting other components.

Protocol Layering

- **Network Protocols**:
  - Organized in layers for structure.
  - Each layer offers specific services and uses services from the layer below.
- **Implementation**:
  - Layers can be implemented in software, hardware, or a combination.
  - Distributed across end systems, packet switches, and network components.
- **Advantages**:
  - Modularity and ease of updating.
  - Structured approach to discussing system components.
- **Drawbacks**:
  - Possible duplication of functionality.
  - Potential need for inter-layer information, violating separation goals.

Internet Protocol Stack

- **Layers**:
  1. **Application Layer**: Includes protocols like HTTP, SMTP, FTP, and DNS. Handles network applications and messages.
  2. **Transport Layer**: Provides TCP (connection-oriented, reliable delivery) and UDP (connectionless, no-frills service).
  3. **Network Layer**: Handles datagrams with IP protocol and routing protocols. Often referred to as the IP layer.
  4. **Link Layer**: Moves frames between nodes, with protocols like Ethernet, WiFi, and DOCSIS.
  5. **Physical Layer**: Moves bits across the link, with protocols varying by transmission medium (e.g., twisted-pair, fiber).

The OSI Model

- **Seven Layers**:
    1. Application
    2. Presentation
    3. Session
    4. Transport
    5. Network
    6. Data Link
    7. Physical
- **Comparison**:
    - The Internet model roughly matches the OSI model's functionality except for Presentation and Session layers.
    - **Presentation Layer**: Data compression, encryption, and description.
    - **Session Layer**: Data exchange synchronization, checkpointing, and recovery.
- **Internet Approach**:
    - Functions of Presentation and Session layers are handled at the application level if needed.

1.5.2 Encapsulation

- **Overview**:
    - **Path**: Data moves through protocol stacks of sending and receiving end systems, as well as intervening link-layer switches and routers.
    - **Layers Implemented**:
        - **Link-layer Switches**: Layers 1 and 2.
        - **Routers**: Layers 1 through 3.
        - **Hosts**: Implement all five layers.
- **Encapsulation Process**:

- **At Sending Host**:
    - **Application Layer**: Message (M) is generated.
    - **Transport Layer**: Adds transport-layer header information (H_t), creating a transport-layer segment.
    - **Network Layer**: Adds network-layer header information (H_n), forming a network-layer datagram.
    - **Link Layer**: Adds link-layer header information, creating a link-layer frame.

- **Analogy**:
  - **Interoffice Memo**:
    - **Application-Layer Message**: Memo.
    - **Transport-Layer Segment**: Memo in an interoffice envelope with header information.
    - **Datagram**: Interoffice envelope in a postal envelope with postal addresses.
    - **De-encapsulation**: Receiving end extracts the memo from the postal envelope and interoffice envelope.
- **Complexity**:
  - **Large Messages**: May be divided into multiple segments and datagrams, requiring reassembly at the receiving end.

▼ 1.6 Networks Under Attack

- **Importance of Network Security**:
  - The Internet is critical for institutions and individuals.
  - Network security involves defending against attacks and designing secure architectures.
- **Prevalent Security Issues**:
  - **Malware**:
    - **Types**:

            - **Viruses**: Require user interaction to spread (e.g., via email attachments).
            - **Worms**: Spread without user interaction, exploiting vulnerabilities in network applications.
        - **Effects**: Deleting files, installing spyware, creating botnets for attacks.
    - **Denial-of-Service (DoS) Attacks**:
        - **Types**:
            - **Vulnerability Attacks**: Exploit flaws in applications or systems to crash services.
            - **Bandwidth Flooding**: Overwhelm the target's access link with excessive traffic.
            - **Connection Flooding**: Saturate the target with numerous bogus connections.
        - **Distributed DoS (DDoS)**: Uses multiple sources to overwhelm a target, making it harder to detect and defend against.
    - **Packet Sniffing**:
        - **Vulnerability**: Wireless and wired environments can be vulnerable to packet sniffers that capture sensitive data.
        - **Defense**: Cryptography and secure protocols to protect data.
    - **IP Spoofing**:
        - **Vulnerability**: Crafting packets with false source addresses to deceive receivers.
        - **Defense**: End-point authentication to verify message origins.
- **Historical Context**:
    - **Original Internet Design**: Based on mutual trust and transparency, lacking built-in security.
    - **Current Challenges**: Addressing security issues in a context where mutual trust is not always present.

- **Future Focus**:
    - Develop defenses against various attacks including malware, sniffing, spoofing, and DDoS.

▼ 1.7 History of Computer Networking and the Internet

1.7.1 The Development of Packet Switching: 1961–1972

- **Origins**:
    - In the early 1960s, the telephone network used circuit switching for constant-rate voice transmission.
    - Increasing use of computers and timesharing led to the need for a more efficient method for bursty traffic.
- **Key Developments**:
    - **Packet Switching Invention**:
        - **Leonard Kleinrock** (MIT): Demonstrated the effectiveness of packet switching using queuing theory (1961-1964).
        - **Paul Baran** (Rand Institute): Investigated packet switching for secure military communications (1964).
        - **Donald Davies and Roger Scantlebury** (National Physical Laboratory, England): Developed packet switching concepts concurrently.
- **ARPAnet**:
    - **J.C.R. Licklider and Lawrence Roberts**: Led ARPA's computer science program and planned the ARPAnet.
    - **1969**: ARPAnet's initial installation with four nodes: UCLA, Stanford Research Institute, UC Santa Barbara, and University of Utah.
    - **1972**: ARPAnet grew to 15 nodes and demonstrated its first host-to-host protocol, NCP.

    - **Ray Tomlinson**: Developed the first e-mail program in 1972.

1.7.2 Proprietary Networks and Internetworking: 1972–1980

- **Expansion of Networks**:
    - **Early 1970s**: Emergence of additional packet-switching networks:
        - **ALOHANet**: Microwave network linking Hawaiian universities.
        - **DARPA's Packet-Satellite and Packet-Radio Networks**: Innovations in satellite and radio packet-switching.
        - **Telenet**: Commercial packet-switching network based on ARPAnet technology.
        - **Cyclades**: French packet-switching network developed by Louis Pouzin.
        - **Tymnet and GE Information Services**: Time-sharing networks.
        - **IBM’s SNA (1969–1974)**: Parallel development to ARPAnet.
- **Internetworking Developments**:
    - **Vinton Cerf and Robert Kahn**: Pioneered interconnecting networks, leading to the concept of "internetting."
    - **Early TCP and IP**:
        - **TCP**: Initially combined reliable data delivery with forwarding functions.
        - **Separation of IP and TCP**: Led to the development of UDP for non-flow-controlled transport.
        - **By the end of the 1970s**: TCP, UDP, and IP were conceptually established.
- **Notable Contributions**:
    - **ALOHA Protocol**: First multiple-access protocol developed by Norman Abramson for ALOHAnet.

    - **Ethernet Protocol**:
        - **Developed by Metcalfe and Boggs**: Based on ALOHA protocol principles for wire-based shared networks.
        - **Purpose**: Designed to connect multiple PCs, printers, and shared disks.

1.7.3 A Proliferation of Networks: 1980–1990

- **Growth of Hosts**:
    - **End of 1970s**: Approximately 200 hosts on ARPAnet.
    - **End of 1980s**: 100,000 hosts on the public Internet.
- **Key Network Developments**:
    - **BITNET**: Provided e-mail and file transfers among Northeast universities.
    - **CSNET**: Linked university researchers without ARPAnet access.
    - **NSFNET (1986)**: Linked NSF-sponsored supercomputing centers; backbone speed increased from 56 kbps to 1.5 Mbps by decade's end.
- **ARPAnet and Internet Architecture**:
    - **January 1, 1983**: TCP/IP officially deployed as the standard protocol for ARPAnet (replacing NCP).
    - **Late 1980s**: Extensions to TCP for host-based congestion control; development of DNS for mapping Internet names to IP addresses.
- **International Development**:
    - **Minitel Project (Early 1980s)**:
        - **France**: Public packet-switched network based on X.25; free terminals distributed to French households.
        - **Success**: Offered over 20,000 services by mid-1990s, including home banking and research databases.

1.7.4 The Internet Explosion: The 1990s

- **End of ARPAnet**:
  - ARPAnet ceased to exist.
  - NSFNET lifted commercial use restrictions in 1991; decommissioned in 1995.
- **Emergence of the World Wide Web**:
  - **Invention**: Tim Berners-Lee developed the Web at CERN (1989-1991).
  - **Components**: HTML, HTTP, Web server, and browser.
  - **Early Growth**: About 200 Web servers by late 1993; Web browsers with GUI interfaces developed, including Mosaic (later Netscape).
- **Browser Wars**:
  - **Netscape**: Gained popularity in the mid-1990s.
  - **Microsoft**: Entered the browser market in 1996, eventually dominating the browser market.
- **Internet Innovations and Growth**:
  - **Major Applications**:
    - E-mail (with attachments and Web-accessible)
    - Web browsing and Internet commerce
    - Instant messaging with contact lists
    - Peer-to-peer file sharing (e.g., Napster)
  - **Impact**: Hundreds of applications by the end of the 1990s.
- **Financial Market Trends**:
  - **Dot-Com Bubble**: Many startups went public before becoming profitable; market collapse in 2000-2001.
  - **Winners**: Microsoft, Cisco, Yahoo, eBay, Google, and Amazon emerged successful.

1.7.5 The New Millennium

- **Broadband Internet Access**:
    - **Deployment**: Cable modems, DSL, fiber to the home.
    - **Applications**: User-generated video (YouTube), on-demand streaming (Netflix), multi-person video conferencing (Skype).
- **High-Speed Wireless Networks**:
    - **WiFi and Cellular**: High-speed public WiFi (54 Mbps+), medium-speed 3G/4G.
    - **Impact**: Ubiquitous connectivity, rise of hand-held devices (iPhones, Androids, iPads).
- **Online Social Networks**:
    - **Platforms**: Facebook, Twitter.
    - **Features**: Massive people networks, APIs for networked applications and distributed games.
- **Private Networks by Online Service Providers**:
    - **Examples**: Google, Microsoft.
    - **Function**: Connect global data centers, bypass the Internet by peering directly with lower-tier ISPs.
- **Cloud Computing**:
    - **Providers**: Amazon EC2, Google App Engine, Microsoft Azure.
    - **Usage**: Internet applications, email, Web hosting.
    - **Benefits**: Scalable computing/storage, high-performance private networks.