Problem Solver (DI03000131) - Problem Solver

Antigravity AI

June 4, 2026

Contents

CHAPTER 1

Introduction to Computer Networks

1.1 Need Advantages and Applications of Computer Networks

A computer network is a system of interconnected computers and peripheral devices that can communicate with each other and share resources. The primary purpose of a computer network is to facilitate data exchange and resource sharing among users.

1.1.1 Need for Computer Networks

- **Resource Sharing**: Networks allow users to share hardware resources like printers and scanners, as well as software resources and data files.
- **Communication**: Networks provide a fast and reliable medium of communication through emails, instant messaging, and video conferencing.
- **Cost Reduction**: By sharing resources, organizations can significantly reduce the cost of purchasing individual hardware and software licenses.
- **Data Backup and Reliability**: Critical data can be stored on centralized servers and backed up regularly, ensuring data integrity and availability in case of hardware failures.

1.1.2 Advantages of Computer Networks

- **Enhanced Connectivity**: Users can connect to the network from various locations, promoting remote work and collaboration.
- **Centralized Administration**: Network administrators can manage and secure the entire network from a single central location.
- **Scalability**: New devices can be easily added to the network to accommodate growth without disrupting existing services.
- **Security**: Networks offer security mechanisms like firewalls and user authentication to protect sensitive data from unauthorized access.

1.1.3 Applications of Computer Networks

- **Financial Services**: Electronic banking, online transactions, and ATM networks rely heavily on computer networks.
- **Education**: E-learning platforms, digital libraries, and online examination systems are built upon networking technologies.
- **Healthcare**: Telemedicine, remote patient monitoring, and centralized electronic health records require robust networks.
- **Entertainment**: Streaming services, online gaming, and social media platforms are major applications of computer networks.

1.2 Physical Topologies of Network

The physical topology of a network refers to the geometric arrangement of the devices (nodes) and the physical links (cables) connecting them. The choice of topology affects the network's performance, cost, and reliability.

Methodology:

Key Considerations for Network Topology When selecting a network topology the following factors should be considered:

- **Cost**: The amount and type of cabling required.
- **Scalability**: How easily new nodes can be added.
- **Reliability**: The impact of a node or cable failure on the entire network.
- **Performance**: The data transfer rate and the likelihood of network congestion.

1.2.1 Bus Topology

In a bus topology, all nodes are connected to a single central cable, known as the bus or backbone. Data is transmitted in both directions along the cable and every node receives the data but only the intended recipient processes it.

- **Advantages**: Easy to install and requires less cabling compared to other topologies. It is cost-effective for small networks.
- **Disadvantages**: If the main cable fails, the entire network goes down. Performance degrades as more nodes are added or network traffic increases.

1.2.2 Star Topology

In a star topology, each node is connected to a central device, such as a hub or a switch. All communication between nodes passes through the central device.

- **Advantages**: Easy to install and manage. A failure in one cable or node does not affect the rest of the network. The central device helps in troubleshooting and monitoring.
- **Disadvantages**: The entire network depends on the central device; if it fails, the whole network fails. It requires more cabling than a bus topology.

1.2.3 Ring Topology

In a ring topology, each node is connected to exactly two other nodes, forming a closed loop or ring. Data travels in one direction (unidirectional) or both directions (bidirectional) around the ring.

- **Advantages**: Data flows in a systematic manner, reducing the chances of packet collisions. It can handle high volumes of traffic better than a bus topology.
- **Disadvantages**: A failure in any single node or cable can break the loop and bring down the entire network (in a unidirectional ring). Adding or removing nodes can disrupt network operations.

1.2.4 Mesh Topology

In a mesh topology, every node is connected to every other node (full mesh) or to a selected group of nodes (partial mesh). This provides multiple paths for data to travel from source to destination.

- **Advantages**: Extremely reliable and fault-tolerant because of multiple paths. It provides high security and privacy since connections are dedicated.
- **Disadvantages**: Installation and configuration are complex. It requires a massive amount of cabling and numerous I/O ports, making it very expensive.

1.2.5 Tree Topology

A tree topology is a hierarchical structure that combines characteristics of both star and bus topologies. Groups of star-configured networks are connected to a linear bus backbone.

- **Advantages**: Highly scalable and easy to manage. Fault isolation is relatively straightforward. It is well-suited for large organizational networks.
- **Disadvantages**: If the backbone cable fails, the entire network gets partitioned. It is heavily dependent on the central hub or switch of each star segment.

1.2.6 Hybrid Topology

A hybrid topology is a combination of two or more different types of topologies (e.g., star-bus or star-ring) to leverage their respective advantages and mitigate their disadvantages.

- **Advantages**: Highly flexible and reliable. It can be tailored to meet specific organizational needs and is easily scalable.
- **Disadvantages**: Network design, installation, and troubleshooting are complex. It is generally more expensive to implement than simple topologies.

1.3 Internet Standards Protocol and Interface

To ensure that diverse hardware and software from different vendors can interoperate seamlessly, networking relies on established standards.

1.3.1 Protocols

A protocol is a set of rules and conventions that govern how data is formatted, transmitted, and received over a network. It defines what is communicated, how it is communicated, and when it is communicated.

- **Syntax**: Refers to the structure or format of the data, meaning the order in which they are presented.
- **Semantics**: Refers to the meaning of each section of bits. It determines how a particular pattern should be interpreted and what action to take.
- **Timing**: Determines when data should be sent and how fast it can be sent.

1.3.2 Interfaces

An interface defines the boundary and the rules of interaction between two adjacent layers in a network architecture or between two devices. It specifies the services a lower layer provides to an upper layer and how those services can be accessed. For example, a network interface card (NIC) acts as the physical interface between a computer and a local area network (LAN).

Worked Example:

Identify Protocol versus Interface A user connects their laptop to a Wi-Fi network to browse a website. Identify the role of protocols and interfaces in this scenario.
Solution:

- **Protocol**: When the user types a URL, the HTTP/HTTPS protocol dictates how the web browser requests the webpage and how the web server formats and sends the response. TCP/IP protocols ensure the data packets reach the correct destination over the internet.
- **Interface**: The wireless network adapter inside the laptop serves as the hardware interface to connect to the physical Wi-Fi signal. The API (Application Programming Interface) provided by the operating system acts as the software interface for the web browser to access the network hardware.

1.4 Network Classification

Computer networks can be classified based on various criteria such as transmission technologies, geographical scale, and architecture.

1.4.1 Based on Transmission Technologies

- **Point-to-Point Networks**: These networks establish a dedicated link between two specific devices. The entire capacity of the link is reserved for transmission between those two devices. Data travels from the sender directly to the receiver.
- **Broadcast Networks**: These networks have a single communication channel that is shared by all the machines on the network. Short messages, called packets, sent by any machine are received by all the others. An address field within the packet specifies the intended recipient. Upon receiving a packet, a machine checks the address field; if the packet is intended for it, it processes the packet, otherwise, it ignores it.

1.4.2 Based on Scale

- **PAN (Personal Area Network)**: A network organized around an individual within a range of a few meters (e.g., connecting a smartphone to a Bluetooth headset).
- **LAN (Local Area Network)**: Covers a small geographical area like a home, office, or building. LANs are typically privately owned and offer high-speed data transfer. Ethernet and Wi-Fi are common LAN technologies.
- **MAN (Metropolitan Area Network)**: Covers a larger geographical area than a LAN, such as a city or a large campus. A MAN can connect several LANs together. Cable television networks are an example of MANs.
- **WAN (Wide Area Network)**: Spans a large geographical area, such as a country, continent, or the entire globe. WANs use complex communication links like satellites and leased telecommunication lines. The Internet is the largest WAN.
- **VPN (Virtual Private Network)**: Creates a secure, encrypted connection over a less secure network, such as the public internet. It allows remote users to securely access a private corporate network.
- **Internet**: A global system of interconnected computer networks that use the standard Internet protocol suite (TCP/IP) to serve billions of users worldwide. It is a "network of networks."

1.4.3 Based on Architecture

- **Peer-to-Peer (P2P) Model**: In a P2P network, all computers (nodes) have equal status and capabilities. There is no central server managing the network. Each node can act as both a client (requesting resources) and a server (providing resources). P2P is suitable for small networks where security and centralized management are not critical priorities.
- **Client-Server Model**: This architecture involves two distinct types of computers. **Servers** are powerful machines designed to provide specific services or resources (such as files, web pages, or email). **Clients** are user devices (like laptops or smartphones) that request these services from the servers. The server processes the request and sends the appropriate response back to the client.

1.5 Advantages of Client Server over Peer-to-Peer Model

While P2P networks are easy to set up and cost-effective for very small environments, the Client-Server model offers several significant advantages for larger and more complex networks:

- **Centralized Security**: Security policies, user authentication, and access controls are managed centrally on the server. This makes the network much more secure compared to P2P, where each user manages their own security.
- **Centralized Data Backup**: Data is stored centrally on servers, making it easy to schedule regular and reliable backups. In P2P, data is scattered across multiple machines, complicating backup procedures.
- **Scalability**: Client-server networks are highly scalable. New clients can be added without significantly impacting performance, and servers can be upgraded or expanded to handle increased load.
- **Easier Management**: Network administration, software updates, and hardware maintenance are simplified because they can be coordinated from a central location.
- **Higher Performance**: Dedicated servers are optimized for specific tasks (e.g., file sharing, database management), providing faster response times and better overall performance for clients.

1.6 OSI and TCP/IP Models and their Comparison

Network models provide a conceptual framework for understanding how networks operate and how different protocols interact. The two most prominent models are the OSI model and the TCP/IP model.

1.6.1 The OSI Model

The Open Systems Interconnection (OSI) model is a conceptual model created by the International Organization for Standardization (ISO). It standardizes the communication functions of a telecommunication or computing system into seven abstract layers.

Methodology:

OSI Model Layers The OSI model consists of the following seven layers from bottom to top:

1. **Physical Layer**: Deals with the physical transmission of raw bits over a communication medium.
2. **Data Link Layer**: Responsible for node-to-node data transfer and error detection/correction at the physical layer.
3. **Network Layer**: Handles routing of data packets from source to destination across multiple networks (e.g., IP addressing).
4. **Transport Layer**: Ensures reliable, end-to-end data delivery, error recovery, and flow control (e.g., TCP, UDP).
5. **Session Layer**: Establishes, manages, and terminates communication sessions between applications.
6. **Presentation Layer**: Translates, encrypts, and compresses data so it can be properly understood by the receiving application.
7. **Application Layer**: Provides network services directly to the user's applications (e.g., HTTP, FTP, SMTP).

1.6.2 The TCP/IP Model

The Transmission Control Protocol/Internet Protocol (TCP/IP) model is a concise framework that predates the OSI model and is the basis for the modern Internet. It groups the networking functions into four broader layers.

Methodology:

TCP/IP Model Layers The TCP/IP model consists of four layers:

1. **Network Access Layer (Link Layer)**: Corresponds to the Physical and Data Link layers of the

OSI model. It handles the physical connections and framing of data.

2. **Internet Layer**: Corresponds to the OSI Network layer. It is responsible for logical addressing and routing packets across networks using the IP protocol.
3. **Transport Layer**: Matches the OSI Transport layer. It provides end-to-end communication services using protocols like TCP (reliable) and UDP (unreliable).
4. **Application Layer**: Combines the functions of the OSI Session, Presentation, and Application layers. It includes high-level protocols like HTTP, DNS, and FTP.

1.6.3 Comparison of OSI and TCP/IP Models

- **Number of Layers**: OSI has 7 layers, whereas TCP/IP has 4 layers. The TCP/IP Application layer encompasses the OSI Application, Presentation, and Session layers. The TCP/IP Network Access layer combines the OSI Data Link and Physical layers.
- **Development Process**: The OSI model was developed as a theoretical framework *before* actual protocols were implemented. The TCP/IP model was created based on *existing* protocols that were already in use for the ARPANET (the precursor to the Internet).
- **Protocol Independence**: The OSI model clearly distinguishes between services, interfaces, and protocols, making it more flexible for introducing new protocols. The TCP/IP model is heavily dependent on the TCP and IP protocols; it is less flexible for supporting alternative protocol suites.
- **Strictness of Boundaries**: Layer boundaries are strictly defined in the OSI model. In TCP/IP, layer boundaries are more flexible, and protocols can sometimes span multiple layers or skip layers.
- **Usage**: The OSI model is primarily used as an educational tool and reference model to understand network concepts. The TCP/IP model is the practical, implemented architecture of the modern Internet.

Worked Example:

Mapping Network Devices to OSI Layers Identify which layer of the OSI model the following network devices operate at: Switch, Router, Hub.
Solution:

- **Hub**: Operates at Layer 1 (Physical Layer). It simply receives electrical signals on one port and broadcasts them to all other ports without understanding the data content or addresses.
- **Switch**: Operates at Layer 2 (Data Link Layer). It inspects the MAC (Media Access Control) addresses in data frames and forwards them only to the appropriate destination port, improving network efficiency.
- **Router**: Operates at Layer 3 (Network Layer). It inspects IP addresses in packets and uses routing tables to determine the best path to forward the packets across different networks.

CHAPTER 2

Network Devices and Technologies

2.1 Classification of Transmission Media and Role of Different Devices

Transmission media provide the physical pathway over which data travels from a sender to a receiver. They are broadly classified into two main categories: guided (wired) and unguided (wireless) media.

Guided media, such as twisted-pair cable, coaxial cable, and fiber-optic cable, use a physical conductor to constrain and direct the signal. Unguided media transmit electromagnetic waves without using a physical conductor, commonly involving radio waves, microwaves, and infrared signals.

Network devices are crucial for interconnecting devices and routing data across these transmission media. Depending on their operating layer in the OSI model, these devices handle signal regeneration, collision avoidance, and optimal data routing.

2.2 Repeaters Hubs Bridges and Switches

2.2.1 Repeaters

A repeater operates at the Physical layer (Layer 1) of the OSI model. Its primary function is to regenerate and amplify incoming signals before retransmitting them. This helps in extending the network's geographical reach by compensating for signal attenuation over long cable runs. Repeaters do not filter data or read MAC addresses; they simply forward all incoming bits to all connected segments.

2.2.2 Hubs

A hub is essentially a multiport repeater. It operates at Layer 1 and connects multiple devices in a local area network (LAN), forming a star topology physically while maintaining a bus topology logically. When a hub receives a data frame on one port, it broadcasts the frame to all other ports. It does not possess any intelligence to inspect data or manage traffic, which leads to increased collisions and wasted bandwidth in busy networks.

2.2.3 Bridges

A bridge operates at the Data Link layer (Layer 2). Unlike a hub, a bridge is an intelligent device that can filter traffic by inspecting the MAC addresses of incoming frames. It divides a large network into smaller collision domains, which significantly reduces network congestion. A bridge builds a forwarding table to learn the MAC addresses of devices on each segment and forwards frames only to the segment where the destination device resides.

2.2.4 Switches

A switch is a more advanced multiport bridge operating primarily at Layer 2. It learns the MAC addresses of connected devices and forwards frames selectively to the correct destination port, thus virtually eliminating collisions and providing dedicated bandwidth to each port.

Layer 3 Switches: While traditional switches operate at Layer 2, Layer 3 switches incorporate routing functionalities. They can forward packets based on IP addresses, combining the speed of Layer 2 switching with the intelligence of Layer 3 routing.

Methodology:

Configuring a Basic Switch To effectively configure a network switch for initial use:

1. Connect a console cable from your computer to the switch console port.
2. Open a terminal emulator program and configure the serial connection settings.
3. Enter global configuration mode using the command `configure terminal`.
4. Assign a hostname to the switch using the `hostname` command.
5. Configure a management IP address on the default VLAN (VLAN 1) to enable remote administration.
6. Enable port security to prevent unauthorized devices from connecting.

2.3 Routers

A router is a fundamental networking device that operates at the Network layer (Layer 3) of the OSI model. Its primary responsibility is to forward data packets between different computer networks, essentially directing traffic on the Internet and within large enterprise networks.

Routers maintain routing tables that store information about network topology and available paths. When a router receives a packet, it reads the destination IP address, consults its routing table, and determines the most efficient path to forward the packet toward its destination. They also play a crucial role in creating broadcast domains, thereby limiting the spread of broadcast traffic.

Worked Example:

Selecting Router Paths Consider a router receiving a packet destined for the IP address 192.168.10.50.
Analysis: The router consults its routing table which contains the following entries:

- 192.168.10.0/24 via Interface GigabitEthernet0/0
- 192.168.0.0/16 via Interface Serial0/1/0
- Default route (0.0.0.0/0) via Interface Serial0/1/1

Decision Process: The router uses the longest prefix match rule to determine the best path. The destination IP address 192.168.10.50 matches both the /24 and the /16 networks. Since /24 is a more specific match (longer subnet mask) than /16, the router forwards the packet out of interface GigabitEthernet0/0.

2.4 Access Points

A Wireless Access Point (WAP or simply AP) is a networking hardware device that allows other Wi-Fi devices to connect to a wired network. Operating primarily at Layer 2, an access point acts as a central transmitter and receiver of wireless radio signals.

In a typical corporate setup, multiple APs are strategically placed to ensure seamless coverage, allowing users to roam freely without losing their network connection. APs connect to a wired router, switch, or hub via an Ethernet cable, and project a Wi-Fi signal to a designated area.

2.5 Firewalls: Concept and Principles

A firewall is a network security system designed to monitor and control incoming and outgoing network traffic based on predetermined security rules. It establishes a barrier between a trusted internal network and an untrusted external network (such as the Internet).

Operating Principles:

- **Packet Filtering:** Examines each packet passing through the network and accepts or rejects it based on user-defined rules.
- **Stateful Inspection:** Tracks the operating state and characteristics of network connections traversing it. It only allows packets that belong to a known active connection.
- **Proxy Service:** Acts as an intermediary, preventing direct connections between clients and servers. It evaluates requests according to filtering rules before forwarding them.

2.6 Introduction to Network Management System

A Network Management System (NMS) is an application or set of applications that lets network engineers manage independent components inside a broader network framework. It helps in monitoring, maintaining, and optimizing a network.

Key Components:

- **Operating System (OS):** Network devices run specialized OSs (like Cisco IOS or Juniper Junos) that manage hardware resources and support routing and switching protocols.
- **Command Line Interface (CLI):** A text-based interface used by administrators to configure devices directly. It is powerful and allows for scripting and rapid configuration.
- **Administrative Functions:** These involve performance monitoring, fault management, configuration management, accounting, and security management (often referred to as FCAPS).
- **Interfaces:** NMS utilizes various interfaces like SNMP (Simple Network Management Protocol) or RESTful APIs to gather data and push configurations to network devices.

2.7 Ethernet Fast Ethernet and Gigabit Ethernet

Ethernet is the most widely installed LAN technology. It operates at the physical and data link layers and standardizes the way data is transmitted over cables.

- **Standard Ethernet (10Base-T):** Operates at a speed of 10 Mbps. It typically uses twisted-pair cables and was historically implemented using bus or star topologies.
- **Fast Ethernet (100Base-T):** An upgrade to the original standard providing data transmission speeds up to 100 Mbps. It retains the original frame format, allowing backward compatibility.
- **Gigabit Ethernet (1000Base-T):** Delivers data at 1000 Mbps (1 Gbps). It heavily utilizes fiber optic cables for backbone connectivity but also supports transmission over Cat5e or higher twisted-pair cables.

2.8 Wireless LAN

A Wireless Local Area Network (WLAN) uses wireless communication technologies, primarily IEEE 802.11 standards (Wi-Fi), to link two or more devices within a limited area such as a home, school, or office building. It offers the flexibility of mobility while remaining connected to the network. Security is a major concern in WLANs, requiring robust encryption protocols like WPA2 or WPA3 to protect data transmissions from unauthorized interception.

2.9 FDDI and CDDI

FDDI (Fiber Distributed Data Interface): FDDI is a standard for data transmission on fiber optic lines in LANs that can extend in range up to 200 kilometers. It operates using a dual-ring topology, providing high reliability and fault tolerance. It transmits data at 100 Mbps and is primarily used for network backbones.

CDDI (Copper Distributed Data Interface): CDDI is a variation of FDDI that uses unshielded twisted-pair (UTP) or shielded twisted-pair (STP) copper wire instead of fiber optic cable. It is less expensive than FDDI but has a significantly shorter maximum transmission distance.

2.10 Software Defined Network

Software Defined Networking (SDN) is an architectural approach that makes networks agile and flexible. The core principle of SDN is the separation of the network control plane (the brains of the network that decides where traffic should go) from the forwarding plane (the underlying systems that push packets to selected destinations).

In an SDN architecture, an application centralized controller manages the entire network globally. This abstraction allows administrators to programmatically initialize, control, change, and manage network behavior dynamically using open interfaces. This contrasts with traditional networks where each device is configured individually and makes autonomous routing decisions.

CHAPTER 3
Physical and Data Link Layers

3.1 Introduction

In the OSI and TCP/IP models, the physical, data link, and network layers play fundamental roles in transmitting data from a source to a destination. The physical layer deals with the raw transmission of bits over a communication medium. The data link layer provides reliable node-to-node data transfer and error control. The network layer is responsible for logical addressing and routing packets across multiple networks.

3.2 Physical Layer and Transmission Media

The physical layer defines the electrical, mechanical, and procedural specifications for activating, maintaining, and deactivating the physical link between communicating network systems.

3.2.1 Transmission Media

Transmission media are the physical pathways that connect computers and other devices on a network. They are broadly classified into guided (wired) and unguided (wireless) media.

Twisted Pair Cable

Twisted pair consists of two insulated copper wires twisted around each other to reduce electromagnetic interference (EMI) and crosstalk from neighboring pairs.

- **Unshielded Twisted Pair (UTP):** Commonly used in telephone networks and local area networks (LANs). It is cost-effective but susceptible to interference.
- **Shielded Twisted Pair (STP):** Includes a metallic foil or braided shield to provide better protection against interference, used in environments with high EMI.

Coaxial Cable

Coaxial cable contains a central copper conductor surrounded by an insulating layer, a metallic shield (mesh or foil), and an outer plastic jacket. This structure allows it to carry higher frequency signals than twisted pair cables. It is widely used in cable television networks and earlier Ethernet setups.

Fiber Optic Cable

Fiber optic cables transmit data using pulses of light through a core of glass or plastic.

- **Advantages:** Extremely high bandwidth, low attenuation, complete immunity to electromagnetic interference, and secure data transmission.
- **Types:** Single-mode fiber (uses a laser source for long-distance communication) and multi-mode fiber (uses an LED source for shorter distances).

3.2.2 Wireless Medium as Physical Layer

In unguided or wireless media, data is transmitted through the air using electromagnetic waves without any physical conductor. Wireless communication uses radio waves, microwaves, or infrared signals. Antennas are used at both the transmitter and receiver ends. Wireless media provide mobility and ease of installation, especially in areas where laying cables is difficult.

3.2.3 ISM Band

The Industrial, Scientific and Medical (ISM) radio bands are portions of the radio spectrum reserved internationally for the use of radio frequency energy for industrial, scientific, and medical purposes other than telecommunications. However, due to their license-free nature, these bands are widely used for short-range communication systems. Popular technologies operating in the ISM band include Wi-Fi (2.4 GHz and 5 GHz bands), Bluetooth, and Zigbee.

3.2.4 Cable Modem

A cable modem is a hardware device that allows your computer to communicate with an Internet service provider over a landline connection using coaxial cables, the same ones used to deliver cable television. It modulates digital signals into radio frequency (RF) signals for transmission and demodulates incoming RF signals back into digital data. Cable modems utilize different frequency channels to separate upstream (user to internet) and downstream (internet to user) traffic.

3.3 Data Link Layer

The Data Link Layer transforms the physical layer into a reliable link. It is responsible for node-to-node delivery, framing, physical addressing, error control, and flow control.

3.3.1 Sub Layers of Data Link Layer

The IEEE 802 standard divides the data link layer into two sub-layers:

- **Logical Link Control (LLC):** The upper sub-layer that interacts with the network layer. It provides multiplexing mechanisms that make it possible for several network protocols to coexist within a multipoint network and be transported over the same network medium.
- **Media Access Control (MAC):** The lower sub-layer that interacts with the physical layer. It provides addressing and channel access control mechanisms, resolving conflicts when multiple devices attempt to transmit simultaneously.

3.3.2 Functions: Error Control and Flow Control

Two critical functions of the data link layer are error control and flow control.

Methodology:

Flow Control Mechanisms Flow control regulates the amount of data a sender can transmit before receiving an acknowledgment from the receiver. This prevents the sender from overwhelming a slow receiver.

- **Stop-and-Wait:** The sender transmits one frame and waits for an acknowledgment before sending the next frame.
- **Sliding Window:** The sender can transmit multiple frames up to a specified window size without waiting for an acknowledgment, improving channel utilization.

Methodology:

Error Control Mechanisms Error control detects and retransmits frames that have been lost or damaged during transmission.

- **Error Detection:** Techniques like Parity Check, Checksum, and Cyclic Redundancy Check (CRC) are used to detect errors.
- **Automatic Repeat Request (ARQ):** Involves retransmission of damaged or lost frames. Variants include Stop-and-Wait ARQ, Go-Back-N ARQ, and Selective Repeat ARQ.

Worked Example:

Calculating Even Parity for Error Detection A sender wants to transmit the 7-bit ASCII character 'A' which has the binary representation 1000001. Calculate the transmitted codeword if the system uses an even parity scheme.
Solution:

1. Count the number of 1s in the data bits. The binary representation 1000001 has two 1s.
2. In an even parity scheme, the total number of 1s in the transmitted codeword (including the parity bit) must be an even number.
3. Since there are already two 1s (an even number), the parity bit appended to the data must be 0.
4. The transmitted codeword becomes 10000010 (assuming the parity bit is appended at the end).

If the receiver receives a codeword with an odd number of 1s, it knows an error has occurred during transmission.

3.4 Network Layer

The network layer is responsible for routing packets from the source to the destination across multiple networks. It provides logical addressing and path determination.

3.4.1 Packet Switching

Packet switching is a method of grouping data transmitted over a digital network into packets. Unlike circuit switching, where a dedicated communication path is established, in packet switching, each packet is routed individually based on the destination address it contains.

- **Datagram Approach:** Each packet is treated independently. Packets may take different routes and arrive out of order.
- **Virtual Circuit Approach:** A logical path is established before any packets are sent. All packets follow this path and arrive in order.

3.4.2 IP Addressing

An IP address is a unique numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication. An IPv4 address is a 32-bit number, typically represented in dotted-decimal notation (e.g., 192.168.1.1). It is divided into a Network ID (which identifies the specific network) and a Host ID (which identifies the specific device on that network). Originally, IP addresses were divided into classes (Class A, B, C, D, and E) based on the number of bits allocated to the network and host portions.

3.4.3 CIDR and NAT

As the internet grew, the classful addressing scheme became inefficient.

- **Classless Inter-Domain Routing (CIDR):** A method of allocating IP addresses that replaces the older system based on classes A, B, and C. CIDR uses a suffix to indicate the number of network bits (e.g., 192.168.1.0/24), allowing for variable-length subnet masking (VLSM) and much more efficient allocation of IP space.
- **Network Address Translation (NAT):** A technique used to translate private IP addresses within a local network to a single public IP address (or a pool of public addresses) before routing the traffic to the internet. NAT helps conserve the limited pool of IPv4 addresses and provides a level of security by hiding internal network structures.

3.4.4 IP Layer Protocols

Several key protocols operate at the network layer to support IP communication:

- **ICMP (Internet Control Message Protocol):** Used by network devices, like routers, to send error messages and operational information (e.g., a requested service is not available or a host could not be reached). The `ping` utility uses ICMP.
- **ARP (Address Resolution Protocol):** Maps an IP address (logical) to a MAC address (physical) on a local network.
- **RARP (Reverse Address Resolution Protocol):** Maps a MAC address to an IP address (obsolete, largely replaced by DHCP).
- **DHCP (Dynamic Host Configuration Protocol):** Dynamically assigns an IP address and other network configuration parameters to each device on a network, so they can communicate with other IP networks.
- **BOOTP (Bootstrap Protocol):** An earlier protocol used to automatically assign IP addresses; DHCP is built upon BOOTP but offers more advanced dynamic IP leasing.

3.4.5 IPv4 and IPv6 Comparison

IPv6 was developed to address the exhaustion of IPv4 addresses.

- **Address Size:** IPv4 uses 32-bit addresses (allowing approx. 4.3 billion addresses). IPv6 uses 128-bit addresses, offering a virtually unlimited address space.
- **Representation:** IPv4 is represented in dotted-decimal format (e.g., 192.168.1.1). IPv6 is represented in hexadecimal format separated by colons (e.g., `2001:0db8:85a3:0000:0000:8a2e:0370:7334`).
- **Header Complexity:** IPv4 has a variable-length header with a minimum of 20 bytes. IPv6 has a fixed-length header of 40 bytes, simplifying processing by routers.
- **Security:** IPsec is optional in IPv4 but built-in and mandatory in IPv6, ensuring greater security.
- **Configuration:** IPv4 relies heavily on manual configuration or DHCP. IPv6 supports stateless address autoconfiguration (SLAAC), allowing hosts to generate their own IP addresses automatically.

Methodology:

Key Takeaways for Data Link and Network Layers 1. The Data Link Layer handles node-to-node delivery, framing, and MAC addressing. 2. The Network Layer handles host-to-host delivery, logical (IP) addressing, and routing. 3. CIDR and NAT were introduced to extend the life of IPv4 before the full transition to IPv6. 4. Protocols like ARP and ICMP are essential for the proper functioning and troubleshooting of IP networks.

CHAPTER 4

Transport and Application Layers

4.1 Transport Layer

The transport layer is responsible for end-to-end communication between application processes. It provides services such as multiplexing, demultiplexing, reliable data transfer, flow control, and congestion control.

4.1.1 Elements of Transport Protocols

The transport layer utilizes specific protocols to ensure that data packets are correctly delivered from a source process to a destination process. The two primary protocols used at this layer in the Internet protocol suite are the Transmission Control Protocol (TCP) and the User Datagram Protocol (UDP).

Transmission Control Protocol (TCP)

TCP is a connection-oriented, reliable transport protocol. It provides features that guarantee the delivery of packets in the correct order.

- **Connection-oriented:** A connection must be established before data can be transferred (the three-way handshake).
- **Reliable delivery:** It uses acknowledgments, sequence numbers, and retransmissions to ensure no data is lost.
- **Flow control:** It uses a sliding window mechanism to prevent the sender from overwhelming the receiver.
- **Congestion control:** It throttles the transmission rate when it detects network congestion.

Methodology:

TCP Three-Way Handshake The process of establishing a TCP connection involves three steps:

1. **SYN:** The client sends a segment with the SYN (Synchronize) flag set to the server.
2. **SYN-ACK:** The server responds with a segment that has both the SYN and ACK (Acknowledgment) flags set.
3. **ACK:** The client acknowledges the server's SYN by sending an ACK segment. The connection is now established.

User Datagram Protocol (UDP)

UDP is a connectionless, unreliable transport protocol. It provides a simple mechanism for sending datagrams with minimal overhead.

- **Connectionless:** No connection establishment is required before sending data.
- **Unreliable delivery:** There are no guarantees that the data will reach its destination or arrive in the correct order.

- **No flow or congestion control:** It sends data as fast as the application generates it, regardless of the network or receiver's state.
- **Low overhead:** Because it lacks the complex mechanisms of TCP, UDP has a smaller header (8 bytes compared to TCP's 20 bytes) and less processing delay.

4.1.2 Connection-Oriented vs Connectionless Services

- **Connection-Oriented Service:** Requires a session to be established before communication can begin. It is analogous to a telephone call. It is typically reliable and orderly. Example: TCP.
- **Connectionless Service:** Does not require a pre-established session. Each packet is treated independently and can take different paths to the destination. It is analogous to sending a letter via postal mail. It is typically faster but unreliable. Example: UDP.

Worked Example:

Choosing Between TCP and UDP A developer is creating a video streaming application and a file transfer application. Which transport protocols should be used?
Solution:

- For the **video streaming application**, UDP is preferred. Video streaming can tolerate some lost frames, but it requires continuous, real-time data flow. TCP's retransmissions would cause unacceptable delays (buffering).
- For the **file transfer application**, TCP is required. A file must be transferred completely and accurately. Any lost packets must be retransmitted to ensure the file is intact upon reception.

4.2 Application Layer: Domain Name System (DNS)

The Application Layer contains the protocols that provide specific network services to user applications. One of the most critical services is the Domain Name System (DNS).

DNS is a hierarchical, decentralized naming system for computers, services, or other resources connected to the Internet or a private network. It translates easily memorized domain names (like `www.google.com`) to the numerical IP addresses (like `142.250.190.46`) needed for locating and identifying computer services and devices with the underlying network protocols.

4.2.1 How DNS Works

1. **DNS Resolver:** The client machine asks the DNS resolver (usually provided by the ISP) to find the IP address for a domain name.
2. **Root Name Server:** If the resolver doesn't have the IP address cached, it queries a root name server.
3. **TLD Name Server:** The root server directs the resolver to a Top-Level Domain (TLD) server (e.g., the server responsible for `.com` or `.org`).
4. **Authoritative Name Server:** The TLD server directs the resolver to the authoritative name server for the specific domain, which holds the actual IP address record.

4.3 Internet Services

The application layer provides various services that allow users to interact with the Internet.

4.3.1 World Wide Web (WWW)

The World Wide Web is an information system where documents and other web resources are identified by Uniform Resource Locators (URLs), which may be interlinked by hyperlinks, and are accessible over the Internet.

Web Browser

A web browser is a software application for accessing information on the World Wide Web. When a user requests a web page from a particular website, the web browser retrieves the necessary content from a web server and then displays the page on the user's device. Popular examples include Google Chrome, Mozilla Firefox, and Apple Safari.

HyperText Markup Language (HTML)

HTML is the standard markup language for documents designed to be displayed in a web browser. It defines the structure and meaning of web content. HTML elements are the building blocks of HTML pages, represented by tags (like `<h1>`, `<p>`, `<a>`).

4.4 Electronic Mail

Electronic mail (email) is a method of exchanging digital messages between people using digital devices.

4.4.1 Functions of an Email System

An email system must perform several key functions:

- **Composition:** Creating the message and addressing it.
- **Transfer:** Moving the message from the sender to the recipient's mail server.
- **Reporting:** Providing confirmation of delivery or notification of failure.
- **Displaying:** Allowing the user to read incoming messages.
- **Disposition:** Saving, deleting, or forwarding messages.

4.4.2 User Agent and Message Format

- **User Agent (UA):** A software program that allows users to read, reply to, forward, save, and compose emails. Examples include Microsoft Outlook, Mozilla Thunderbird, and web-based interfaces like Gmail.
- **Message Format:** An email message consists of an envelope (used for routing) and the content. The content is divided into a header (containing fields like To, From, Subject, Date) and a body (the actual message).

4.4.3 Mail Protocols

Several protocols are involved in sending and receiving emails.

- **Simple Mail Transfer Protocol (SMTP):** Used for sending emails from the sender's mail client to the mail server, and between mail servers. It relies on TCP port 25 (or 587 for encrypted submission).
- **Post Office Protocol version 3 (POP3):** Used by local email clients to retrieve emails from a remote server. It typically downloads the emails to the local device and deletes them from the server. It uses TCP port 110.

4.5 Other Application Layer Protocols

4.5.1 File Transfer Protocol (FTP)

FTP is a standard network protocol used for the transfer of computer files between a client and server on a computer network. It is built on a client-server model architecture using separate control and data connections between the client and the server. FTP uses TCP port 21 for the control connection and port 20 for the data connection.

4.5.2 Remote Login (Telnet and SSH)

Remote login allows a user to access and control a remote computer over a network just as if they were sitting at the remote computer's keyboard.

- **Telnet:** An older protocol that sends data, including passwords, in plain text. It is considered insecure.
- **Secure Shell (SSH):** A cryptographic network protocol for operating network services securely over an unsecured network. It provides a secure channel over an unsecured network.

4.6 Voice and Video over IP

Voice over Internet Protocol (VoIP) and Video over IP refer to the delivery of voice and multimedia communications over Internet Protocol (IP) networks, such as the Internet.

- Instead of using traditional circuit-switched networks (like the public switched telephone network, PSTN), VoIP converts analog voice signals into digital data packets and transmits them over a packet-switched network.
- **Challenges:** Real-time communications are highly sensitive to delay, jitter, and packet loss.
- **Protocols Used:**
  - **Real-Time Transport Protocol (RTP):** Used for delivering audio and video over IP networks. It typically runs over UDP.
  - **Session Initiation Protocol (SIP):** A signaling protocol used for initiating, maintaining, and terminating real-time sessions that include voice, video, and messaging applications.

Methodology:

VoIP Process The basic steps involved in a VoIP call are:

1. **Signaling:** Establish the call connection between the caller and the receiver using protocols like SIP.
2. **Encoding:** The analog voice signal is converted into a digital format using an audio codec.
3. **Packetization:** The digital data is broken down into IP packets.
4. **Transmission:** The packets are sent over the IP network, typically using RTP over UDP.
5. **Decoding and Playback:** The receiver reassembles the packets, decodes the digital data back into an analog signal, and plays the audio.

CHAPTER 5
Network Security

5.1 Introduction to Network Security and Cryptography

Network security is a broad term that covers a multitude of technologies, devices, and processes. In its simplest term, it is a set of rules and configurations designed to protect the integrity, confidentiality, and accessibility of computer networks and data using both software and hardware technologies.

5.1.1 Need for Network Security

With the exponential growth of the Internet, virtually every organization relies heavily on their network to perform daily operations. An insecure network can lead to data breaches, loss of sensitive information, financial loss, and damage to the organization's reputation.

5.1.2 Cryptography

Cryptography is the mathematical foundation of data security. It provides mechanisms for ensuring data confidentiality, integrity, authentication, and non-repudiation.

Methodology:

Types of Cryptography There are primarily three types of cryptographic techniques used in network security:

1. **Symmetric Key Cryptography**: The sender and receiver share a single, common key that is used for both encryption and decryption. Examples include AES and DES.
2. **Asymmetric Key Cryptography**: Also known as Public Key Cryptography. It uses a pair of keys: a public key for encryption and a private key for decryption. Examples include RSA and ECC.
3. **Hash Functions**: These do not use keys but instead use a mathematical algorithm to convert data into a fixed-length string of characters, ensuring data integrity. Examples include SHA-256 and MD5.

Worked Example:

Understanding Caesar Cipher Shift The Caesar Cipher is one of the simplest and most widely known encryption techniques. It is a type of substitution cipher in which each letter in the plaintext is replaced by a letter some fixed number of positions down the alphabet.
Suppose the plaintext is `SECURITY` and the shift is 4. Find the ciphertext.
Solution: We shift each letter in `SECURITY` forward by 4 positions in the alphabet:

- S $\rightarrow$ W
- E $\rightarrow$ I
- C $\rightarrow$ G
- U $\rightarrow$ Y
- R $\rightarrow$ V

- I → M
- T → X
- Y → C (wrapping around the alphabet)

Thus, the resulting ciphertext is `WIGYVMXC`.

5.2 Security Topologies

Network security topology refers to the physical and logical design of a network with security as the primary objective. Proper zoning and segregation of network resources are fundamental to a defense-in-depth strategy.

5.2.1 Security Zones and DMZ

Security zones segment the network into isolated areas based on the trust level of the devices and data within them. A Demilitarized Zone (DMZ) is a perimeter network that protects an organization's internal local-area network (LAN) from untrusted traffic. The DMZ acts as a buffer zone between the public Internet and the private Intranet. Services that are accessible from the Internet, such as Web servers, Mail servers, and DNS servers, are typically placed in the DMZ.

5.2.2 Internet and Intranet

- **Internet**: The global system of interconnected computer networks. From a security perspective, it is the most untrusted zone.
- **Intranet**: A private enterprise network, designed to securely share company information and computing resources among employees. It is highly trusted.

5.2.3 VLAN and Security Implications

A Virtual Local Area Network (VLAN) creates logically segmented networks within a single physical network infrastructure. By placing different departments (e.g. HR, Finance, IT) into separate VLANs, network administrators can control broadcast domains and apply security access control lists (ACLs) to restrict inter-VLAN communication, significantly reducing the attack surface.

5.2.4 Tunnelling

Tunnelling is the process by which VPNs encapsulate one network protocol within another network protocol to transfer data across a public network securely.

Methodology:

Tunnelling Process To understand how tunnelling works, consider the following steps:

- **Encapsulation**: The original data packet (payload) is wrapped with a new header. This new header contains the routing information for the public network.
- **Transmission**: The encapsulated packet travels across the untrusted network (like the Internet).
- **Decapsulation**: Once the packet reaches its destination, the outer header is removed, and the original packet is delivered to the internal network.

Often, the payload is also encrypted to prevent eavesdropping during transmission.

5.3 IP Security (IPsec)

IPsec (Internet Protocol Security) is a framework of open standards for ensuring private, secure communications over Internet Protocol (IP) networks through the use of cryptographic security services.

5.3.1 Overview and Architecture

IPsec provides security at the Network Layer (Layer 3) of the OSI model. It can protect any protocol that runs on top of IP, such as TCP and UDP.

The IPsec architecture consists of three main protocols:

1. **Authentication Header (AH)**: Provides data integrity, data origin authentication, and an optional anti-replay service. It does not provide data confidentiality (encryption).
2. **Encapsulating Security Payload (ESP)**: Provides confidentiality (encryption), in addition to the services provided by AH.
3. **Internet Key Exchange (IKE)**: A protocol used to securely exchange keys and negotiate security associations (SAs) between communicating parties.

5.3.2 Configuration

IPsec can be configured to operate in two modes:

- **Transport Mode**: Only the payload (the data) of the IP packet is encrypted and/or authenticated. The original IP header remains intact. This mode is typically used for host-to-host communications.
- **Tunnel Mode**: The entire original IP packet (both payload and header) is encrypted and authenticated. A new IP header is added for routing over the internet. This mode is typically used for network-to-network communications (e.g. between two routers to form a VPN).

5.4 Virtual Private Network (VPN)

A Virtual Private Network (VPN) extends a private network across a public network. It enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

VPNs are widely used by corporate employees to securely connect to the corporate network from remote locations. They ensure confidentiality and integrity of data by creating an encrypted tunnel for the data to pass through.

Worked Example:

Difference between Intranet and VPN Many students confuse an Intranet with a VPN. Describe the key differences.

Solution: An Intranet is a private network that is contained within an enterprise and is normally accessible only to members of the organization while they are physically on the premises.

A VPN, on the other hand, is a technology that creates a secure, encrypted connection over a less secure network (like the Internet). A VPN is often used to provide remote employees with secure access to the company's Intranet when they are not physically in the office.

5.5 Email Security

Email security involves protecting email accounts, contents, and communications against unauthorized access, loss, or compromise.

5.5.1 Email Security Standards

Standard email protocols like SMTP (Simple Mail Transfer Protocol), POP3, and IMAP were designed without security in mind. Therefore, various standards have been developed to secure email communications:

- **Working principles of SMTP**: SMTP handles the sending of emails. By default, it transmits data in plaintext. STARTTLS is an extension to SMTP that upgrades a plaintext connection to a secure encrypted connection (TLS or SSL).
- **PEM (Privacy Enhanced Mail)**: An early standard proposed by the IETF to provide secure email over the internet, utilizing cryptographic techniques for confidentiality and authentication.
- **PGP (Pretty Good Privacy)**: A data encryption and decryption computer program that provides cryptographic privacy and authentication. PGP is widely used for signing, encrypting, and decrypting texts and emails.
- **S/MIME (Secure/Multipurpose Internet Mail Extensions)**: A widely accepted method for sending digitally signed and encrypted messages. S/MIME allows the sender to mathematically sign a message, providing authentication, message integrity, and non-repudiation.

5.5.2 Spam

Spam refers to unsolicited bulk email. Apart from being a nuisance, spam is a significant security threat as it is commonly used as a delivery mechanism for malware, phishing attacks, and scams. Implementing spam filters, SPF (Sender Policy Framework), DKIM (DomainKeys Identified Mail), and DMARC (Domain-based Message Authentication, Reporting, and Conformance) helps in verifying the sender's identity and reducing spam.

5.6 Information Security Standards

To establish a baseline for security practices, organizations follow established information security standards and comply with relevant cyber laws.

5.6.1 ISO Standards

The ISO/IEC 27000 series (also known as the ISMS Family of Standards) helps organizations keep information assets secure.

- **ISO/IEC 27001**: Specifies the requirements for establishing, implementing, maintaining, and continually improving an Information Security Management System (ISMS).
- **ISO/IEC 27002**: Provides a code of practice for information security controls, serving as a reference point for selecting controls within the process of implementing an ISMS.

5.6.2 Cyber Laws in India

Cyber laws provide a legal framework for addressing cybercrimes, electronic commerce, and digital signatures.

- **Copyright Act**: Protects intellectual property rights, including software, digital content, and databases, against unauthorized reproduction and distribution.

5.6.3 IT Act 2000 Provisions and Latest Amendments

The Information Technology Act, 2000, is the primary law in India dealing with cybercrime and electronic commerce.

- **Provisions**: It provides legal recognition for transactions carried out by means of electronic data interchange. It defines offenses such as tampering with computer source documents, hacking with computer systems, and publishing obscene information in electronic form.

- **Amendments**: The Information Technology (Amendment) Act, 2008, introduced comprehensive changes, including definitions for cyber terrorism, data protection provisions (Section 43A), and the establishment of the Indian Computer Emergency Response Team (CERT-In).

5.7 Social Issues, Hacking and Precautions

5.7.1 Social Issues

The pervasive nature of the Internet has led to several social issues:

- **Privacy Loss**: Extensive tracking and data collection by websites and applications compromise user privacy.
- **Cyberbullying and Harassment**: The anonymity of the internet facilitates abusive behavior.
- **Misinformation**: Fake news and rumors spread rapidly across social media platforms, potentially causing social unrest.

5.7.2 Hacking

Hacking is the act of identifying and exploiting vulnerabilities in a computer system or network to gain unauthorized access to data.

- **Ethical Hackers (White Hats)**: Security professionals who use their skills to identify and patch vulnerabilities legally and ethically.
- **Malicious Hackers (Black Hats)**: Individuals who hack into systems for personal gain, malice, or disruption.

5.7.3 Precautions

To mitigate security risks, users and organizations should adopt the following precautions:

Methodology:

Best Practices for Network Security

1. **Regular Updates**: Keep operating systems, applications, and firmware updated with the latest security patches.
2. **Robust Authentication**: Use strong, unique passwords and enable Multi-Factor Authentication (MFA) wherever possible.
3. **Network Defense Tools**: Deploy firewalls, Intrusion Detection Systems (IDS), and Intrusion Prevention Systems (IPS) to monitor and filter network traffic.
4. **Antivirus and Anti-malware**: Install and maintain updated security software to detect and remove malicious code.
5. **User Education**: Conduct regular security awareness training to educate users about phishing, social engineering, and safe browsing practices.
6. **Data Backup**: Maintain regular, encrypted backups of critical data, ideally following the 3-2-1 backup rule (3 copies, 2 different media, 1 offsite).

Appendix: Key Formulae

This appendix provides a quick reference to the key formulae and mathematical relationships discussed in this book.

Unit 1: Networking Basics

- **Propagation Delay (D_{prop}):** The time it takes for a signal to travel from the sender to the receiver.

$$D_{prop} = \frac{d}{s}$$

  where d is the distance and s is the propagation speed.

- **Transmission Delay (D_{trans}):** The time required to push all the packet's bits into the link.

$$D_{trans} = \frac{L}{R}$$

  where L is the packet length and R is the transmission rate.

- **Total Nodal Delay (D_{total}):** The total delay experienced by a packet at a single node.

$$D_{total} = D_{proc} + D_{queue} + D_{trans} + D_{prop}$$

  where D_{proc} is the processing delay and D_{queue} is the queuing delay.

- **Total Transfer Time (T):** The time taken to transfer a file of size F over a link with a specific throughput.

$$T = \frac{F}{R_{throughput}}$$

- **Throughput ($R_{throughput}$):** In a network with multiple links in series, the end-to-end throughput is determined by the bottleneck link.

$$R_{throughput} = \min(R_1, R_2, \ldots, R_N)$$

- **Number of Links in a Mesh Topology (L):** The total number of links required for a fully connected mesh topology with n nodes.

$$L = \frac{n(n-1)}{2}$$

- **Ports per Node in a Mesh Topology (P):** The number of ports required on each node for a fully connected mesh network with n nodes.

$$P = n - 1$$

Unit 3: Data Link Layer

- **Link Utilization / Efficiency (η):** Efficiency of a sliding window protocol (like Go-Back-N or Selective Repeat).

$$\eta = \frac{W}{1 + 2a}$$

  where W is the window size and a is the ratio of propagation delay to transmission delay ($a = \frac{D_{prop}}{D_{trans}}$).

Unit 4: Transport and Application Layers

- **Bandwidth-Delay Product (BDP):** The maximum amount of data that can be in transit over the network.
$$BDP = \text{LinkBandwidth} \times \text{RTT}$$
- **Optimal Window Size:** To fully utilize a link, the window size should equal the BDP.
$$\text{OptimalWindowSize} = BDP$$
- **Throughput:** The effective rate of data transfer based on the window size and Round Trip Time (RTT).
$$\text{Throughput} = \frac{\text{WindowSize}}{\text{RTT}}$$
- **Link Utilization:** The percentage of the link's bandwidth that is being actively used.
$$\text{Utilization} = \frac{\text{Throughput}}{\text{LinkBandwidth}} \times 100\%$$
- **TCP Estimated Round Trip Time (EstimatedRTT):** An exponentially weighted moving average of sampled RTTs.
$$\text{EstimatedRTT} = (1 - \alpha) \times \text{EstimatedRTT} + \alpha \times \text{SampleRTT}$$
- **TCP RTT Deviation (DevRTT):** The estimated deviation of the SampleRTT from the EstimatedRTT.
$$\text{DevRTT} = (1 - \beta) \times \text{DevRTT} + \beta \times |\text{SampleRTT} - \text{EstimatedRTT}|$$
- **TCP Timeout Interval:** The calculated time to wait before retransmitting a packet.
$$\text{TimeoutInterval} = \text{EstimatedRTT} + 4 \times \text{DevRTT}$$
- **Total Time for Non-Persistent HTTP:** The total time required to fetch N objects.
$$\text{Total Time} = N \times (2 \times \text{RTT} + T_t)$$
where T_t is the transmission time of a single object.
- **Total Time for Persistent HTTP (without pipelining):**
$$\text{Total Time} = (2 \times \text{RTT} + T_{t,base}) + (N - 1) \times (1 \times \text{RTT} + T_t)$$
- **Total Time for Persistent HTTP (with pipelining):**
$$\text{Total Time} = (2 \times \text{RTT} + T_{t,base}) + 1 \times \text{RTT} + \sum_{i=1}^{N-1} T_{t,i}$$

Unit 5: Cryptography and Network Security

- **Caesar Cipher Encryption:**
$$C = (P + K) \pmod{26}$$
where C is the ciphertext, P is the plaintext, and K is the key (shift).
- **Caesar Cipher Decryption:**
$$P = (C - K) \pmod{26}$$
- **RSA Encryption:**
$$C = M^e \pmod{n}$$
where M is the message, C is the ciphertext, and (e, n) is the public key.

- **RSA Decryption:**

$$M = C^d \pmod{n}$$

  where d is the private key.

- **Diffie-Hellman Key Exchange:**
  - Public key generation for Alice (A) and Bob (B) using a prime P and base G:

$$A = G^a \pmod{P}$$
$$B = G^b \pmod{P}$$

    where a and b are private keys.
  - Shared secret (S) computation:

$$S = B^a \pmod{P} \quad \text{(calculated by Alice)}$$
$$S = A^b \pmod{P} \quad \text{(calculated by Bob)}$$