MODULE-1: Data Communications & Networks

1. DATA COMMUNICATIONS

Data communication is the process of transferring data from one point to another using a communication system. It involves several essential components and mechanisms to ensure the accurate and timely delivery of data.

1.1.Components

A data communication system includes the following components:

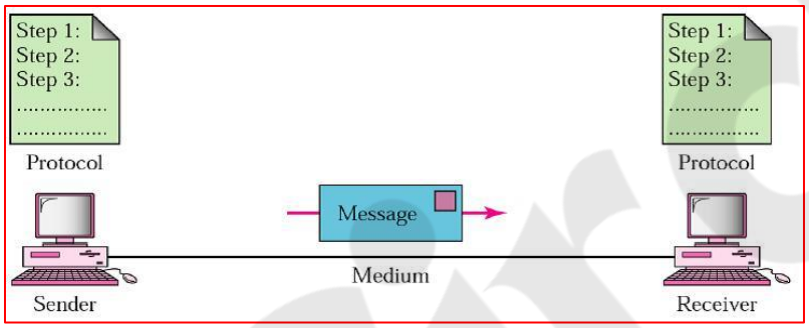

Figure 1.1: A data communications system has five components

1. **Message:** The data or information being communicated (e.g., text, images, audio).
2. **Sender:** The device that sends the message, such as a computer or smartphone.
3. **Receiver:** The device that receives the message, like another computer or a printer.
4. **Transmission Medium:** The physical path through which the data is transmitted, like cables or radio waves.
5. **Protocol:** A set of rules that governs the communication between devices to ensure proper data exchange.

The performance of a data communication system relies on four key characteristics: delivery, accuracy, timeliness, and jitter.

1. **Delivery**: The system must ensure that data reaches the correct destination. Only the intended recipient—whether a device or a user—should receive the data.
2. **Accuracy**: Data must be transmitted without errors. If data is altered during transmission and not corrected, it becomes unusable.
3. **Timeliness**: Data must be delivered promptly. Delayed data, especially in applications like video and audio, lose their value. For real-time transmission, data must be delivered in the same sequence and without significant delays.

4. **Jitter**: Jitter refers to the inconsistency in packet arrival times. Inconsistent delays, such as video packets arriving at varying intervals, can degrade the quality of the audio or video. For instance, if video packets are sent every 30 ms, but some arrive after 40 ms, the video quality will be affected.

1.2. Data Representation

Data can be represented in various forms to suit the type of communication. Common types of data representation include:

- **Text**: Represented as a sequence of bits using encoding systems like ASCII or Unicode.
- **Numbers**: Represented directly in binary form, which allows for efficient computation and transmission.
- **Images**: Represented as a matrix of pixels, where each pixel is assigned a bit pattern based on the image's color or intensity. Color images often use RGB (Red, Green, Blue) or YCM (Yellow, Cyan, Magenta) encoding.
- **Audio**: Audio data is captured as a continuous signal, which can be sampled and digitized for transmission.
- **Video**: A sequence of images or frames is used to convey motion, with each frame represented as individual bit patterns.

1.3. Data Flow

Data flow refers to the manner in which data is transmitted between two devices. It can happen in three modes:

1. **Simplex**: Data flows in one direction only, like a keyboard sending data to a computer (one-way communication).
2. **Half-Duplex**: Both devices can send and receive data, but not at the same time. For example, a walkie-talkie allows communication in both directions, but one at a time.
3. **Full-Duplex**: Both devices can transmit and receive data simultaneously, like in a phone conversation where both parties can speak and listen at the same time.

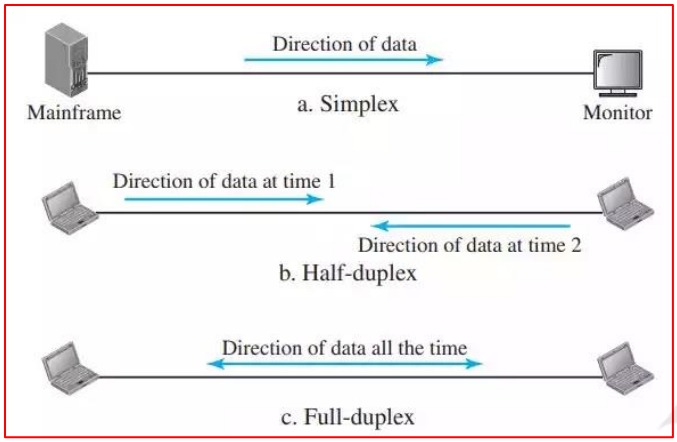

Figure 1.2: Data flow (simplex, half-duplex, and full-duplex)

2. NETWORKS

A network refers to the interconnection of a set of devices capable of communication. These devices can include hosts such as computers, smartphones, and security systems, as well as connecting devices like routers, switches, and modems. Networks are connected through transmission media, either wired (like cables) or wireless (like air).

2.1.Network Criteria

Networks must meet several essential criteria to be effective, namely:

1. **Performance**: This is evaluated by:
    - **Transit time**: Time for a message to travel between two devices.
    - **Response time**: Time between sending a request and receiving a response. Factors influencing performance include the number of users, the transmission medium, hardware capabilities, and software efficiency. Key metrics include:
    - **Throughput**: Amount of data transmitted successfully.
    - **Delay**: Time taken for data to reach its destination. Optimizing both often leads to trade-offs.
2. **Reliability**: This includes:
    - Accuracy in data delivery.
    - Frequency and recovery time from network failures.
    - The network's ability to function during a catastrophe.
3. **Security**: It encompasses protecting data from unauthorized access, damage, or corruption and establishing recovery procedures for security breaches.

2.2. Physical Structures

Networks can be categorized by their **connection types** and **topologies**:

1. **Type of Connection**:
    - **Point-to-Point**: A direct link between two devices, providing the full capacity of the link for communication (e.g., remote control to TV).
    - **Multipoint (Multidrop)**: Multiple devices share a single link, either spatially (simultaneous use) or temporally (taking turns).

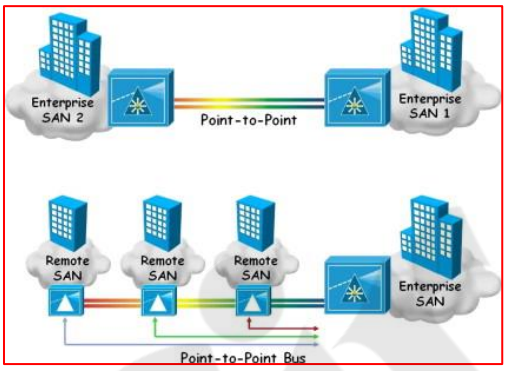

Figure 1.3: Types of connections: point-to-point and multipoint

2. **Physical Topology**: Refers to how devices are physically arranged in a network. Four main topologies include:
    - **Mesh Topology**:
        - Every device is connected to every other device, requiring $n(n-1)/2$ links for n devices.
        - Node 1 must be connected to n – 1 nodes, node 2 must be connected to n – 1 nodes, and finally node n must be connected to n – 1 nodes. We need n (n – 1) physical links. However, if each physical link allows communication in both directions (duplex mode), we can divide the number of links by 2. In other words, we can say that in a mesh topology, we need n (n – 1) / 2 duplex-mode links.
        - Advantages: Dedicated links, fault isolation, robust, secure.
        - Disadvantages: Expensive, complex installation, excessive cabling.
        - Example: Telephone networks between regional offices.

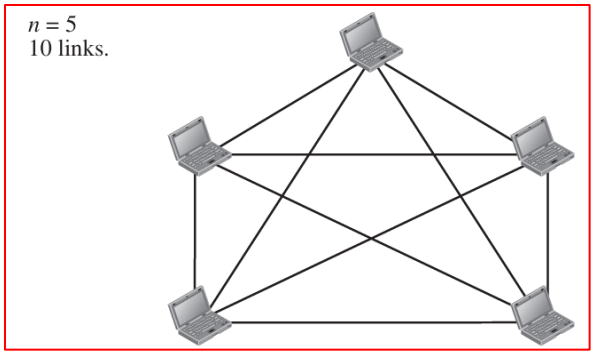

Figure 1.4 A fully connected mesh topology (five devices)

- **Star Topology**:
  - Each device is connected to a central hub, which manages communication.
  - Advantages: Easy installation and fault isolation; if a link fails, only that device is affected.
  - Disadvantages: Entire system fails if the hub goes down.
  - Common in local area networks (LANs).

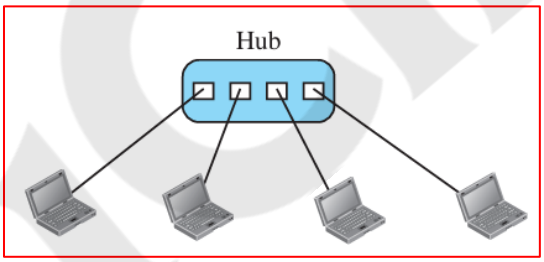

Figure 1.5: A star topology connecting four stations

- **Bus Topology**:
  - All devices are connected to a single backbone cable.
  - Advantages: Easy installation, less cabling than mesh.
  - Disadvantages: Difficult to add devices, faults in the backbone disrupt the entire network.
  - Example: Early Ethernet LANs.

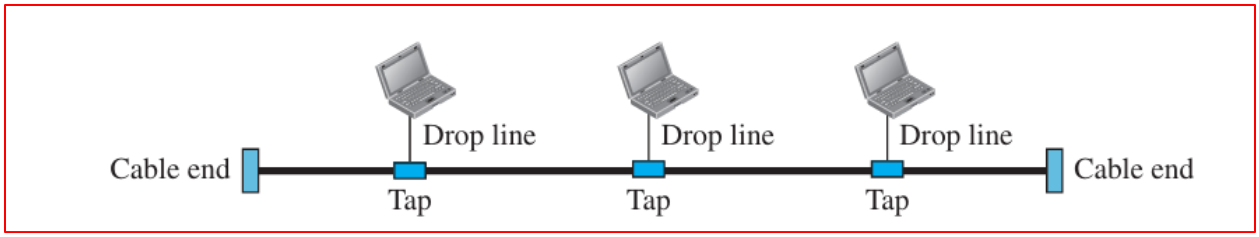

Figure 1.6: A bus topology connecting three stations

- **Ring Topology**:
  - Devices are connected in a loop, with signals traveling in one direction through repeaters.
  - Advantages: Easy to install, simple fault detection.
  - Disadvantages: A break in the ring can disable the entire network, though dual rings or switches can mitigate this.
  - Example: IBM's Token Ring LANs.

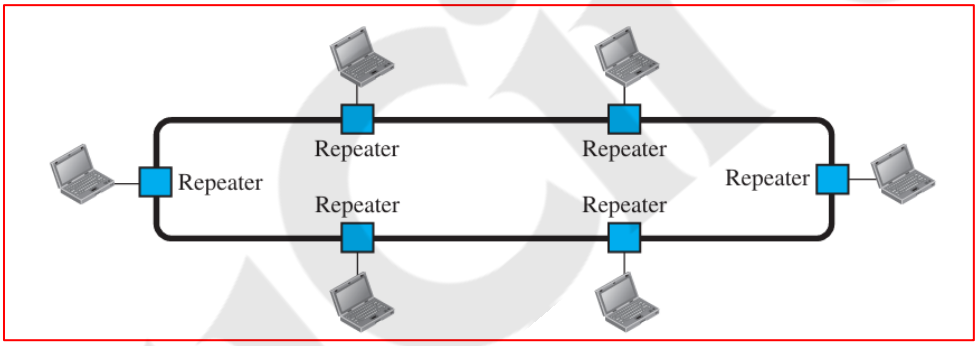

Figure 1.7: A ring topology connecting six stations

3. NETWORK TYPES

Which is used to connect networks to form an internetwork (a network of networks).

3.1.Local Area Network (LAN)

A LAN is a network that connects computers and devices within a small geographical area, such as a home, office, or campus.

Characteristics:

- Covers a limited area.
- High data transfer rates (up to 10 Gbps).
- Typically owned and managed by a single organization.

Examples: Ethernet networks, Wi-Fi networks in homes and small offices.

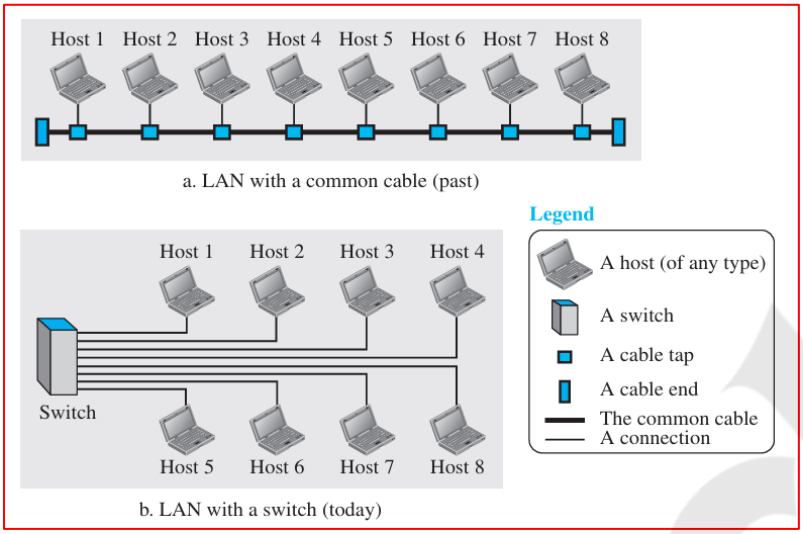

Figure 1.8: An isolated LAN in the past and today

LAN Setup:

- **Common Cable Connection**: In the past, all hosts within a Local Area Network (LAN) were connected via a single common cable.
    - **Packet Transmission**: When one host sent a packet to another, it was broadcast to all hosts on the network.
    - **Packet Filtering**: The intended recipient would accept the packet, while all other hosts would drop it.
    - **Drawback**: This method created significant network congestion, as every packet was visible to all hosts, even when they weren't the intended recipient.

Modern LAN Setup:

- **Switch-Based LAN**: Today, most LANs use **smart switches** to handle packet delivery.
    - **Address Recognition**: A switch is intelligent enough to recognize the destination address of each packet.
    - **Selective Packet Forwarding**: Instead of broadcasting packets to all hosts, the switch sends the packet directly to the destination host.
    - **Benefits**:
        - **Reduced Traffic**: Since packets are only sent to the intended recipient, overall network traffic is significantly reduced.
        - **Simultaneous Communication**: More than one pair of hosts can communicate simultaneously as long as they have different source and destination addresses. This improves network efficiency.

LAN Capacity:

- **Flexibility**: The term "LAN" does not specify any constraints on the number of hosts. A LAN can accommodate a wide range of host numbers, depending on the network's size and structure.

3.2. Wide Area Network (WAN)

A WAN covers a large geographical area, such as a city, country, or even globally. It connects multiple LANs.
Characteristics:

- Slower data transfer rates than LANs.
- Often managed by multiple entities (e.g., ISPs, governments).
- Utilizes routers and public or private communication links.

Examples: The Internet itself is a WAN, Private networks connecting different company branches.

A point-to-point WAN:

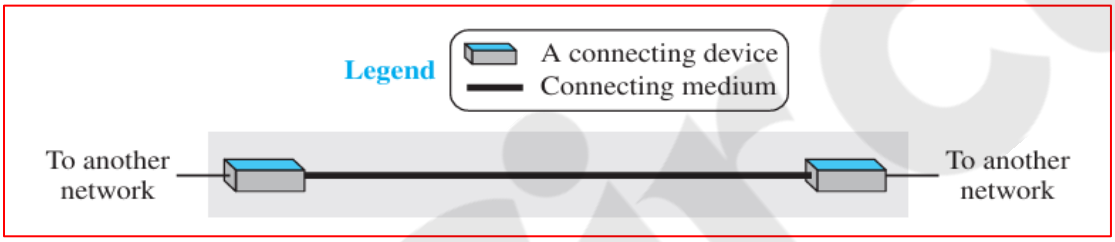

Figure 1.9: A point-to-point WAN

A Point-to-Point WAN is a network that connects two communication devices directly via transmission media, such as cables or wireless links. This type of network allows data transmission between just two endpoints, ensuring a dedicated and private communication link. Used by businesses to link branch offices or remote locations.

Transmission Media:

- **Cable**: Examples include fiber optic, coaxial, or twisted-pair cables.
- **Air**: Wireless links like microwave or satellite connections.

Advantages:

- **Dedicated Line**: Since only two devices share the link, there is minimal congestion and consistent bandwidth.
- **Security**: Limited exposure to external devices reduces the risk of unauthorized access.

A switched WAN:

A switched Wide Area Network (WAN) is a network infrastructure with multiple endpoints that are interconnected. Unlike traditional point-to-point WANs, which only connect two endpoints, a switched WAN allows for dynamic routing between several nodes through switches.

Role in Global Communication: Switched WANs are fundamental in the backbone of modern global communication systems, facilitating data transfer across vast geographical areas.

- A switched WAN is scalable and can connect many endpoints.
- The switches in the network are responsible for choosing the best path for data to travel.
- It is commonly used in large-scale, high-traffic networks like the internet.

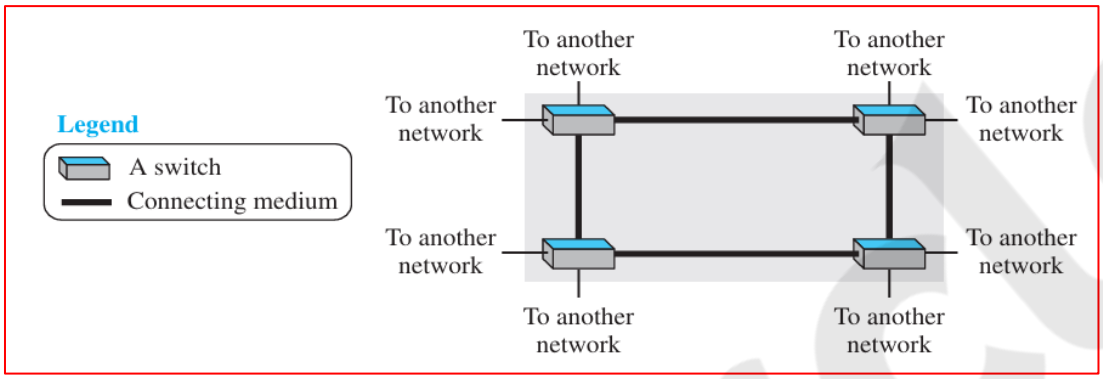

Figure 1.10: A switched WAN

Internetwork

In modern networks, it's uncommon to find a LAN (Local Area Network) or WAN (Wide Area Network) operating independently. Instead, they are often connected. When two or more networks connect, they form an internetwork, or internet.

For example, imagine a company with offices on the east and west coasts. Each office has a LAN where employees can communicate within the office. To allow communication between employees at both locations, the company leases a dedicated WAN connection from a service provider. This WAN links the two LANs, creating an internetwork, or a private internet. Now, employees from both offices can communicate with each other

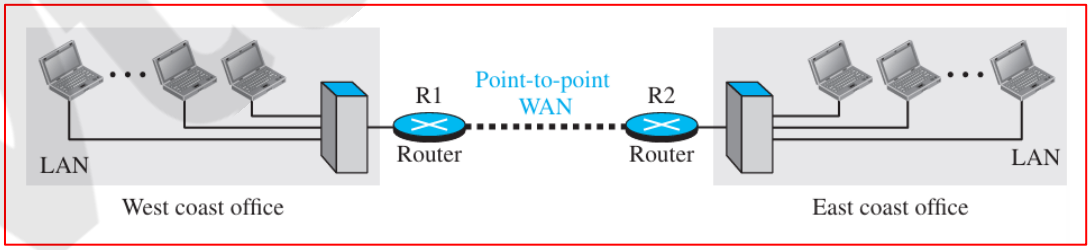

Figure 1.11: An internetwork made of two LANs and one point-to-point WAN

A heterogeneous network

A **heterogeneous network** is a system that connects various types of devices and network architectures. The term "heterogeneous" signifies diversity in the types of networks, which may

include different hardware, operating systems, and communication protocols. When combining WANs and LANs into a heterogeneous network, the WANs provide the backbone for long-distance communication, while the LANs allow for local connectivity.

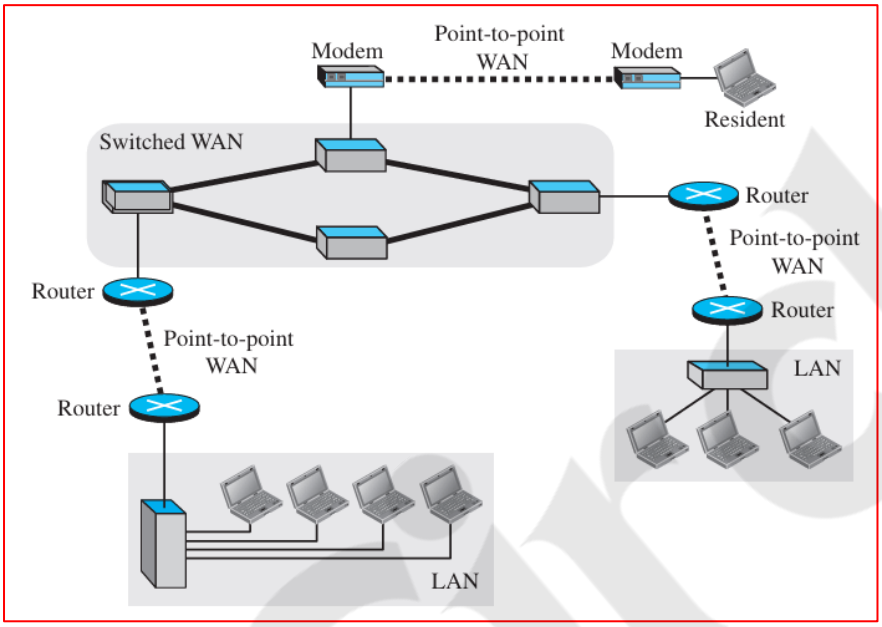

Figure 1.12: A heterogeneous network made of four WANs and three LANs

3.3.Switching

Switching is the process of forwarding data packets in a network from a source to a destination through intermediate devices called switches.
Types of Switching:

1. **Circuit Switching**:

In a circuit-switched network, a fixed connection (circuit) is always available between two devices, like telephones, and it can be activated or deactivated by the network switch.

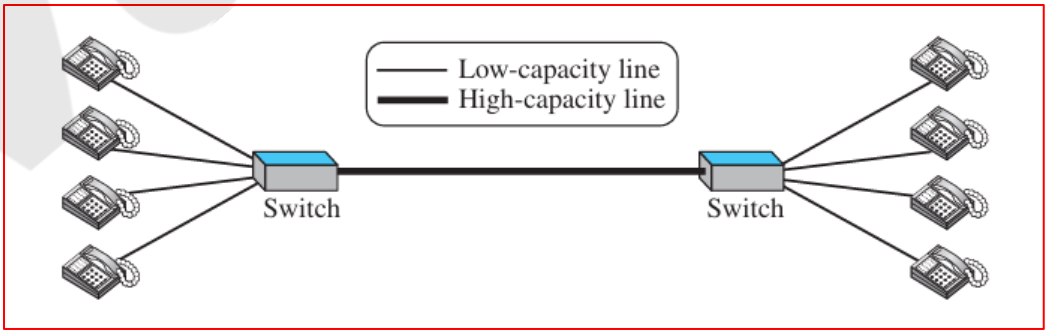

Figure 1.13: A circuit-switched network

Example Figure 1.13

- The network consists of four telephones on each side, connected to a switch.
- When a call is made, the switch connects a phone on one side to a phone on the other side.
- A thick line connects the two switches, with enough capacity to support four simultaneous voice calls. This line's capacity is shared by all phone pairs.

Two Scenarios:

1. **All phones are in use:** Four people on one side are talking to four people on the other side, using the full capacity of the line.
2. **One phone in use:** Only one pair of phones is talking, using only one-quarter of the line's capacity.

Disadvantages: A circuit-switched network is only efficient when operating at full capacity. If fewer devices are active, the unused capacity leads to inefficiency. The thick line needs four times the capacity of a single voice line to prevent call failures when all phones are in use simultaneously.

2. **Packet Switching**:

In a computer network, communication between devices is carried out in blocks of data called **packets**, rather than as continuous streams, as seen in phone calls. These packets are independent units, which makes it possible for network switches to store and forward them later if needed.

Example Figure 1.14

A packet-switched network where two sets of four computers are connected across two sites. In this setup, a router queues the packets and sends them when the network is ready.

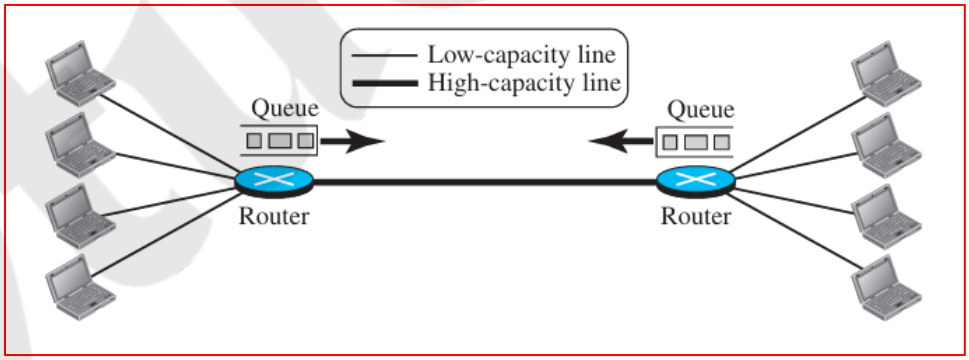

Figure 1.14: A packet-switched network

Consider a scenario where the thick line (the main connection) has twice the capacity of the smaller data lines that connect computers to routers. If only two computers (one from each site) are communicating, the packets move without delay. However, if the thick line is busy and more packets arrive, they are queued and sent in order of arrival.

Disadvantages: This demonstrates the efficiency of packet-switched networks over circuit-switched networks. However, packet-switching can introduce delays when network traffic is heavy.

3. **Message Switching**:
    - Entire messages are stored and forwarded from one switch to another (obsolete in modern networks).

3.4. The Internet

The Internet is a global system of interconnected computer networks that use the TCP/IP protocol to link billions of devices worldwide.
Characteristics:

- Decentralized: No central controlling entity.
- Based on TCP/IP for communication.
- Enables various services such as web browsing, email, file sharing, etc.

Components:

- **Clients**: Devices that request services from servers.
- **Servers**: Systems that provide resources and services to clients.
- **Routers and switches**: Devices that direct data traffic across the network.
- **ISPs (Internet Service Providers)**: Organizations that provide access to the Internet.

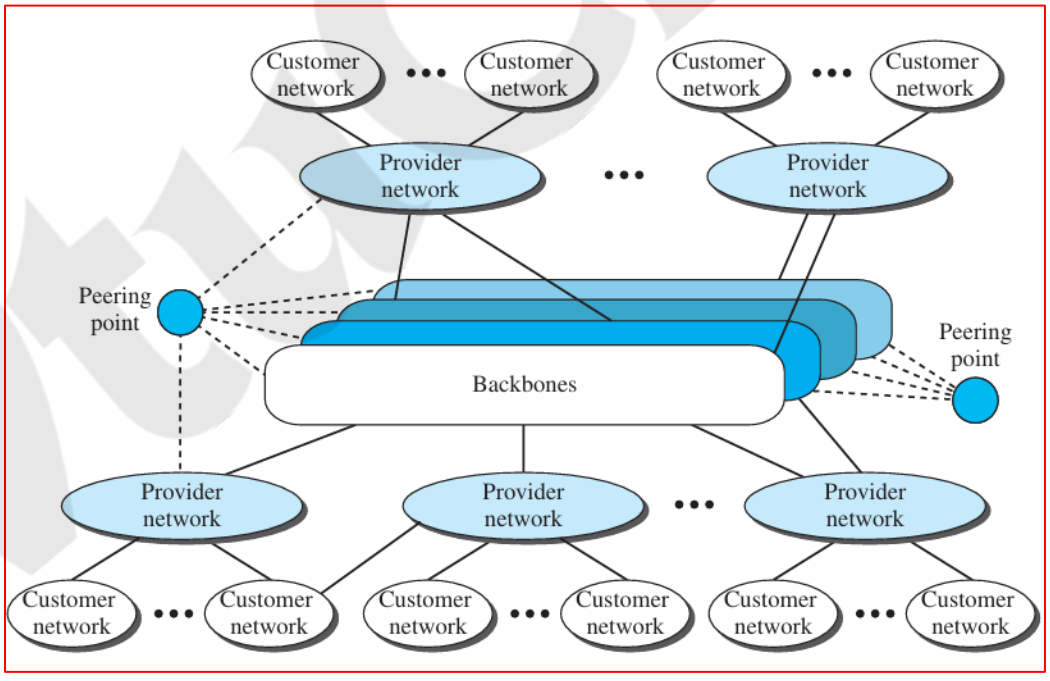

Figure 1.15: The Internet today

3.5. Accessing the Internet

Methods of Access:

1. **Dial-up**:
   - Connects to the Internet using a telephone line.
   - Low-speed, outdated method (up to 56 kbps).
2. **DSL (Digital Subscriber Line)**:
   - Uses telephone lines but allows simultaneous voice and data transmission.
   - Faster than dial-up (up to 100 Mbps).
3. **Cable**:
   - Uses cable television lines to provide high-speed Internet (up to 1 Gbps).
4. **Fiber Optic**:
   - Uses light to transmit data through optical fibers.
   - Extremely high-speed (up to 10 Gbps and beyond).
5. **Satellite**:
   - Provides Internet access via satellite communication, useful in remote areas.
   - Slower than fiber or cable but offers wide coverage.
6. **Mobile Broadband**:
   - Wireless Internet access through cellular networks (3G, 4G, 5G).
   - Widely accessible but may have data limits.
7. **Wi-Fi Access**:

   - Wireless local area networking technology that allows devices to access the Internet within the range of a wireless router.
   - Common in homes, offices, and public places.

4. PROTOCOL LAYERING

Protocol layering is a design principle in computer networks where communication tasks are broken down into multiple layers. Each layer performs a specific function, and the layers work together to enable communication between devices over a network.

4.1. Scenarios

First Scenario: Simple Communication in One Layer

Figure 1.16: A single-layer protocol

In the first scenario, communication is straightforward and occurs in a single layer. Imagine Maria and Ann, who are neighbors and share many common interests. Their interaction happens face-to-face, in the same language, as depicted in Figure 1.16. Despite its simplicity, certain rules govern their communication.

Second Scenario: A three-layer protocol

In this scenario, Ann is offered a promotion requiring her to relocate far from her friend Maria. Despite the distance, they wish to continue their communication to collaborate on an innovative project for their future retirement business. To maintain the confidentiality of their exchange, they decide to use a secure encryption/decryption technique. This technique ensures that their letters remain unreadable to unauthorized individuals.

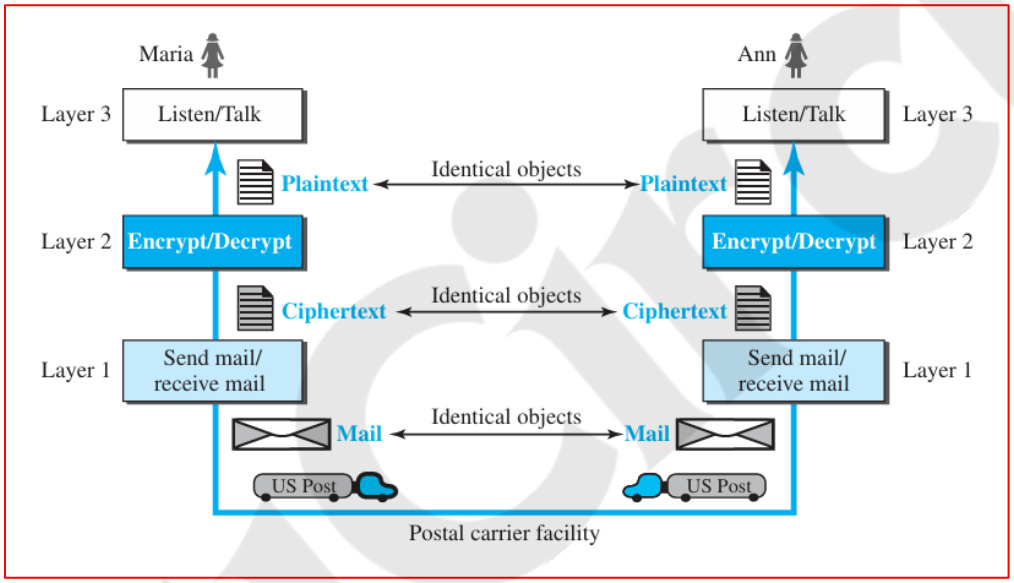

Figure 1.17 A three-layer protocol

The communication between Ann and Maria can be visualized as taking place in three distinct layers:

1. **Third Layer (Plaintext Creation):** Maria speaks to the third-layer machine, which listens and generates the plaintext (the original letter). This plaintext is then handed over to the second-layer machine.
2. **Second Layer (Encryption/Decryption):** The second-layer machine encrypts the plaintext, creating ciphertext (the encrypted letter). This ciphertext is then passed to the first-layer machine.
3. **First Layer (Mailing):** The first-layer machine puts the ciphertext in an envelope, adds the sender's and receiver's addresses, and mails it.

Protocol layering is useful in various scenarios, such as:

- **Data transmission** over the internet where multiple types of data (emails, videos, web pages) are transmitted using different protocols at each layer.
- **Device communication** between a computer and a printer, where layered protocols manage data transfer and error detection.
- **Telecommunication systems**, where layered protocols ensure voice signals are transmitted efficiently and correctly.
- **Multimedia streaming**, where protocols manage data buffering, synchronization, and error correction to deliver seamless audio and video streams.

Advantages of Protocol Layering:

1. **Modularity:** Each layer is independent, allowing for changes in one layer without affecting others. For example, if Ann and Maria decide that the encryption needs to be upgraded, they can replace only the second-layer machine without altering the other layers.
2. **Service Separation:** Protocol layering separates the services from their implementation. Maria could perform the tasks of the first layer herself if needed, as long as she provides the required services.
3. **Intermediate Systems:** In more complex networks, intermediate systems only need to handle specific layers, making the overall system less complex and less expensive.

Disadvantages of Protocol Layering:

1. **Complexity in Layer Integration:** While modularity offers flexibility, it can add complexity. A single machine performing all tasks could simplify the setup, but if there are issues, the entire system might need to be replaced rather than just one layer.

4.2. Principles of Protocol Layering

First Principle: Bidirectional Communication

To achieve bidirectional communication in protocol layering, each layer must be designed to handle two complementary tasks, one for each direction of communication. For example:

Third Layer: Responsible for listening in one direction and transmitting in the other.
Second Layer: Handles encryption in one direction and decryption in the other.
First Layer: Manages sending and receiving mail.

Each layer must be capable of performing its specific function for both incoming and outgoing data.

Second Principle: Identical Objects

In protocol layering, the objects processed by each layer at both communicating sites must be identical. For instance:

Layer 3: The object should be a plaintext letter at both sites.
Layer 2: The object should be a ciphertext letter at both sites.
Layer 1: The object should be a piece of mail at both sites.

Consistency in the objects at each layer ensures proper communication and processing across different layers.

4.3. Logical Connections

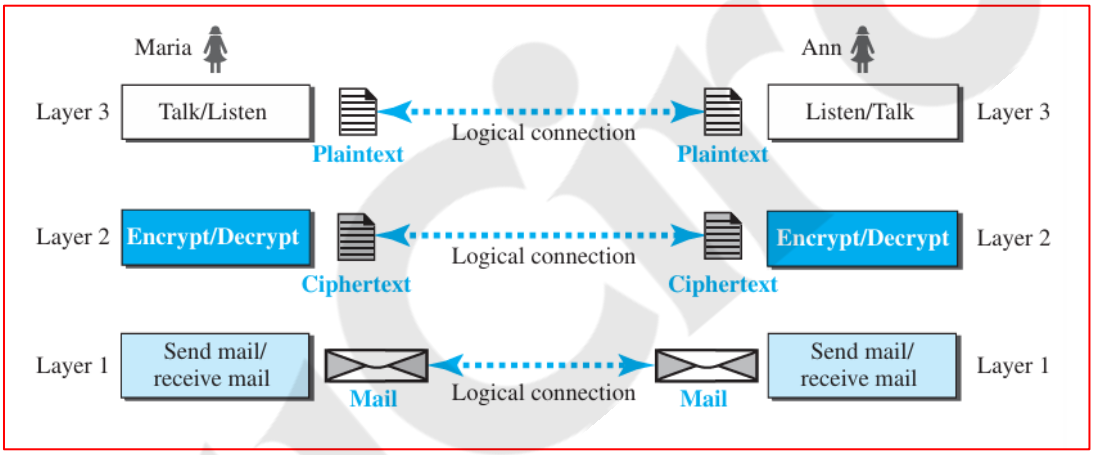

Figure 1.18: Logical connection between peer layers

This means there is communication from one layer to the next. Imagine that Maria and Ann view each layer as having a logical (or imaginary) connection that allows them to transmit objects created at that layer. Understanding these logical connections will enhance your comprehension of layering in data communication and networking.

In a layered model, **logical connections** refer to virtual connections established between the same layers in different devices. For example:

- The application layers of two computers communicate as though they are directly connected, even though physical transmission occurs across multiple lower layers.
- Logical connections provide the abstraction necessary to hide the complexities of the underlying transmission methods, giving the appearance that communication occurs at a single layer.

Logical connections ensure that communication protocols at each layer, such as TCP (Transport Layer) or HTTP (Application Layer), interact correctly without the user needing to understand the intricacies of network transmission.

5. TCP/IP PROTOCOL SUITE

TCP/IP is the protocol suite widely used for communication on the Internet today. It is a collection of protocols organized into different layers, where each layer handles specific tasks, making it easier to manage complex communication processes. TCP/IP is a **hierarchical protocol**, meaning that each higher-level protocol depends on the services provided by one or more lower-level protocols. This layered structure ensures efficient and organized communication across networks. However, today, it is more commonly represented as a **five-layer model**. These layers work together to ensure smooth data transmission over the network.

5.1.Layered Architecture

To understand how the layers in the TCP/IP protocol suite work during communication between two hosts, let's consider a small network composed of three local area networks (LANs), each connected by a link-layer switch. These LANs are also interconnected through a router. Figure 1.20 illustrates this setup.

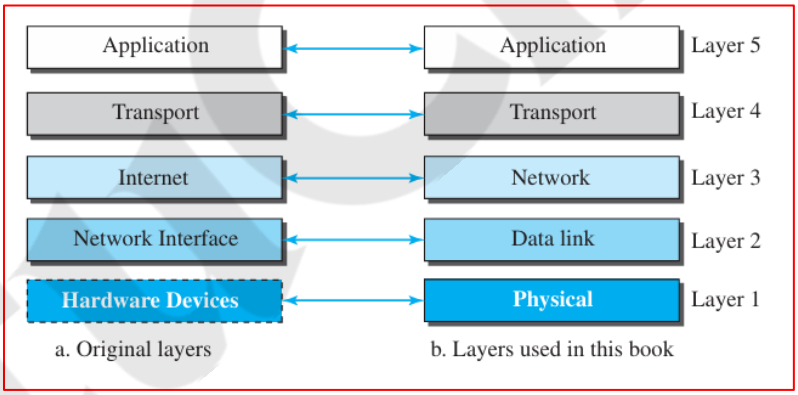

Figure 1.19: Layers in the TCP/IP protocol suite

In this scenario, imagine that **Host A** (the source) communicates with **Host B** (the destination). The communication process involves five devices:

1. Source Host (Computer A)
2. Link-layer switch in LAN 1
3. Router
4. Link-layer switch in LAN 2
5. Destination Host (Computer B)

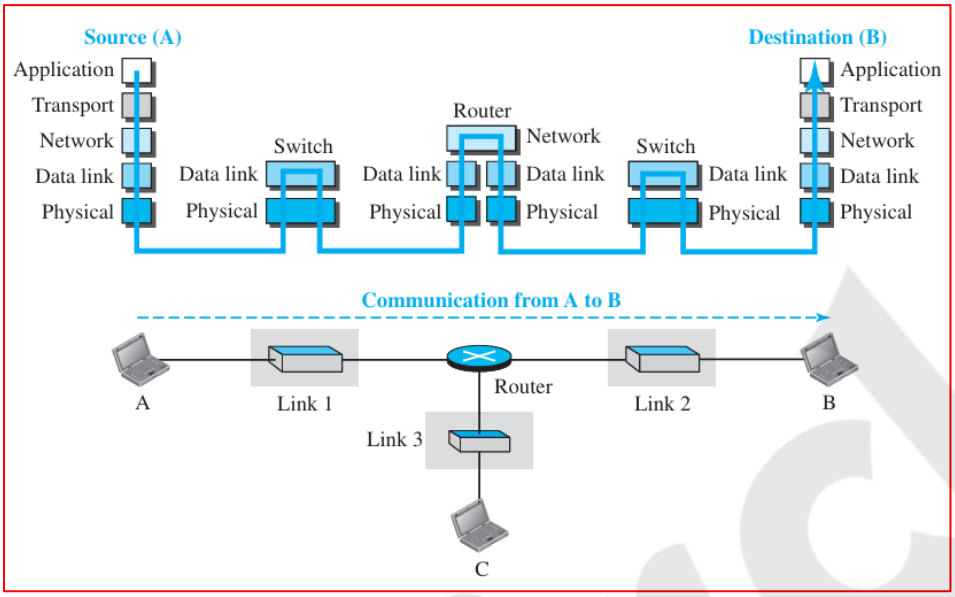

Figure 1.20: Communication through an internet

Each of these devices operates at different layers of the TCP/IP protocol stack, depending on its role in the network:

1. Hosts (Source and Destination)

Both **Host A** and **Host B** are involved in all five layers of the TCP/IP model:

- **Application Layer**: The source host (Host A) creates a message at the application layer and sends it down through the stack.
- **Transport Layer**: The message is passed to the transport layer, which ensures reliable delivery.
- **Network Layer**: At the network layer, the message is encapsulated into packets for transmission across the network.
- **Data Link Layer**: The packets are then prepared for transmission over the physical network in the data-link layer.
- **Physical Layer**: Finally, the message is sent through the physical medium (wires, cables, etc.) to reach the destination host.

At the destination, **Host B** receives the message at the physical layer and passes it up through the layers until it reaches the application layer for processing.

2. Router

A **router** plays a different role and operates at three layers of the TCP/IP model:

- **Network Layer**: The router's primary function is routing packets across networks. It forwards packets based on their destination IP address.
- **Data Link Layer & Physical Layer**: A router is connected to multiple links, and each link may use a different data-link and physical-layer protocol. For instance, if a packet arrives from **LAN 1** (Link 1) using one set of protocols, the router must handle it and forward it to **LAN 2** (Link 2) using another set of protocols.

Importantly, the router does not deal with the transport or application layers, as its role is solely to move packets between networks.

3. Link-Layer Switch

A **link-layer switch** operates only at the data-link and physical layers:

- **Data Link Layer**: The switch processes the data frames and ensures they are forwarded to the correct device within the same LAN.
- **Physical Layer**: The switch forwards the data through the physical medium.

Unlike routers, link-layer switches do not need to handle different sets of protocols for different links. They operate within a single LAN, using a single protocol set for the data-link and physical layers.

5.2. Layers in the TCP/IP Protocol Suite

TCP/IP protocol suite functions and responsibilities of each layer.

Understanding the Logical Connections Between Layers

To grasp the role of each layer, it's helpful to visualize the **logical connections** between them. Figure 1.21 in the book illustrates these connections in a simple internet model.

- **End-to-End vs. Hop-to-Hop Duties:**
  - The **application, transport, and network layers** are responsible for **end-to-end** communication, meaning they manage data from one end device to the other across the network.
  - The **data-link and physical layers**, on the other hand, handle communication on a **hop-to-hop** basis, where each "hop" refers to a host or router.

This distinction is key: the top three layers operate across the entire internet, while the lower two layers manage communication on individual network segments or "links."

Data Units and Layer Responsibilities

Another important way to understand these connections is by considering the **data units** created at each layer.

- In the **top three layers**, the data units (referred to as packets) are **not modified** by routers or link-layer switches.
- In the **bottom two layers**, however, the packet created by the host can be modified by routers but **not** by link-layer switches.

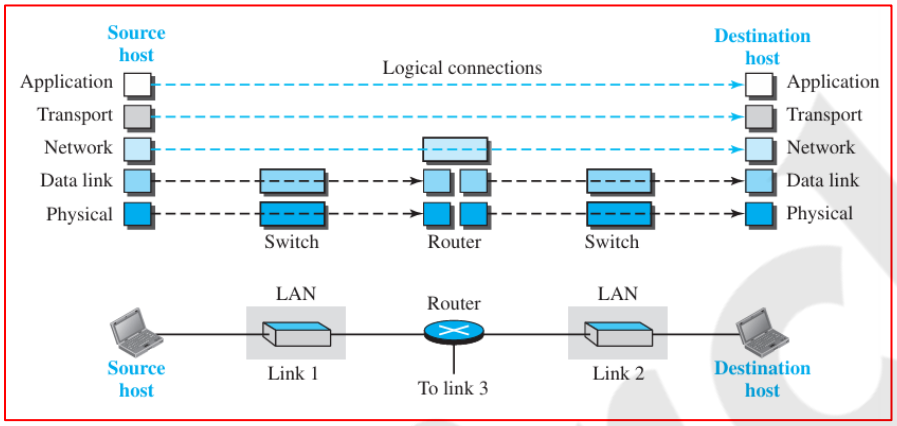

Figure 1.21: Logical connections between layers of the TCP/IP protocol suite

Figure 1.22 shows a second principle of protocol layering: identical objects exist below each layer for connected devices.

- At the **network layer**, even though there's a logical connection between two hosts, a router might fragment packets into smaller units.
- The link between two hops does not alter these packets.

This layering approach allows for a structured, predictable method of managing data as it moves across the network.

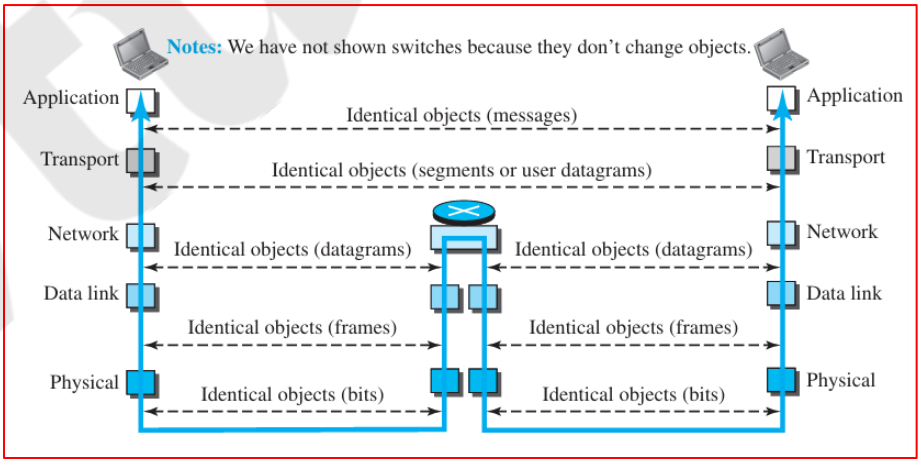

Figure 1.22: Identical objects in the TCP/IP protocol suite

5.3. Description of Each Layer

Physical Layer:

Role of the Physical Layer:

- The physical layer focuses on transmitting the bits from the data-link layer as electrical or optical signals over a physical medium (such as cables or wireless channels).
- It converts bits from the data-link layer into signals that can travel through the medium connecting the devices.

Transmission Media:

- The physical connection between two devices is made through a transmission medium, which can be either **cables** (like twisted-pair, fiber-optic cables) or **air** (wireless communication).
- The **transmission medium** does not directly carry bits; instead, it transmits **signals** (electrical or optical) that represent the bits.

Logical Communication:

- Despite being the lowest layer, the physical layer enables **logical communication** between devices by ensuring that signals are accurately transmitted and interpreted.
- From a logical perspective, the unit of data at this layer is the **bit**, even though the actual signals sent over the medium are different in nature.

Signal Transformation:

- The physical layer converts bits into appropriate forms of signals (either electrical or optical) depending on the medium used.
- Protocols at this layer define how these bits are transformed into signals to be carried over the medium.

Data-link Layer:

In an internet, multiple links (LANs and WANs) are connected by routers. There are often multiple paths that a datagram can take from the host to its destination. Routers are responsible for determining the most efficient route. Once the next link is chosen by a router, the **data-link layer** manages the process of transmitting the datagram across that link.

These links can vary widely and include:

- Wired LANs with link-layer switches
- Wireless LANs
- Wired WANs
- Wireless WANs

Each type of link may use different protocols, but the **data-link layer** has the essential role of ensuring that the packet is successfully transmitted across any type of link.

The **TCP/IP model** does not mandate a specific protocol for the data-link layer. Instead, it accommodates a wide range of both standard and proprietary protocols. Any protocol that can encapsulate a datagram and move it across a link is considered acceptable.

At the data-link layer, the datagram is encapsulated into a packet, referred to as a **frame**.

- Some link-layer protocols offer **both error detection and correction**, ensuring that transmitted data is free from errors.

Network Layer:

The network layer is crucial for establishing communication between the source and destination computers. It manages **host-to-host communication** across multiple devices (routers) in the path. Each router ensures that packets are directed along the most efficient route. The main role of the network layer is to enable communication between hosts and determine the best path for data transmission.

Internet Protocol (IP)

The primary protocol of the network layer is the **Internet Protocol (IP)**, which defines the structure and format of data packets, known as **datagrams** at this level. IP also determines the addressing system, ensuring each packet is sent from its source to its destination. The forwarding of packets from router to router is a fundamental part of IP's function.

- **Connectionless Protocol**: IP is connectionless, meaning it does not manage flow control, error control, or congestion control. These features are handled by the transport layer if needed by an application.
- **Routing Protocols**: While IP is responsible for actual routing, protocols like **unicast** (one-to-one) and **multicast** (one-to-many) create forwarding tables to assist routers with routing decisions.

Auxiliary Protocols Supporting IP

Several additional protocols work alongside IP to assist in the routing and delivery process:

- **ICMP (Internet Control Message Protocol)**: Helps IP report issues encountered during packet routing.
- **IGMP (Internet Group Management Protocol)**: Supports IP with multicast communication.
- **DHCP (Dynamic Host Configuration Protocol)**: Assigns network-layer addresses to hosts.
- **ARP (Address Resolution Protocol)**: Converts a network-layer address into a link-layer address for communication with a specific host or router.

These protocols ensure efficient routing and network management, enabling seamless host-to-host communication in complex networks.

Transport Layer:

The **Transport Layer** plays a crucial role in ensuring **end-to-end communication between hosts** in a network. It handles the transfer of data between the application layer on one device and the corresponding application layer on another device, making sure that messages are transmitted reliably and efficiently.

Key Functions:

- **Encapsulation and Transmission**: The transport layer at the source host takes messages from the application layer, encapsulates them into transport layer packets (called *segments* in TCP or *user datagrams* in UDP), and transmits them to the destination transport layer.
- **End-to-End Communication**: Even though the application layer provides an end-to-end connection, the transport layer separates tasks, handling data transmission independently from the application. This separation allows flexibility by providing multiple protocols suited for different needs.

Protocols in the Transport Layer:

1. **Transmission Control Protocol (TCP)**:
    - **Connection-Oriented**: TCP establishes a connection between two hosts before transferring data. It creates a virtual "pipe" for sending a continuous stream of bytes.
    - **Flow Control**: Ensures that the data sent matches the receiving capability of the destination, preventing data loss due to overwhelming the receiver.
    - **Error Control**: TCP checks for errors in data transmission and ensures that any corrupted segments are retransmitted.
    - **Congestion Control**: Helps avoid network congestion by adjusting the transmission rate based on the current network conditions.
2. **User Datagram Protocol (UDP)**:
    - **Connectionless**: Unlike TCP, UDP does not establish a connection before sending data. Each user datagram is sent independently, without reference to previous or subsequent datagrams.
    - **Simplicity**: UDP is lightweight, with minimal overhead. However, it does not provide flow control, error control, or congestion control.
    - **Use Case**: Best suited for applications that need to send small, independent messages, where speed is critical and retransmission (as in TCP) would be inefficient.
3. **Stream Control Transmission Protocol (SCTP)**:
    - **Designed for Modern Applications**: SCTP is tailored for emerging multimedia applications, offering more advanced features suited to high-demand data transmissions.

By providing these different protocols, the transport layer allows application programs to choose the one that best suits their specific requirements, whether they prioritize reliability, simplicity, or speed.

Application Layer:

The application layer in a network facilitates end-to-end communication between two application layers. It appears as though a direct bridge exists between them, but in reality, communication passes through all layers of the networking model.

At this layer, the communication happens between two processes (programs running on separate machines). One process sends a request, and the other process responds. This process-to-process communication is the core responsibility of the application layer. While many predefined protocols exist at this level, users can also create their own custom processes to communicate across hosts.

Key protocols in the application layer include:

- **HTTP (Hypertext Transfer Protocol)**: Used for accessing the World Wide Web (WWW).
- **SMTP (Simple Mail Transfer Protocol)**: The primary protocol for sending and receiving email.
- **FTP (File Transfer Protocol)**: Enables the transfer of files between hosts.
- **TELNET and SSH (Secure Shell)**: Facilitate remote access to a site.
- **SNMP (Simple Network Management Protocol)**: Allows administrators to manage Internet resources both globally and locally.
- **DNS (Domain Name System)**: Helps find the network-layer address (IP address) of a computer for other protocols.
- **IGMP (Internet Group Management Protocol)**: Collects information on group membership for multicast communication.

5.4. Encapsulation and Decapsulation

Encapsulation and decapsulation are key concepts in protocol layering within the Internet. These processes occur at both the source and destination hosts, as well as at intermediary devices like routers.

I. Encapsulation at the Source Host

At the source host, the encapsulation process involves the following steps:

1. **Application Layer**: The data generated by the application is called a *message*. This message typically doesn't have a header or trailer, but if it does, the whole unit is still referred to as a message. This message is passed to the transport layer.

2. **Transport Layer**: The transport layer treats the message as a payload. It adds a transport layer header, which includes details like the source and destination application program identifiers and information necessary for tasks such as flow control, error control, or

congestion control. The resulting packet is known as a *segment* (in TCP) or a *user datagram* (in UDP). This transport layer packet is then passed to the network layer.

3. **Network Layer**: At this layer, the transport layer packet is treated as the payload. A network layer header is added, which contains the source and destination IP addresses, as well as additional information for error checking and fragmentation. The final packet is referred to as a *datagram*, which is then passed to the data-link layer.

4. **Data-Link Layer**: The network layer packet is encapsulated in a data-link layer frame. A header is added here, which includes the addresses of the sending host and the next hop (e.g., a router). The frame is then passed to the physical layer for transmission over the network.

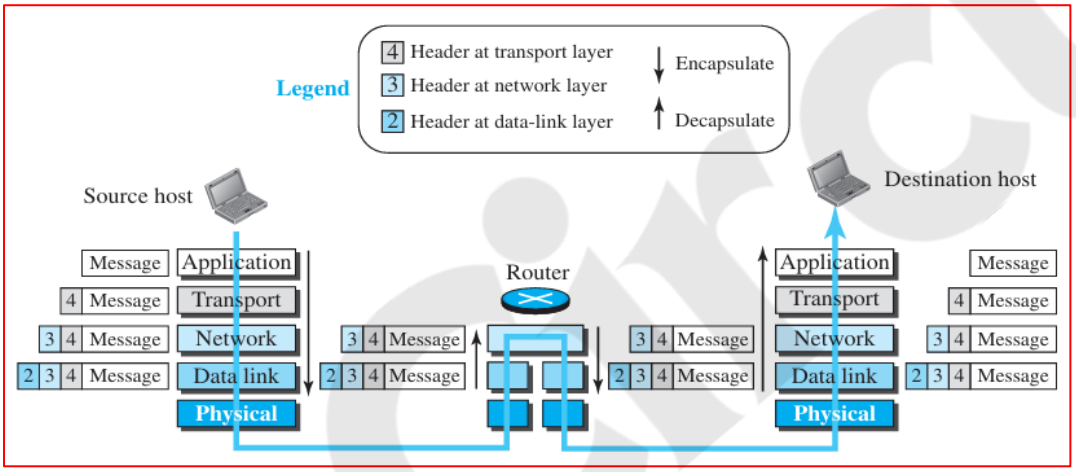

Figure 1.23: Encapsulation/Decapsulation

II. Encapsulation and Decapsulation at the Router

Routers perform both encapsulation and decapsulation, as they are connected to multiple network links. Here's how this works:

1. **Decapsulation at Data-Link Layer**: When the router receives a frame, the data-link layer extracts the *datagram* from the frame and passes it to the network layer.

2. **Network Layer Processing**: The router's network layer examines the source and destination addresses within the datagram header. Using its forwarding table, the router determines the next hop for the datagram. The content of the datagram is not altered unless it requires fragmentation to pass through the next link. Once processed, the datagram is passed to the data-link layer of the next link.

3. **Encapsulation at Data-Link Layer**: The datagram is encapsulated into a new frame suitable for the next link, and the frame is passed to the physical layer for transmission.

III. Decapsulation at the Destination Host

At the destination host, the reverse process of encapsulation—decapsulation—occurs:

1. **Data-Link Layer**: The frame is received, and the data-link layer removes its header to extract the network layer *datagram*.
2. **Network Layer**: The network layer removes its header to extract the transport layer *segment* or *user datagram*.
3. **Transport Layer**: The transport layer removes its header to deliver the original *message* to the application layer.

During decapsulation, error checking is performed at each layer to ensure data integrity. The process continues until the original message reaches the application layer, where it can be used by the application program.

5.5. Addressing in Network

In the context of the Internet and network protocol layering, **addressing** is a key concept that ensures logical communication between pairs of layers. For any communication between two parties, there must be two essential addresses: a **source address** and a **destination address**. Although it might seem like each layer of the protocol model would require a separate pair of addresses, in practice only four are needed, as the **physical layer** does not use addresses. The physical layer deals with bits, and individual bits do not have addresses.

Addressing at Different Layers

Each layer in the protocol stack uses specific types of addresses, which relate to the type of communication and the name of the data unit used at that layer. Here's a breakdown:

1. **Application Layer**:
    - At this layer, addresses are typically **names**, such as a domain name (e.g., someorg.com) or an email address (e.g., somebody@coldmail.com). These names represent the service or resource being accessed.
    - **Packet name**: *Message*.
2. **Transport Layer**:
    - Addresses here are called **port numbers**. Port numbers identify the specific application-layer programs (e.g., web server-Port 80, email client - Port 25) on the source and destination devices. Each running program has its own port number, ensuring that data reaches the correct application.
    - **Packet name**: *Segment* (for TCP) or *User Datagram* (for UDP).

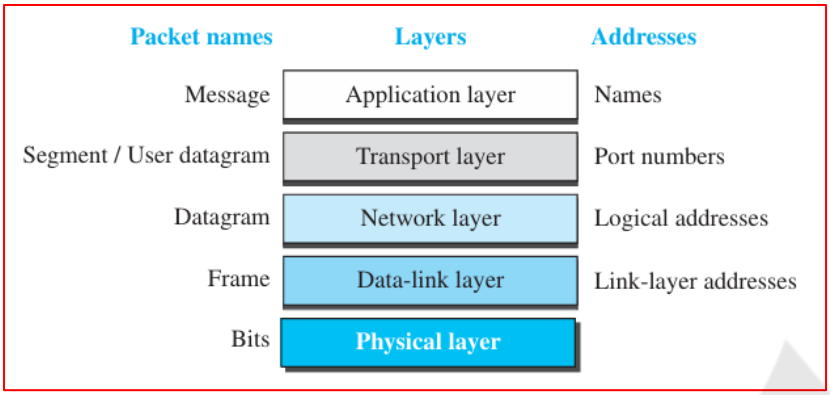

Figure 1.24: Addressing in the TCP/IP protocol suite

3. **Network Layer**:
    - The network layer uses **global addresses**, which are known as **IP addresses (45.113.122.159)**. These uniquely identify a device's connection to the Internet and allow data to be routed across networks.
    - **Packet name**: *Datagram*.
4. **Link Layer**:
    - At this layer, **link-layer addresses** (also known as **MAC addresses 78-45-C4-29-17-E8**) are used. These are local addresses that uniquely identify specific devices on a network (such as a LAN or WAN), ensuring that data reaches the correct physical machine.
    - **Packet name**: *Frame*.

5.6. Multiplexing and Demultiplexing

In the TCP/IP protocol suite, multiplexing and demultiplexing are essential concepts for managing data flow between different layers of the protocol stack.

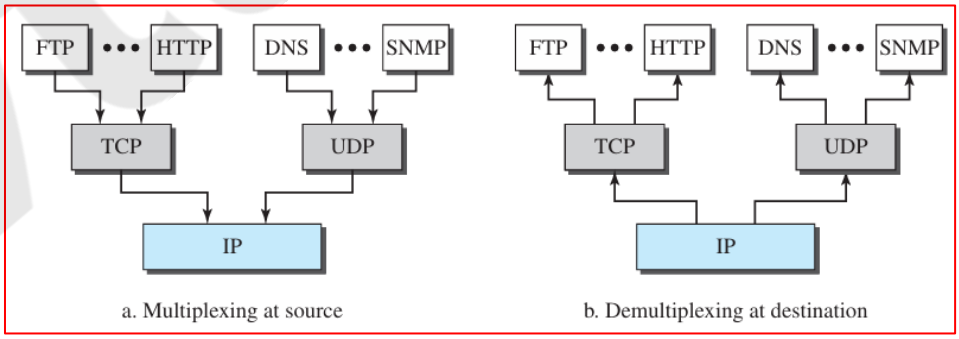

Figure 1.25: Multiplexing and demultiplexing

Multiplexing at the Source: Multiplexing occurs when a protocol at a certain layer can handle multiple types of data from higher layers. For example, at the transport layer, protocols like TCP and UDP can receive messages from various application-layer protocols (such as FTP, HTTP, DNS, and SNMP). The transport layer encapsulates these messages into segments and adds a header field to indicate which application-layer protocol the data belongs to.

Demultiplexing at the Destination: Demultiplexing happens at the destination when a protocol needs to deliver the data to the appropriate higher-layer protocol. At the transport layer, TCP or UDP will examine the header to determine which application-layer protocol should receive the data. Similarly, at the network layer, IP can handle segments from TCP or datagrams from UDP, and it can also process packets from other protocols like ICMP or IGMP. At the data-link layer, a frame may carry payloads from various protocols, such as IP or ARP.

Illustration:

- **At the Transport Layer:** UDP or TCP encapsulates data from application-layer protocols (e.g., FTP, HTTP, DNS, SNMP).
- **At the Network Layer:** IP handles segments from TCP, datagrams from UDP, and packets from other protocols.
- **At the Data-Link Layer:** Frames may include payloads from IP or other protocols like ARP.

6. TRANSMISSION MEDIA

Transmission media are essentially the physical substances through which information travels. They operate at a level below the physical layer of the OSI model, often referred to as "layer zero." Essentially, transmission media can be considered as a fundamental layer that directly interfaces with the physical layer.

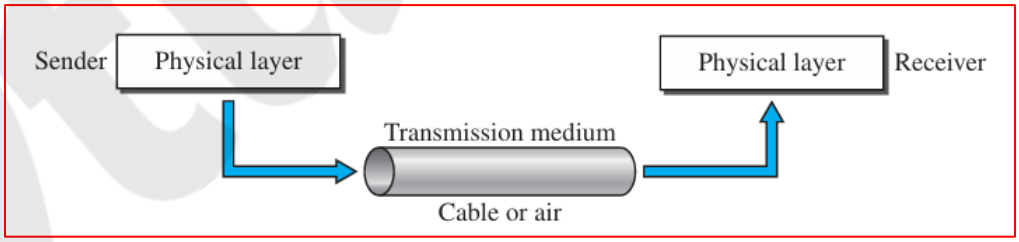

Figure 1.26: Transmission medium and physical layer

Data Communications Examples:

- Transmission media include free space, metallic cables, or fiber-optic cables.
- The information transmitted is usually in the form of signals generated from data.

- **Telegraph (19th Century):** Invented by Morse, it was an early long-distance communication technology using metallic wires, but was slow.
- **Telephone (1869):** Allowed voice transmission over long distances via metallic cables, though communication quality was poor due to inferior wires.
- **Wireless Communication (1895):** Hertz transmitted high-frequency signals, and Marconi later improved this by sending messages across the Atlantic Ocean.

- **Improved Metallic Media:** Development of twisted-pair and coaxial cables has enhanced data transmission.
  - **Optical Fibers:** The advent of fiber-optic cables has significantly increased data transmission rates.
  - **Efficient Use of Free Space:** Advances in modulation and multiplexing have optimized the use of free space (air, vacuum, water) for communication.

Electromagnetic Spectrum:

- **Signals and Electromagnetic Energy:** Computers and telecommunication devices transmit data as electromagnetic energy, which includes power, radio waves, infrared, visible light, ultraviolet light, and X-rays.
- **Spectrum Usability:** Not all parts of the electromagnetic spectrum are suitable for telecommunications. Only certain portions are used, and the types of media to harness these are limited.

Categories of Transmission Media:

1. **Guided Media:** These include twisted-pair cables, coaxial cables, and fiber-optic cables.
2. **Unguided Media:** This refers to free space, such as air and vacuum.

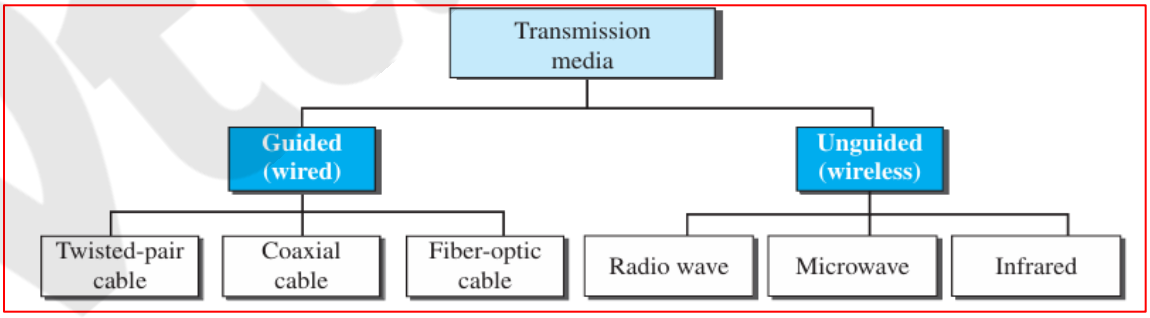

Figure 1.27: Classes of transmission media

6.1. Guided Media

Guided media are types of communication channels that provide a specific path for signals to travel from one device to another. These include:

1. **Twisted-Pair Cable**: This type of cable consists of pairs of insulated copper wires twisted together. The twisting helps reduce electromagnetic interference and maintains signal quality.
2. **Coaxial Cable**: Coaxial cables have a central conductor, an insulating layer, a metallic shield, and an outer insulating layer. This structure helps to protect the signal from interference and allows for high-speed data transmission.
3. **Fiber-Optic Cable**: Unlike twisted-pair and coaxial cables, fiber-optic cables use light signals to transmit data. They consist of thin strands of glass or plastic that carry light pulses over long distances with minimal signal loss.

6.2. Twisted-Pair Cable

A twisted pair cable consists of two insulated copper conductors twisted together. Each wire in the pair serves a different function: one carries the signal to the receiver, and the other acts as a ground reference. The receiver processes the difference between the two wires to retrieve the signal.

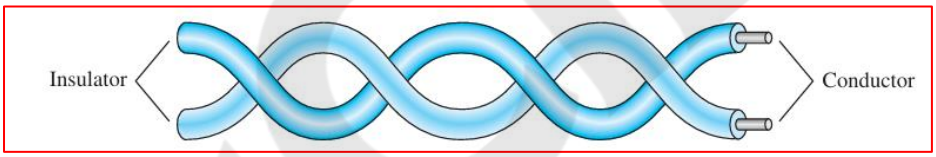

Figure 1.28: Twisted-pair cable

Noise and Interference

Twisted pair cables are designed to minimize the impact of interference (noise) and crosstalk. When the wires are parallel, noise or crosstalk can affect each wire differently due to their varying distances from the sources of interference. By twisting the wires, the cable maintains a balance. In each twist, the relative positions of the wires to the noise source change, helping to ensure that both wires experience similar levels of interference. This twisting reduces the impact of unwanted signals, as the receiver calculates the difference between the wires, canceling out most of the noise.

Shielded vs. Unshielded Twisted-Pair Cables

- **Unshielded Twisted-Pair (UTP):** The most common type used in communications, UTP cables do not have additional shielding. They are less expensive and less bulky but can be more susceptible to interference.
- **Shielded Twisted-Pair (STP):** STP cables have an additional metal foil or braided mesh covering each pair of conductors. This shielding reduces interference and improves signal

quality but makes the cables bulkier and more costly. STP is primarily used by IBM and is less common outside of their applications.

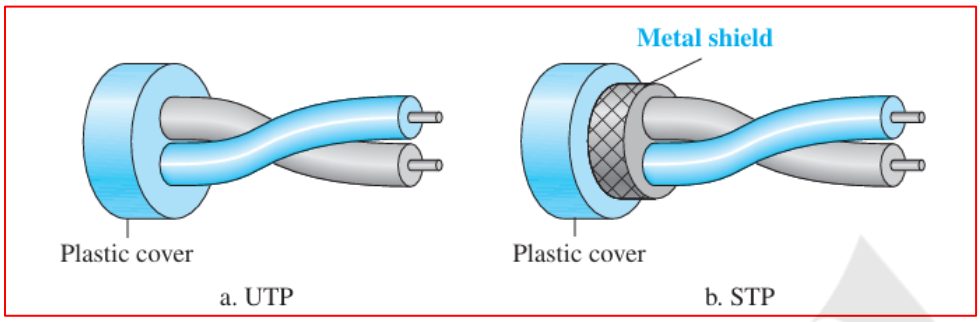

Figure 1.29: UTP and STP cables

Categories of UTP Cables

The Electronic Industries Association (EIA) classifies UTP cables into seven categories, with Category 1 being the lowest quality and Category 7 being the highest. Each category is suitable for specific applications, and the standards help ensure the cable meets certain performance criteria.

Connectors

The RJ45 connector is the most common connector for UTP cables. It is a keyed connector, meaning it can only be inserted in one direction, which ensures a proper connection.

Table 1.1: Categories of unshielded twisted-pair cables

Category	Specification	Data Rate (Mbps)	Use
1	Unshielded twisted-pair used in telephone lines	2	Telephone
2	Unshielded twisted-pair originally used in T1 lines	10	T1 Lines
3	Improved Category 2 used in LANs	20	LANs
4	Improved Category 3 used in Token Ring networks	100	Token Ring Networks
5	Cable wire is normally 24 AWG with a jacket and outside sheath	125	LANs
5E	An extension of Category 5 with additional features to minimize crosstalk and electromagnetic interference	125	LANs
6	New category with matched components from the same manufacturer; cable tested at a 200-Mbps data rate	200	LANs
7	Sometimes called SSTP (Shielded Screen Twisted-Pair); each pair is wrapped in helical metallic foil followed by a metallic foil shield	600	LANs

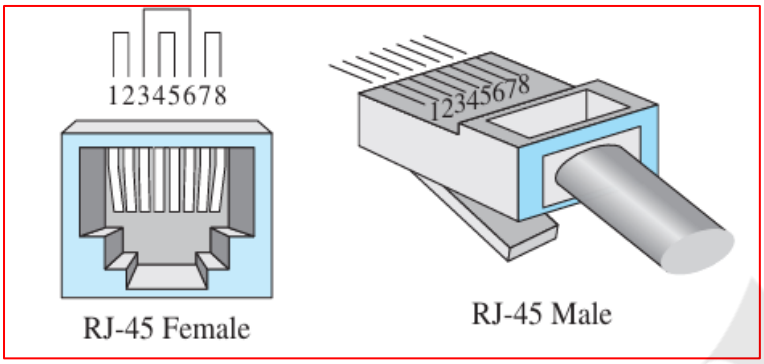

Figure 1.30: UTP connector

Performance

The performance of twisted-pair cables is often assessed by measuring attenuation (signal loss) in relation to frequency and distance. Although twisted-pair cables can handle a broad range of frequencies, attenuation increases significantly at frequencies above 100 kHz. Attenuation is measured in decibels per kilometer (dB/km), and higher frequencies result in greater signal loss.

Applications

Twisted-pair cables are widely used in various applications:

- **Telephone Lines:** Used for voice and data transmission in the local loop connecting subscribers to telephone offices.
- **DSL Lines:** Provide high-data-rate connections by utilizing the high bandwidth of UTP cables.
- **Local-Area Networks (LANs):** Employed in networks such as 10Base-T and 100Base-T for data transmission.

6.3.Coaxial Cable

Coaxial cable, often referred to as coax, is designed to carry high-frequency signals, unlike twisted-pair cables. It consists of the following parts:

- **Central Core Conductor**: A solid or stranded copper wire, responsible for carrying the signal.
- **Insulating Sheath**: Surrounds the core conductor, separating it from the outer conductor.
- **Outer Conductor**: Made of metal foil, braid, or both, which serves two purposes:
  - Acts as a shield against external noise.
  - Functions as the second conductor to complete the circuit.
- **Additional Insulation**: Encases the outer conductor for further protection.
- **Plastic Cover**: Provides external protection for the entire cable.

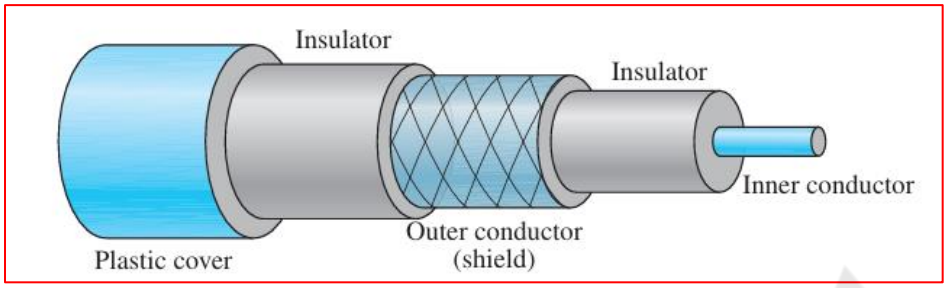

Figure 1.31 Coaxial cable

This design helps coaxial cables transmit signals with less interference and at higher frequencies compared to twisted-pair cables.

Coaxial Cable Standards (RG Ratings)

Coaxial cables are classified based on Radio Government (RG) ratings. Each RG number specifies certain physical characteristics of the cable, such as:

- **Wire Gauge**: Thickness of the inner conductor.
- **Insulation**: Thickness and material of the inner insulator.
- **Shielding**: Design and construction of the outer conductor.
- **Outer Casing**: Size and type of the protective cover.

These RG-rated cables are suited for different specialized applications, as indicated by their specifications.

Table 1.2: RG-rated cables are suited for different specialized applications.

Category	Use
RG-59 75 Ω	Cable TV
RG-58 50 Ω	Thin Ethernet
RG-11 50 Ω	Thin Ethernet

Coaxial Cable Connectors

To connect coaxial cables to devices, special connectors are required. The most common connector type is the **Bayonet Neill-Concelman (BNC)** connector. There are different variations of this connector:

- **BNC Connector**: Used to connect the cable to a device (e.g., a TV).
- **BNC T Connector**: Often used in Ethernet networks to split the signal to multiple devices.
- **BNC Terminator**: Placed at the end of the cable to prevent signal reflection and ensure stable transmission.

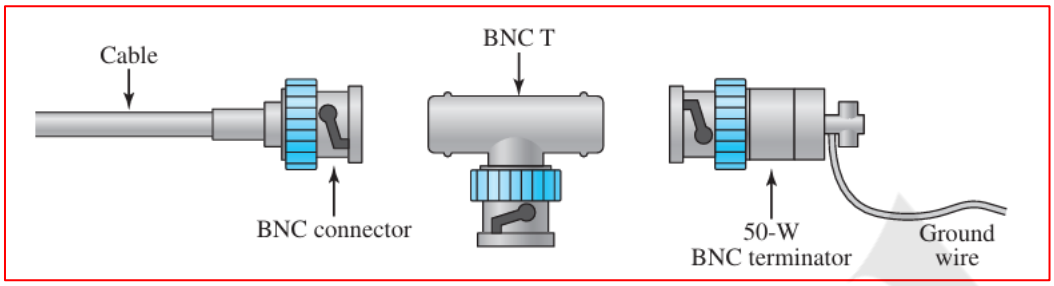

Figure 1.32: BNC connectors

Performance of Coaxial Cables

Coaxial cables provide higher bandwidth compared to twisted-pair cables, allowing them to carry more data. However, their **attenuation** (signal weakening) is greater, meaning the signal degrades over distance and requires frequent use of **repeaters** to maintain signal strength.

Applications

- **Analog Telephone Networks**: Coaxial cables were used to carry large amounts of voice signals, with one cable supporting up to 10,000 voice channels.
- **Digital Telephone Networks**: Coaxial cables were capable of transmitting digital data at speeds up to 600 Mbps.

Today, **fiber optic cables** have largely replaced coaxial cables in telephone networks due to their superior performance.

6.4. Fiber-Optic Cable

A **fiber-optic cable** is a medium made of glass or plastic that transmits signals as light. To understand how it works, it's important to first grasp the nature of light.

Properties of Light

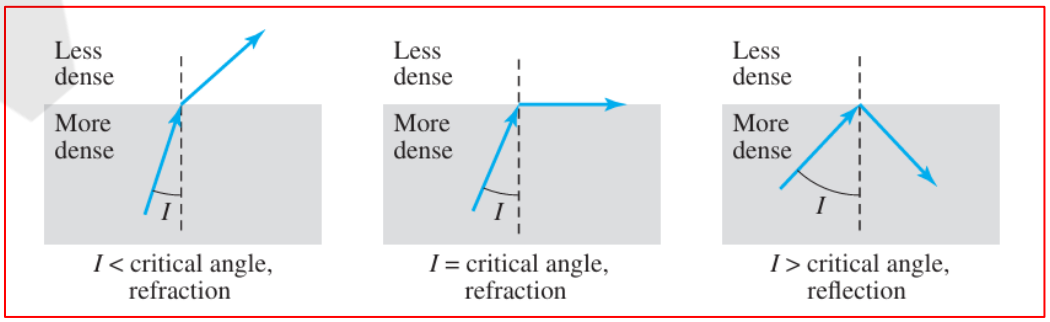

Figure 1.33: Bending of light ray

- **Light travels in a straight line** when moving through a uniform material.
- If light passes from one substance into another with a different density, the direction changes (refraction).
- **Critical Angle**: The angle of incidence at which light bends along the boundary between two materials. If the angle is greater than the critical angle, the light reflects instead of refracting.

Structure of Optical Fibers

Optical fibers guide light through **internal reflection**. The core (made of glass or plastic) is surrounded by a **cladding** with lower density. This ensures that light reflecting off the core-cladding boundary remains in the core.

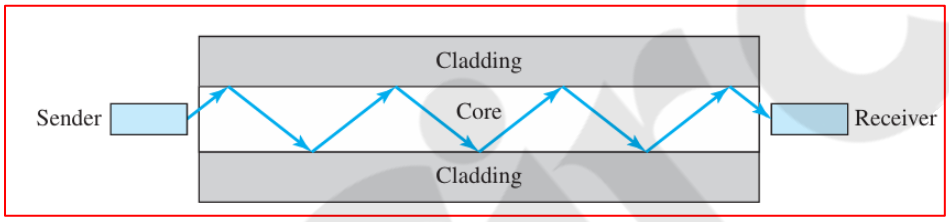

Figure 1.34: Optical fiber

Propagation Modes

Optical fibers use two main modes for light propagation:

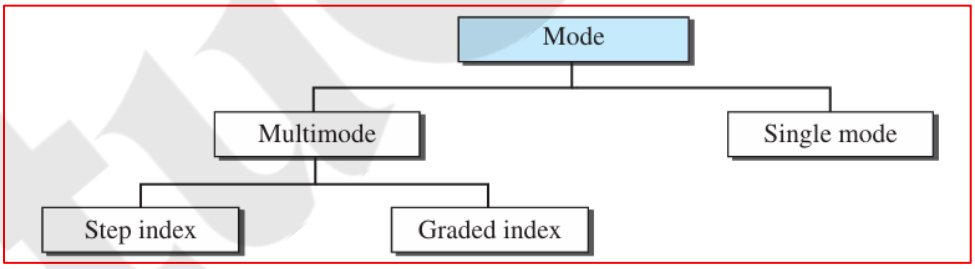

Figure 1.35: Propagation modes

1. **Multimode**: Multiple light beams travel through the core along different paths.
    - **Step-Index Fiber**: The core has uniform density, and light changes direction abruptly at the core-cladding interface.
    - **Graded-Index Fiber**: The core's density gradually decreases from the center, reducing signal distortion.
2. **Single-Mode**: Uses step-index fiber but has a smaller core and tightly focused light. The beams travel nearly parallel, minimizing delay and distortion.

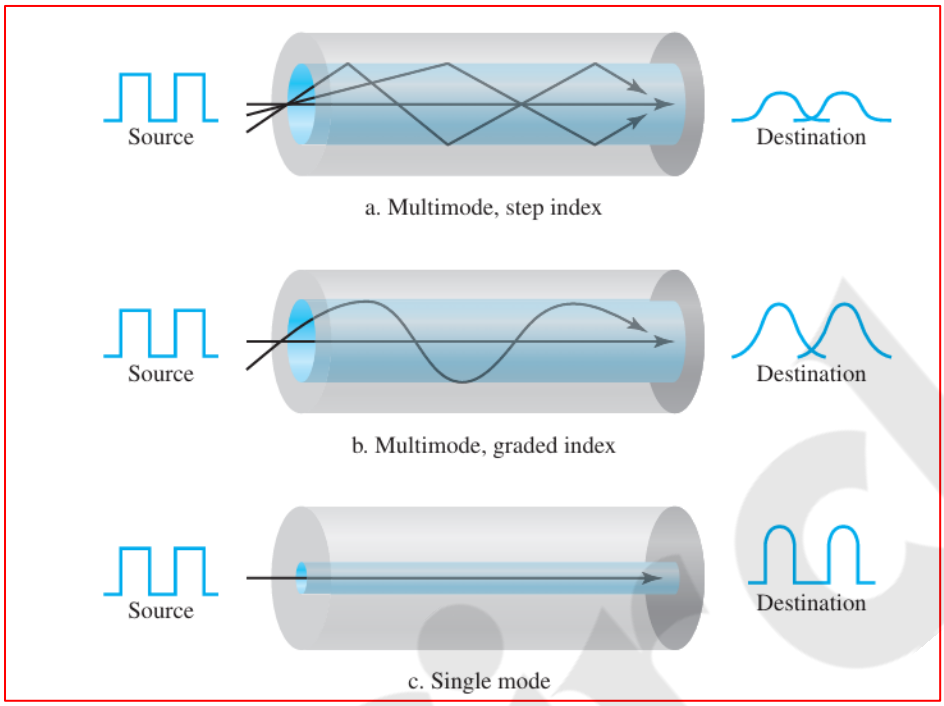

Figure 1.36: Modes

Fiber Sizes

Optical fibers are classified by the ratio of core diameter to cladding diameter (both measured in micrometers). Single-mode fibers typically have a smaller core diameter compared to multimode fibers.

Fiber-Optic Cable Composition

A typical fiber-optic cable consists of:

- **Outer jacket** (PVC or Teflon)
- **Kevlar strands** for strength
- **Plastic coating** for cushioning
- **Core and cladding** for light transmission

Fiber-Optic Connectors

There are three types of connectors:

1. **SC (Subscriber Channel)**: Push/pull locking, used in cable TV.
2. **ST (Straight Tip)**: Bayonet locking, used in networking.
3. **MT-RJ**: Same size as RJ45, used for data networks.

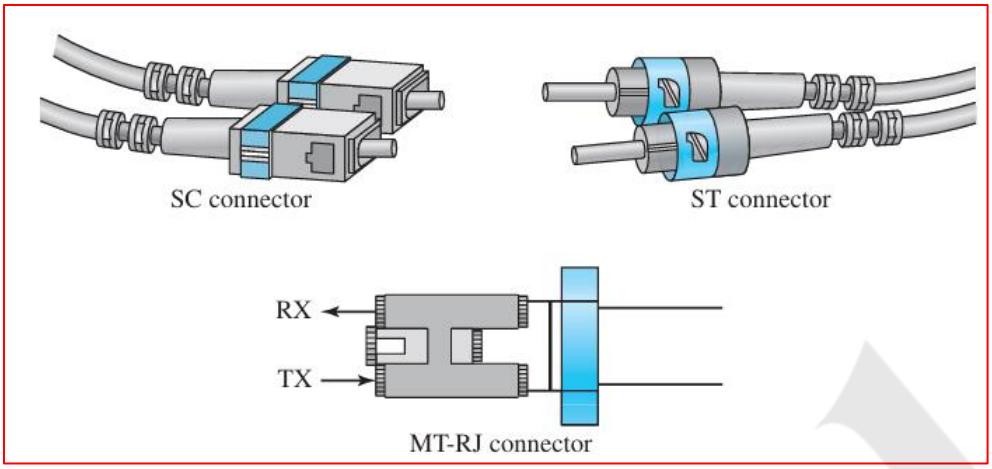

Figure 1.37: Fiber-optic cable connectors

Performance

Fiber-optic cables experience less signal attenuation than twisted-pair or coaxial cables, requiring fewer repeaters. They also support higher data transfer rates, especially with **wavelength-division multiplexing (WDM)**.

Applications

- **Backbone Networks**: Due to their wide bandwidth, fiber-optic cables are used in backbone networks, such as SONET.
- **Hybrid Networks**: Some cable TV companies use a mix of fiber-optic and coaxial cables.
- **Local Area Networks (LANs)**: Fiber-optic cables are used in networks like 100Base-FX and 1000Base-X.

Advantages of Optical Fiber

1. **Higher Bandwidth**: Supports higher data rates.
2. **Less Signal Attenuation**: Can transmit over longer distances without needing repeaters.
3. **Immunity to Electromagnetic Interference**: Not affected by electromagnetic noise.
4. **Resistance to Corrosive Materials**: More durable in harsh environments.
5. **Lightweight**: Lighter than copper cables.
6. **Greater Immunity to Tapping**: More secure than copper cables.

Disadvantages of Optical Fiber

1. **Installation and Maintenance**: Requires specialized skills.
2. **Unidirectional Light Propagation**: Requires two fibers for bidirectional communication.
3. **Cost**: More expensive than other cables, especially if bandwidth demand is low.

Fiber-optic cables offer numerous benefits, particularly in high-bandwidth and long-distance applications, but their costs and technical requirements must be carefully considered.

7. UNGUIDED MEDIA: WIRELESS

Unguided media refers to communication channels that use wireless signals to transmit data. These signals travel through the air without any physical conductor. Common types of wireless transmission include radio waves, microwaves, and infrared.

Wireless communication involves transmitting electromagnetic waves without using physical conductors like cables or wires. Instead, signals are broadcast through free space, making them accessible to any device equipped to receive them.

Electromagnetic Spectrum for Wireless Communication

Wireless communication utilizes a portion of the electromagnetic spectrum, ranging from 3 kHz to 900 THz, as shown in Figure 1.38. This spectrum includes a variety of frequencies that allow different methods of signal transmission.

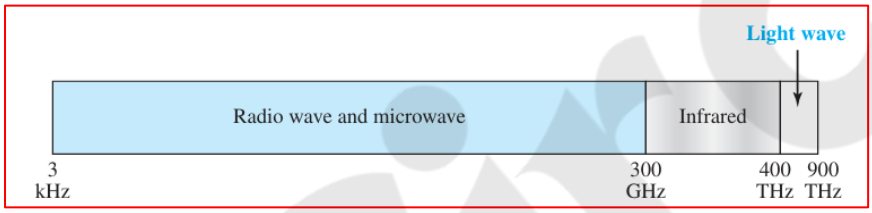

Figure 1.38 Electromagnetic spectrum for wireless communication

Types of Propagation

Unguided signals, such as radio waves, can travel from the source to the destination in three main ways, illustrated in Figure 1.40:

1. **Ground Propagation**:
    - In this method, low-frequency radio waves travel close to the Earth's surface, following the curvature of the planet.
    - These signals radiate from the transmitting antenna in all directions, and the distance they cover depends on the power of the signal—the higher the power, the farther the signal can travel.
2. **Sky Propagation**:
    - Higher-frequency radio waves are transmitted upward into the ionosphere, where they are reflected back to Earth.
    - This method enables long-distance communication with relatively low power.

3. **Line-of-Sight Propagation**:
    - In this method, very high-frequency signals are transmitted directly between antennas in a straight line.
    - The antennas must be properly aligned and either tall enough or close enough to avoid being affected by the curvature of the Earth. This method is more complex because radio waves can't be perfectly focused.

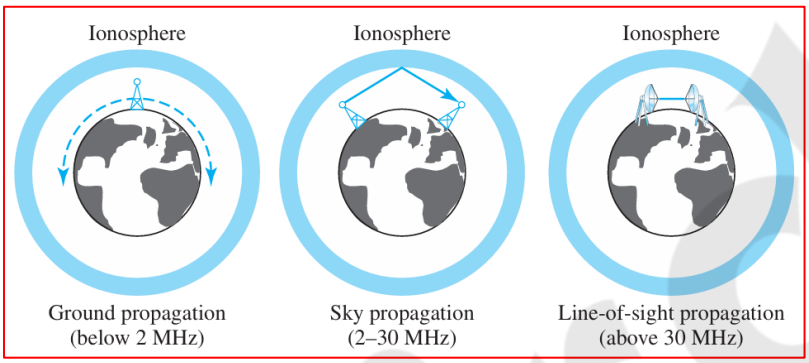

Figure 1.40: Propagation methods

Frequency Bands

The electromagnetic spectrum for wireless communication is divided into eight different ranges or "bands." These bands are classified based on frequency and are regulated by government authorities. The ranges extend from Very Low Frequency (VLF) to Extremely High Frequency (EHF). Each band has specific propagation characteristics and applications, as summarized in Table 1.3.

Table 1.3: Frequency Bands for Applications

Band	Range	Propagation	Application
Very Low Frequency (VLF)	3–30 kHz	Ground	Long-range radio navigation
Low Frequency (LF)	30–300 kHz	Ground	Radio beacons, navigational locators
Middle Frequency (MF)	300 kHz–3 MHz	Sky	AM radio
High Frequency (HF)	3–30 MHz	Sky	Citizens band (CB), ship/aircraft communication
Very High Frequency (VHF)	30–300 MHz	Sky and Line-of-sight	VHF TV, FM radio
Ultra-High Frequency (UHF)	300 MHz–3 GHz	Line-of-sight	UHF TV, cellular phones, paging, satellite
Super High Frequency (SHF)	3–30 GHz	Line-of-sight	Satellite communication
Extremely High Frequency (EHF)	30–300 GHz	Line-of-sight	Radar, satellite communication
Light Wave (Infrared)	300 GHz–900 THz	Line-of-sight	Infrared communication

This breakdown of the spectrum ensures efficient and organized use of frequencies for various communication purposes.

7.1.Radio Waves

Frequency Range: Typically, from 3 kHz to 1 GHz.

Characteristics of Radio Waves:

- **Omnidirectional Propagation**: Radio waves are mostly omnidirectional, meaning they spread out in all directions from the transmitting antenna. The sending and receiving antennas don't need to be aligned for successful communication, as any receiving antenna in range can pick up the signal. However, this characteristic also leads to a disadvantage: **interference**. Multiple antennas transmitting on the same frequency or band can interfere with one another.
- **Long-Distance Travel**: Radio waves, especially those that propagate in the **sky mode**, can travel long distances, making them ideal for applications like **AM radio broadcasting**.
- **Penetration of Walls**: Radio waves, particularly those with **low and medium frequencies**, can penetrate walls. This is useful because devices like AM radios can receive signals indoors. However, it can also be a disadvantage, as signals cannot be restricted to only the inside or outside of a building, leading to potential **signal leakage**.

Limitations:

- The radio wave band is **relatively narrow**, just under 1 GHz. When divided into subbands, the limited width of these subbands results in **low data rates** for digital communications.
- Most of the radio wave spectrum is **regulated** by government authorities, like the **FCC** in the United States and Department of Telecommunications (DoT) & Telecom Regulatory Authority of India (TRAI) in India. Any use of this spectrum requires **official permission**.
- Licensed Frequency Bands: FM band is licensed between **88-108 MHz** for radio broadcasting and Unlicensed Frequency Bands: Wi-Fi: 2.4 GHz, **5 GHz** band.

Omnidirectional Antenna:

Radio waves typically utilize **omnidirectional antennas**, which transmit signals in all directions. These antennas come in various types, depending on factors like **wavelength, signal strength**, and the intended purpose of transmission.

Applications of Radio Waves:

Thanks to their omnidirectional nature, radio waves are widely used for **multicasting**, where one sender transmits to many receivers. Common examples include:

- **AM and FM radio**
- **Television broadcasting**

- **Maritime radio**
- **Cordless phones**
- **Paging systems**

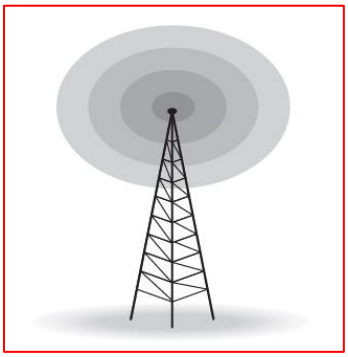

Figure 1.41: Omnidirectional antenna

7.2. Microwaves

Frequency Range: From 1 GHz to 300 GHz.
Characteristics: Microwaves require line-of-sight transmission, meaning the transmitter and receiver must be directly visible to each other. They are less effective in penetrating obstacles like buildings.

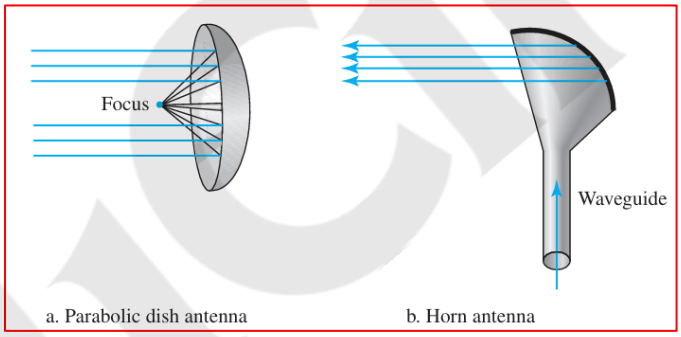

Figure 1.42 Unidirectional antennas

Applications: Satellite communications, radar systems, and microwave ovens. In networking, microwaves are used for point-to-point communication links and cellular networks.

7.3. Infrared

Frequency Range: From 300 GHz to 400 THz.
Characteristics: Infrared signals are used for short-range communication and do not penetrate walls, making them suitable for indoor use. They are highly directional and require line-of-sight transmission.
Applications: Remote controls, short-range data transmission (such as between computers and peripherals), and infrared sensors for detecting heat in security systems or medical devices.

8. PACKET SWITCHING

In data communication, when a message needs to be sent from one end system to another through a **packet-switched network**, it must be divided into smaller units called **packets**. These packets can be of either fixed or variable sizes, depending on the network and the protocol being used.

Key Features of Packet Switching:

1. **No Resource Allocation:**
    - Unlike circuit-switched networks, packet switching does not reserve any specific resources like bandwidth or processing time for the packets.
    - Resources are allocated only when needed, and packets are processed on a **first-come, first-served** basis.
2. **Possible Delays:**
    - Since there is no dedicated path or reserved resources, packets might experience delays. For instance, if a switch is busy processing other packets, newly arrived packets must wait their turn, which can increase transmission time.

Types of Packet-Switched Networks:

1. **Datagram Networks:** In these networks, each packet is treated independently, and it may take different routes to reach the destination.
2. **Virtual Circuit Networks:** These networks establish a pre-determined path before any data packets are sent, ensuring all packets follow the same route.

Packet switching is an efficient way to transfer data, especially in systems where multiple users need to share the same network resources.

8.1. Datagram Networks

In a **datagram network**, each packet is handled independently, even if it's part of a larger transmission. The network treats each packet as if it stands alone. These individual packets are known as **datagrams**.

Key Features of Datagram Networks:

1. **Packet Independence**: Each packet in a datagram network can take a different path to its destination, and the network doesn't maintain any connection state between sender and receiver.
2. **Routing**: Packet routing is typically done at the **network layer**, where packets are forwarded based on their destination address. The devices that manage packet routing are called **routers**.

3. **No Fixed Path**: Since packets may travel along different routes, they might reach their destination out of order or with varying delays. Some packets could even be dropped if the network runs out of resources.

4. **Connectionless**: A datagram network is often referred to as a **connectionless network** because it doesn't require a setup phase (like circuit-switched networks). No information about the connection is saved, and each packet is routed independently.

How Datagram Networks Work

In Figure 1.43, four packets are sent from station A to station X using the datagram approach. Here, switches are called routers, and they are depicted with a different symbol. Although these four packets belong to the same message, they might take different paths to reach their destination due to varying link capacities and network congestion. This can lead to packets arriving out of order, with differing delays, or even being lost or dropped due to insufficient resources. Upper-layer protocols typically handle the reordering and retransmission of lost packets before delivering them to the application.

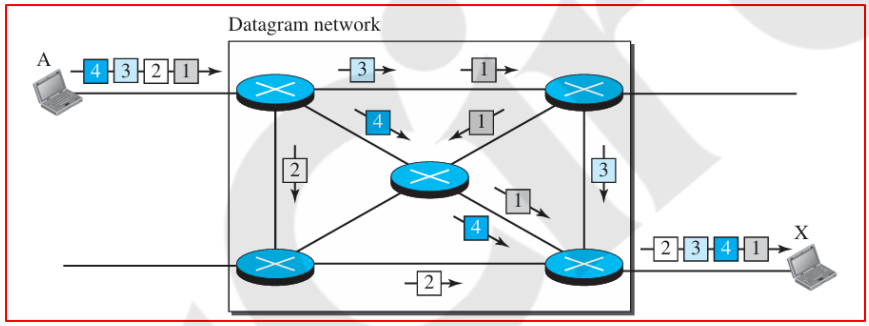

Figure 1.43: A datagram network with four switches (routers)

Routing Table

In a datagram network, each switch uses a routing table based on destination addresses to forward packets. These tables are dynamic and updated regularly.

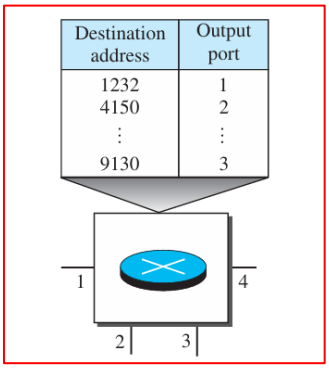

Figure 1.44: Routing table in a datagram network

The routing table records destination addresses and the corresponding output ports. This differs from circuit-switched networks, where entries are created during the setup phase and removed during teardown.

Destination Address

Every packet in a datagram network has a header containing a destination address. Upon receiving a packet, the switch checks this address and uses the routing table to determine the appropriate forwarding port. This destination address remains unchanged throughout the packet's journey.

Delay

Despite their efficiency, datagram networks can experience higher delays compared to virtual-circuit networks. Although there are no setup or teardown phases, each packet may encounter waiting times at switches. Additionally, since packets from the same message may travel through different routes, delays are not uniform. Figure 1.45, illustrates the delay for a packet traveling through two switches, including transmission times (3T), propagation delays (3τ), and waiting times (w1 + w2). The total delay is given by:

$$\boxed{Total\ delay = 3T + 3\tau + w1 + w2}$$

- **Transmission Time**: The time to send a packet from one point to another.
- **Propagation Delay**: The time it takes for the signal to travel through the medium.
- **Waiting Time**: Time spent at routers before being forwarded.

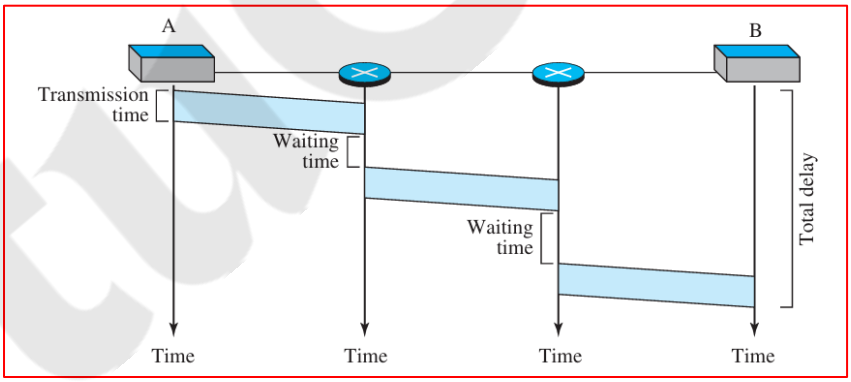

Figure 1.45: Delay in a datagram network

Advantages:

- **Efficiency**: Datagram networks can be more efficient than circuit-switched networks. Resources like bandwidth are allocated only when packets are being transmitted, allowing for better utilization of network resources.

8.2. Virtual-Circuit Networks

A **virtual-circuit network (VCN)** is a hybrid network model that combines features of both **circuit-switched** and **datagram networks**. It provides a balance between connection-oriented and connectionless transmission methods.

Key Features:

1. **Connection Phases:**
    - A VCN has three distinct phases: **setup**, **data transfer**, and **teardown**.
        - **Setup Phase**: A path is established between the sender and receiver before data transmission.
        - **Data Transfer Phase**: Data is sent along the established path in packets.
        - **Teardown Phase**: After data transmission, the connection is terminated, and resources are released.

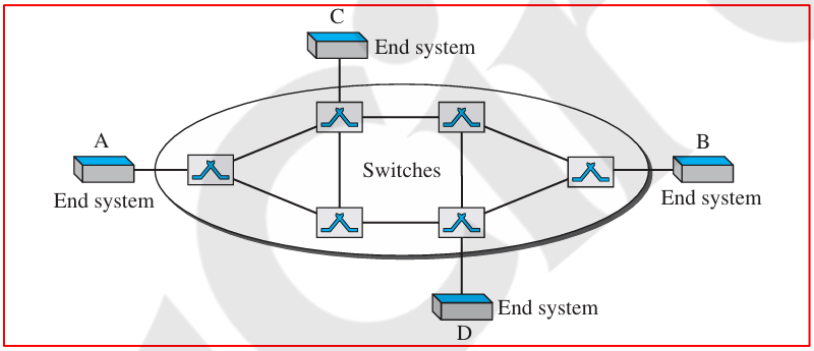

Figure 1.46: Virtual-circuit network

2. **Resource Allocation:**
    - Resources can either be allocated during the setup phase (as in a circuit-switched network) or dynamically during data transmission (similar to a datagram network).
3. **Packetized Data with Local Addressing:**
    - Data is divided into packets, each of which carries an address. However, unlike in a datagram network, the address is not end-to-end but **local**, meaning it only tells the next switch where to send the packet.
4. **Consistent Path for Packets:**
    - Once a connection is established, all packets follow the same predetermined path. This ensures a predictable route for all the packets between the sender and receiver, akin to a circuit-switched network.

5. **Layer of Operation:**
    - Virtual-circuit networks typically operate at the **data-link layer**, while circuit-switched networks operate at the physical layer, and datagram networks at the network layer.

Addressing in Virtual-Circuit Networks:

1. **Global Addressing:**
    - A global address is used to uniquely identify the source and destination during the setup phase. This address is typically unique within the network or globally if the network is part of a larger system.
2. **Virtual-Circuit Identifier (VCI):**
    - During the data transfer phase, a **virtual-circuit identifier (VCI)** is used instead of the global address. The VCI is a small number with local scope, meaning it only identifies the path between two adjacent switches.
    - The VCI changes at each switch, as each switch uses its own set of VCIs to manage the connection. This allows efficient and simple management of packet forwarding.

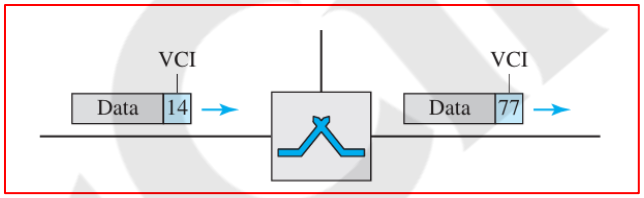

Figure 1.47: Virtual-circuit identifier

Three Phases in a Virtual-Circuit Network

In a virtual-circuit network, the communication between a source and destination involves three phases: **setup**, **data transfer**, and **teardown**. These phases ensure that a reliable path is established and maintained for the communication session.

1. **Setup Phase**:
    - The source and destination use their global addresses to establish a connection. During this phase, switches along the path create table entries to store information about the virtual circuit. This phase ensures that each switch is prepared to route the data properly.
2. **Data Transfer Phase**:
    - After the setup phase, data is transferred between the source and destination. The switches use the table entries created during the setup phase to route the frames.

The switches maintain information like the incoming and outgoing ports and Virtual Circuit Identifiers (VCI). Each frame is processed the same way, with the VCIs changing at each switch to ensure the data follows the correct path. This phase continues until all frames are transferred.

3. **Teardown Phase**:
    - Once the data transfer is complete, the source and destination send signals to the switches to remove the corresponding table entries, effectively ending the virtual circuit.

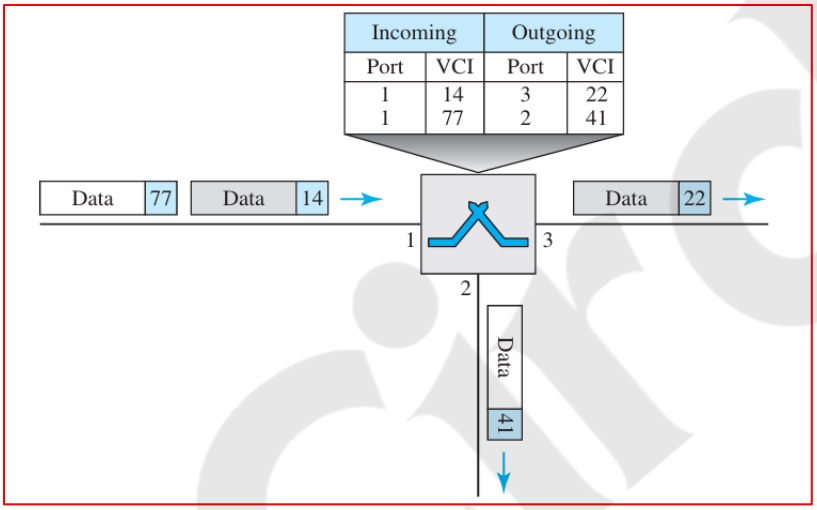

Figure 1.48: Switch and tables in a virtual-circuit network

Data-Transfer Phase

During data transfer, the key action is switching the frames between the source and destination. Each switch in the path must have a table with entries corresponding to the virtual circuit. A table typically consists of four columns: incoming port, incoming VCI, outgoing port, and outgoing VCI.

- When a frame arrives at a switch, the switch looks for the entry that matches the incoming port and VCI.
- After identifying the entry, the switch updates the VCI to the new value and forwards the frame to the next switch via the outgoing port.

For example, if a frame arrives at switch 1 with VCI 14 on port 1, the switch finds this entry in its table, updates the VCI to 22, and forwards the frame through port 3. This process repeats at each switch, ensuring the frame reaches its destination.

Setup Phase

In the setup phase, a virtual circuit is established between the source and destination by creating table entries at each switch. This phase consists of two main steps:

1. **Setup Request**:
    - A setup request frame is sent from the source (A) to the destination (B). As the frame passes through each switch, the switch creates an entry in its table.
    - For example, when the setup frame reaches switch 1, it identifies that the outgoing port for the connection is port 3 and assigns an incoming VCI (14) for the frame coming from port 1. At this point, the outgoing VCI remains unknown.

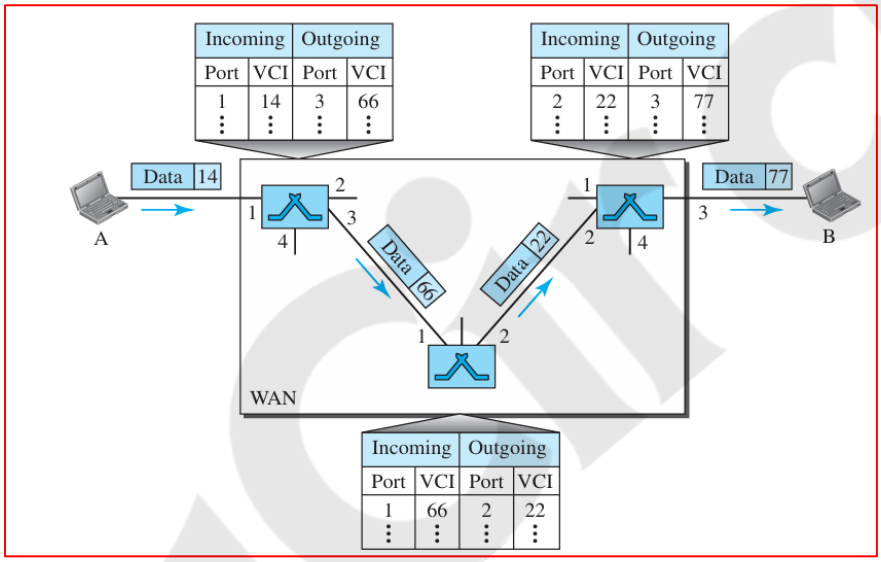

Figure 1.49: Source-to-destination data transfer in a virtual-circuit network

2. **Acknowledgment**:
    - Once the setup request reaches the destination, the destination assigns a VCI (e.g., 77) for incoming frames from the source. The acknowledgment is sent back to the source, and each switch updates its table to complete the missing outgoing VCI information.

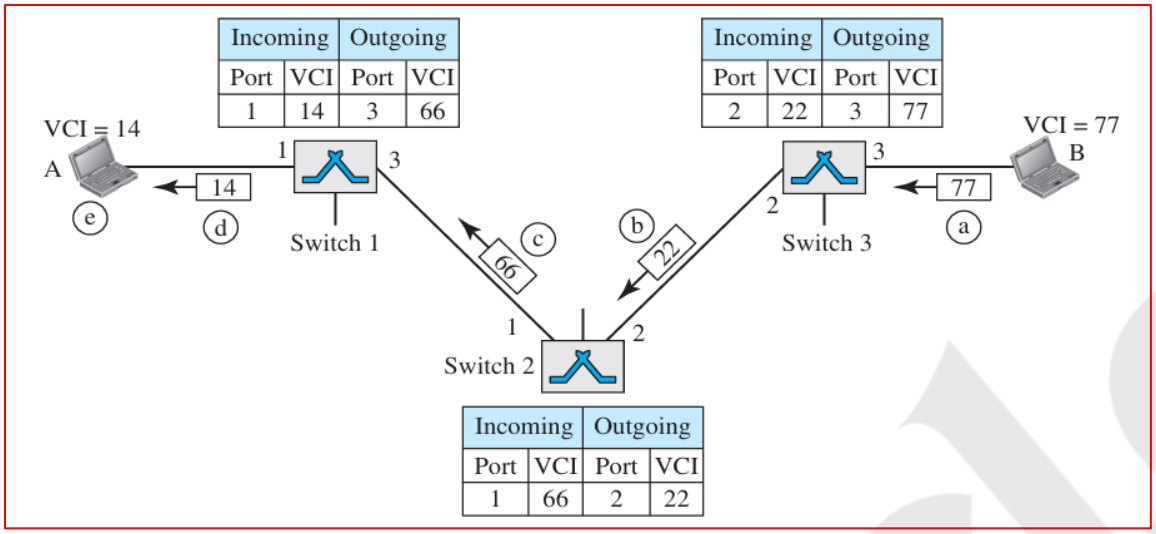

Figure 1.50: Setup acknowledgment in a virtual-circuit network

3. Teardown Phase

When the communication is finished, the source and destination send a signal to the switches to remove the corresponding table entries, thus ending the virtual circuit. This process frees up the resources for future virtual circuits.

Efficiency in Virtual-Circuit Networks

In a virtual-circuit network, resource allocation can happen either during the **setup phase** or on demand during the **data-transfer phase**. When resources are reserved during the setup phase, each packet experiences the same delay. However, if resources are allocated on demand, packet delays may vary.

Even when resource allocation is on demand, a significant advantage of virtual-circuit networks is that the source can check resource availability before data transfer.

In virtual-circuit switching, all packets from the same source to the same destination follow the same path. However, with on-demand resource allocation, packets may arrive with different delays depending on resource availability.

Delay in Virtual-Circuit Networks

In a virtual-circuit network, delays occur during the **setup** and **teardown** phases. These are one-time delays. If resources are allocated during setup, there is no additional waiting time for individual packets during data transfer.

The total delay in such a network includes:

- **Three transmission times (3T)**: the time taken for the packet to be transmitted across links.

- **Three propagation times (3τ)**: the time taken for the packet to travel across physical distances.
- **Setup delay**: includes transmission and propagation in both directions during the setup phase.
- **Teardown delay**: includes transmission and propagation in one direction during the teardown phase.

For simplicity, processing delays at the switches (routers) are ignored in this calculation.
Thus, the total delay for the packet is:

$$\boxed{Total\ delay = 3T + 3\tau + setup\ delay + teardown\ delay}$$

QUESTIONS

1. Data Communications

1. What are the five key components of a data communication system, and what role does each play in ensuring effective communication?
2. Explain the different forms of data representation used in data communications and provide examples for each.
3. Describe the three modes of data flow and provide real-world examples where each mode is used.

2. Networks

1. What are the key criteria used to evaluate the performance, reliability, and security of a network?
2. Explain the difference between point-to-point and multipoint physical structures in network connections. Provide advantages and disadvantages of each.

3. Network Types

1. Compare and contrast a Local Area Network (LAN) and a Wide Area Network (WAN) in terms of characteristics, speed, and geographical coverage.
2. Define packet switching and explain the key differences between circuit switching and packet switching.
3. Discuss the role of routers and switches in the structure of the Internet. How do they contribute to efficient data transfer?
4. What are the different ways to access the Internet, and how do factors like speed and coverage differ between these methods?

4. Protocol Layering

1. Explain the key principles of protocol layering and discuss how these principles ensure efficient communication between two devices over a network.
2. What are logical connections in the context of protocol layering, and how do they facilitate communication between peer layers on different devices?
3. Explain the layered architecture of the TCP/IP protocol suite. How does each layer contribute to overall network communication?
4. Discuss the main functions of the following layers in the TCP/IP protocol suite:
    a. Application Layer
    b. Transport Layer
    c. Network Layer
    d. Data Link Layer
    e. Physical Layer
5. Describe the process of encapsulation and decapsulation in the TCP/IP protocol suite. Why are these processes crucial for data communication?
6. Explain the different types of addresses used at each layer of the TCP/IP protocol stack. Why is addressing critical for network communication?
7. What is multiplexing and demultiplexing in the TCP/IP protocol suite? How do these processes ensure that data is correctly sent and received by the right application?

5. Transmission Media

1. Define guided media and list and explain three types of guided media used in network communications.
2. Explain the difference between unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cables. What are their primary uses?
3. Describe how the twisting of pairs in twisted-pair cables helps to reduce crosstalk.
4. What are the main components of a coaxial cable, and how do they contribute to its performance?
5. Describe the principle of operation of fiber-optic cables and explain why they provide high-speed data transmission.
6. Discuss the advantages and disadvantages of fiber-optic cables compared to coaxial and twisted-pair cables.
7. What are radio waves, and how are they used in wireless communication? Provide an example of a common application.
8. Explain the concept of frequency allocation in radio wave communication and its importance.
9. Discuss the characteristics of microwave transmission and its typical uses in communication systems.
10. Describe how infrared communication works and list two common applications where infrared technology is used.

6. Packet Switching

1. What is a datagram network? Describe its key characteristics and how it handles packet routing and delivery.
2. Compare and contrast datagram networks with virtual-circuit networks in terms of reliability, complexity, and overhead.
3. In a datagram network, how does the destination node determine the correct order of packets? What issues might arise from the unordered delivery of packets?
4. Explain how a datagram network handles packet fragmentation and reassembly. What are the potential impacts on network performance and reliability?
5. Define a virtual-circuit network and describe the main phases involved in setting up, maintaining, and tearing down a virtual circuit.
6. Discuss the advantages and disadvantages of virtual-circuit networks compared to datagram networks. Include aspects such as connection setup, resource allocation, and data transfer efficiency.
7. How does a virtual-circuit network handle data transfer once the connection is established? What mechanisms are in place to ensure data integrity and order?
8. Explain the role of signaling in virtual-circuit networks. How does signaling contribute to the establishment and teardown of virtual circuits?
9. Describe a scenario where virtual-circuit networks would be preferred over datagram networks. Justify your choice based on factors such as performance requirements and network management.