Bachelor of Computer Applications (BCA)

COMPUTER NETWORKS

(OBCACO304T24)

Self-Learning Material
(SEM III)

Jaipur National University
Centre for Distance and Online Education

Established by Government of Rajasthan
Approved by UGC under Sec 2(f) of UGC ACT 1956
&
NAAC A+ Accredited

TABLE OF CONTENTS

EXPERT COMMITTEE

Prof. Sunil Gupta
(Computer and Systems Sciences, JNU Jaipur)

Dr. Satish Pandey
(Computer and Systems Sciences, JNU Jaipur)

Dr. Shalini Rajawat
(Computer and Systems Sciences, JNU Jaipur)

COURSE COORDINATOR

Mr. Pawan Jakhar
(Computer and Systems Sciences, JNU Jaipur)

UNIT PREPARATION

Unit Writer(s)	Assisting & Proofreading	Unit Editor
Mr. Pawan Jakhar (Computer and Systems Sciences, JNU Jaipur) (Unit 1-5)	Mr. Satender Singh (Computer and Systems Sciences, JNU Jaipur)	Dr. Deepak Shekhawat (Computer and Systems Sciences, JNU Jaipur)
Mr. Hitendra Agarwal (Computer and Systems Sciences, JNU Jaipur) (Unit 6- 9)		

Secretarial Assistance

Mr. Mukesh Sharma

COURSE INTRODUCTION

On the internet, even private is public. ~Terri Guillemets, 2007

This course has 3 credits and is divided into 9 Units. The main emphasis of this course is on the organization and management of local area networks (LANs). The course objectives include learning about computer network organization and implementation, obtaining a theoretical understanding of data communication and computer networks, and gaining practical experience in installation, monitoring, and troubleshooting of current LAN systems. The course introduces computer communication network design and its operations. The course includes the following topics: Open Systems Interconnection (OSI) communication model; error detection and recovery; local area networks; bridges, routers and gateways; network naming and addressing; and local and remote procedures. On completion of the course, the student should be able in part to design, implement and maintain a typical computer network (LAN).

Course Outcomes:

At the completion of the course, a student will be able to:

1. Independently understand basic computer network technology.
2. Identify the different types of network topologies and protocols.
3. Enumerate the layers of the OSI model and TCP/IP. Explain the function(s) of each layer.
4. Identify the different types of network devices and their functions within a network
5. Understand the basic protocols of computer networks, and how they can be used to assist in network design and implementation.

Acknowledgements:

The content we have utilized is solely educational in nature. The copyright proprietors of the materials reproduced in this book have been tracked down as much as possible. The editors apologize for any violation that may have happened, and they will be happy to rectify any such material in later versions of this book.

Unit 1: Network Characterisation

Learning Outcomes:

- Students will be able to define the goals and applications of computer networks.
- Students will be able to categorise networks based on size, purpose, design issues, and transmission technologies.
- Students will be able to compare the OSI and TCP/IP reference models, emphasising key differences.
- Students will be able to explain the functions of layers and protocols in the TCP/IP model.
- Students will be able to demonstrate an understanding of data transmission using TCP/IP and apply this knowledge in practical scenarios.

Structure:

1.1 Network Characterisation

- **Goals and Applications:**

Goals of Computer Networks:

1. **Resource Sharing:** Enable multiple users to share resources like printers, files, and applications. Enhances resource utilisation efficiency, minimising the need for redundant resources.

2. **Reliability:** Ensure data availability and network accessibility despite failures.Boosts overall network dependability, crucial for ensuring uninterrupted operations.
3. **Communication:** Facilitate efficient and timely communication among users and devices. Improves collaboration, information flow, and decision-making processes.
4. **Cost Efficiency:** Minimise costs related to hardware, software, and maintenance.
   Promotes effective resource utilisation and cost-effective network management.
5. **Scalability:** Design networks capable of easy expansion to accommodate growing user and device numbers.
   Ensures adaptability to changing organisational requirements and technological advancements.
6. **Performance:** Optimise network speed and efficiency for a satisfactory user experience.
   Supports applications with low latency requirements, such as real-time video conferencing.
7. **Security:** Protect data from unauthorised access, ensure privacy, and prevent network attacks.
   Critical for safeguarding sensitive information and maintaining network integrity.
8. **Manageability:** Simplify network administration and troubleshooting processes. Reduces operational complexities, enhancing overall network manageability.

Applications of Computer Networks:

1. **File Sharing:** Users can collaboratively access and share files across the network.
2. **Email and Communication:** Email, instant messaging, and video conferencing facilitate real-time communication.
3. **Internet Access:** Provides users with internet access for research, online services, and information retrieval.
4. **Remote Access:** Allows users to connect to the network remotely, enhancing flexibility and productivity.
5. **Distributed Computing:** Enables the distribution of computational tasks across networked computers for parallel processing.
6. **Database Access:** Facilitates access and manipulation of databases over the network, supporting data storage and retrieval.

7. **Print Serving:** Enables multiple users to share printing resources, reducing the need for individual printers.
8. **Collaborative Tools:** Supports collaborative tools and platforms, fostering teamwork and project management.
9. **E-commerce:** Enables online transactions, electronic payments, and e-commerce activities.
10. **Cloud Computing:** Utilises network resources to deliver computing services, storage, and applications over the Internet.

- **Categorisation according to Size, Purpose, Design issues, & Transmission Technologies:**

Categorisation according to size: Computer networks can be categorised as follows:

1. **Personal Area Network (PAN):** Connects devices within an individual workspace, typically within a few meters.

   Characteristics**:** Utilises technologies like Bluetooth or infrared for short-range communication.

   Examples include connecting a smartphone to a laptop or using wireless headphones.
2. **Local Area Network (LAN):** Spans a limited geographic area, such as a single building, campus, or office.

   Characteristics: High data transfer rates, suitable for resource sharing and collaborative work.

   Commonly employs Ethernet technology and various topologies like star or bus.
3. **Metropolitan Area Network (MAN):** Covers a larger geographic area than "LAN" but is confined to a city or metropolitan region.

   Applications: Connects multiple LANs within the same city, often used for city-wide networking.

   Enables the interconnection of various organisational branches.
4. **Wide Area Network (WAN):** Spans a large geographic area, often across cities, countries, or continents.

   Transmission: Utilises public or private communication links, including leased lines or satellite connections.

   Characteristics: Supports lower data transfer rates compared to LANs but facilitates long-distance connectivity.

   The backbone for global communications, linking remote offices or data centres.

5. **Global Area Network (GAN):** Encompasses a global scale, connecting networks across the world.

   Technology: Relies on satellite communication, submarine cables, and long-distance technologies.

   Significance: Forms the foundation for the global Internet, enabling worldwide connectivity. Facilitates international communication and data exchange.

Categorisation according to Purpose:

1. **Home Network:** Connects devices within a household, facilitating resource sharing and internet connectivity.

   Components: Typically includes a router, computers, smart TVs, and other smart devices.

   Use Cases: Enables sharing of files, printers, and internet access among family members. Supports the integration of smart home devices for automation.
2. **Enterprise Network:** Serves the communication needs of a business or organisation.

   Components: Comprises intranets, extranets, servers, and various networked services.

   Characteristics: Emphasises security, scalability, and efficient data management.

   Facilitates internal and external communication for employees.
3. **Internet:** A global network connecting millions of smaller networks.

   Characteristics: Enables worldwide communication, information exchange, and online services.

   Use Cases: Provides access to a vast array of resources, including websites, emails, and multimedia content. Supports e-commerce, social networking, and collaborative platforms.
4. **Intranet:** An internal network within an organisation, isolated from the public internet.

   Functionality: Hosts internal services, documents, and collaborative tools for employees.

   Benefits: Enhances internal communication, knowledge sharing, and document management. Provides a secure platform for sensitive company information.
5. **Extranet:** An extension of an intranet that allows limited external access.

   Use Cases: Facilitates collaboration with suppliers, clients, or partners. Enables secure sharing of specific resources with external entities.

   Security Measures: Implements access controls to regulate external user permissions. Ensures secure data exchange with authorised external parties.

Categorisation of Computer Networks According to Design Issues:

1. Topology: Refers to the physical or logical arrangement of devices in a network.

Types:

Star Topology:

Centralised with all devices connected to a central hub.

Advantages include fault isolation, but it is dependent on the central hub.

Ring Topology:

Devices are connected in a circular fashion.

Ensures continuous data flow but is susceptible to a single point of failure.

Mesh Topology:

Every device is connected to every other device.

Provides high redundancy but can be complex to implement.

2. Scalability: The ability of a network to accommodate growth in terms of users, devices, or data.

Considerations: Achieved through hardware upgrades, load balancing, and efficient network protocols. Ensures the network can adapt to increased demands without compromising performance.

3. Reliability: Ensuring continuous and reliable network operation.

Strategies: Implementing redundancy measures such as backup links and servers. Employing fault tolerance mechanisms to minimise downtime. Regular maintenance and monitoring to identify and address potential issues promptly.

4. Security: The implementation of measures to protect data and prevent unauthorised access.

Components: Firewalls to control incoming and outgoing network traffic. Encryption protocols for securing data in transit. Access control mechanisms to restrict unauthorised access to network resources.

5. Performance: Optimising network speed, bandwidth, and latency.

Optimisation Techniques: Efficient protocols like Transmission Control Protocol (TCP) for reliable data transfer. Quality of Service (QoS) implementations for prioritising critical traffic.

Bandwidth management and optimisation for improved overall network performance.

Categorisation of Computer Networks According to Transmission Technologies:

1. Wired Technologies:

i. Ethernet: Ethernet is a widely used wired technology for "Local Area Networks" (LANs), standardised by "Institute of Electrical and Electronics Engineers" (IEEE) under 802.3 standard.

Media: It operates over various media types, with twisted pair and fiber optic cables being the most common.

Speeds: Ethernet supports different speeds, ranging from traditional Fast Ethernet (100 Mbps) to Gigabit Ethernet (1 Gbps) and even 10 Gigabit Ethernet for higher data rates.

Applications: Commonly deployed in LAN environments, Ethernet facilitates high-speed and reliable data transfer within a confined geographic area.

ii. Fiber Optics: Advantages: Fiber optic cables use light signals for data transmission, offering significantly higher bandwidth compared to traditional copper cables.

They are immune to electromagnetic interference, making them suitable for environments with high electrical noise.

Applications: Fiber optics are widely employed for long-distance communication, connecting cities or even continents. Fibre optics serve as backbone networks in networking, supporting high-speed and long-distance data transmission.

iii. Coaxial Cable: Structure: Coaxial cable consists of a central conductor insulated from an outer metal shield by a dielectric insulator.

Applications: Historically used in cable television networks to deliver television signals. In networking, coaxial cable has been largely replaced by other technologies like twisted pair and fiber optics but is still occasionally used in specific applications.

2. Wireless Technologies:

i. Wi-Fi (Wireless Fidelity): Standards: Wi-Fi is based on IEEE 802.11 standards, with various amendments (e.g., 802.11ac, 802.11ax) to improve performance.

Applications: Wi-Fi is prevalent in wireless LANs, providing connectivity for devices like smartphones, laptops, tablets, and smart home devices.

It allows for flexible and convenient access to the network without the need for physical cables.

ii. Bluetooth: Range: Bluetooth is a short-range wireless technology, typically operating within a range of about 10 meters.

Applications: Commonly used for connecting devices in proximity, such as wireless keyboards, mice, headphones, and smartphones.

Bluetooth facilitates the creation of Personal Area Networks (PANs) for device-to-device communication.

iii. Cellular Networks: Generations: Cellular networks have evolved through generations, including 2G, 3G, 4G, and 5G, each introducing speed, capacity, and functionality improvements.

Applications: Cellular networks provide mobile communication services, allowing users to make voice calls, send text messages, and access data services.

They cover large geographic areas, enabling wireless connectivity for mobile devices in diverse locations.

- **Network Architecture and Service Models**

Network architecture can be divided into two parts as follows:

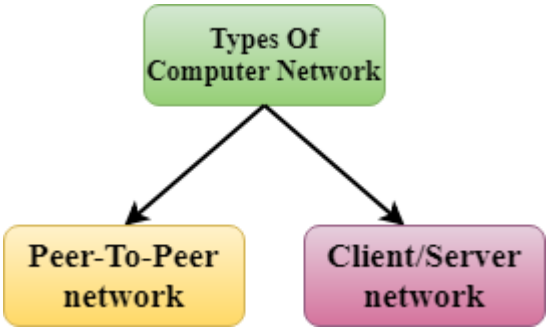


Figure 1.1: Types of computer network

1. Client-Server Architecture:

In a client-server architecture, the network is organised around the concept of clients and servers. Clients are "devices that request services, and servers are devices that provide those services".

Key Characteristics:

Centralised Model: Services are centralised on dedicated servers, and clients communicate with these servers to access resources or services.

Communication Flow: Clients initiate requests, and servers respond to those requests. The server handles resource-intensive tasks.

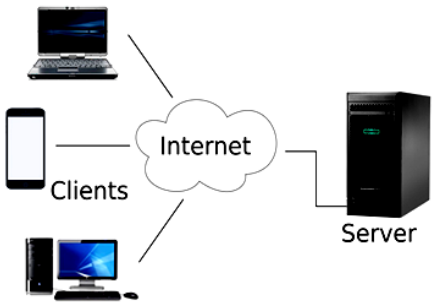


Figure 1.2: Client-Server Architecture

Advantages:

Centralised Control: Easier management and control of resources and security policies.

Specialised Servers: Servers can be specialised for specific tasks, enhancing efficiency.

2. Peer-to-Peer (P2P) Architecture:

In a P2P architecture, all devices in network can act as both clients and servers, sharing resources directly without a centralised server.

Key Characteristics:

Decentralised Model: No central server; all devices are equal and can communicate directly with each other.

Resource Sharing: Devices can share files, processing power, or other resources without relying on a dedicated server.

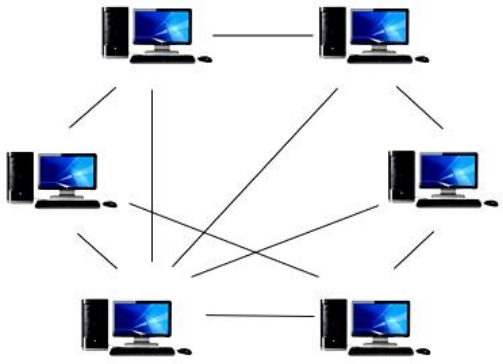


Figure 1.3: Peer-to-Peer Architecture

Advantages:

Decentralisation: No single point of failure, making the network more robust.

Scalability: Easily scalable as each device contributes to the network's capabilities.

- **Design issues for the Layers:**

1. Introduction:

Designing the layered architecture of a computer network involves addressing various critical issues to ensure its efficiency, scalability, and robustness. Here are key design considerations for the layers:

2. Layer Independence:

Ensure that each layer operates independently without relying on the internal details of other layers.

Implementation: Achieved through well-defined interfaces and standardised protocols.

Allows for changes or upgrades in one layer without affecting the functionality of other layers. Enhances modularity, making the network more flexible and easier to manage.

3. Encapsulation:

Protect data integrity during transmission by adding headers and trailers at each layer. Each layer adds its own information to the data, creating a layered structure.

Enables data to traverse heterogeneous networks without losing its original format.

Facilitates data security, as each layer's information remains encapsulated until it reaches its destination.

4. Compatibility:

Ensure seamless communication between devices and systems, even from different manufacturers. Adherence to standardised protocols ensures interoperability.

Compatibility extends to hardware, software, and communication protocols. Enables the integration of diverse devices into a unified network environment.

5. Scalability:

Design network to accommodate growth in terms of “users, devices, and data volume”.

Scalability involves the ability to handle increased traffic and data without compromising performance. Implemented through scalable protocols, efficient routing mechanisms, and adaptable network architectures.

Ensures that the network can evolve to meet the demands of a growing user base and technological advancements.

6. Performance Optimisation:

Optimise the performance of each layer to achieve efficient data transmission.

Implementation of algorithms and protocols that minimise latency and maximise throughput. Balancing the trade-off between reliability and speed, depending on the requirements of specific applications.

Regular monitoring and optimisation to maintain optimal performance levels as network conditions change.

7. Security:

Implement measures to protect the network from unauthorised access, data breaches, and other security threats. Integration of encryption protocols to secure data during transmission. Implementation of firewalls, intrusion detection systems, and other security mechanisms. Regular updates and patches to address vulnerabilities and ensure network resilience against evolving threats.

8. Interoperability:

Enable different devices and systems to work together seamlessly within the network. Adherence to open standards and widely accepted protocols.

Testing and certification processes to ensure compatibility between different vendors' products. Facilitation of communication and data exchange between diverse devices, fostering a more versatile network ecosystem.

9. Maintainability:

Design the network in a way that allows for easy maintenance, troubleshooting, and upgrades. Clear documentation of network configurations, protocols, and procedures.

Implementation of effective monitoring tools to identify and address issues promptly.

Training of network administrators for efficient management and maintenance.

- **OSI and TCP/IP Reference Models**

The “OSI” reference model is the “hierarchical structure of seven layers that defines the requirements for communication between two computers”. The International Standards Organisation defined model.

The OSI model was created with the following principles:

1. “A layer should be created where a different level of abstraction is necessary so that each layer can perform a well-defined function”.

2. "The function of each layer should conform to the internationally standardised protocols".
3. "Layer boundaries should be such that minimum information flows across the interfaces".

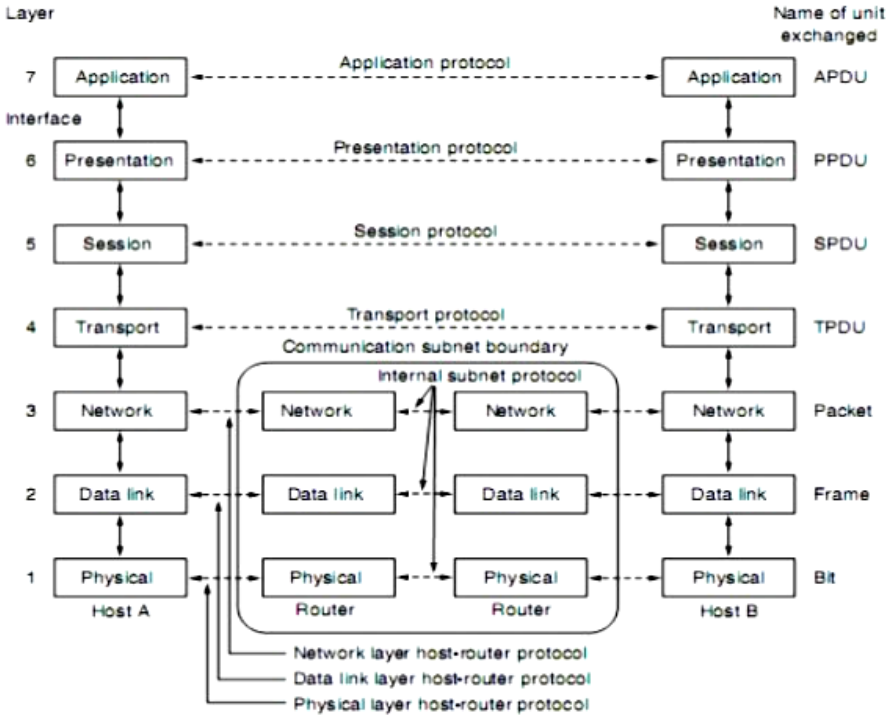


Fig. ISO-OSI Reference Model

1. Physical Layer:

It is concerned with transmitting raw bits over a communication channel. It deals with physical layer devices and components required for data communication.

The physical layer deals with the following issues:

- **a. Mechanical:**"Consider the physical properties of the medium and interfaces between devices like connectors, cables, etc".
- **b. Signal representation: "**How to represent data bits on the transmission medium Encoding mechanism".
- **c. Timing:** Number of bits sent per second, i.e., transmission rate and bit duration.
- **d. Synchronisation:** Sequence of events, Synchronisation between sender and receiver, connection establishment, release, etc, simplex or duplex communication.

e. **Line Configuration:** Connection of devices to communication links – point-to-point, multipoint, etc.
f. **Physical topology:** How to connect the devices- mesh, star, ring, etc.
g. **Devices operating at the Physical Layer:** Hub, Repeater.

2. Data Link Layer:

The data link layer, the second layer in both the OSI (Open Systems Interconnection) model and the TCP/IP model, plays a pivotal role in facilitating reliable communication between network devices. It operates primarily at the local area network (LAN) level, focusing on the transmission of data frames over the physical layer, which encompasses the actual transmission medium, such as Ethernet cables or Wi-Fi signals.

Within the data link layer, there are two primary sublayers:

1. **Logical Link Control (LLC) Sublayer:** The LLC sublayer serves as an interface between the higher-level network layer and the underlying MAC (Media Access Control) layer. Its main function is to provide a uniform interface to the network layer protocols, ensuring that data frames are delivered to the correct destination. The LLC sublayer also handles error detection and correction, flow control, and frame synchronization.

2. Media Access Control (MAC) Sublayer: The MAC sublayer is responsible for controlling access to the physical transmission medium and addressing devices on the network. It assigns unique identifiers, known as MAC addresses, to network interface cards (NICs) to facilitate communication between devices within the same network segment. The MAC sublayer also manages frame transmission, including frame assembly, collision detection, and collision avoidance mechanisms.

The main functions of the data link layer include:

1. Frame Synchronization: Ensuring that data frames are properly synchronized and delimited to facilitate accurate transmission and reception.

2. Error Detection and Correction: Detecting and correcting errors that may occur during data transmission using techniques such as checksums and cyclic redundancy checks (CRC).

3. Flow Control: Managing the rate at which data is transmitted between network devices to prevent buffer overflow and ensure efficient communication.

4. Addressing: Assigning unique identifiers (MAC addresses) to network devices to enable accurate addressing and routing of data frames within the local network segment.

5. Access Control: Controlling access to the physical transmission medium to prevent collisions and ensure fair and efficient use of network resources.

Overall, the data link layer acts as a crucial intermediary between the physical layer and the higher-level network protocols, providing the necessary mechanisms for reliable and efficient communication within a local network environment.

3. **Network Layer :**The network layer is responsible for the transfer of data packets from source to destination machines across the communication subnet, i.e. across multiple networks.
The Main functions of the Network Layer are:

a. **Addressing:** The network layer identifies a machine on the basis of its logical address (the data link layer uses a physical address). The logic identifies the network to which the machine belongs.
b. **Routing:** Routing packets from source to destination is a key design issue. Therefore, routine algorithms are used.
c. **Congestion control:** Since the data packets have to travel through the communication subnet, congestion control is another function of this layer.
d. **Devices operating at Network Layer:** Router.

4. **Transport Layer :** The transport layer is responsible for end-to-end communication, ensuring process-to-process delivery from the source to the destination. Its primary role is to guarantee that the entire message arrives at the destination intact and in the correct order. By doing so, it

shields the upper layers from the complexities of the physical and logical characteristics of the subnet, providing a simplified interface to the end users.

Main functions of the Transport Layer:

a. Port Addressing: The transport layer identifies the specific application on the host machine for which the data is intended through a port address.

b. Segmentation and Reassembly: This layer handles the division of larger messages into smaller segments when necessary and ensures their correct sequencing and reassembly at the destination.

c. Service Type Determination: It determines the type of service to provide to the upper layers, whether connectionless or connection-oriented.

d. Flow and Error Control: The transport layer provides end-to-end flow control and ensures the error-free delivery of data.

e. Devices Operating at Network Layer: The transport layer interacts with devices such as gateways that operate at the network layer.

5. Session Layer :

The session layer enables users on different machines to establish sessions with each other. It provides various services, such as dialog control (handling both half-duplex and full-duplex communication), token management (preventing simultaneous execution of critical operations by both parties), authorization, synchronization, and checkpoint mechanisms. These checkpoints ensure that communication can resume from the last successful point in case of a crash.The Main functions of the Session Layer are :

a. Dialog Control: This function allows communicating entities to establish a dialog that can be either half-duplex or full-duplex.

b. Synchronization: It enables the addition of checkpoints, so communication can continue from these points in case of a crash or disconnection**.**

6. Presentation Layer:

The presentation layer deals with the syntax and semantics of the information being transmitted. It defines the data formats to be exchanged between applications and provides services like data format transformation, encryption, and compression.

Main functions of the Presentation Layer:

a. **Translation**: This function translates data from an application-specific format to a standard format suitable for network transmission.

b. **Encryption**: This allows for the encryption of data to ensure the secrecy and security of sensitive information.

c. **Compression**: This reduces the size of large data volumes, such as videos, images, and audio, to optimize bandwidth usage.

7. Application Layer:

The application layer provides a platform for user applications to access network services. It encompasses a variety of services commonly used by users, such as file transfer, email, remote terminal access, and web access.

Services provided by the Application Layer:

a. **File Transfer**: This service enables users to send, access, and retrieve files on remote machines. b. **Email**: This service allows users to create, send, and receive electronic mail.

c. **Remote Access**: Also known as network virtual terminal service, it allows users to log into remote machines.

1.2 Summary

- Explore the diverse purposes of computer networks, from resource sharing to communication and collaboration.
- Classify networks based on their size, intended purpose, design considerations, and the underlying transmission technologies.
- Examine network architectures, distinguishing between client-server and peer-to-peer models, and understand how services are delivered in these structures.
- Analyse specific challenges encountered at each layer during the design of a network, addressing issues related to functionality and interoperability.

- Understand the conceptual frameworks of the OSI and TCP/IP models, which provide a structured approach to network communication.
- Explore the functions and specific protocols associated with each layer of the TCP/IP model, which is fundamental for internet communication.
- Contrast the OSI model and the TCP/IP model in terms of their layering, functionality, and adoption in network architectures.
- Delve into the process of data transmission over networks using the TCP/IP protocol suite, emphasising reliability and efficiency.

1.3 Keywords

- **TCP/IP "(Transmission Control Protocol/Internet Protocol)":** A suite of communication protocols that form foundation of Internet.
- **OSI "(Open Systems Interconnection Reference Model)":** A conceptual framework defining functions of telecommunication or computing system into seven abstraction layers.

1.4 Self-Assessment Questions

1. What are the primary goals and applications of computer networks?
2. Explain the categorisation of networks based on size, purpose, design issues, and transmission technologies.
3. How does network architecture influence the design and functionality of a network?

1.5 References / Reference Reading

- Data Communications and Networking By Behrouz A.Forouzan.

Unit 2: TCP/IP

Learning Outcomes:

- Students will be able to define the goals and applications of computer networks.
- Students will be able to categorise networks based on size, purpose, design issues, and transmission technologies.
- Students will be able to compare the OSI and TCP/IP reference models, emphasising key differences.
- Students will be able to explain the functions of layers and protocols in the TCP/IP model.
- Students will be able to demonstrate an understanding of data transmission using TCP/IP and apply this knowledge in practical scenarios.

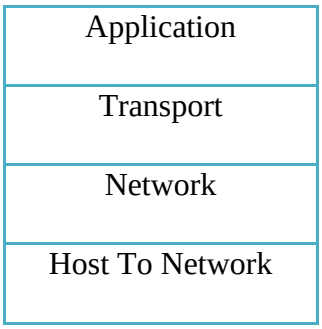
Structure:

2.1 Network Characterisation

- **Functions of layers and protocols of TCP/IP**

TCP/IP means "Transmission Control Protocol" and "Internet Protocol". This model is used in Internet architecture. These protocols describe "the movement of data between the source and destination or the internet".

The TCP/IP model is a four layered model as shown below.



TCP/IP Model

1. **Host-to-host Layer:** The "TCP/IP" model does not define for low-level communication. This layer corresponds to "physical and Data Link layer" of "OSI" model. It supports any low-level communication protocol.
2. **Network (Internet) Layer:** The requirement to connect multiple diverse networks in a seamless manner led to choice of a packet-switching network. This network is based on a connectionless communication layer. This layer is called "*Internet layer"*. The main job of this is to transport data packets (datagram) from the source machine to the destination. These datagrams travel independently and hence may arrive in a different order than they are sent.
   a. **Internet Protocol (IP):** The network layer protocol in TCP/IP model is IP (Internet Protocol), which takes care of addressing and routing the diagrams through the internetwork. Hence, its functionality is similar to the OSI network layer. It is an "unreliable", "connectionless protocol" that operates on a best-effort delivery basis. This implies that the protocol does not ensure "error-free transmission".
   b. **Network layer Protocol:**IP(Internet Protocol), ICMP(Internet Control Message Protocol), ARP(Address Resolution Protocol), DHCP(Dynamic Host Configuration Protocol)
3. **Transport Layer (Host-to-Host):** This layer is designed to allow communication "between peer entities on the source and destination hosts, just as in the OSI transport layer". Two end-to-end protocols are defined in this layer.
   a. **TCP (Transmission Control Protocol):** TCP is a "dependable, connection-oriented protocol" that ensures end-to-end delivery without errors. It manages the "reassembly of packets at the destination and uses flow control to prevent a fast sender from overwhelming a slow receiver". TCP divides data into smaller units called "segments",

which are encapsulated within IP packets for transmission. At the receiving end, TCP reassembles these segments into a single data stream and delivers them to the application layer.

b. UDP (User Datagram Protocol): UDP is an "unreliable, connectionless protocol" primarily used in scenarios where prompt delivery is prioritized over accuracy, such as client-server and request-reply applications. Since it is connectionless, UDP has lower overhead compared to TCP.

4. Application Layer: This model does not have a session and presentation layer. The application layer contains an "all higher-level protocol" for commonly required user services like e-mail(SNTP), File transfer(FTP), Remote Terminal Access (TELNET), Domain name system (DNS) for mapping host names to network addresses, access to the world wide web (HTTP)

- **Comparison of OSI & TCP/IP**

OSI Model:

1. Developed by the "International Organization for Standardization" (ISO).
2. Comprises seven layers: "Physical, Data Link, Network, Transport, Session, Presentation, and Application".
3. Each layer has specific functions and interacts with adjacent layers.
4. Aims for protocol independence, providing a theoretical framework for network communication.
5. Emphasizes rigid layering with distinct boundaries between layers.
6. Used as a reference model for understanding and designing network architectures.
7. Provides detailed guidelines for error detection and correction.

TCP/IP Model:

1. Developed by the U.S. Department of Defense (DoD).
2. Consists of four layers: Network Interface, Internet, Transport, and Application.
3. Built around specific protocols like TCP, UDP, and IP.
4. Offers greater flexibility, allowing layer functions to overlap as needed.
5. Widely implemented in real-world networking scenarios.

6. Focuses more on practical error handling and flow control mechanisms.
7. Forms the basis of the internet and is widely used for actual network communication.

This comparison highlights the differences in development, structure, flexibility, and practical application between the OSI and TCP/IP models.

- **Data Transmission using TCP/IP**

Introduction: Data transmission is a fundamental aspect of computer networks, enabling the exchange of information between devices. The TCP/IP (Transmission Control Protocol/Internet Protocol) suite, a foundational set of protocols, plays a crucial role in ensuring reliable and efficient data transmission across the Internet.

TCP/IP Protocol Stack:

The TCP/IP protocol stack comprises four essential layers: "Link, Internet, Transport, and Application". Each layer has specific functions that contribute to the seamless flow of data across networks.

Link Layer:

The Link Layer is responsible for framing data for transmission and handling physical addressing. Protocols such as Ethernet and Address Resolution Protocol (ARP) operate at this layer, facilitating efficient data transmission within a local network.

1. **Internet Layer:** The Internet Layer focuses on routing packets across different networks based on logical addressing. Internet Protocol (IP) assigns unique addresses to devices and plays a key role in forwarding packets between networks. The Internet Control Message Protocol (ICMP) is crucial for error reporting and diagnostics.
2. **Transport Layer:** Ensuring reliable end-to-end communication is the primary function of the Transport Layer. TCP, a connection-oriented protocol, handles ordered and reliable data delivery. In contrast, User Datagram Protocol (UDP) is connectionless, providing faster but non-guaranteed delivery suitable for real-time applications.
3. **Application Layer:** The top layer, the Application Layer, is where end-user interactions are governed. Protocols like "Hypertext Transfer Protocol" (HTTP), "File Transfer Protocol" (FTP), and "Simple Mail Transfer Protocol" (SMTP) operate at this layer, enabling various applications to communicate over the network.

Data Transmission Process:

The process of data transmission using TCP/IP involves a sequence of steps across these layers:

Link Layer: Frames data for transmission and manages physical addressing.

Internet Layer: Routes packets based on logical addressing.

Transport Layer: TCP ensures reliable and ordered delivery, while UDP provides faster but connectionless communication.

Application Layer: Governs end-user interactions, defining how data is presented and exchanged.

Advantages of TCP/IP:

Reliability: TCP ensures reliable and ordered delivery of data, which is crucial for applications requiring accuracy.

Versatility: TCP/IP supports a wide range of applications, from web browsing (HTTP) to file transfers (FTP).

Compatibility: Being a universal protocol suite, TCP/IP is widely adopted and compatible across diverse devices and platforms.

Scalability: TCP/IP accommodates both small-scale and large-scale networks, making it scalable for various requirements.

Challenges and Considerations:

Overhead: TCP introduces additional overhead due to connection establishment and error recovery mechanisms.

Real-Time Constraints: UDP, while faster, does not guarantee data delivery, making it unsuitable for applications sensitive to packet loss.

Security: Additional security measures, such as encryption, are often required to protect data during transmission over public networks.

- **Knowledge Check 1**

Fill in the Blanks.

1. Networks can be categorised based on their _____ (size, purpose), _____ considerations, and underlying _____ technologies. (**Security,Communication/path**, series)

2. Network architecture encompasses the structure and organisation of a network, while service models define how _____ are delivered over the network. (**Services**_/ products)
3. Design issues at each layer in a network address specific challenges to ensure _____ and interoperability. (**Efficiency**/ Dependency)
4. The OSI and TCP/IP reference models provide conceptual frameworks for understanding network _____ and communication. (**Protocol**/ rules)
5. Each layer in the TCP/IP model serves specific functions, and protocols at each layer facilitate _____ communication. (**End-to-end**/ peer-to-peer)

- **Outcome-Based Activity 1**

  Design a network solution for an organization emphasizing communication efficiency, secure data transmission, scalability, and cost-effectiveness. Include applications like email, file sharing, database access, video conferencing, and cloud services. Categorize the network as medium-sized, primarily for internal communication and data access, addressing scalability, security, and data transmission efficiency. Choose a star network architecture with client-server and peer-to-peer models. Use Ethernet for wired connections and Wi-Fi for wireless. Implement the TCP/IP model for reliability and efficiency. Conclude with a comparative analysis, highlighting TCP/IP's wider adoption due to its practicality.

2.2 Summary

- Differentiate between centralised, decentralised, and distributed network architectures, each with unique characteristics in terms of control and resource distribution.
- Explore the characteristics of client-server and peer-to-peer network structures, understanding how devices interact within these models.
- Understand the dynamics of file sharing networks and web-based applications, considering the implications for distributed collaboration and information sharing.
- Gain insights into Content Distribution Networks (CDN) and their role in efficiently delivering web content by strategically distributing it across multiple servers.
- Understand the fundamental concept and structure of the Internet as a global network of interconnected devices.

- Explore the methods through which users connect to and access resources on the Internet, considering various technologies and protocols.
- Learn about X.25 networks, which operate on a connection-oriented communication model, and understand their historical significance.

2.3 Keywords

- **CDN: Content Distribution Network:** A system of distributed servers that work together to deliver web content more efficiently to users based on their geographic locations.

2.4 Self-Assessment Questions

1. Identify and discuss design issues specific to different layers in a network.
2. Compare the OSI and TCP/IP reference models, highlighting key similarities and differences.

2.5 References / Reference Reading

- Data Communications and Networking By Behrouz A.Forouzan.

Unit 3: Networking Models & Applications

Learning Outcomes:

- Students will be able to define the goals and applications of computer networks.
- Students will be able to categorise networks based on size, purpose, design issues, and transmission technologies.
- Students will be able to compare the OSI and TCP/IP reference models, emphasising key differences.
- Students will be able to explain the functions of layers and protocols in the TCP/IP model.
- Students will be able to demonstrate an understanding of data transmission using TCP/IP and apply this knowledge in practical scenarios.

Structure:

3.1 Networking Models & Applications

Networking models serve as blueprints for designing and implementing computer networks. They provide a structured approach to understanding how data flows within a network. Three fundamental networking models—Centralised, Decentralised, and Distributed—offer different paradigms for organising and managing network resources.

- **Centralised, Decentralised, and Distributed:**

Centralised Networking Model:

In a centralised networking model, a single central node or server holds significant control and authority over the entire network.

Characteristics:

Single Control Point: A central server governs all network resources and decisions.

High Dependency: The entire network's functionality relies on the central node.

Scalability Challenges: Difficult to scale as the network grows, potentially leading to performance bottlenecks.

Applications:

Client-Server Architectures:

Often used in client-server models where clients request services or resources from a centralised server.

Enterprise Networks: Suited for small to medium-sized enterprises with centralised data storage and management needs.

Decentralised Networking Model: In a decentralised networking model, control and decision-making are distributed among multiple nodes or entities within the network.

Characteristics:

Distributed Authority: Each node possesses a degree of autonomy and decision-making capability.

Improved Scalability: More scalable than centralised models as tasks are distributed among multiple nodes.

Reduced Dependency: Less reliance on a single point of control, enhancing network resilience.

Applications:

Peer-to-Peer Networks: Common in peer-to-peer (P2P) architectures where nodes can act as both clients and servers.

Collaborative Systems: Utilised in collaborative platforms where multiple users contribute to shared resources.

Distributed Networking Model:

Distributed networking involves interconnected nodes working together to achieve a common goal, and there is no single point of control.

Characteristics:

Shared Control: Control and decision-making are distributed across multiple nodes without a single point of authority.

Enhanced Fault Tolerance: Greater resilience to failures as the network can adapt to the loss of individual nodes.

Complexity: More complex in terms of design and management due to the absence of a central controller.

Applications:

Cloud Computing: Fundamental in cloud computing, where resources are distributed across multiple servers.

Blockchain Technology: Utilised in blockchain networks where the ledger is distributed among all participating nodes.

Content Delivery Networks (CDN): CDNs distribute content across multiple servers globally for efficient content delivery.

- **Client-Server and Peer-to-Peer**

Client-Server Model:

Definition: The client-server model is a network architecture where tasks are divided between the client, which requests services or resources, and the server, which provides these services or resources.

Communication Flow: Clients initiate requests to servers, and servers respond to those requests. This model enables centralised control and efficient resource management.

Examples: Web browsing is a common example, where the client (web browser) requests web pages from a server, and the server delivers the requested content.

Peer-to-Peer Model:

Definition: In a peer-to-peer (P2P) network, all devices (peers) have equal status and can act as both clients and servers. Each peer can request and provide services or resources.

Communication Flow: Peers communicate directly with each other without the need for a centralised server. This decentralised structure promotes collaboration and resource sharing among peers.
Examples: File-sharing applications like BitTorrent use a peer-to-peer model, where users share files directly with one another without relying on a central server.

- **File sharing & Web-based:**

File Sharing: File sharing is a core aspect of computer networking that enables the exchange of digital files between connected devices. It's a mechanism for distributing and accessing documents, media, software, and other data across a network.

Mechanism: Client-Server Model: In this model, a central server is responsible for storing and managing files. Clients, which can be computers or devices, request access to these files.
Peer-to-Peer (P2P) Model: In a P2P network, individual devices, or "peers," share files directly with each other without the need for a centralised server. This decentralised approach enhances scalability and resilience.

Protocols: Server Message Block (SMB): Commonly used in Windows environments, SMB facilitates file and printer sharing.
Network File System (NFS): Predominantly used in Unix-based systems, NFS allows remote access to files.
BitTorrent: An example of a P2P protocol, BitTorrent enables distributed file sharing where users download and upload parts of a file from and to each other.

Security Considerations: Implementing robust security measures is crucial for file sharing to prevent unauthorised access and protect data integrity. Encryption, access control, and authentication mechanisms are commonly employed.

Web-Based Network Model:

The web-based network model involves accessing applications, services, or content through web browsers over the Internet or an intranet. It has become a predominant paradigm for delivering a wide range of online resources.

Client-Server Architecture:

Web-based systems typically follow a client-server architecture:

Client: A user's web browser which sends requests to a remote server.

Server: Hosts and processes the requested content or services, then sends the results back to the client.

Protocols:

Communication between the client and server occurs using the Hypertext Transfer Protocol (HTTP) or its secure variant, HTTPS. These protocols define how data is exchanged between the user's device and the remote server.

Web Technologies:

HTML (Hypertext Markup Language): Structures content on web pages.

CSS (Cascading Style Sheets): Controls the presentation and layout of web pages.

JavaScript: Adds interactivity and dynamic elements to web pages.

Examples:

Websites: Platforms like Google, Wikipedia, or news websites.

Web Applications: Online tools, email services, and social media platforms.

- **Content Distribution Network:**

A Content Distribution Network (CDN) is a distributed network of servers strategically positioned across multiple geographical locations to deliver web content efficiently and enhance the performance, reliability, and scalability of delivering web content to users.

Key Components:

1. **Origin Server:** The origin server is the original location where the web content is stored. It houses the master copies of all files, such as HTML, CSS, images, and videos.

2. **Edge Servers:** Edge servers are the distributed servers strategically placed in various locations worldwide. They form the CDN infrastructure and store cached copies of the content from the origin server.
3. **Points of Presence (PoPs):** PoPs are locations where CDN providers place their edge servers. These are typically data centers strategically positioned in different regions, ensuring proximity to end-users for faster content delivery.
4. **Cache:** Caching involves storing copies of web content on edge servers. When a user requests a particular resource, the CDN serves it from the nearest edge server's cache, reducing latency.

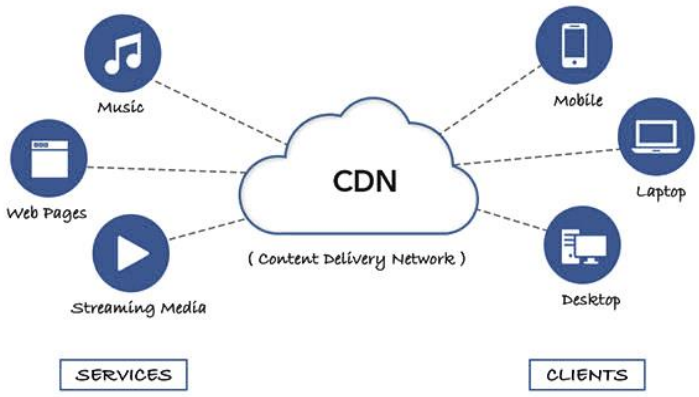


Figure: 3.1: Content Delivery Network (CDN)

How CDNs Work:

Request Routing: When a user requests web content, the CDN employs intelligent algorithms to determine the optimal edge server (PoP) to fulfill the request. This decision is based on factors like proximity, server load, and network conditions.

Content Delivery: If the requested content is already cached on the edge server, it is delivered directly to the user. If not, the CDN retrieves the content from the origin server, caches it at the edge server, and then delivers it to the user.

Caching Strategies: CDNs employ various caching strategies, such as time-based expiration or event-driven invalidation, to ensure that cached content remains fresh and relevant.

Benefits of CDNs:

1. **Improved Performance:** CDNs reduce latency by serving content from edge servers close to users, leading to faster load times and improved user experience.
2. **Scalability:** CDNs distribute the load across multiple servers, ensuring that web applications can handle increased traffic without overloading the origin server.
3. **Reliability:** CDNs enhance reliability by providing redundancy. If one server fails, the CDN can route requests to another available server.
4. **Global Reach:** CDNs enable global content delivery by placing edge servers in various locations, ensuring users worldwide experience fast and consistent access.
5. **Security:** CDNs can provide security features such as DDoS protection and SSL termination, safeguarding websites and applications from malicious attacks.

Use Cases:

1. **Media Streaming:** CDNs are commonly used for delivering video and audio content efficiently, ensuring smooth streaming experiences.
2. **E-commerce:** Online retailers use CDNs to accelerate the delivery of product images, videos, and other content, enhancing the shopping experience.
3. **Dynamic Content:** CDNs can also cache dynamic content, such as personalised web pages, by employing intelligent caching strategies.

- **Knowledge Check 2**

  State True or False.

  1. In a centralised network, control and decision-making are distributed among multiple nodes. (True)
  2. Client-server networks are characterised by a central server that manages resources, while peer-to-peer networks distribute responsibilities among all connected devices. (False)
  3. File-sharing networks typically use a peer-to-peer model, allowing users to exchange files directly between their devices. (True)
  4. Content Distribution Networks (CDN) are primarily used for centralised storage and distribution of large files. (False)
  5. Web-based networks rely on a client-server architecture for delivering content and services to users. (True)

- **Outcome-Based Activity 2**

  Design a network for a hypothetical organization, choosing between centralized, decentralized, or distributed architecture. Justify client-server or peer-to-peer models based on organizational needs. Implement efficient file sharing and web communication strategies for seamless collaboration. Integrate a Content Distribution Network (CDN) for improved content delivery. Emphasize practical application of chosen structures and proficiency in addressing challenge

3.2 Summary

- Gain insights into Content Distribution Networks (CDN) and their role in efficiently delivering web content by strategically distributing it across multiple servers.
- Understand the fundamental concept and structure of the Internet as a global network of interconnected devices.
- Explore the methods through which users connect to and access resources on the Internet, considering various technologies and protocols.

3.3 Keywords

- **ATM: Asynchronous Transfer Mode:** A high-speed networking standard that transmits data in fixed-size cells or packets, suitable for voice, video, and data.
- **Peer-to-Peer:** A network model where each device on the network can act both as a client and a server, sharing resources directly with other devices.

3.4 Self-Assessment Questions

3. Describe the functions of layers and protocols within the TCP/IP model.
4. What challenges arise in data transmission using the TCP/IP protocol suite?
5. Define and differentiate between centralised, decentralised, and distributed network architectures.

3.5 References / Reference Reading

- Data Communications and Networking By Behrouz A.Forouzan.

Unit 4: Example Networks

Learning Outcomes:

- Students will be able to define the goals and applications of computer networks.
- Students will be able to categorise networks based on size, purpose, design issues, and transmission technologies.
- Students will be able to compare the OSI and TCP/IP reference models, emphasising key differences.
- Students will be able to explain the functions of layers and protocols in the TCP/IP model.
- Students will be able to demonstrate an understanding of data transmission using TCP/IP and apply this knowledge in practical scenarios.

Structure:

4.1 Introduction to Example Networks

The introduction to example networks typically involves showcasing various types of networks that serve different purposes and illustrate the diverse applications of networking concepts. Let's explore a brief introduction to example networks across various domains:

Local Area Network (LAN):

Definition: A Local Area Network is a network that spans a small geographic area, such as building or campus. It connects computers and devices to facilitate resource sharing, file sharing, and communication within a limited area.

Use Case: LANs are commonly used in offices, homes, and educational institutions to connect devices like printers, computer and servers.

Wide Area Network (WAN):

Definition: A Wide Area Network covers a broader geographical area, connecting LANs over long distances. WANs use public or private communication links, such as "leased lines or Internet", to enable communication between distant locations.

Use Case: WANs are crucial for connecting branch offices of a company, enabling global communication, and facilitating remote access to resources.

Wireless Local Area Network (WLAN):

Definition: A WLAN is a type of LAN that uses wireless communication technologies, such as Wi-Fi, to connect devices without the need for physical cables.

Use Case: Commonly used in homes, offices, and public spaces, WLANs provide flexible and convenient connectivity for devices like laptops, smartphones, and tablets.

Metropolitan Area Network (MAN):

Definition: A Metropolitan Area Network "covers a larger geographic area than a LAN but is smaller than a WAN". It typically spans a city or a large campus, connecting multiple LANs.

Use Case: MANs are employed in urban areas to connect various local networks, supporting applications like video surveillance, public Wi-Fi, and traffic management.

Cloud Computing Network:

Definition: In a cloud computing network, resources and services are delivered over the Internet. It involves a combination of hardware, software, and virtualised components to provide scalable and on-demand computing resources.

Use Case: Cloud computing networks are used for hosting applications, storing data, and delivering various services without the need for users to own or manage physical infrastructure.

Industrial Control System (ICS) Network:

Definition: ICS networks are used in industrial settings to control and monitor physical processes, such as manufacturing or energy production. They often include specialised protocols for automation and control.

Use Case: ICS networks are vital in manufacturing plants, power plants, and other industrial facilities to automate processes and improve efficiency.

Sensor Network (IoT):

Definition: Sensor networks, part of the Internet of Things (IoT), involve interconnected sensors and devices that collect and exchange data. They enable the monitoring and control of physical environments.

Use Case: IoT sensor networks are utilised in smart cities, agriculture, healthcare, and various industries for applications like environmental monitoring, smart grids, and asset tracking.

- **The Internet and its Conceptual View:**

The Internet: The Internet is a global network that connects millions of private, public, academic, business, and government networks. It allows the exchange of information, communication, and access to a vast array of resources, services, and applications. The Internet is decentralised, comprising interconnected networks that follow a set of standardised protocols for communication.

Key Components and Conceptual View:

End-User Devices:

Computers, Smartphones, Tablets: These devices serve as the endpoints for users to access the Internet. They run web browsers, email clients, and other applications that leverage Internet connectivity.

Internet Service Providers (ISPs):

ISPs are organisations that provide Internet connectivity to end-users. They offer various connection types, including broadband, DSL, fiber-optic, and wireless connections.

Network Infrastructure:

Routers, Switches, and Cables: The physical and logical components that form the backbone of the Internet. Routers direct traffic between networks, switches enable local communication, and cables (fiber optics, copper, etc.) carry data between devices.

Protocols:

"Transmission Control Protocol" (TCP) and "Internet Protocol" (IP): Fundamental protocols that govern data transmission over the Internet. TCP ensures reliable data delivery, while IP handles addressing and routing.

Domain Name System (DNS):

DNS translates human-readable domain names (e.g., www.example.com) into "IP" addresses. It acts as a decentralised directory that helps users access websites using memorable names.

Web Servers and Clients:

Web Servers: Host and serve web pages and content. They respond to user requests, providing the requested information.

Web Clients: Browsers (e.g., Chrome, Firefox) on end-user devices that request and display web pages served by web servers.

Applications and Services:

Email, File Transfer, Social Media: Numerous applications and services operate on the Internet, enabling communication, collaboration, and information sharing.

Conceptual View:

1. **Client-Server Model:** The Internet follows a client-server model. Clients (end-user devices) make requests to servers (computers hosting content or services). For example, when a user accesses a website, the web browser (client) sends a request to the web server, which responds by delivering the requested content.
2. **Packet Switching:** Data on the Internet is broken into packets for efficient transmission. Each packet carries a portion of the data and is independently routed from the source to the destination. This allows for flexible and robust communication.

3. **Decentralisation:** The Internet is decentralised, meaning there is no central governing authority. Instead, it relies on a distributed network of interconnected routers and servers. This decentralisation contributes to the Internet's resilience and scalability.
4. **Open Standards:** The Internet is built on open standards, such as TCP/IP, HTTP, and DNS. These standards ensure interoperability, allowing diverse devices and systems to communicate effectively.
5. **World Wide Web (WWW):** The WWW is a subset of the Internet that consists of interconnected web pages. Users navigate the web using hyperlinks, and web browsers provide a graphical interface for accessing and interacting with web content.
6. **Hyper Text Transfer Protocol (HTTP) and Secure HTTP (HTTPS):** HTTP is the protocol used for transferring web pages on the Internet. "HTTPS" adds a layer of security through encryption, ensuring that data exchanged between the client and server remains confidential.
7. **Search Engines:** Search engines, such as Google, Bing, and Yahoo, index the vast amount of information on the Internet. Users can search for and discover relevant content by entering keywords.
8. **E-commerce and Online Transactions:** The Internet facilitates e-commerce, allowing users to buy and sell goods and services online. Secure protocols like HTTPS ensure the confidentiality and integrity of online transactions.
9. **Social Media:** Platforms like Facebook, Twitter, and Instagram enable social interactions and content sharing on a global scale. Users connect, communicate, and share information with others across the Internet.

- **Accessing The Internet:**

Accessing the Internet involves connecting devices to the global network, typically through an Internet Service Provider (ISP). Here's a detailed explanation of the process:

1. End-User Devices:

Devices such as computers, smartphones, tablets, and IoT devices are equipped with network interfaces (Wi-Fi, Ethernet, cellular) for connecting to the Internet.

2. Internet Service Provider (ISP):

Users subscribe to an ISP, which provides Internet connectivity. ISPs can offer various types of connections, including:

Broadband: High-speed Internet delivered over cable or DSL.

Fiber-Optic: Uses optical fibers for faster data transmission.

Wireless: Includes satellite, Wi-Fi, and cellular connections.

3. Network Infrastructure:

Routers and Modems: A modem connects the user's device to the ISP's network. It modulates and demodulates signals for transmission over different media.

A router directs data between the user's network and the ISP. It manages the flow of data packets.

Local Network Setup: In a home or office, a router may be used to create a Local Area Network (LAN). Devices within this network can communicate with each other and share an Internet connection.

4. Connection Types:

Wired Connections: Ethernet cables connect devices directly to the router or modem for stable and high-speed connections.

Wireless Connections: Wi-Fi allows devices to connect to the Internet without physical cables. Users need the correct authentication credentials (Wi-Fi password) to join the network.

5. IP Address Assignment:

“Dynamic Host Configuration Protocol” (DHCP): The router may use “DHCP” to automatically assign IP addresses to devices in the local network. Each device receives a unique IP address for identification.

Static IP Addresses: Some networks use static IP addresses, where each device has a manually configured, fixed IP address.

6. Domain Name System (DNS):

Resolution of Domain Names: When a user enters a domain name (e.g., www.example.com) in a web browser, DNS resolves it to an IP address. This translation allows the device to locate the server hosting the requested content.

7. Transmission Control Protocol (TCP) and Internet Protocol (IP):

Data Packets: TCP breaks data into packets, assigns sequence numbers, and ensures reliable, ordered delivery.

IP handles addressing and routing of packets between devices on the Internet.

8. Web Browsing:

Hypertext Transfer Protocol (HTTP) and HTTPS:

Browsers use HTTP or its secure version, HTTPS, to request and receive web pages from servers.

Web Servers: When a user enters a web address, the browser sends an "HTTP" request to the corresponding web server. The server processes the request and sends back the requested web page.

9. Secure Sockets Layer (SSL) / Transport Layer Security (TLS):

Encryption: HTTPS uses "SSL/TLS" protocols to "encrypt data exchanged between user's device and web server", ensuring confidentiality and integrity of information.

10. Search Engines and Online Services:

Interactions with Servers: Users interact with search engines, social media platforms, and other online services, sending and receiving data over the Internet.

11. E-commerce and Transactions:

Secure Transactions: E-commerce websites use secure protocols to encrypt sensitive information, such as credit card details, during online transactions.

12. Firewalls and Security Measures:

Firewalls: Routers and security software often include firewalls to monitor and control incoming and outgoing network traffic, enhancing security.

13. Continuous Data Exchange:

Real-Time Communication: Applications like messaging, video calls, and online collaboration tools involve continuous data exchange over the Internet.

14. Internet of Things (IoT):

Connected Devices: IoT devices, such as smart home appliances, also access the Internet to send and receive data.

15. Cloud Computing:

Accessing Cloud Services: Users access cloud-based applications and storage services over the Internet, contributing to the shift from locally hosted to cloud-hosted resources.

16. Mobile Connectivity:

Cellular Networks: Smartphones and tablets access the Internet through cellular networks, using technologies like 4G or 5G.

17. Continuous Monitoring and Improvement:

Quality of Service (QoS):

ISPs monitor and manage network performance, ensuring a reliable and consistent user experience.

Upgrades and Innovations:

ISPs regularly upgrade infrastructure and adopt new technologies to provide faster and more efficient Internet access.

- **Connection-Oriented Networks: X.25**

X.25 is a historic and widely used standard for connection-oriented networks, particularly in the context of wide-area networks (WANs). Developed by the International Telecommunication Union (ITU), X.25 defines the protocol suite for packet-switched networks, providing reliable and efficient communication over diverse and often unreliable network infrastructures.

The X.25 standard is structured into three primary layers: Physical Layer (Layer 1), Data Link Layer (Layer 2), and Network Layer (Layer 3). Let's explore each layer in detail:

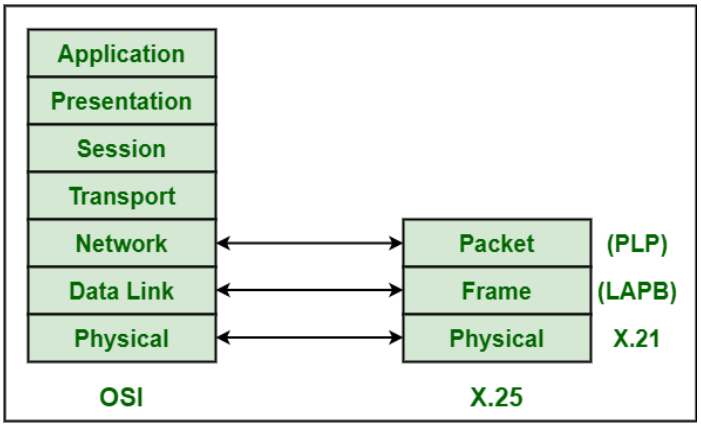


Fig.4.1 X.25 Layer mapping with OSI Model

1. Physical Layer (Layer 1):

Purpose: The Physical Layer is responsible for the actual transmission and reception of raw bit streams over the physical medium, which could be copper wires, optical fibers, or radio waves.

Characteristics:

Specifies electrical and mechanical characteristics of the interface.

Defines signalling, voltage levels, and physical connectors.

Components:

Modems and Converters: Used to convert digital signals from the network into a form suitable for the physical medium and vice versa.

2. Data Link Layer (Layer 2):

Purpose: The Data Link Layer manages the reliable transmission of data frames between directly connected nodes over the physical layer.

Sublayers:

Logical Link Control (LLC):

Responsible for flow control and error checking within the frame.

Manages logical connections between devices.

Packet Layer (PLP):

Assembles data into packets before transmission.

Handles addressing and error detection at the packet level.

Error Handling:

Implements error detection and correction mechanisms to ensure the integrity of the transmitted frames.

Flow Control:

Manages the flow of data between the sender and receiver to prevent congestion and ensure efficient communication.

Addressing:

Assigns unique addresses to devices within the network, facilitating the routing of data frames.

3. Network Layer (Layer 3):

Purpose: The Network Layer is responsible for the end-to-end routing of data packets across the entire network, providing logical addressing and ensuring proper delivery.

Sublayers:

Packet Assembler/Disassembler (PAD):

Responsible for breaking data into smaller packets for transmission and reassembling received packets at the destination.

Packet Level Protocol (PLP):

Provides addressing and sequencing information for packets.

Routing:

Determines the optimal path for data packets to reach their destination, considering factors like network topology and traffic conditions.

Addressing:

Assigns network addresses to devices to enable end-to-end communication.

Error Handling:

Implements error detection and correction mechanisms at the network layer.

Interaction between Layers:

Layered Communication:

Each layer communicates with its counterpart layer on another device, providing a modular and standardised approach to network communication.

Layer N to Layer N Communication:

The Physical Layer on one device communicates with the Physical Layer on another device, and the process continues through the Data Link and Network Layers.

Encapsulation:

Data moves down the layers during transmission and up the layers during reception. At each layer, additional information is added, forming a hierarchical structure known as encapsulation.

Key Components and Features:

1. **Packet Switching:** X.25 employs packet switching as its underlying communication paradigm. Data is broken into packets before transmission, and these packets are individually routed through the network.

2. **Virtual Circuits:** X.25 establishes virtual circuits between communicating devices. A virtual circuit is a logical connection that emulates a dedicated physical circuit for the duration of the communication session.
3. **Packet Structure:** X.25 packets consist of a “header and data” field. The header contains information about “virtual circuit, error checking, and sequencing information”.
4. **Error Detection and Correction:** X.25 includes mechanisms for error detection and correction. It uses techniques like cyclic redundancy check (CRC) to ensure data integrity.
5. **Flow Control:** Flow control mechanisms in X.25 help manage the flow of data between devices. It prevents overwhelming the receiving device by controlling the rate of data transmission.
6. **Addressing:** Each device in an X.25 network has a unique address, allowing for proper routing of packets between source and destination.

DTE and DCE:

X.25 distinguishes between “Data Terminal Equipment” (DTE) and “Data Circuit-terminating Equipment” (DCE). DTE refers to end-user devices, while DCE refers to the equipment connecting the DTE to the network.

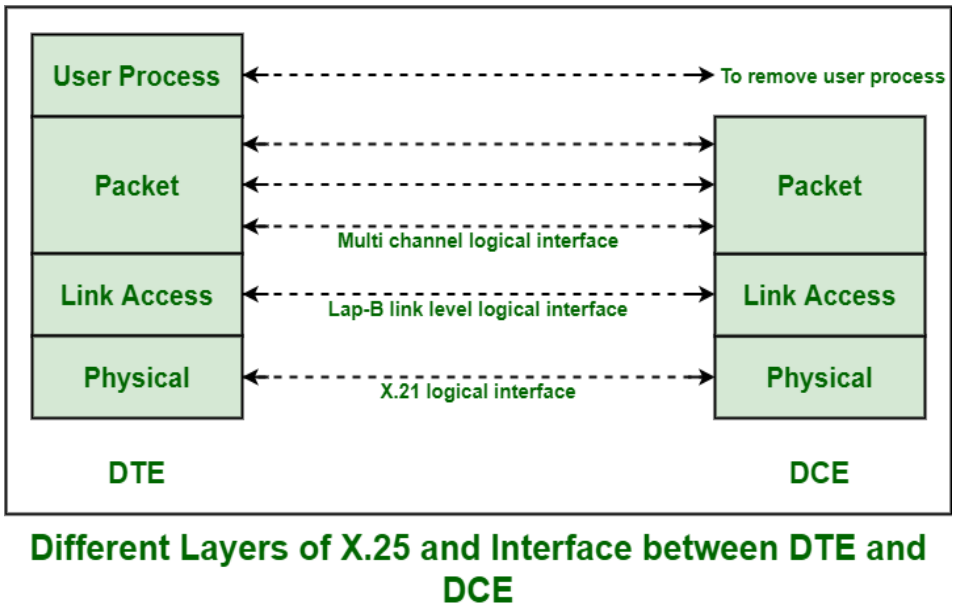


Fig.4.2 Different Layers of X.25 and interface between DTE and DCE

Operation:

Call Setup: Before communication begins, X.25 devices establish a virtual circuit through a process known as call setup. This involves exchanging control packets to negotiate parameters and allocate resources for the communication session.

Data Transfer: Once the virtual circuit is established, data transfer occurs in packets. X.25 ensures reliable delivery through error detection and correction mechanisms.

Call Termination: After the data transfer is complete, devices initiate call termination to release the allocated resources and end the virtual circuit.

Applications:

Legacy WANs: X.25 was widely used in legacy wide-area networks (WANs) before being largely replaced by more modern technologies like Frame Relay and, later, IP-based networks.

Financial Transactions: X.25 has historically been used for financial transactions, such as Automated Teller Machine (ATM) networks, due to its reliability and connection-oriented nature.

Telemetry and SCADA Systems: Supervisory Control and Data Acquisition (SCADA) systems and telemetry applications have employed X.25 for its reliable communication capabilities.

Challenges and Legacy:

1. Slow Data Rates: One of the challenges of X.25 is its relatively slow data rates compared to modern networking technologies. Its legacy nature means it might not be suitable for high-speed data communication.
2. Transition to IP: As networks transitioned to Internet Protocol (IP)-based technologies, X.25 networks gradually diminished. However, some legacy systems may still rely on X.25.

- **Frame Relay and ATM:**

Frame Relay:

1. Definition: Frame Relay is a high-performance packet-switched WAN (Wide Area Network) technology. It operates at the Data Link Layer (Layer 2) of the OSI model and is known for its simplicity and efficiency.

2. Frame Structure: Frame Relay frames consist of “header and trailer”. The header contains information such as “source and destination addresses, frame type, and control bits”. The trailer includes error-checking information.

3. Connection Type: Frame Relay is connection-oriented, but it uses a virtual circuit concept rather than physical circuits. Virtual circuits are established between endpoints to facilitate communication.

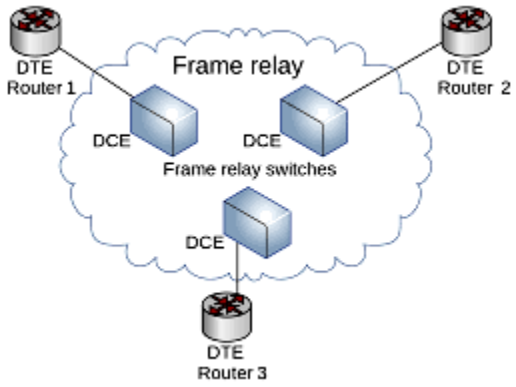


Figure: 4.3: Frame Relay

4. Virtual Circuits: Frame Relay offers two types of virtual circuits:

Permanent Virtual Circuit (PVC): A predefined and permanent connection between two endpoints.

Switched Virtual Circuit (SVC): A dynamically established connection that is created and torn down as needed.

5. Encapsulation: Data is encapsulated into frames for transmission. The encapsulation process involves adding the Frame Relay header and trailer to the user's data.

6. Efficiency: Frame Relay is designed for efficiency in transmitting variable-length frames. It supports multiple logical connections over a single physical link.

7. Speed and Scalability: Frame Relay is well-suited for high-speed data transmission over WANs. It provides scalable solutions for networks with varying bandwidth requirements.

8. Usage: Frame Relay was widely used in the late 20th century for connecting remote office networks. However, it has largely been replaced by more modern technologies like MPLS and Ethernet.

Asynchronous Transfer Mode (ATM):

1. Definition: ATM is a high-speed, connection-oriented switching technology that operates at the cell-switching layer (Layer 2.5) of the OSI model. It was designed to support various types of traffic, including “voice, video, and data”.

2. Cell Structure: ATM uses fixed-size cells, each consisting of 53 bytes (48 bytes of data and 5 bytes of header). The fixed size ensures predictable and consistent handling of traffic.

3. Connection Type: ATM is connection-oriented, and it establishes virtual circuits for communication. Virtual circuits can be either Permanent Virtual Circuits (PVC) or Switched Virtual Circuits (SVC).

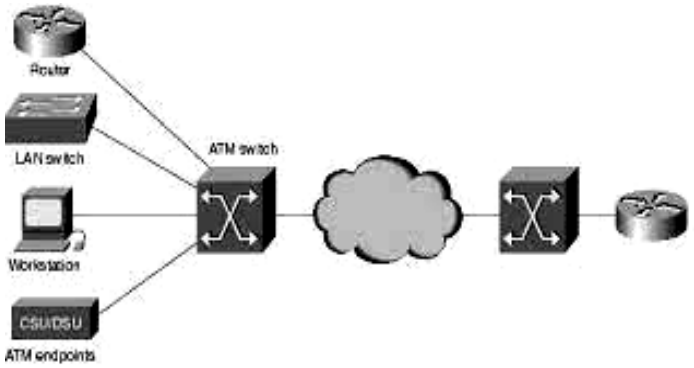


Figure: 4.4: Asynchronous Transfer Mode (ATM)

4. Switching: ATM switches use fast hardware-based switching, providing low-latency and high-throughput communication.

5. Quality of Service (QoS):

ATM is known for its advanced QoS capabilities, allowing the prioritisation of different types of traffic. This makes it suitable for applications with specific performance requirements, such as voice and video.

6. Broadband Integration: ATM was designed to integrate various types of traffic over a single network infrastructure, supporting both low-bandwidth and high-bandwidth applications.

7. Usage: While ATM was once widely used, especially in telecommunication networks, it has faced challenges in the face of emerging technologies. Today, it is less prevalent, with many networks transitioning to more IP-centric solutions.

8. Adaptation Layer (AAL): ATMs use an Adaptation Layer (AAL) to adapt various types of traffic (voice, video, data) into a format suitable for transport over ATM cells.

9. Scalability: ATM was initially designed to scale to high speeds and support a large number of virtual circuits. However, its adoption declined with the rise of IP-based technologies.

10. Legacy Considerations: While ATM is not as widely deployed as it once was, there are still legacy networks and systems that use ATM technology.

4.2 Summary

- Learn about X.25 networks, which operate on a connection-oriented communication model, and understand their historical significance.
- Gain an introductory understanding of Frame Relay and Asynchronous Transfer Mode (ATM) technologies, which were once prevalent in wide-area networking.

4.3 Keywords

- **X.25:** A standard protocol suite for packet-switched wide area network (WAN) communication.

4.4 Self-Assessment Questions

4 Discuss the characteristics of both client-server and peer-to-peer network models.

5 How does a Content Distribution Network (CDN) optimise content delivery in web-based networks?

4.5 References / Reference Reading

- Data Communications and Networking By Behrouz A.Forouzan.

Unit 5: Data Link layer

Learning Outcomes:

- Students will define the concept of social responsibility in business.
- Students will identify and differentiate between various types of social responsibilities in business.
- Students will demonstrate effective communication and collaboration in addressing environmental issues.
- Students will evaluate the management hierarchy in an organization.
- Students will analyze environmental concerns at different management levels within an organization.

Structure:

5.1 Data Link Layer

- **Communication at the Data Link Layer:**

The Data Link Layer operates at second layer of “OSI” (Open Systems Interconnection) model, facilitating communication between directly connected devices on the same network segment.

Its primary responsibility is to ensure “reliable and error-free” transmission of data frames across the physical medium.

The Data Link Layer accomplishes this through various mechanisms, including framing, addressing, error detection, and flow control.

Framing involves breaking data packets received from the Network Layer into smaller units called frames, each containing a header and a trailer. The header includes control information like frame synchronization, addressing, and error checking, while the trailer typically contains error detection information, such as a CRC (Cyclic Redundancy Check) code.

Addressing at the Data Link Layer is primarily done using “MAC” (Media Access Control) addresses, which are unique identifiers assigned to each “network interface card” (NIC) in a device. MAC addresses are used to ensure that frames are delivered to the correct destination device on the same network segment.

Error detection mechanisms at the Data Link Layer involve checking for transmission errors, such as bit errors or frame corruption, using techniques like CRC. If errors are detected, the frame may be discarded or retransmitted to ensure data integrity.

Flow control mechanisms regulate “flow of data between sender and receiver to prevent congestion and buffer overflow”. This may involve techniques such as sliding window protocols, where the sender adjusts its transmission rate based on feedback from the receiver.

- **Nodes and Links**

In networking, a "node" refers to “any device connected to a network that can send, receive, or process data”. Examples: computers, routers, switches, printers, and servers.

A "link" represents the physical or logical connection between two nodes on a network. Links can be established using various transmission media, such as copper wires, fiber optic cables, or wireless signals.

Nodes communicate with each other by sending data packets over these links. The Data Link Layer ensures that these packets are properly formatted into frames and delivered to the correct destination node.

- **Link Layer Addressing**

Link Layer addressing, also known as MAC addressing, is used to uniquely identify devices on a network segment.Each “network interface card” (NIC) in a device is assigned a unique MAC address, typically represented as a 48-bit hexadecimal number.

MAC addresses are hardcoded into “NIC”s by manufacturers and remain fixed throughout the device's lifetime, making them globally unique identifiers for network devices.

The Data Link Layer uses MAC addresses to determine the source and destination of frames transmitted over the network. When a frame is sent, the sender includes the MAC address of the destination device in the frame header, allowing switches and routers to forward the frame to the correct destination.

- **Examples of Data Link layer protocols**

Ethernet: Ethernet is one of the most widely used Data Link layer protocols in wired LAN (Local Area Network) environments. It defines standards for frame formats, addressing (using MAC addresses), collision detection, and media access control. Ethernet frames typically consist of a preamble, destination and source “MAC” addresses, a type field indicating upper-layer protocol, data, and a CRC checksum for error detection.

Wi-Fi (IEEE 802.11): Wi-Fi is a wireless Data Link layer protocol based on the IEEE 802.11 standard. It enables wireless communication between devices within a local area network (LAN) or wireless access to the internet. Wi-Fi uses carrier-sense multiple access with collision avoidance (CSMA/CA) for media access control and includes features for authentication, encryption, and roaming.

Point-to-Point Protocol (PPP):“PPP” is a Data Link layer protocol used to “establish a direct connection between two network nodes over a serial link, such as a dial-up or leased line connection”. PPP encapsulates data packets into frames for transmission and supports features like authentication, error detection, and multilink negotiation.

High-Level Data Link Control (HDLC):"HDLC" is a synchronous Data Link layer protocol used for communication "between devices in a point-to-point or multipoint network". It defines frame formats, control mechanisms for error detection and flow control, and procedures for frame acknowledgement and retransmission. HDLC frames consist of a flag sequence, address, control, data, and CRC fields.

- **Knowledge Check 1**

  Fill in the Blanks

  1. The Data Link Layer ensures reliable transmission through mechanisms such as _____ & _____. (**framing, error detection**/ packets, error correction)
  2. Examples of network nodes include computers_____ and printers. **(Routers/** hubs**)**
  3. MAC addresses are represented as _____hexadecimal numberse.g., 00:1A:2B:3C:4D:5E. **(48-bit/** 32 bit**)**
  4. _____frames typically consist of a preamble, destination and source MAC addresses and a CRC checksum. **(Ethernet/** Internet**)**
  5. _____uses carrier-sense multiple access with collision avoidance (CSMA/CA) for media access control and includes features for authentication, encryption, and roaming. **(Wi-Fi /** Piconet**)**

- **Outcomes-Based Activity 1**

  Analyzing Ethernet frames is crucial for understanding network communication. How would you approach analyzing a sample Ethernet frame, and what key components would you look for to decipher its structure and purpose?

5.2 Design Issues

- **Framing techniques: Byte-Oriented and Bit-Oriented Protocols**

Introduction to Framing Techniques:

In data communication, framing is the process of delineating the boundaries of data units within a stream of bits. Framing is essential for the receiver to correctly interpret and extract the transmitted data.

There are two primary framing techniques: byte-oriented and bit-oriented protocols.

“Byte-Oriented Protocols”:

Byte-oriented protocols frame data into fixed-size units, typically bytes. Each byte serves as a distinct data unit. This approach simplifies the processing and transmission of data as it aligns with the byte-oriented nature of most computer systems. Let's delve into byte-oriented protocols with an example:

Example: HDLC (High-Level Data Link Control)

HDLC is a widely used byte-oriented protocol that operates at data link layer of OSI model. It provides reliable and efficient communication over point-to-point and multipoint links. HDLC frames consist of a header, data field, and trailer. The header and trailer contain control information, while the data field carries the actual payload.

Flag: Special bit pattern indicating the beginning and end of the frame.

Address: Specifies the destination or source address.

Control: Control information including frame type and sequence numbers.

Data: Payload data.

FCS (Frame Check Sequence): Error detection code (e.g., CRC).

Flag: Indicates the end of the frame.

Bit-Oriented Protocols:

Bit-oriented protocols frame data into variable-size units based on bit patterns or special characters rather than fixed-size bytes. This flexibility allows bit-oriented protocols to handle diverse data structures efficiently. Let's explore a common bit-oriented technique:

Example: Manchester Encoding in Ethernet

Ethernet, a widely used networking technology, employs Manchester encoding as its bit-oriented framing technique. In Manchester encoding, each bit is represented by a transition in the middle of a bit period. A high-to-low transition indicates a 0, while a low-to-high transition indicates a 1. This ensures synchronization between sender and receiver and facilitates reliable data transmission. Here's an illustration of Manchester encoding:

Start Bit: Indicates the beginning of a frame.

Data (encoded): Payload data encoded using Manchester encoding.

Stop Bit: Marks the end of the frame.

- **Error Control: Error Detection and Correction**

Error control in data communication refers to the techniques used to ensure the integrity and reliability of transmitted data. This involves both detecting errors that may occur during transmission and correcting them if possible.

Error Detection: Error detection techniques are used to determine whether errors have occurred during data transmission. These techniques do not necessarily correct the errors but simply identify their presence. Common error detection methods include:

Parity Check: Parity bits are added to data to make the total number of 1s either even (even parity) or odd (odd parity). If the number of bits in the transmitted data differs from the expected parity, an error is detected.

Checksum: Checksum is a value calculated from the data using an algorithm. This value is sent along with the data. At the receiver's end, the checksum is recalculated, and if it doesn't match the received checksum, an error is detected.

Cyclic Redundancy Check (CRC): CRC is a more sophisticated error detection technique. It involves generating a CRC polynomial from the data and appending it to the message. At the receiver's end, the same polynomial is applied, and if the result doesn't match the appended CRC, an error is detected.

Error Correction: Error correction techniques not only detect errors but also attempt to recover the original data. Common error correction methods include:

Automatic Repeat reQuest (ARQ): ARQ is a protocol that requests retransmission of data when errors are detected. It operates by sending data packets and waiting for an acknowledgement (ACK) from the receiver. If no ACK is received or a negative acknowledgement (NAK) is received, indicating an error, the sender retransmits the packet.

Forward Error Correction (FEC): FEC is a technique that adds redundant information to the transmitted data, allowing the receiver to correct errors without needing to request retransmission. Reed-Solomon codes and Hamming codes are examples of FEC.

- **Sliding Window Flow Control Protocols**

Sliding window protocols are a fundamental aspect of data communication, especially in scenarios where data needs to be transmitted efficiently between a sender and a receiver. These protocols allow the sender to transmit multiple frames of data without waiting for

acknowledgement from the receiver for each individual frame. Let's delve deeper into the basic concepts and types of sliding window protocols:

Basic Concepts:

Window Size:

The window size refers to the maximum number of frames that the sender can transmit before it must receive an acknowledgement from the receiver.

It determines the amount of unacknowledged data that can be in transit at any given time.

Acknowledgement:

An acknowledgement (ACK) is a confirmation from the receiver indicating that a frame has been received successfully without errors.

ACKs are essential for the sender to know which frames have been successfully received and can be removed from the window.

Timeout:

The timeout duration is the time period after which the sender assumes that a frame has been lost if it does not receive an acknowledgement within that time.

If the sender doesn't receive an ACK within the timeout period, it will retransmit the unacknowledged frames.

Types of Sliding Window Protocols:

Stop-and-Wait Protocol:

This is the simplest form of sliding window protocol.

In this protocol, the sender transmits one frame at a time and waits for acknowledgement from the receiver before sending the next frame.

After sending a frame, the sender waits for an acknowledgement. If it doesn't receive an acknowledgement within the timeout period, it retransmits the same frame.

Selective Repeat:

In selective repeat, the sender can transmit multiple frames without waiting for an acknowledgment.

The receiver individually acknowledges each received frame.

If a frame is lost or corrupted, only that specific frame is retransmitted, while other frames continue to be processed.

Go-Back-N:

Similar to selective repeat, but with a slight difference in behaviour upon error detection.

If a frame is lost or corrupted, the sender retransmits all frames starting from the one that was not acknowledged.

This means that all frames sent after the lost/corrupted frame are retransmitted, leading to potential inefficiency if errors occur frequently.

Sliding Window:

Sliding window is a generalized term for all protocols that allow the sender to transmit multiple frames before receiving an acknowledgment.

It encompasses both selective repeat and go-back-n protocols, as they both utilize a sliding window mechanism for managing data transmission.

- **Knowledge Check 2**

  State True or False.

  1. Byte-oriented protocols frame data into variable-size units based on bit patterns. (**False**)
  2. HDLC is an example of a bit-oriented protocol. (**False**)
  3. Manchester encoding is commonly used in byte-oriented protocols like HDLC. (**False**)
  4. In Manchester encoding, each bit is represented by a transition in the middle of a bit period. (**True**)
  5. Framing techniques are crucial for delineating the boundaries of data units within a stream of bits. (**True**)

5.3 Summary

- Communication mechanisms at the Data Link Layer involve protocols for transferring data between network nodes.
- Addressing schemes for nodes and links provide unique identifiers for network devices and connections.
- Framing techniques, such as Byte-Oriented and Bit Oriented Protocols, structure data into frames for transmission.
- Examples of Data Link layer protocols include Ethernet, HDLC, and PPP.

- Error control methods like Error Detection and Correction ensure data integrity during transmission.
- Flow control protocols like Sliding Window manage the rate of data transmission to prevent congestion.
- Cellular Networks, including GSM & CDMA Technologies, represent different generations of mobile telecommunications standards.

5.4 Keywords

- **DLC (Data Link Layer):** The "second layer of OSI model is responsible for error-free transmission of data frames between devices on same network segment".
- **MAC Protocols (Media Access Control):** Protocols governing access to the transmission medium in a shared network environment, ensuring fair and efficient utilization.

5.5 Self-Assessment Questions

1. Explain the role of the Data Link Layer in the OSI model and discuss its primary functions.
2. Compare and contrast Byte-Oriented and Bit-Oriented framing techniques used in data communication.
3. Describe the operation of the CSMA/CD (Carrier Sense Multiple Access with Collision Detection) protocol and how it helps in managing collisions in Ethernet networks.
4. What are the key features and advantages of Wi-Max technology compared to IEEE 802.11 Wireless LAN?
5. Discuss the significance of Channelization techniques such as FDMA, TDMA, and CDMA in wireless communication systems.

5.5 References / Reference Reading

- Comer, D. E., "Computer Networks and Internets." Pearson, 2015.
- Stallings, W., "Wireless Communications & Networks." Pearson, 2017.
- Andrews, J. G., Ghosh, A., & Muhamed, R., "Fundamentals of WiMAX: Understanding Broadband Wireless Networking." Prentice Hall, 2007.
- Miller, M., "Bluetooth Essentials for Programmers." Cambridge University Press, 2007.
- Rappaport, T. S., "Wireless Communications: Principles and Practice." Pearson, 2001.

- Schwartz, M., "Broadband Integrated Networks." Prentice Hall, 1996.
- Kurose, J. F., & Ross, K. W., "Computer Networking: A Top-Down Approach." Pearson, 2016.

Unit 6: Media Access Control and IEEE Standard

Learning Outcomes:

- Students will define the concept of social responsibility in business.
- Students will identify and differentiate between various types of social responsibilities in business.
- Students will demonstrate effective communication and collaboration in addressing environmental issues.
- Students will evaluate the management hierarchy in an organization.
- Students will analyze environmental concerns at different management levels within an organization.

Structure:

6.1 Media Access Control

- Aloha, CSMA, CSMA/CD, CSMA/CA
- Collision free protocols with Controlled Access
- Limited Contention Protocols; Channelization: FDMA, TDMA, CDMA
- Wavelength Division Multiple Access for Fiber-Optic Data Communication.
- Knowledge Check 3
- Outcome-Based Activity 3

6.2 IEEE LAN standards

- Ethernet (Physical specifications, Encoding, Frame Format & MAC protocol)
- Binary Exponential Back off algorithm;
- Token Ring and FDDI
- Knowledge Check 4
- Outcome-Based Activity 4

6.3 Introduction to Wireless Networks

- IEEE 802.11 Wireless LAN
- Wi-Max
- Bluetooth and other wireless PAN technologies & their applications

- Cellular Networks: Generations
- GSM & CDMA Technologies.
- Knowledge Check 5
- Outcome-Based Activity 5

6.4 Summary

6.5 Keywords

6.6 Self-Assessment Questions

6.7 References / Reference Reading

6.1 Media Access Control

- **Aloha, CSMA, CSMA/CD, CSMA/CA:**

Introduction to MAC Protocols:

MAC protocols govern how devices in a network share and access the transmission medium, ensuring efficient and orderly communication. They manage contention for the medium among multiple nodes, preventing data collisions and maximizing network throughput. Here, we'll explore four key MAC protocols: Aloha, CSMA, CSMA/CD, and CSMA/CA.

- **Aloha Protocol:**

Aloha is a simple random-access MAC protocol.

Nodes transmit data whenever they have packets to send, without coordinating with other nodes.

Collisions may occur when two or more nodes transmit simultaneously, leading to data loss.

Operation:

When a node has data to transmit, it sends the packet onto the network.

If no acknowledgement is received within a timeout period, the node assumes the packet collides with another transmission.

Upon collision detection, nodes wait for a random backoff period before retransmitting to reduce the likelihood of subsequent collisions.

Example:

Consider a scenario where two nodes, A and B, attempt to transmit packets simultaneously.

If their transmissions overlap, a collision occurs, causing both nodes to retransmit after a random backoff period.

1. Pure Aloha:

Overview:

Pure Aloha is one of the earliest random-access MAC protocols.

In Pure Aloha, nodes transmit data packets whenever they have data to send, without any synchronization or coordination.

Collisions occur when two or more nodes transmit simultaneously, leading to data loss.

Operation:

Transmission: When a node has a data packet to send, it transmits it onto the network immediately.

Collision Detection: After transmission, nodes listen to the network to determine if their packet collide with others.

Acknowledge or Retransmission: If a node does not receive an acknowledgement for its transmitted packet within a specified time frame, it assumes a collision occurred and initiates a random backoff period before retransmitting the packet.

Example:

Node A and Node B both attempt to transmit packets at the same time.

If their transmissions overlap, a collision occurs.

Both nodes then enter a random backoff period before attempting to retransmit their packets, hoping to avoid another collision.

2. Slotted Aloha:

Overview:

Slotted Aloha improves upon Pure Aloha by dividing time into discrete slots.

Nodes are allowed to transmit only at the beginning of each time slot.

This synchronization reduces the probability of collisions and improves channel utilization.

Operation:

Time Slot Synchronization: Time is divided into fixed-length slots, ensuring all nodes begin transmission attempts at the start of a slot.

Transmission: Nodes attempt to transmit their data packets at the beginning of the next available time slot.

Collision Detection: After transmission, nodes listen for acknowledgements. If no acknowledgement is received, the node assumes a collision occurred.

Backoff and Retransmission: Upon collision detection, nodes wait for a random backoff period before attempting to retransmit the packet in the next available time slot.

Example:

In Slotted Aloha, if Node A and Node B both attempt to transmit packets, they must wait for the beginning of the next time slot.

If Node A successfully transmits its packet in the current time slot, it receives an acknowledgement.

If Node B attempts to transmit in the same slot and a collision occurs, it waits for a random backoff period before attempting to retransmit in the next available time slot.

- **Carrier Sense Multiple Access (CSMA)**

Overview: CSMA is a fundamental MAC protocol used in computer networks to manage access to the shared transmission medium. It allows multiple nodes to share the medium by sensing its availability before transmitting data.

Key Concepts:

Carrier Sense: Nodes listen to the channel before initiating transmissions to detect ongoing transmissions or carrier signals.

If the channel is idle, indicating no ongoing transmissions, nodes proceed with transmission.

If the channel is busy, nodes wait for it to become idle before transmitting.

Multiple Access: Multiple nodes share the same transmission medium.

Each node can attempt to transmit data independently.

Collision Detection: While transmitting, nodes continue to listen to the channel for collisions.

If a collision is detected (e.g., another transmission overlaps), nodes stop transmitting immediately and handle the collision accordingly.

Backoff Mechanism: Upon detecting a collision, nodes enter a backoff period, during which they wait before attempting to retransmit. Backoff periods are random and help prevent repeated collisions among nodes.

Operation of CSMA:

Channel Sensing: Before initiating transmission, nodes listen to the channel to determine if it is idle. If the channel is busy, nodes defer transmission and wait for the channel to become idle.

Transmission Attempt: Upon sensing an idle channel, nodes attempt to transmit their data packets. Nodes continue to monitor the channel during transmission to detect collisions.

Collision Detection: While transmitting, if a node detects another transmission overlapping with its own, it stops transmitting immediately. Collisions are detected by comparing the transmitted signal with the received signal.

Backoff and Retransmission: After a collision is detected, nodes enter a random backoff period before attempting to retransmit the packet.

This random backoff period reduces the likelihood of collisions during retransmission attempts.

Variants of CSMA: CSMA/CD (Carrier Sense Multiple Access with Collision Detection):

Used in Ethernet networks. Incorporates collision detection to handle collisions effectively.

Upon detecting a collision, nodes stop transmitting immediately and enter a backoff period before retransmitting.

CSMA/CA (Carrier Sense Multiple Access with Collision Avoidance): Commonly used in wireless networks. Focuses on collision avoidance rather than collision detection.

Utilizes mechanisms such as Request-to-Send (RTS) and Clear-to-Send (CTS) to reserve the channel before transmission.

Example Scenario:

Consider a scenario where multiple nodes in an Ethernet network attempt to transmit data packets simultaneously:

Node A senses the channel and determines it is idle, so it starts transmitting its data packet.

However, while Node A is transmitting, Node B also attempts to transmit, leading to a collision.

Upon detecting the collision, both Node A and Node B cease transmission and enter a random backoff period before attempting to retransmit their packets.

- **Carrier Sense Multiple Access with Collision Detection (CSMA/CD)**

Overview: CSMA/CD is a MAC protocol commonly used in Ethernet networks to regulate access to the shared transmission medium. It combines carrier sensing with collision detection to manage collisions effectively and ensure efficient data transmission.

Key Concepts:

Carrier Sense (CS):

- Nodes listen to the channel before initiating transmissions to detect ongoing transmissions or carrier signals.
- If the channel is idle, nodes proceed with transmission; otherwise, they defer transmission until the channel becomes idle.

Multiple Access (MA):

- Multiple nodes share the same transmission medium.
- Each node can attempt to transmit data independently.

Collision Detection (CD):

- While transmitting, nodes continue to monitor the channel for collisions.
- If a collision is detected (e.g., another transmission overlaps), nodes immediately stop transmitting and enter a collision recovery process.

Backoff Mechanism:

- Upon detecting a collision, nodes enter a random backoff period before retransmitting.
- Backoff periods help prevent repeated collisions among nodes and manage contention for the medium.

Operation of CSMA/CD:

Channel Sensing:

- Before initiating transmission, nodes listen to the channel to determine its status.
- If the channel is idle, indicating no ongoing transmissions, nodes begin transmitting their data packets.

Transmission Attempt:

- Upon sensing an idle channel, nodes attempt to transmit their data packets.
- Nodes continue to monitor the channel during transmission to detect collisions.

Collision Detection:

- While transmitting, if a node detects another transmission overlapping with its own, it immediately stops transmitting.
- Collision detection is achieved by comparing the transmitted signal with the received signal.

Collision Recovery:

- Upon detecting a collision, nodes enter a collision recovery process.
- They abort the current transmission and enter a random backoff period before reattempting transmission.
- This backoff period helps mitigate the probability of another collision during retransmission attempts.

Example Scenario:

- Consider a scenario where multiple nodes in an Ethernet network attempt to transmit data packets simultaneously:
- Node A senses the channel and determines it is idle, so it starts transmitting its data packet.
- However, while Node A is transmitting, Node B also attempts to transmit, leading to a collision.
- Upon detecting the collision, both Node A and Node B immediately stop transmitting and enter a random backoff period before attempting to retransmit their packets.

- **Carrier Sense Multiple Access with Collision Avoidance (CSMA/CA)**

Overview:

CSMA/CA is a MAC protocol commonly used in wireless networks to regulate access to the shared transmission medium. Unlike CSMA/CD, which focuses on collision detection, CSMA/CA emphasizes collision avoidance by employing a Request-to-Send (RTS) and Clear-to-Send (CTS) mechanism.

Key Concepts:

Carrier Sense (CS):

Nodes listen to the channel before initiating transmissions to detect ongoing transmissions or carrier signals.

If the channel is idle, nodes may proceed with the RTS/CTS exchange to reserve the channel.

Multiple Access (MA): Multiple nodes share the same wireless transmission medium.

Each node can attempt to transmit data independently.

Collision Avoidance (CA): Rather than relying solely on collision detection, CSMA/CA employs collision avoidance techniques.

Nodes use RTS and CTS frames to reserve the channel and avoid potential collisions.

RTS/CTS Exchange: Before transmitting data, a node sends an RTS frame to the intended receiver, requesting permission to transmit.

If the receiver is ready to receive, it responds with a CTS frame, granting permission to the sender to transmit. This exchange helps ensure that only one node transmits at a time, minimizing the likelihood of collisions.

Operation of CSMA/CA:

Channel Sensing:

- Before initiating transmission, nodes listen to the channel to determine its status.
- If the channel is idle, nodes may proceed with the RTS/CTS exchange to reserve the channel.

RTS/CTS Exchange:

If a node has data to transmit, it sends an RTS frame to the intended receiver, requesting permission to transmit.

The receiver responds with a CTS frame if it is ready to receive, indicating that the channel is reserved for the sender.

Upon receiving the CTS frame, the sender transmits its data.

Transmission Attempt:

After receiving the CTS frame, the sender proceeds with transmitting its data packet.

During transmission, nodes continue to monitor the channel to detect any potential collisions.

Collision Avoidance:

By using the RTS/CTS exchange, CSMA/CA helps prevent collisions before they occur.

Nodes reserve the channel before transmission, reducing the likelihood of collisions and improving overall network efficiency.

Example Scenario:

Consider a scenario where multiple nodes in a Wi-Fi network attempt to transmit data packets simultaneously:

Node A senses the channel and determines it is idle, so it initiates the RTS/CTS exchange by sending an RTS frame.

The intended receiver (Node B) responds with a CTS frame, indicating that the channel is reserved for Node A.

Node A proceeds with transmitting its data packet, knowing that it has exclusive access to the channel during the transmission.

- **Collision-free protocols with Controlled Access**

Collision-free protocols with controlled access are MAC (Media Access Control) protocols designed to eliminate collisions entirely by providing a controlled mechanism for accessing the shared transmission medium. These protocols ensure that only one node can transmit at a time, thus avoiding contention and collisions.

Key Concepts:

Controlled Access:

Unlike random access protocols, controlled access protocols regulate access to the transmission medium using predefined rules and mechanisms.

These protocols typically involve a central authority or a predetermined schedule for allocating transmission opportunities to nodes.

Collision-Free Operation:

The primary goal of collision-free protocols is to eliminate collisions entirely, ensuring efficient and reliable data transmission.

By allowing only one node to transmit at a time, these protocols prevent contention and contention-related collisions.

Scheduling Mechanisms:

Collision-free protocols often employ scheduling mechanisms to allocate transmission opportunities to nodes.

Schedules may be fixed or dynamically adjusted based on network conditions and traffic patterns.

Token Passing:

In some collision-free protocols, nodes pass a token or permission to transmit sequentially.

Only the node holding the token is allowed to transmit, ensuring collision-free operation.

Operation of Collision-Free Protocols:

Schedule Initialization:

The collision-free protocol initializes a schedule or mechanism for allocating transmission opportunities to nodes.

Schedules may be predetermined or dynamically generated based on network requirements.

Transmission Opportunity Allocation:

Nodes follow the schedule or mechanism to determine when they are allowed to transmit.

Only one node is permitted to transmit at a time, as defined by the protocol rules.

Transmission Process:

When a node's turn arrives according to the schedule, it initiates the transmission of its data packet.

Other nodes listen to the channel and refrain from transmitting during this time to avoid collisions.

Completion and Next Transmission:

After completing transmission, the node releases control of the channel or token, allowing the next node in the schedule to transmit.

The process repeats, ensuring collision-free operation and efficient data transmission.

Example Scenario:

Consider a collision-free protocol with controlled access implemented in a token-passing network:

Nodes in the network pass a token sequentially, with each node holding the token granted permission to transmit.

When a node receives the token, it checks its data queue and initiates transmission if it has data to send.

Other nodes listen to the channel during transmission and refrain from transmitting until they receive the token.

- **Limited Contention Protocols**

Limited contention protocols are a class of Medium Access Control (MAC) protocols designed to minimize contention for the shared transmission medium in computer networks. Unlike random access protocols, which can lead to high collision rates in high-density networks, limited contention protocols aim to reduce contention by introducing structured access mechanisms.

These protocols balance the need for efficient medium utilization with the overhead of contention resolution.

Key Concepts:

Structured Access:

Limited contention protocols introduce structure into the access mechanism to reduce contention.

This structure can take the form of predefined time slots, priority levels, or access tokens.

Dynamic Adjustments:

Some limited contention protocols dynamically adjust access parameters based on network conditions and traffic patterns.

This adaptability helps optimize medium utilization while minimizing contention.

Contention Window:

Limited contention protocols often incorporate a contention window, which defines the range of possible contention levels.

Nodes contend for access within this window, with narrower windows indicating lower contention levels.

Collision Resolution:

In the event of contention or collisions, limited contention protocols employ mechanisms to resolve conflicts and ensure fair access to the medium.

This may involve back-off strategies, prioritization schemes, or token-based access control.

Operation of Limited Contention Protocols:

Initialization:

Limited contention protocols initialize parameters such as contention window size, priority levels, or access schedules.

These parameters may be statically configured or dynamically adjusted based on network conditions.

Contention Resolution:

When multiple nodes attempt to access the medium simultaneously, contention occurs.

Limited contention protocols employ strategies such as exponential backoff, where nodes increase their contention window size after each collision to reduce contention levels gradually.

Structured Access:

Nodes contend for access to the medium based on the defined structure, such as time slots or priority levels.

Access may be granted based on predefined rules or dynamically allocated based on contention levels.

Medium Utilization:

Limited contention protocols aim to strike a balance between medium utilization and contention avoidance.

Through structured access and dynamic adjustments, these protocols optimize medium utilization while minimizing the likelihood of collisions.

Example Scenario:

Consider a limited contention protocol with a dynamic contention window adjustment mechanism:

Initially, all nodes have a small contention window size, allowing for quick access to the medium.

If a collision occurs, nodes double their contention window size and attempt to retransmit after a random backoff period.

This process continues, with nodes progressively increasing their contention window size until access is granted or a maximum limit is reached.

- **Channelization: FDMA, TDMA, CDMA**

Channelization refers to the division of the available bandwidth into smaller channels or time slots to facilitate communication between multiple users in a shared medium. Different channelization techniques, such as “Frequency Division Multiple Access” (FDMA), “Time Division Multiple Access” (TDMA), and “Code Division Multiple Access (CDMA)”, offer unique approaches to efficiently allocate resources and enable simultaneous communication among multiple users.

Key Concepts:

“Frequency Division Multiple Access” (FDMA): FDMA divides the available frequency spectrum into non-overlapping frequency bands or channels.

Each user is allocated a dedicated frequency band for communication.

Users transmit and receive data simultaneously on their allocated frequency bands.

“Time Division Multiple Access” (TDMA): TDMA divides the available time into discrete time slots. Each user is assigned exclusive access to one or more time slots within a predefined frame.
Users take turns transmitting and receiving data within their allocated time slots.

“Code Division Multiple Access” (CDMA): CDMA allows multiple users to share the same frequency band simultaneously. Each user is assigned a unique spreading code, which spreads the data across the entire bandwidth. Users transmit data simultaneously, and the receiver uses correlation techniques to extract the desired data.

- **Frequency Division Multiple Access (FDMA):**

FDMA is a channelization technique where the available frequency spectrum is divided into non-overlapping frequency bands, with each band allocated to individual users for communication.

Frequency Bands Allocation:

The frequency spectrum is divided into multiple frequency bands, each with a specific range of frequencies. Each user is assigned one or more frequency bands for communication.
Users transmit and receive data using their allocated frequency bands simultaneously.

Bandwidth Utilization: FDMA enables efficient utilization of the available bandwidth by allowing multiple users to communicate simultaneously without interfering with each other.
Each user operates within its assigned frequency band, minimizing the likelihood of interference and collisions.

Example Application:

In a cellular network, FDMA is used to allocate different frequency bands to individual cell phone users. Each user communicates with the base station using its allocated frequency band, allowing multiple users to communicate simultaneously within the same cell without interference.

- **Time Division Multiple Access (TDMA):**

TDMA is a channelization technique where the available time is divided into discrete time slots, with each slot allocated to individual users for communication.

Time Slots Allocation:

The available time is divided into frames, each containing multiple time slots.

Each user is assigned one or more time slots within the frame for communication.

Users take turns transmitting and receiving data during their allocated time slots.

Frame Structure:

Each frame consists of a fixed number of time slots, with each slot having a predetermined duration.

Users synchronize their transmissions based on the frame structure, ensuring orderly communication.

Example Application:

In a GSM (Global System for Mobile Communications) network, TDMA is used to divide the time into frames, with each frame containing multiple time slots. Each cell phone user is assigned one or more time slots within the frame for transmitting and receiving data.

- **Code Division Multiple Access (CDMA):**

CDMA is a channelization technique based on spread spectrum technology, where users share the same frequency band simultaneously using unique spreading codes.

Spreading Codes:

Each user is assigned a unique spreading code, which spreads the data signal across a wide bandwidth.

Spreading codes are orthogonal to each other, meaning they are statistically independent and do not interfere with each other.

Simultaneous Transmission:

Multiple users transmit data simultaneously on the same frequency band using their unique spreading codes.

The receiver correlates the received signal with the spreading code of the desired user to extract the data.

Interference Rejection:

CDMA systems use correlation techniques to separate the desired signal from other users' signals, even in the presence of interference.

Interference from other users appears as noise, which can be minimized through advanced signal processing techniques.

Example Application:

In a CDMA-based cellular network, multiple users share the same frequency band simultaneously using their unique spreading codes. The base station employs correlation techniques to separate and decode the signals from individual users, allowing simultaneous communication without interference.

Comparison:

FDMA: Efficient for systems with a fixed number of users and well-defined frequency bands. Suitable for applications with limited mobility and relatively stable communication requirements.

TDMA: Suitable for systems with a dynamic number of users and varying communication needs. Allows flexible allocation of resources based on changing traffic patterns.

CDMA: Provides efficient use of available bandwidth and robustness against interference. Suitable for systems with a large number of users and varying communication requirements, such as cellular networks.

Wavelength Division Multiple access for Fiber-Optic Data Communication

Wavelength Division Multiple Access (WDMA) is a channelization technique utilized in fibre-optic communication systems to enable multiple users to share the same optical fiber for data transmission. It operates on the principle of dividing the optical spectrum into distinct wavelength channels, with each channel assigned to individual users or data streams.

Optical Spectrum Division:

WDMA divides the optical spectrum of the fiber into multiple wavelength channels, with each channel corresponding to a unique optical carrier frequency.

The optical spectrum can span a wide range, typically from the near-infrared to the visible spectrum.

Each wavelength channel operates independently, allowing multiple users or data streams to share the same fiber without interference.

Wavelength Assignment:

Each user or data stream is assigned a specific wavelength channel for communication.

Wavelength channels are typically spaced apart at specific intervals, such as 100 GHz or 50 GHz, to avoid crosstalk and spectral overlap.

Multiplexing and Demultiplexing:

Multiplexing devices, such as optical multiplexers, combine multiple optical signals from different wavelength channels into a single composite signal for transmission over the fiber.

At the receiving end, demultiplexing devices, such as optical demultiplexers, separate the composite signal into individual wavelength channels, allowing each user or data stream to retrieve its data.

Bandwidth Utilization:

WDMA enables efficient utilization of the available optical bandwidth by allowing multiple users or data streams to transmit simultaneously on different wavelength channels.

The total capacity of the fiber-optic link is determined by the number of wavelength channels and the data rate supported by each channel.

Flexibility and Scalability:

WDMA offers flexibility and scalability in fiber-optic communication systems, as additional users or data streams can be accommodated by simply assigning them unused wavelength channels.

The capacity of the system can be easily expanded by adding more wavelength channels or upgrading to higher-capacity multiplexing technologies.

Example Application:

In a WDMA-based fiber-optic communication system, multiple users or organizations may share the same optical fiber infrastructure for data transmission.

Each user is assigned a dedicated wavelength channel, allowing them to transmit data independently without interference from other users.

Wavelength channels can be dynamically allocated and reallocated based on user demand and network requirements.

Advantages of WDMA:

High Capacity: WDMA allows for high-capacity data transmission by leveraging the wide optical bandwidth available in fiber-optic cables.

Flexibility: WDMA offers flexibility in assigning and reallocating wavelength channels to accommodate changing user demands and network conditions.

Scalability: WDMA-based systems can easily scale to support additional users or data streams by adding more wavelength channels or upgrading multiplexing technologies.

Interference-Free: Each user operates on a dedicated wavelength channel, ensuring interference-free communication and high-quality data transmission.

- **Knowledge Check 3**

  Fill in the Blanks

  1. FDMA divides the available _____ spectrum into non-overlapping frequency bands, with each band allocated to individual users for communication. (**frequency**)
  2. TDMA divides the available time into discrete _____, with each slot allocated to individual users for communication within a predefined frame. **(time slots)**
  3. CDMA allows multiple users to share the same _____ band simultaneously using unique spreading codes. **(frequency)**
  4. In FDMA, each user is assigned a specific _____ band for communication, minimizing the likelihood of interference and collisions. **(frequency)**
  5. TDMA enables flexible allocation of resources based on changing traffic patterns by assigning users exclusive access to specific _____ within a frame. **(time slots)**

6.2 IEEE LAN standards:

- **Ethernet (Physical specifications, Encoding, Frame Format & MAC protocol)**
- **Physical Specifications:**

Ethernet is a widely used IEEE LAN standard that defines “physical and data link layer specifications for wired Ethernet networks”. It primarily operates over twisted-pair copper cables or fiber optic cables.

Twisted-Pair Ethernet:

Twisted-pair Ethernet commonly utilizes RJ-45 connectors and Category 5 (Cat5) or higher-grade cables.

It supports various data rates, including "10 Mbps (Ethernet), 100 Mbps (Fast Ethernet), 1 Gbps (Gigabit Ethernet), 10 Gbps (10 Gigabit Ethernet)", and beyond.

Ethernet over twisted pair employs differential signalling, where data is transmitted over pairs of wires with opposite polarity to reduce electromagnetic interference.

Fiber Optic Ethernet:

Fiber optic Ethernet employs optical fibers for data transmission, offering higher bandwidth and longer transmission distances compared to twisted-pair Ethernet.

It supports data rates ranging from 100 Mbps (Fast Ethernet) to 100 Gbps (100 Gigabit Ethernet) and beyond.

Fiber optic Ethernet is commonly used in high-speed and long-distance network applications, such as backbone connections between buildings or data centers.

- **Encoding:**

Ethernet utilizes various encoding schemes to represent digital data as electrical or optical signals for transmission over the physical medium.

Manchester Encoding:

In Manchester encoding, "each bit is represented by a transition from one voltage level to another within a clock period".

The transition from a "high to low voltage level (or vice versa) at the middle of the clock period represents a binary 1, while the absence of a transition represents a binary 0".

Manchester encoding ensures reliable clock recovery at the receiver and provides DC balance, making it suitable for Ethernet transmission.

4B/5B Encoding:

Ethernet frames use 4B/5B encoding to achieve DC balance and ensure sufficient transitions for clock recovery.

In 4B/5B encoding, each 4-bit data nibble is encoded into a 5-bit code group, expanding the data size by 25%.

The additional bits in the code group allow for efficient clock recovery and error detection at the receiver.

- **Frame Format:**

Ethernet frames consist of various fields that encapsulate data for transmission over the network.

The preamble “consists of a sequence of alternating 1s and 0s, followed by a unique synchronization pattern (10101011)”, which helps receiver synchronize its clock with the incoming data stream.

Start Frame Delimiter (SFD):

The SFD marks end of preamble and indicatesstart of frame.

It consists of a specific bit pattern (10101011), serving as a signal to the receiver that the frame's data payload is about to begin.

Destination and Source MAC Addresses:

These fields specify the MAC addresses of the destination and source devices, respectively.

MAC addresses uniquely identify network interfaces and are used for addressing and routing Ethernet frames within the network.

Length/Type Field:

The Length/Type field indicates the length of the data payload or specifies the type of protocol encapsulated in the Ethernet frame.

For Ethernet II frames, this field indicates the type of higher-layer protocol (e.g., IPv4, ARP, IPv6) carried within the Ethernet frame.

For “IEEE 802.3” frames, this field specifies “length of data payload”.

Data Payload:

The data payload contains the encapsulated data from the higher-layer protocol, such as IP packets, ARP requests, or TCP segments.

The length of the data payload can vary, depending on the Length/Type field in the Ethernet frame.

Frame Check Sequence (FCS):

The FCS field contains a “cyclic redundancy check” (CRC) value computed over the entire Ethernet frame.

The CRC value is used by the receiver to detect and discard frames with errors introduced during transmission.

- **MAC Protocol:**

Ethernet uses a contention-based “MAC” (Media Access Control) protocol, known as “Carrier Sense Multiple Access with Collision Detection” (CSMA/CD), to control access to the shared transmission medium.

Carrier Sense (CS):

Before transmitting data, Ethernet nodes listen to the network to detect ongoing transmissions or carrier signals.

If the channel is idle, nodes initiate transmission; otherwise, they wait for the channel to become idle.

Multiple Access (MA):

Multiple nodes share the same Ethernet segment and compete for access to the transmission medium.

Each node can attempt to transmit data independently.

Collision Detection (CD):

While transmitting data, nodes continue to monitor the network for collisions.

If a collision is detected (e.g., another node simultaneously transmits data), nodes abort transmission and enter a backoff period before retransmitting.

Ethernet's CSMA/CD protocol ensures fair and efficient access to the shared medium, minimizing the likelihood of collisions and maximizing network throughput.

- **BinaryExponential Backoff algorithm**

The Binary Exponential Backoff algorithm is a critical component of the “Carrier Sense Multiple Access with Collision Detection” (CSMA/CD) protocol, commonly used in Ethernet networks. This algorithm plays a crucial role in managing network congestion and resolving collisions that occur when multiple devices attempt to transmit data simultaneously on a shared medium.

1. Background:

In Ethernet networks, multiple devices share the same transmission medium.

The CSMA/CD protocol allows devices to sense the medium before transmitting data to avoid collisions.

However, collisions can still occur if two or more devices begin transmitting data simultaneously.

2. Collision Detection:

When a collision is detected, devices involved in the collision stop transmitting and enter a recovery phase.

The Binary Exponential Backoff algorithm is used during this recovery phase to determine when each device can reattempt transmission.

3. Algorithm Overview:

The Binary Exponential Backoff algorithm dynamically adjusts the retransmission time for devices involved in a collision, reducing the likelihood of repeated collisions.

It operates by selecting a random backoff interval from a range of possible values, based on the number of collisions experienced by a device.

4. Steps of the Algorithm:

When a collision occurs, each device involved doubles its contention window size.

The contention window represents the range of possible backoff values.

Devices then select a random backoff value from the updated contention window and wait for that duration before attempting to transmit again.

5. Binary Exponential Backoff Calculation:

After each collision, the contention window size is doubled, increasing the range of possible backoff values.

For example, if the initial contention window size is set to CW, the range of possible backoff values is [0, CW-1].

After the first collision, the contention window size is doubled to 2CW, and the range of possible backoff values becomes [0, 2CW-1].

Devices then select a random value from this expanded range as their backoff interval.

6. Adaptive Behavior:

The Binary Exponential Backoff algorithm exhibits adaptive behaviour, adjusting the retransmission time based on network conditions.

In cases of heavy network congestion or frequent collisions, devices increase their contention window size, leading to longer backoff intervals.

Conversely, in periods of low network activity, devices decrease their contention window size, reducing backoff intervals and improving network efficiency.

7. Efficiency and Fairness:

The Binary Exponential Backoff algorithm helps improve network efficiency by dynamically adjusting retransmission times, reducing the likelihood of repeated collisions.

It also promotes fairness by providing all devices with an equal opportunity to reattempt transmission, regardless of their previous collision history.

8. Implementation Considerations:

Implementation of the Binary Exponential Backoff algorithm requires maintaining state information for each device, including the current contention window size and collision count.

Devices must generate random backoff values within the specified range and adhere to the selected backoff interval before attempting transmission.

- **Token Ring and FDDI**

Token Ring is a LAN technology that utilizes a token-passing mechanism for controlling access to the shared network medium. It was developed by IBM in the 1980s and was standardized under IEEE 802.5.

Token Passing:

In a Token Ring network, devices are connected in a “logical ring topology”.

A special token “circulates around the ring, granting devices permission to transmit data”.

Only the device holding the token is allowed to transmit, ensuring fair access to the network.

Token Frame:

The token is encapsulated within a special frame format known as a token frame.

The token frame contains control information, including the address of the device holding the token.

Token Rotation:

When a device completes transmission, it releases the token, allowing it to circulate to the next device in the ring.

Token rotation continues indefinitely, ensuring that every device has an opportunity to transmit data.

Benefits of Token Ring:

Token Ring offers deterministic access to the network, as devices must wait for the token to transmit.

It provides predictable latency and guarantees fairness, as each device receives an equal share of network bandwidth.

Disadvantages of Token Ring:

Token Ring networks can experience performance degradation if a device fails or the token frame is lost.

Troubleshooting and maintenance of Token Ring networks can be more complex compared to other LAN technologies.

Fiber Distributed Data Interface (FDDI)

"Fiber Distributed Data Interface" (FDDI) is a high-speed LAN technology designed for reliable data transmission over fiber optic cables. It was developed in the 1980s and standardized by the "American National Standards Institute" (ANSI) and "International Organization for Standardization" (ISO).

Dual Counter-Rotating Rings:

FDDI networks utilize dual counter-rotating rings for redundancy and fault tolerance.

Data is transmitted in both directions simultaneously on the primary and secondary rings.

Token Passing:

Similar to Token Ring, FDDI uses a token-passing mechanism for controlling access to the network.

Devices in an FDDI network take turns transmitting data by capturing and releasing the token.

Frame Format:

FDDI frames consist of a header, data payload, and trailer, similar to Ethernet frames.

The header contains control information, including the source and destination addresses.

The trailer contains error-checking information, such as a cyclic redundancy check (CRC).

Fiber Optic Transmission:

FDDI networks utilize fiber optic cables for data transmission, offering high bandwidth and immunity to electromagnetic interference.

Fiber optic transmission enables long-distance communication and supports data rates of up to 100 Mbps.

Fault Tolerance and Redundancy:

FDDI networks are designed for fault tolerance, with dual rings providing redundancy in case of ring breaks or failures.

If a break occurs in one ring, traffic is automatically rerouted through the secondary ring to maintain network connectivity.

Station Management:

FDDI networks employ a station management protocol to coordinate token passing and monitor network performance. Station management functions include token circulation, ring initialization, and fault detection.

- **Knowledge Check 4**

  State True or False

  1. Ethernet utilizes twisted-pair copper cables for data transmission. (**True**)
  2. Binary Exponential Backoff algorithm dynamically adjusts retransmission times to resolve collisions in Ethernet networks. (**True**)
  3. Token Ring uses a contention-based MAC protocol for controlling access to the shared medium. (**False**)
  4. FDDI networks utilize fiber optic cables for data transmission. (**True**)
  5. Token Ring employs token passing as its access control mechanism. (**True**)

- **Outcome-based Activity 4**

  "A company is looking to upgrade its LAN infrastructure to meet growing demands. Evaluate Ethernet, Token Ring, and FDDI LAN standards, considering physical specifications, encoding, frame format, and MAC protocols. Recommend the most suitable standard and propose a collision avoidance mechanism. Justify your recommendations."

6.3 Introduction to Wireless Networks:

- **IEEE 802.11 Wireless LAN**

Wireless networks have become increasingly prevalent in modern communication systems, offering flexible connectivity without the constraints of physical cables. One of the most widely used standards for wireless local area networks (LANs) is “IEEE 802.11”, commonly known as Wi-Fi. IEEE 802.11 defines specifications for wireless communication in “2.4 GHz and 5 GHz” frequency bands, enabling devices to connect to wireless networks seamlessly.

Wireless LAN Architecture:

IEEE 802.11 Wireless LANs are designed to provide wireless connectivity within a limited geographic area, such as a home, office, or public hotspot.

Devices equipped with IEEE 802.11-compatible network interface cards (NICs) can connect to wireless access points (APs) to establish communication with the network.

Frequency Bands:

IEEE 802.11 operates in two primary frequency bands: “2.4 GHz and 5 GHz”.

The 2.4 GHz band offers wider coverage and better penetration through walls and obstacles but may suffer from interference from other devices operating in the same frequency range, such as microwaves and Bluetooth devices.

The 5 GHz band provides higher data rates and less interference, making it suitable for applications requiring higher performance and reliability.

PHY Layer:

The Physical (PHY) layer of IEEE 802.11 specifies the modulation techniques, data rates, and channel access methods used for wireless communication.

IEEE 802.11 defines multiple PHY standards, including “802.11a, 802.11b, 802.11g, 802.11n, 802.11ac, and 802.11ax”, each offering different data rates and capabilities.

MAC Layer:

The Medium Access Control (MAC) layer of IEEE 802.11 governs access to the wireless medium and manages communication between devices.

IEEE 802.11 MAC protocols include Distributed Coordination Function (DCF) and Point Coordination Function (PCF), providing contention-based and contention-free access mechanisms, respectively.

Wireless Security:

IEEE 802.11 defines security mechanisms to protect wireless networks from unauthorized access and data interception.

Common security protocols include “Wired Equivalent Privacy (WEP)”, “Wi-Fi Protected Access (WPA)”, and “WPA2/WPA3”, offering encryption and authentication mechanisms to secure wireless communication.

Service Sets:

IEEE 802.11 networks are organized into “Basic Service Sets” (BSS) and “Extended Service Sets” (ESS) to facilitate network management and roaming.

A BSS consists of a single AP and the associated wireless devices, while an ESS encompasses multiple interconnected BSSs, allowing devices to roam seamlessly between APs.

- **Wi-Max**

WiMAX (Worldwide Interoperability for Microwave Access)

WiMAX, an abbreviation for Worldwide Interoperability for Microwave Access, is a wireless communication technology designed to provide high-speed broadband access over long distances. It is based on the IEEE 802.16 standard and offers a wireless alternative to traditional wired broadband technologies, such as DSL and cable modems.

IEEE 802.16 Standard:

WiMAX is based on the IEEE 802.16 family of standards, which define the specifications for wireless metropolitan area networks (MANs).

The IEEE 802.16 standard encompasses multiple variants, including IEEE 802.16-2004 (802.16d), IEEE 802.16e, IEEE 802.16m, and IEEE 802.16n, each offering different features and capabilities.

Deployment Scenarios:

WiMAX can be deployed in various scenarios, including fixed WiMAX for stationary connections and mobile WiMAX for mobile access.

Fixed WiMAX is suitable for providing broadband access to homes, businesses, and remote areas with limited wired infrastructure.

Mobile WiMAX enables high-speed internet access on the go, supporting mobility for users within a WiMAX coverage area.

Frequency Bands:

WiMAX operates in licensed and unlicensed frequency bands, depending on regulatory requirements and spectrum availability.

Licensed WiMAX deployments typically operate in “2.3 GHz, 2.5 GHz, and 3.5 GHz” frequency bands, offering interference-free communication and better quality of service.

Unlicensed WiMAX deployments may utilize the 5 GHz frequency band, providing flexibility but potentially facing interference from other wireless devices operating in the same spectrum.

PHY and MAC Layers:

The Physical (PHY) layer of WiMAX defines the modulation techniques, frame structure, and channel access methods used for wireless communication.

The Medium Access Control (MAC) layer governs access to the wireless medium, scheduling of transmissions, and quality of service (QoS) management.

WiMAX supports both Time Division Duplexing (TDD) and Frequency Division Duplexing (FDD) modes, offering flexibility in deployment and spectrum utilization.

Advanced Features:

WiMAX offers advanced features such as adaptive modulation and coding, automatic repeat request (ARQ), and multiple-input multiple-output (MIMO) technology to enhance spectral efficiency and improve coverage and capacity.

These features enable WiMAX networks to adapt to changing environmental conditions and optimize performance for varying user requirements.

- **Bluetooth and other wireless PAN technologies & their applications**

Bluetooth and other wireless Personal Area Network (PAN) technologies enable short-range wireless communication between devices within a limited geographical area. These technologies facilitate seamless connectivity between various devices, such as smartphones, laptops, tablets, and IoT devices, without the need for physical cables. In addition to Bluetooth, other PAN technologies include Zigbee, Z-Wave, and NFC (Near Field Communication), each offering unique features and capabilities for specific applications.

Bluetooth Technology:

Bluetooth is a widely used wireless communication standard for short-range connectivity between devices.

It operates in the 2.4 GHz frequency band and supports multiple profiles for various applications, including “audio streaming” (A2DP), “file transfer” (FTP), and “device control” (HID).

Bluetooth employs “frequency hopping spread spectrum” (FHSS) and “adaptive frequency hopping” (AFH) techniques to minimize interference and ensure robust communication in noisy environments.

Other Wireless PAN Technologies:

Zigbee: Zigbee is a low-power wireless communication protocol designed for IoT and home automation applications.

It operates in the 2.4 GHz frequency band (Zigbee 2.4) or 800-900 MHz frequency bands (Zigbee PRO).

Zigbee networks typically consist of a coordinator, routers, and end devices, enabling mesh networking and peer-to-peer communication.

Z-Wave: Z-Wave is another “wireless communication protocol” used primarily in home automation and smart home devices.

It operates in the sub-1 GHz frequency bands, offering a longer range and better penetration through walls compared to 2.4 GHz technologies.

Z-Wave networks follow a star topology, with a central controller (hub) coordinating communication between devices.

NFC (Near Field Communication): NFC is a “short-range wireless technology” used for contactless communication between devices in close proximity (typically within a few centimetres).

NFC enables convenient interactions such as mobile payments, electronic ticketing, and device pairing.

It operates at 13.56 MHz and supports three modes of operation: “reader/writer mode”, “card emulation mode”, and “peer-to-peer mode”.

Applications of Wireless PAN Technologies:

Bluetooth: Bluetooth is used in various applications, including:

Wireless audio streaming (e.g., Bluetooth headphones, speakers).

Hands-free calling in cars (Bluetooth hands-free kits).

File transfer between smartphones, tablets, and computers.

IoT devices and smart home automation (Bluetooth Low Energy, or BLE).

Zigbee: Zigbee is deployed in:

Smart home devices such as smart lighting, thermostats, and door locks.

Industrial automation and control systems.

Wireless sensor networks for environmental monitoring and asset tracking.

Z-Wave: Z-Wave finds applications in:

Home automation systems for controlling lights, appliances, and security devices.

Energy management solutions for monitoring and controlling energy usage.

Elderly care and assisted living applications for remote monitoring and emergency alerts.

NFC: NFC is used for:

Contactless payments and mobile wallets.

Access control systems for buildings and public transport.

Pairing Bluetooth devices and exchanging contact information between smartphones.

- **Cellular Networks: Generations**

Cellular networks have evolved through multiple generations, each offering advancements in wireless communication technology. These generations, denoted by G1, G2, G3, and so on, represent significant milestones in the development of mobile telecommunications. Key generations include 1G (analog), 2G (digital), 3G (mobile broadband), 4G (LTE), and 5G (ultra-fast, low-latency connectivity).

1G (First Generation):

1G cellular networks were the first commercially available mobile networks, introduced in the 1980s.

These networks used analog signals for voice communication and offered limited coverage and capacity.

Examples of 1G systems include “Advanced Mobile Phone System” (AMPS) in North America and “Total Access Communication System” (TACS) in Europe.

2G (Second Generation):

2G networks marked the transition to digital communication, offering improved voice quality and security.

The two main standards for 2G were “GSM (Global System for Mobile Communications) and CDMA (Code Division Multiple Access)”.

GSM became the dominant standard globally, while “CDMA” was primarily used in North America and some other regions.

3G (Third Generation):

3G networks introduced mobile broadband services, enabling faster data transmission rates and support for multimedia applications.

Standards such as “UMTS (Universal Mobile Telecommunications System)” and “CDMA2000” were deployed to deliver 3G services.

3G networks facilitated the adoption of services like video calling, mobile internet browsing, and mobile TV.

4G (Fourth Generation):

4G networks, based on LTE (Long-Term Evolution) technology, offered significant improvements in data speeds, latency, and spectral efficiency.

LTE networks provided faster download and upload speeds, making high-definition video streaming and online gaming possible on mobile devices.

4G networks also supported advanced features such as “Voice over LTE” (VoLTE) for high-quality voice calls over IP.

5G (Fifth Generation):

5G represents the latest evolution in cellular technology, promising ultra-fast data rates, low latency, and massive connectivity.

5G networks leverage technologies such as millimeter-wave spectrum, massive MIMO (Multiple-Input Multiple-Output), and network slicing to deliver high-performance connectivity.

Applications of 5G include augmented reality (AR), virtual reality (VR), autonomous vehicles, remote healthcare, and industrial IoT (Internet of Things).

- **GSM & CDMA Technologies**

GSM (Global System for Mobile Communications):

GSM is a digital cellular technology widely deployed globally for mobile telecommunications. It was introduced in the 1980s and has since become the dominant standard for 2G (second generation) and later generations of mobile networks.

TDMA (Time Division Multiple Access):

GSM employs TDMA technology, where the radio spectrum is divided into time slots or frames.

Each time slot is assigned to a specific user, allowing multiple users to share the same frequency channel.

TDMA enables efficient use of the radio spectrum, maximizing network capacity and accommodating multiple users simultaneously.

Architecture:

GSM networks consist of several components, including “mobile stations (MS)”, “base transceiver stations” (BTS), “mobile switching centres” (MSC), and “home location registers” (HLR).

Mobile stations, such as mobile phones, communicate with base stations, which are connected to the core network through mobile switching centres.

Home location registers store subscriber information, including authentication data and subscriber profiles.

Services and Features:

GSM networks offer a wide range of services and features, including voice communication, text messaging (SMS), multimedia messaging (MMS), and data services.

Additional features include caller ID, call waiting, call forwarding, conference calling, and voicemail.

SIM (Subscriber Identity Module) cards are used in GSM networks to authenticate subscribers and store subscriber information, enabling seamless roaming between different networks.

Security:

GSM incorporates security mechanisms to protect user privacy and prevent unauthorized access to the network.

Authentication and encryption algorithms are used to verify the identity of subscribers and encrypt communication between mobile devices and the network.

SIM cards play a crucial role in authentication, storing secret keys and authentication data used to verify subscriber identities.

Evolution:

GSM has evolved over the years to support higher data rates and advanced services.

Enhanced versions of GSM, such as EDGE (Enhanced Data Rates for GSM Evolution), introduced higher data speeds for internet browsing and multimedia applications.

GSM technology served as the foundation for subsequent generations of mobile networks, including 3G (UMTS) and 4G (LTE).

CDMA (Code Division Multiple Access):

CDMA is a digital cellular technology that utilizes spread spectrum techniques for communication. Unlike GSM, which uses TDMA, CDMA assigns a unique code to each user to transmit data simultaneously over the same frequency band.

Spread Spectrum Technology:

CDMA employs spread spectrum modulation techniques, where each user is assigned a unique code to transmit data over the entire frequency band simultaneously.

The unique codes allow multiple users to share the same frequency resources without causing interference.

CDMA systems use complex signal processing algorithms to decode and separate signals from different users.

Architecture:

CDMA networks consist of base stations, mobile stations, and network elements such as base station controllers (BSC) and mobile switching centres (MSC).

Base stations communicate with mobile stations, which may include mobile phones, tablets, or other wireless devices.

Network elements manage call routing, handover between cells, and subscriber authentication.

Advantages:

CDMA offers several advantages, including increased capacity, improved call quality, and enhanced security.

By allowing multiple users to transmit data simultaneously over the same frequency band, CDMA networks can accommodate more users and support higher data rates compared to TDMA systems.

CDMA technology also provides better call quality and coverage in areas with high interference or noise.

Deployment:

CDMA technology was initially deployed in North America and some other regions, primarily by carriers such as Verizon Wireless and Sprint.

While CDMA networks were prevalent in the 2G and 3G eras, many operators have transitioned to newer technologies such as LTE (4G) and 5G for higher data speeds and improved performance.

Evolution:

CDMA technology has evolved over the years to support higher data rates and advanced services.

Enhanced versions of CDMA, such as CDMA2000, introduced improvements in data speeds, multimedia capabilities, and support for packet-switched data services.

However, with the emergence of LTE and 5G technologies, many operators have phased out CDMA networks in favour of newer, more efficient technologies.

- **Knowledge Check 5**

  Fill in the Blanks

  1. IEEE 802.11 Wireless LAN operates in the _____ GHz and _____ GHz frequency bands. **(2.4, 5)**
  2. Wi-Max stands for Worldwide Interoperability for Microwave _____. (**Access**)
  3. Bluetooth operates in the _____ GHz frequency band and supports multiple _____ profiles. **(2.4, Bluetooth)**

4. The latest generation of cellular networks, known as _____, promises ultra-fast data rates and low _____. **(5G, latency)**
5. GSM uses _____ Division Multiple Access (TDMA) technology, while CDMA utilizes Code Division Multiple Access (_____). **(Time, CDMA)**

- **Outcome-Based Activity 5**

  Create a brief comparison chart for IEEE 802.11 Wireless LAN, Wi-Max, Bluetooth, other wireless PAN technologies, and Cellular Networks' Generations (including GSM & CDMA). Each group will research one technology and present its key features and applications. Afterwards, students will rotate between groups to learn about each technology. Finally, students will discuss similarities, differences, and potential impacts on communication.

6.4 Summary

- Limited Contention Protocols reduce contention among network nodes to improve efficiency.
- Channelization techniques like FDMA, TDMA, and CDMA divide the communication channel into sub-channels for multiple users.
- Wavelength Division Multiple Access enables multiple data streams to share a fiber-optic communication link.
- Ethernet specifications define the Physical Layer, Encoding, Frame Format, and MAC protocol for wired LANs.
- Binary Exponential Backoff algorithm is used in Ethernet networks to manage retransmissions after collisions.
- Token Ring and FDDI protocols are alternative LAN technologies with unique architectures and features.
- IEEE 802.11 Wireless LAN provides wireless connectivity for devices within a local area network.
- Wi-Max technology offers high-speed wireless broadband access over long distances.
- Bluetooth and other wireless PAN technologies enable short-range communication between devices.

6.5 Keywords

- **WDMA (Wavelength Division Multiple Access):** A technique used in fiber-optic communication systems to allow multiple signals to be transmitted simultaneously over different wavelengths of light.
- **Wi-Max (Worldwide Interoperability for Microwave Access):** A wireless communication technology that provides high-speed broadband access over long distances, suitable for metropolitan area networks (MANs).

6.6 Self-Assessment Questions

6. Describe the concept of Wavelength Division Multiple Access (WDMA) and its role in fiber-optic communication.
7. Discuss the differences between GSM and CDMA technologies in cellular networks, including their advantages and limitations.
8. Explain the role of Limited Contention Protocols in improving network performance and reducing collisions in shared media networks.

6.7 References / Reference Reading

- Stallings, W., "Wireless Communications & Networks." Pearson, 2017.
- Andrews, J. G., Ghosh, A., & Muhamed, R., "Fundamentals of WiMAX: Understanding Broadband Wireless Networking." Prentice Hall, 2007.
- Miller, M., "Bluetooth Essentials for Programmers." Cambridge University Press, 2007.
- Rappaport, T. S., "Wireless Communications: Principles and Practice." Pearson, 2001.
- Schwartz, M., "Broadband Integrated Networks." Prentice Hall, 1996.
- Kurose, J. F., & Ross, K. W., "Computer Networking: A Top-Down Approach." Pearson, 2016.

Unit 7: Transport Layer

Learning Outcomes:

- Students will be able to define TCP and UDP protocols' key characteristics and functions in network communication.
- Students will be able to differentiate between connection-oriented and connectionless protocols and explain their respective advantages and limitations.
- Students will be able to analyze the addressing and header formats of IPv4 and IPv6, identifying key fields and their functions.
- Students will be able to describe the services the network layer provides in the OSI model and their importance in data transmission.
- Students will be able to apply knowledge of network layer protocols and congestion control mechanisms to design and troubleshoot network architectures.

Structure:

7.1 Transport layer

- **Addressing Services and Protocols:**

The Transport layer of the OSI model is primarily responsible for facilitating communication between processes running on different hosts. It ensures accurate and trustworthy data transfer

between endpoints. Ports are used to identify these endpoints to address them within the Transport layer.

Applications communicate with one another through ports, which are essentially virtual endpoints. They help distinguish between different programs or services that are operating on the same device. A distinct number, ranging from 0 to 65535, is allocated to every port.

Before being sent via a network, data is divided into packets or segments at the transport layer. These sections contain a variety of data, including.

1. **Source Port:** This is the port the sending process or program uses. It facilitates the identification of the service or program that created the data by the receiving device.
2. **Destination Port:** This is the port number the data addresses on the receiving device. It facilitates the receiving device's ability to direct incoming data to the relevant service or application.

The source and destination ports can uniquely identify a communication session between two hosts. Furthermore, ports allow several network services to run concurrently on a single device.

There are different categories of ports:

1. **Well-known ports**: These ports, which are designated for particular, standardized services, are numbered 0 through 1023. For instance, port 80 is usually used for HTTP, and port 443 is used for HTTPS.
2. **Registered ports**: The Internet Assigned Numbers Authority (IANA) has allocated these ports, which span from 1024 to 49151, to certain services or protocols.
3. **Dynamic or private ports**: These ports are open for any application or service to use on an as-needed basis and span from 49152 to 65535. They are frequently utilized as the source ports for connections that go out.

Two main protocols manage communication within the Transport layer: UDP (User Datagram Protocol) and TCP (Transmission Control Protocol).

TCP delivers data in an orderly and dependable manner and is connection-oriented. Prior to data exchange, it creates a link between the sender and the recipient, guaranteeing error-free and sequential delivery of the data.

In contrast, UDP offers a lightweight data transmission technique and is connectionless. It doesn't wait for a connection to be established before transmitting data and doesn't ensure

ordered delivery or dependability. Applications like streaming media and online gaming, which value speed and efficiency over dependability, frequently use UDP.

- **TCP and UDP services & header formats:**

TCP (Transmission Control Protocol) Services:

The connection-oriented TCP protocol ensures dependable, systematic data transfer between connected devices. It guarantees that data packets are sent precisely, error-free, and in the right order. TCP provides a number of important services:

Reliable Data Delivery: TCP ensures that information transferred between two endpoints will be received by the other endpoint intact. To accomplish this reliability, it uses techniques like acknowledgements, retransmissions, and sequence numbers.

Ordered Delivery: Data packets are delivered in the same sequence as they were sent, thanks to TCP. This is essential for applications where the sequence of data matters, such as file transfers and web browsing.

Flow Control: By controlling the data transfer rate, TCP keeps the sender from overloading the recipient. Using a sliding window technology, it dynamically modifies the transmission rate according to the receiver's buffer capacity.

Congestion Control: By modifying the transmission rate in response to network conditions, TCP helps avoid network congestion. It uses techniques including gradual start, congestion avoidance, and quick retransmit to control congestion and guarantee effective data transfer.

TCP Header Format:

The TCP header, which encapsulates TCP segments, has a number of fields that regulate how the TCP protocol behaves. The following fields make up the header format:

“Source Port”: “16 bits”. Specifies the port number of the sending application.

“Destination Port”: “16 bits”. Specifies the port number of the receiving application.

“Sequence Number”: “32 bits”. Used to ensure the correct sequencing of data packets.

“Acknowledgment Number”: “32 bits”. Indicates the next sequence number the sender expects to receive.

“Data Offset”: 4 bits. Specifies the length of the TCP header in 32-bit words.

“Reserved”: 6 bits. Reserved for future use.

“Flags”: Various control flags, including:

“SYN”: Synchronize sequence numbers to initiate a connection.

“ACK”: Acknowledge receipt of data.

“FIN”: Indicate the end of data transmission.

“RST”: Reset the connection.

“URG”: Urgent data pointer field is significant.

“Window Size”: “16 bits”. Specifies the size of the receive window used for flow control.

“Checksum”: “16 bits”. Used for error detection to ensure the integrity of the TCP segment.

“Urgent Pointer”: “16 bits”. Indicates the end of urgent data in the TCP segment.

“Options”: Variable length. Optional fields are used for various purposes, such as “maximum segment size” (MSS), “selective acknowledgments” (SACK), and “timestamp”.

UDP (User Datagram Protocol) Services:

UDP is a lightweight protocol that allows data to be transmitted between devices on a network without requiring a connection. UDP does not provide error checking, ordered delivery, or reliability like TCP does. The following services are provided by UDP:

Low Overhead: Because UDP has less overhead than TCP, it is a good choice for applications like multimedia streaming and real-time communication, where efficiency and speed are more crucial than reliability.

Connectionless Communication: UDP transmits data without first establishing a connection. Independent UDP packet transmission occurs without any prior preparation.

No Flow Control or Congestion Control: Neither flow control nor congestion control are handled by UDP. Applications can send data at their own speed, thanks to this, but if it's not handled correctly, it may cause network congestion.

UDP Header Format:

The UDP header is used to encapsulate UDP datagrams and consists of the following fields:

“Source Port”: “16 bits”. Specifies the port number of the sending application.

“Destination Port”: “16 bits”. Specifies the port number of the receiving application.

“Length”: “16 bits”. Specifies the length of the UDP datagram, including the header and data.

“Checksum”: “16 bits”. Used for error detection to ensure the integrity of the UDP datagram (optional in IPv4, mandatory in IPv6).

- **Knowledge Check 1**

  Fill in the Blanks

  1. Among devices on a network, TCP is a _____ protocol that offers dependable, organized data transfer. **(connection-oriented/** Connectionless**)**
  2. The TCP header consists of various fields, including the _____ field, which specifies the port number of the sending application. **(Source Port** / Destination port)
  3. UDP is a _____ protocol that provides a lightweight mechanism for transmitting data between devices on a network. **(connectionless /** Connection-Oriented**)**
  4. Unlike TCP, UDP does not perform _____ or _____ control. **(flow control, congestion control/**flooding Control, error control**)**
  5. A _____ field in the UDP header indicates how long the UDP datagram will be, including the header and data. **(Length/**header**)**

- **Outcome-Based Activity 1**

  When designing a network protocol for a new application, would you choose TCP or UDP for a video conferencing application requiring real-time communication? Justify your choice briefly based on the key characteristics of TCP and UDP.

7.2 Summary

- Discusses how addressing works at the transport layer and the various services and protocols provided.
- Provides an in-depth explanation of the services offered by TCP and UDP, along with detailed descriptions of their respective header formats.

7.3 Keywords

- **TCP**–"Transmission Control Protocol": A reliable, connection-oriented protocol that ensures the ordered and error-checked delivery of data packets over a network.
- **UDP**–"User Datagram Protocol": A connectionless protocol that provides a lightweight and fast transmission of data packets without guaranteeing delivery or order.

7.4 Self-Assessment Questions

1 What are the key differences between TCP and UDP protocols in terms of reliability and connection-oriented nature?

7.5 References / Reference Reading

- Michael A. Gallo, William M. Hancock, Computer Communications and Networking Technologies, CENGAGE learning.
- William Stallings, Data and Computer Communications, PHI

Unit 8: Network layer

Learning Outcomes:

- Students will be able to define TCP and UDP protocols' key characteristics and functions in network communication.
- Students will be able to differentiate between connection-oriented and connectionless protocols and explain their respective advantages and limitations.
- Students will be able to analyze the addressing and header formats of IPv4 and IPv6, identifying key fields and their functions.
- Students will be able to describe the services the network layer provides in the OSI model and their importance in data transmission.
- Students will be able to apply knowledge of network layer protocols and congestion control mechanisms to design and troubleshoot network architectures.

Structure:

8.1 Network Layer:

- Services
- Routing Algorithms: Shortest path Routing
- Flooding
- Distance Vector Routing, Link State Routing
- Hierarchical Routing, Multi Cast Routing
- Routing for Mobile hosts
- Knowledge Check 2,Outcome-Based Activity 2

8.2 Network layer in TCP/IP: Basic characteristics of IP protocol

- Addressing and header format of IPv4
- IPv6: Major goals& features

8.3 Summary

8.4 Keywords

8.5 Self-Assessment Questions

8.6 References / Reference Reading

8.1 Network Layer

- **Services**

Routing: Data packets are routed to find the most efficient path from a source to a destination across a network.

Choosing the most effective path takes into account variables, including traffic volume, link fees, and network topology.

Router-to-router communication is facilitated by routing protocols like as BGP, OSPF, and RIP.

Addressing: In order to facilitate communication, devices in a network are assigned unique identifiers, usually IP addresses. This process is known as addressing.

Routers can forward packets to the appropriate destination based on the destination IP address thanks to IP addressing.

Forwarding: Using the target address as a guide, forwarding routes incoming packets from one router interface to the proper outgoing interface.

Forwarding tables sometimes referred to as routing tables, are used by routers to decide which packets to forward depending on destination IP addresses.

- **Routing Algorithms: Shortest path Routing**

In computer networks, telecommunications systems, transportation networks, and many other fields where determining the most effective path between two places is the goal, the shortest path routing algorithms are essential components. Within a network, these algorithms seek to identify the path that minimizes both cost and distance between a source and a destination node. The following is a thorough explanation of some shortest-path routing algorithm-related topics:

Definition and Objective:

Algorithms for shortest-path routing are made to determine the cheapest path between two nodes in a network. According to the network context, the "shortest path" is the path with the lowest metric, which may be determined by distance, time, cost, or any other pertinent attribute.

Types of Shortest Path Routing Algorithms:

Dijkstra's Algorithm: This algorithm, which is named after the Dutch computer scientist Edsger W. Dijkstra, determines the shortest path in a weighted graph with non-negative edge weights between a single source node and every other node. It operates by repeatedly choosing

the node with the shortest estimated distance and updating the distances between its nearby nodes.

When all edge weights in a graph are non-negative, Dijkstra's algorithm is a popular tool for determining the shortest path between nodes. It was developed in 1956 by Dutch computer scientist Edsger W. Dijkstra and is now regarded as a fundamental algorithm in network routing and computer science. The operation of Dijkstra's algorithm is explained in full below:

Initialization:

Allocate an approximate distance value to each node within the graph. The distance value represents the shortest path between that node and the source node. Set all other nodes' distances to infinity and the source node's distance to 0.

Designate every node as unvisited.

Selection of the Next Node:

Choose the unexplored node with the least estimated distance at each stage. This will be the source node at first.

The method is complete if the remaining unvisited nodes are all infinitely far apart.

Update Neighboring Nodes:

Take into account each and every one of the chosen node's neighbours (i.e., nodes connected by an edge).

Determine the approximate distance for each neighbour going through the current and source nodes. To do this, multiply the weight of the edge from the current node to its neighbour by the distance from the source node to the current node.

Update the neighbour's distance to reflect the new value if this estimated distance is smaller than the neighbour's prior recorded distance.

Mark the Selected Node as Visited:

Once the chosen node's neighbours have been looked at, designate the chosen node as visited. By doing this, it is guaranteed that the distance will not be adjusted in further iterations.

Repeat:

Repeat steps 2-4 until all nodes have been visited.

Termination:

When every node has been visited or the target node has been designated as visited, the algorithm comes to an end. At this stage, all nodes can be reached from the source node (or the destination node) using the shortest path possible.

Reconstruction of the Shortest Path:

By going backwards from the destination node, the shortest path from the source node to any other node can be recreated once the algorithm has finished. This is accomplished by returning to the source node from the destination node by following the path of predecessors or the nodes that contribute to the shortest path.

Complexity:

When adjacency matrices are used in the implementation of Dijkstra's algorithm, the time complexity is O(V^2), where V is the number of nodes in the graph.

The temporal complexity can be lowered to O((V + E) log V) with more effective data structures such as priority queues, where E is the number of edges in the graph.

Bellman-Ford Algorithm: This approach works well in distributed systems and can handle graphs with negative edge weights. It constantly loops over every edge in the graph, relaxing them by determining if there is a more direct route to a node via the current edge.

To determine the shortest path between a source node and every other node in a weighted network, apply the Bellman-Ford algorithm. Because it can recognize and manage negative cycles, it's especially helpful when negative edge weights exist. This is a thorough description of the Bellman-Ford algorithm's operation:

Initialization:

Each node in the graph should have a distance value assigned to it that indicates the shortest path between it and the source node. Set all other nodes' distances to infinity and the source node's distance to 0.

Remember who each node was before it, as this will help you subsequently reconstruct the shortest path.

Relax Edges:

Repeatedly iterate over each edge of the graph V-1 times, where V is the number of nodes in the graph. This guarantees that, up to convergence, the shortest pathways are updated gradually.

Relax an edge (u, v) in the graph by determining if travelling through u will enhance the shortest path to v, where u is the source node, and v is the destination node.

Update the distance value of v to the new, shorter distance and update the predecessor of v to u if the distance to v may be shortened by taking the edge (u, v).

Detection of Negative Cycles:

All shortest paths with maximum V-1 edges have been identified after V-1 iterations. Nevertheless, if the graph contains negative cycles, more iterations can permanently shorten the nodes' lengths along those cycles.

Make one additional loop through each edge in order to identify negative cycles. A negative cycle that is reachable from the source node is present if any distance value can be further decreased.

Output:

The procedure ends, and each node's shortest distances and predecessors are known if no negative cycles are found during the subsequent iteration.

Upon detection of a negative cycle, the algorithm can either report its existence or handle it according to the needs of the application.

Complexity:

The time complexity of the Bellman-Ford algorithm is O(V*E), where V is the number of nodes in the graph, and E is the number of edges.

Because of this, it is less effective than Dijkstra's algorithm for networks whose edge weights are not negative, but it can still handle graphs whose edge weights are negative and identify negative cycles.

Considerations:

When detecting the existence of negative cycles or for graphs with negative edge weights, the Bellman-Ford approach is appropriate.

Compared to Dijkstra's algorithm, it performs less well on graphs with zero edge weights.

In some situations, the extra iteration required to identify negative cycles causes it to operate more slowly than alternative methods.

Floyd-Warshall Algorithm: Floyd-Warshall computes the shortest paths between every pair of nodes in a graph, in contrast to Dijkstra's and Bellman-Ford's methods. It is based on dynamic

programming and comes in handy when one does not know the precise source-destination pairs in advance.

Finding the shortest pathways between any pair of nodes in a weighted network, including ones with negative edge weights, is possible using the Floyd-Warshall algorithm, a dynamic programming technique. It is especially helpful when the precise source-destination pairs are unknown in advance, as it was independently proposed by Robert Floyd and Stephen Warshall in 1962. This is an in-depth description of the Floyd-Warshall algorithm.:

Initialization:

Make a 2D array dist[][] with the dimensions V x V, where V is the graph's node count. Set the initial value of each dist[][] element to infinity.

Update dist[u][v] to w for each edge (u, v) in the graph with weight w. In the event that u and v have no edges, set dist[u][v] to infinity.

Since there is always a zero distance between a node and itself, initialize the diagonal elements of dist[][] to 0.

Dynamic Programming Iteration:

Go through every node k from 1 to V in iteration.

If there is a shorter path from node k to node j, adjust dist[i][j] for each pair of nodes i and j.

Dist[i][k] + dist[k][j] is the formula for calculating the new distance. Update dist[i][j] to reflect the new distance if it is less than the existing dist[i][j].

Optimization:

By keeping only two 2D arrays—the current distance matrix and an intermediate matrix for the dynamic programming updates—the technique can be made to use space more effectively.

New distances are added to the intermediate matrix every time, which is subsequently used as a basis for updating the current distance matrix. This optimization lowers the space complexity from O(V^3) to O(V^2).

Detection of Negative Cycles:

Once every iteration is finished, look at the diagonal members of the final dist[][] matrix to see if there are any negative cycles. A negative cycle is present in the graph if any diagonal elements are negative.

Output:

The shortest distances between each pair of nodes in the graph are included in the final dist[][] matrix.

The dist[][] matrix can be used to reconstruct the shortest pathways between all pairs of nodes if no negative cycles are found.

Complexity:

The Floyd-Warshall algorithm has an O(V^3) time complexity and an O(V^2) space complexity, where V is the graph's node count.

It works well with graphs that are thick or have a small number of nodes.

Considerations:

For determining the shortest paths in dense graphs or when there aren't many nodes, the Floyd-Warshall technique works well.

It can identify negative cycles and handle graphs with negative edge weights.

In graphs with non-negative edge weights, the approach is not as effective as Dijkstra's algorithm for locating single-source shortest paths.

An Algorithm*: a heuristic search algorithm that blends aspects of the Best-First and Dijkstra search methods. In order to effectively direct the search towards the target, it employs a heuristic to calculate the cost of the cheapest path from the current node to the goal node.

In a weighted network, the A* (pronounced "A-star") algorithm is a well-liked heuristic search algorithm that finds the shortest path between a start node and a goal node. It effectively combines the benefits of greedy best-first search, which is quick but doesn't ensure optimality, with Dijkstra's algorithm, which ensures the shortest path. In order to accomplish this, A* takes into account both the real cost of travelling to each node from the start node and uses a heuristic to direct the search towards the objective. This is an in-depth explanation of how the A* algorithm works:

Initialization:

Set an open set and a closed set to their initial values. Nodes that have been found but not yet evaluated are in the open set, whereas nodes that have been reviewed already are in the closed set.

Add the start node to the open set at a zero cost. Set the start node's cost to zero and initialize it.

Each node should be given a heuristic value that indicates an approximate cost estimate from that node to the goal node. Since this heuristic never overestimates the true cost, it should be accepted.

Search Iteration:

While the open set is not empty:

From the open set, choose the node with the lowest total cost, which is the sum of the heuristic estimate from the current node to the goal node and the actual cost from the start node to the current node.

The shortest path has been discovered if the chosen node is the target node. Put an end to the algorithm and give the path back.

If not, indicate that the selected node has been evaluated by moving it from the open set to the closed set.

Examine every node that the chosen node has nearby that is not part of the closed set.

For each neighbouring node:

Summing the actual cost from the start node to the chosen node and the cost of moving from the selected node to the nearby node, get the approximate total cost from the start node to the neighbouring node.

In the event that the nearby node is not included in the open set or if the estimated cost is less than the node's previously documented cost

Adjust the surrounding node's recorded cost to the estimated cost.

Change the selected node's parent to that of the surrounding node.

Add the surrounding node to the open set if it isn't already there.

Termination:

There is no path connecting the start node and the goal node if the open set is empty and the goal node has not been reached.

Path Reconstruction:

Recreate the shortest path from the start node to the goal node by following the parent pointers from the goal node back to the start node if the goal node has been reached.

Complexity:

Depending on the graph's shape and the heuristic function employed, the A* algorithm's temporal complexity can change. While it is frequently much lower in practice, it can be exponential in the worst-case scenario.

The quality of the heuristic function has a major impact on A*'s efficiency. An effective heuristic can greatly shrink the search space and enhance the efficiency of the program.

Considerations:

Pathfinding and route planning applications, such as GPS navigation systems, video games, robotics, and logistics, frequently use A*.

The admissibility and precision of the heuristic function are critical components of A*'s effectiveness. Faster convergence frequently results from using a heuristic that underestimates the true cost.

It is possible to expand and alter A* to handle a variety of issue domains, such as continuous spaces, grid-based maps, and weighted graphs.

Metrics for Path Calculation:

Distance-Based: Distance in transportation or communication networks can relate to latency, hop count, or actual physical distance.

Cost-Based: Cost can refer to the amount of money spent, the amount of energy used, or any other resource expenditure used to cross a link.

Time-Based: Time may be a crucial component in real-time systems since it represents the amount of time needed to transit between nodes.

Challenges and Considerations:

Scalability: Concerns of scalability and efficiency are vital, particularly in large-scale networks with lots of nodes and linkages.

Dynamic Environments: Algorithms must dynamically react to changes in networks, such as link outages, congestion, or fluctuating traffic loads.

Complexity: Certain algorithms may not be appropriate for real-time applications or devices with limited resources due to their high computational complexity.

Optimality: Although many algorithms promise to identify the shortest path, there are differences in what constitutes the "shortest" path, and certain algorithms may not necessarily result in the best answers.

Applications:

Internet Routing: Internet routing protocols such as IS-IS (Intermediate System to Intermediate System) and OSPF (Open Shortest Path First) are based on the concept of shortest path routing.

Transportation Networks: Internet routing protocols such as IS-IS (Intermediate System to Intermediate System) and OSPF (Open Shortest Path First) are based on the concept of shortest path routing.

Telecommunications: Shortest path routing is used by telecommunication networks to route data packets across several nodes and links effectively.

- **Flooding:**

Flooding, in the context of networking, is a simple but powerful technique used to disseminate information across a network. It involves broadcasting data packets or messages from a source node to all other nodes in the network without regard for the network topology. Description of flooding:

Broadcasting:

A source node initiates the flooding process by wishing to send a message or data packet to every other node in the network.

Initially, the message is sent by the source node to every node that is nearby.

Propagation:

Every neighbouring node that receives the message rebroadcasts it to all of its neighbours—all of them, aside from the node that originally sent it.

To guarantee that the message reaches every node in the network, this process is repeated recursively by each node that receives it and transmits it to its neighbours.

Loop Prevention:

Nodes maintain track of the messages they have already received and only rebroadcast those they have not seen before to avoid infinite loops and excessive message duplication.

A hop count or time-to-live (TTL) parameter, which restricts how many times a message can be transmitted or how far it can go before being deleted, may also be included in flooding algorithms.

Termination:

Flooding keeps up until the message reaches every node in the network.

Depending on the application or protocol, termination criteria could include a certain amount of message transmissions or an acknowledgement of messages received from every node.

Advantages:

Robustness: Flooding doesn't rely on particular routes or network structure information, so it is extremely resistant to network outages and topology changes.

Simplicity: It requires little network configuration or coordination and is simple to implement.

Scalability: Flooding is appropriate for usage in distributed and decentralized systems since it can grow to encompass massive networks with numerous nodes.

Disadvantages:

Packet Redundancy: Over-duplication of messages due to flooding can increase network traffic and resource consumption.

Inefficiency: If there are no measures to prevent unnecessary message transmission, flooding may be inefficient in networks with high connectivity or density.

Security Concerns: Flooding may be threatened by eavesdropping, denial-of-service attacks, packet spoofing, and other security vulnerabilities.

Distance Vector Routing:

Distance vector routing is a type of routing methodology used to determine the best method of forwarding packets from a source node to a destination node in a computer network.

Initialization:

Each node in the network includes a routing table that contains information about the costs and distances needed to connect to each other node.

At first, every node just knows the approximate cost of reaching its immediately linked neighbours. This data is stored in the routing table.

Distance Vector Calculation:

Every node periodically shares its routing table with the nodes nearby.

When a node receives a neighbour's routing table, it updates its own routing table with the neighbour's advertised rates and the cost of going to the neighbour.

The node calculates the distance to each destination node by adding the cost of the neighbour to the cost of going to them.

- **Distance Vector Exchange:**

They share their routing tables with their nearest neighbours in order to communicate information about the network topology and link costs.

Each node sends its entire routing table to its neighbours to update their routing tables appropriately.

Route Selection: After obtaining updated routing tables from its neighbours, a node looks at the total expenses reported by each neighbour to go to a target node.

The node updates its routing table based on its choice of neighbour that offers the cheapest overall cost—the shortest path—to each destination.

Iterative Updates:

Trading and updating routing tables are ongoing iterative procedures.

Nodes progressively approach consistent routing tables, where each node precisely knows the best paths to every other node in the network.

Managing Changes: When a node loses connectivity or a link cost changes, the affected nodes alert their neighbours.

Nodes update their routing tables as needed and recalculate the quickest paths based on the most recent information.

Advantages:

Separation When it comes to implementation and comprehension, Vector Routing is less complicated than other routing algorithms.

Decentralization: Decentralized decision-making and network adaptability are made possible by each node's autonomous maintenance of routing tables.

Robustness: Because Distance Vector Routing uses an iterative update process, it can withstand sporadic network outages or connection failures.

Disadvantages:

Count to Infinity Issue: Inaccurate distance data might result in routing loops or less-than-ideal routes when there is a "count to infinity" issue with distance vector routing methods.

Slow Convergence: Distance vector routing's iterative design can lead to slow convergence, particularly in big networks or networks with a lot of link churn.

Limited Scalability: Distance Vector Routing's scalability is restricted by the overhead of exchanging and updating routing tables in large or dynamic networks.

- **Link State Routing:**

In computer networks, link state routing is a kind of routing algorithm that determines the optimal route for packet forwarding from a source node to a destination node.

Topology Exploration:

Every node in the network collects data on the neighbors it is directly connected to as well as the links that bind them.

This data contains the surrounding nodes' identities, each link's cost (or metric), and other pertinent variables.

Nodes communicate this data to one another in order to create a complete picture of the network topology.

Link State Advertisement: A node creates a packet known as a Link State Advertisement (LSA) after gathering data about its neighbours and the network structure. The LSA contains details about the node itself, its neighbouring nodes, and the state of each link.

In order to guarantee that every node receives accurate and consistent information about the network architecture, the LSA is flooded throughout the network.

Shortest Path Calculation:

Each node builds the Link State Database (LSDB), a comprehensive network topology representation, upon receiving LSAs from nearby nodes.

Every node in the network determines the shortest way to every other node by utilizing the data in the LSDB and a shortest path method (like Dijkstra's algorithm).

The best route to each destination node in the network is contained in the shortest path tree or routing table that is produced.

Routing Table Maintenance:

Nodes forward packets to their destinations using the data in their routing tables.

Nodes update their LSAs and spread these changes to all other nodes in the network in the event that the network topology changes (due to connection failures, new nodes added, etc.).

Nodes adjust their routing tables to consider the network topology modifications after receiving updated LSAs.

Advantages:

Optimality: Link State Routing techniques produce effective routing by ensuring the shortest path to each destination.

Rapid Convergence: Link State Routing techniques reach optimal routing decisions rapidly by executing distributed shortest-path algorithms while thoroughly understanding the network structure.

Scalability: Because Link State Routing is distributed and effectively uses network resources, it grows to large networks.

Drawbacks:

Resource Overhead: More bandwidth and processing power are needed to maintain and exchange LSAs, which raises network overhead.

Complexity: Compared to Distance Vector Routing algorithms, Link State Routing techniques are more difficult to implement and maintain.

Centralization: Although Link State Routing techniques are distributed algorithms, they frequently need a centralized controller or management system to manage LSA flooding and LSDB synchronization.

- **Hierarchical Routing:**

In order to increase scalability, efficiency, and manageability, nodes are arranged into hierarchical levels or layers using the hierarchical routing network design technique.

Hierarchical Structure:

Nodes in a network are arranged into several levels or layers according to their responsibilities, functions, or proximity to one another in a hierarchical routing scheme.

Different network scopes or domains, such as local networks, regional networks, or backbone networks, are represented by each level in the hierarchy.

Each level's nodes mostly communicate with other nodes on that level or with nodes on levels adjacent to their own.

Routing Domains:

With their own routing policies, protocols, and addressing methods, each tier of the hierarchy is regarded as a distinct routing domain or area.

Interior routing protocols are usually used for routing within a domain, and exterior routing protocols are used for routing between domains.

Inter-Level Routing:

In order to facilitate communication between nodes in various domains, inter-level routing entails sharing routing information between levels of the hierarchy.

Higher-ranking nodes in the hierarchy, like backbone routers, connect many domains and forward traffic between them by acting as gateways or border routers.

Traffic across various domains is coordinated, and routing information is shared between border routers via inter-level routing protocols like Border Gateway Protocol (BGP).

Hierarchical Addressing:

Using hierarchical addressing systems, nodes at each level of the hierarchy are given distinct identifiers (such as IP addresses).

Higher-level prefixes indicate larger domains, whereas lower-level prefixes reflect smaller subdomains or single nodes. Address prefixes are organized hierarchically.

By grouping address blocks at higher levels of the hierarchy, hierarchical addressing makes managing routing tables easier and smaller routing tables.

Scalability and Efficiency:

D hierarchical routing increases scalability by breaking the network into smaller, easier-to-manage domains and simplifying routing and addressing.

Because routing decisions are confined inside each domain, the number of routing updates and protocol exchange overheads are decreased.

By limiting the number of routing table entries and the quantity of routing data that needs to be processed and disseminated, hierarchical routing also improves efficiency.

Management and Control:

Hierarchical routing divides nodes into logical groups and domains to provide centralized network management and control.

At various hierarchical levels, network administrators have the authority to establish and implement policies related to traffic engineering, quality of service (QoS), and access control.

Centralized management tools and protocols are employed to maximize network performance, monitor and control routing behaviour, and resolve connectivity issues within and between domains.

- **Multi Cast Routing:**

A networking technique called multicast routing is used to transfer data from one sender to several recipients in a network in an effective manner.

Group Communication: Data is conveyed from a single source to a particular group of interested recipients via multicast routing.

Multicast enables one-to-many communication, in contrast to unicast, which allows data to be transmitted from one sender to one recipient, and broadcast, which allows data to be sent from one sender to all network nodes.

Group Addressing: A distinct multicast group address is given to every multicast group.

By joining a multicast group address, recipients who are interested in receiving data from a certain multicast group subscribe to that group.

Tree-Based Distribution: To effectively distribute data to several receivers, multicast routing usually makes use of a tree-based distribution structure.

Data packets are transferred from the source node to a multicast distribution tree, where each branch points to a distinct recipient or collection of receivers.

Tree Construction: A number of techniques, including the Core-Based Tree (CBT) algorithm and the Reverse Path Forwarding (RPF) algorithm, are used to build multicast distribution trees.

These algorithms aim to minimize duplicate transmissions and network traffic while creating the most effective distribution tree that reaches every receiver.

Data packets are forwarded from the source node to the tree's root after the multicast distribution tree has been built.

In order to guarantee that the packets reach every recipient in the multicast group, each intermediate node in the tree sends the packets to its offspring nodes.

Receiver Joining and Leaving:

Recipients can dynamically join or exit multicast groups by transmitting join or leave messages to the network.

A receiver is added to the multicast distribution tree and subscribes to the group's multicast address when it joins a multicast group.

A multicast receiver unsubscribes from the group's multicast address when it departs, and the multicast distribution tree is modified to reflect the receiver's removal.

Effectiveness and Expandability:

When it comes to efficiency and scalability, multicast routing outperforms unicast or broadcast communication.

By sending data just to those who have specifically asked for it rather than broadcasting it to the entire network, it uses less network traffic.

- **Routing for Mobile hosts:**

A networking technique called routing for mobile hosts, or mobile IP allows mobile devices—like smartphones and tablets—to stay continuously connected to the network even when they switch between various networks.

Home Network:

Every mobile device has a permanent IP address known as the home address, and it is assigned a home network, which is the network to which it was first connected.

When the mobile device is not actively linked to another network or is immobile, the default point of attachment is the home network.

Foreign Network:

A mobile device is considered to be in a foreign network when it leaves its home network and connects to another one.

The mobile device is given a care-of address in the foreign network, which is a temporary IP address given by the foreign network's router.

Mobility Agents:

The Home Agent (HA) and the Foreign Agent (FA) are the two categories of mobility agents found in the mobile IP architecture.

On the home network, the Home Agent is a router that maintains track of the mobile device's location and sends data packets meant for it to the foreign network's care-of address.

When a mobile device is on the foreign network, the Foreign Agent, a router on the foreign network, helps forward data packets to and from the device.

Registration Process:

Through a procedure known as registration, a mobile device that is moving to a foreign network notifies its home agent of its change of address.

The mobile device notifies its home agent of its current care-of address by sending a registration request to it during the registration process.

In order to link the home address of the mobile device with its care-of address in the foreign network, the home agent changes its mobility binding table.

Packet Forwarding:

The home agent intercepts packets sent to the mobile device's home address by devices connected to the home network.

The packet is forwarded to the current care-of address of the mobile device by the home agent after consulting its mobility binding table.

The packet is received by the foreign agent within the foreign network, who then forwards it to the mobile device.

Seamless Handoff:

When a mobile device switches networks, it may change its care-of address multiple times.

The mobile IP protocol ensures seamless handoff by updating the mobility binding table and maintaining continuous communication between the mobile device and its correspondents.

Optimizations:

Various optimizations, such as triangular routing and route optimization, can be employed to reduce latency and improve the efficiency of packet delivery in mobile IP networks.

These optimizations aim to minimize the involvement of mobility agents and establish direct communication paths between the mobile device and its correspondents whenever possible.

- **Knowledge Check 2**

  State True Or False

  1. Dijkstra's algorithm can handle graphs with negative edge weights. (**False**)
  2. Bellman-Ford algorithm guarantees the shortest path even in the presence of negative cycles. (**False**)
  3. The floyd-Warshall algorithm is suitable for finding the shortest path in dense graphs. (**True**)
  4. A* algorithm always finds the shortest path between the source and destination nodes. (**True**)
  5. Shortest path algorithms like Dijkstra's and Bellman-Ford are commonly used in network routing protocols. (**True**)

- **Outcome-Based Activity 2**

  Create a routing algorithm for a network, focusing on efficient pathfinding, handling negative weights, scalability, real-time performance, and algorithm comparison."

8.2 Network layer in TCP/IP: Basic characteristics of IP protocol

In the TCP/IP paradigm, the network layer enables communication between devices on various networks. The Internet Protocol (IP), a foundational protocol that permits packet-switched communication, is at the centre of this layer.

Connectionless Protocol:

Since IP is a connectionless protocol, data transmission occurs without an established connection between the sender and the recipient.

Every packet is handled separately and routed according to the destination address data in the packet header.

Unreliable Delivery:

IP offers best-effort delivery, meaning neither packet delivery nor packet sequencing is guaranteed.

Because packets can be misplaced, copied, or transmitted out of order, higher-layer protocols are needed to manage sequencing and dependability as needed.

Packet Routing:

IP routers handle packet forwarding between networks based on destination IP addresses.

Routers keep routing tables with data on available paths and network topology, which are used to make routing decisions dynamically.

Addressing:

Devices on a network are uniquely identified by their IP addresses thanks to IP. IPv6 addresses are 128 bits long, compared to 32 bits for IPv4 addresses.

IP addresses are hierarchical; some parts of the address identify the network, and the host inside the network is identified by the remaining components.

Packet Header:

IP packets are made up of a payload and header. Important information for delivery and routing is contained in the header.

Version, header length, kind of service, total length, identification, flags, fragment offset, time-to-live (TTL), protocol, header checksum, source IP address, and destination IP address are some of the important fields in the IP header.

Fragmentation and Reassembly

IP allows packets to be broken up into smaller pieces to handle varying network maximum transmission unit (MTU) sizes. This process is known as fragmentation and reassembly.

In the event that a packet's MTU exceeds that of an outgoing interface, routers may fragment it; fragmented packets are then reassembled by receivers prior to being forwarded to protocols at a higher layer.

IPv4 and IPv6:

The most popular version of the IP protocol is IPv4; however, IPv6 was created to offer a wider address space and more functions because of address exhaustion problems.

IPv6 modifies the addressing scheme, packet header format, and other elements to meet the expanding requirements of contemporary networks.

- **addressing and header format of IPv4**

In the TCP/IP paradigm, the network layer enables communication between devices on various networks. The Internet Protocol (IP), a foundational protocol that permits packet-switched communication, is at the centre of this layer.

Connectionless Protocol:

IP is a connectionless protocol, meaning that data is transmitted without creating a dedicated connection between the sender and the recipient.

Every packet is handled separately and routed according to the destination address data in the packet header.

Unreliable Delivery:

IP offers best-effort delivery, which means that neither the delivery nor the sequencing of packets is guaranteed.

Because packets can be misplaced, copied, or transmitted out of order, higher-layer protocols are needed to manage sequencing and dependability as needed.

Packet Routing:

IP routers handle packet forwarding between networks based on destination IP addresses.

Routers keep routing tables with information about available paths and network topology, which are used to make routing decisions dynamically.

Addressing:

IP identifies devices on a network using distinct IP addresses. The length of an IPv4 address is 32 bits, but an IPv6 address is 128 bits.

Parts of an IP address identify the network, and the remaining elements identify the host connected to the network. IP addresses are hierarchical.

Packet Header:

IP packets are made up of a payload and header. Important information for delivery and routing is contained in the header.

Version, header length, kind of service, total length, identification, flags, fragment offset, time-to-live (TTL), protocol, header checksum, source IP address, and destination IP address are some of the important fields in the IP header.

IP allows packets to be broken up into smaller pieces to handle varying network maximum transmission unit (MTU) sizes. This process is known as fragmentation and reassembly.

When a packet's MTU exceeds that of an outgoing interface, routers may fragment it; receivers then reassemble the fractured packet before forwarding it to higher-layer protocols.

IPv4 and IPv6:

The most popular version of the IP protocol is IPv4; however, IPv6 was created to offer a wider address space and more functions because of address exhaustion problems.

IPv6 modifies the addressing scheme, packet header format, and other elements to meet the expanding requirements of contemporary networks.

- **IPv6: Major goals& features**

The purpose of IPv6, which replaced IPv4, was to solve its shortcomings and meet the expanding needs of contemporary networking. Key objectives and characteristics:

Address Space Expansion:

Expanding the address space to support the growing number of devices connected to the Internet was one of IPv6's main objectives.

With 128 bits in length, IPv6 addresses offer a vastly greater address space than IPv4's 32 bits.

With approximately 3.4 × 10^38 unique addresses, IPv6 effectively eliminates the problem of address exhaustion faced by IPv4.

Simplified Header Format:

In comparison to IPv4, IPv6 streamlines the header format, lowering processing overhead and boosting effectiveness.

In contrast to the variable-length header of IPv4, the IPv6 header has a fixed length of 40 bytes.

Some elements from the IPv4 header are removed in IPv6. These include the header checksum (which depends on checksums at higher layers), fields relating to fragmentation (which transfers fragmentation to end systems), and options (which transfer optional functionality to extension headers).

Enhanced Security:

IPsec (IP Security), a group of protocols for protecting communications at the IP layer, is supported by IPv6 by default.

For IPv6 packets, IPsec offers capabilities including integrity, confidentiality, authentication, and anti-replay protection.

IPv6 enhances the general security posture of Internet communications by incorporating security elements within the protocol.

Efficient Routing and Addressing:

IPv6 introduces a hierarchical addressing system to enable more effective routing and routing information aggregation.

Internet service providers (ISPs) and other organizations can more easily assign address blocks because of the wider address space and hierarchical addressing, which encourages scalability and effective routing.

Autoconfiguration:

With its automatic address configuration features, IPv6 makes network setup and administration easier.

Devices can use protocols like Dynamic Host Configuration Protocol version 6 (DHCPv6) or stateless address autoconfiguration (SLAAC) to generate IPv6 addresses automatically.

Transition Mechanisms:

IPv6 has mechanisms to make the switch from IPv4 to IPv6 easier. During this time, IPv4 and IPv6 networks can coexist and communicate with one another.

These technologies include translation (e.g., Network Address Translation 64 [NAT64]), tunnelling (e.g., IPv6-over-IPv4 tunnelling), and dual-stack operation.

8.3 Summary

- Examines the services the network layer provides in the OSI model, including routing, addressing, and packet forwarding.
- Covers various routing algorithms used in network layer protocols.
- Explains the fundamental characteristics of the Internet Protocol (IP), including its connectionless nature, packet forwarding, addressing, and header format.
- Provides a detailed description of IPv4 addressing and header format, highlighting key fields and their functions.
- Discusses the motivations behind IPv6, its expanded address space, simplified header format, enhanced security features, and support for auto-configuration.

8.4 Keywords

- **OSI** - Open Systems Interconnection: A conceptual model that standardizes the functions of a telecommunication or computing system into seven abstract layers, facilitating interoperability between different systems.
- **IPv4** - Internet Protocol version 4: The fourth version of the Internet Protocol uses 32-bit addresses and is the most widely deployed protocol for Internet communication.
- **IPv6** - Internet Protocol version 6: The latest version of the Internet Protocol, designed to replace IPv4 with a larger address space, improved security, and support for new technologies.
- **QoS** - Quality of Service: A set of techniques and mechanisms used to manage network resources and ensure that certain traffic receives preferential treatment based on defined criteria such as latency, bandwidth, and reliability.

8.5 Self-Assessment Questions

1 Explain the concept of packet forwarding and its significance in the network layer of the OSI model.

2 How does IPv6 address the limitations of IPv4, and what are its major features and benefits?

3 Describe the purpose and operation of Quality of Service (QoS) mechanisms in computer networking.

4 What is the role of Resource Reservation Protocol (RSVP) in ensuring quality of service guarantees in network communication?

5 Explain the concept of traffic shaping and its role in controlling the flow of data packets in a network.

6 How do choke packets and load shedding contribute to congestion control in datagram subnets, and what are their respective advantages and limitations?

8.6 References / Reference Reading

- Michael A. Gallo, William M. Hancock, Computer Communications and Networking Technologies, CENGAGE learning.
- William Stallings, Data and Computer Communications, PHI
- Andrew S. Tanenbaum, Computer Networks, PHI.
- Behrouz A Forouzan, Data Communications and Networking, Mc-Graw Hill Education

Unit 9: Congestion Control

Learning Outcomes:

- Students will be able to define TCP and UDP protocols' key characteristics and functions in network communication.
- Students will be able to differentiate between connection-oriented and connectionless protocols and explain their respective advantages and limitations.
- Students will be able to analyze the addressing and header formats of IPv4 and IPv6, identifying key fields and their functions.
- Students will be able to describe the services the network layer provides in the OSI model and their importance in data transmission.
- Students will be able to apply knowledge of network layer protocols and congestion control mechanisms to design and troubleshoot network architectures.

Structure:

9.1 Congestion Control & Quality of Service: General Principals

Quality of service (QoS) and congestion control are essential components of network management that guarantee dependable and effective data transfer. Their overarching beliefs:

Congestion Control:

When network resources are demanded more than they can be supplied, performance deteriorates, and packet loss may occur.

The goal of congestion control techniques is to prevent and manage traffic flow to preserve the network's performance and stability.

Packet queuing, traffic shaping, and admission control are some of the strategies used to control congestion and maximize resource use.

Quality of Service (QoS):

The term Quality of Service (QoS) describes a network's capacity to transport various kinds of data with differing demands on latency, bandwidth, dependability, and other performance indicators.

QoS methods make sure that key apps receive priority traffic based on their significance and features.

Quality of Service (QoS) methods are designed to prioritize traffic according to its importance and characteristics. This helps to guarantee that key applications get the resources they need to accomplish their performance goals.

Traffic policing, shaping, and classification are some techniques used to enforce QoS policies and offer various types of distinct traffic services.

Traffic Prioritization:

One of the fundamental principles of QoS is traffic prioritization, where traffic is classified into different classes or priority levels based on predefined criteria.

High-priority traffic, such as voice and video data, is given preferential treatment over low-priority traffic, such as file downloads or email traffic.

Prioritization ensures that delay-sensitive and mission-critical applications receive timely delivery and minimal packet loss, even under congested network conditions.

Resource Reservation:

QoS systems can utilize resource reservation strategies to pre-allocate network resources, including buffer space and bandwidth, to particular traffic flows.

Applications can request and reserve network resources along the data channel using reservation protocols like RSVP (Resource Reservation Protocol) to guarantee there is enough capacity for their traffic.

QoS supports consistent performance and the quality of service for vital applications by allocating resources.

Congestion Avoidance:

Congestion avoidance strategies are used in addition to congestion control measures to proactively stop congestion before it starts.

In order to maintain optimal performance and prevent congestion, methods like TCP congestion avoidance algorithms, Explicit Congestion Notification (ECN), and active queue management (like Random Early Detection [RED]) monitor network conditions and modify traffic flow.

Feedback Mechanisms:

Feedback systems are essential to both QoS and congestion control techniques as they allow them to keep an eye on network conditions, identify congestion events, and modify traffic management strategies as necessary.

Examples of feedback mechanisms include router congestion signals, packet loss detection, round-trip time measurements, and other performance measures used to evaluate network health and modify congestion control parameters.

- **Congestion Control in Virtual–Circuit Subnets**

Congestion control in virtual circuit subnets involves managing network traffic to prevent congestion and ensure efficient data transmission within virtual circuits. Here's a micro-level description:

Virtual Circuits:

Data transmission is arranged into virtual circuits in virtual-circuit subnets, which are logical connections made between nodes that are in communication.

A distinct identification and particular routing and forwarding data are linked to every virtual circuit.

Traffic Monitoring:

Monitoring traffic within the virtual-circuit subnet is the first step in congestion control; this is done to look for indicators of congestion, such as increased packet loss, delays, or buffer overflows.

Monitoring systems gather performance data from switches and routers along virtual circuits to evaluate the health of the network and the degree of congestion.

Admission Control:

New virtual circuit creation is governed by admission control mechanisms, which take into account resource availability and network capacity.

Admission control determines whether the network has enough bandwidth, buffer space, and computing power to handle the extra traffic before admitting a new virtual circuit.

Traffic Policing:

For each virtual circuit, traffic policing techniques enforce bandwidth allotments and traffic limitations in order to prevent excessive traffic and preserve fairness among competing flows.

Enforcement systems track the volume of incoming data and reject packets that don't fit into pre-established traffic patterns or don't adhere to quality of service (QoS) requirements.

Resource Reservation:

Certain virtual circuits may require reserving network resources, like bandwidth and buffer space, to control congestion in virtual circuit subnets.

In order to guarantee sufficient capacity and quality of service, resource reservation protocols negotiate resource allocations between communication nodes and reserve resources throughout the virtual circuit path.

Dynamic Routing and Load Balancing:

Load-balancing strategies and dynamic routing algorithms, which distribute traffic over several channels and prevent network bottlenecks, are essential for congestion control.

In order to maximize resource efficiency and reduce congestion hotspots, these methods adaptively redirect virtual circuits based on current traffic conditions.

Feedback and Congestion Signaling:

To identify congestion events and launch the proper congestion control measures, congestion control techniques depend on feedback and congestion signalling from routers and switches.

Routers can employ Explicit Congestion Notification (ECN) or other congestion signalling techniques to alert communication nodes to congestion and facilitate traffic changes.

- **Congestion Control in Datagram Subnets: Choke packets, Load Shedding**

In datagram subnets, congestion management uses a variety of strategies, including load shedding and choke packets, to control network congestion and guarantee effective data transfer.

Datagram Subnets:

Connectionless networks, sometimes called datagram subnets, function according to a best-effort delivery model in which every packet is handled separately.

Datagram subnets don't create explicit connections or keep track of state information for ongoing communication sessions, in contrast to virtual-circuit subnets.

Choke Packets:

Special control packets known as "choke packets" are transmitted by routers to senders as a warning when there is congestion.

A router creates and delivers choke packets back to the source of the jammed traffic when it encounters congestion or congestion-related problems like buffer overflow.

In order to notify the sender about the network's congestion, choke packets include explicit congestion notification (ECN) information or congestion indicator flags.

Load Shedding:

Load shedding is a proactive congestion control mechanism that involves discarding or dropping packets during periods of network congestion.

When congestion occurs, and network resources become overwhelmed, routers may selectively discard packets based on predefined criteria or policies.

Load shedding prioritizes packet discard based on factors such as packet priority, traffic class, or importance, aiming to protect critical traffic while sacrificing less important or lower-priority traffic.

Congestion Feedback:

Datagram subnets rely on congestion feedback mechanisms to inform senders about network congestion and trigger appropriate congestion control actions.

In addition to choke packets, routers may use other forms of feedback, such as packet loss notifications, increased round-trip times (RTT), or congestion indications in protocol headers.

Feedback mechanisms provide senders with real-time information about network conditions, enabling them to adjust transmission rates or apply congestion control algorithms accordingly.

Adaptive Rate Control:

In response to congestion feedback, senders may dynamically adjust their transmission rates or window sizes to alleviate network congestion.

Adaptive rate control algorithms monitor feedback signals and regulate the rate at which packets are sent into the network, scaling back transmission rates during periods of congestion and increasing rates when network conditions improve.

Traffic Prioritization:

Traffic prioritization strategies can be utilized in datagram subnets to guarantee that traffic that is vital or time-sensitive is given priority during instances of congestion.

In order to prevent high-priority traffic from being discarded or delayed during congestion situations, prioritization systems categorize packets into distinct traffic classes or quality of service (QoS) levels and allocate network resources accordingly.

- **Random Early Detection, Jitter Control**

Random Early Detection (RED) and Jitter Control are both techniques used in networking to manage congestion and improve the quality of service (QoS).

Random Early Detection (RED):

In packet-switched networks, random early detection is a congestion avoidance technique that is mostly utilized in routers and switches.

In order to function, RED keeps track of how long the packet queue is before dropping or flagging any packets that are not yet ready to be forwarded.

When the queue hits a preset threshold, RED starts marking or discarding packets instead of waiting until the queue is entirely full and dropping packets arbitrarily.

Red helps avoid congestion and encourages sending devices to reduce their transmission rates by discarding or marking packets before the queue becomes too long.

RED's probabilistic algorithm aims to maintain flow fairness by identifying which packets to mark or reject while avoiding any one flow from dominating the system. In packet-switched networks, random early detection is a congestion avoidance technique that is mostly utilized in routers and switches.

In order to function, RED keeps track of how long the packet queue is before dropping or flagging any packets that are not yet ready to be forwarded.

When the queue hits a preset threshold, RED starts marking or discarding packets instead of waiting until the queue is entirely full and dropping packets arbitrarily.

Red helps avoid congestion and encourages sending devices to reduce their transmission rates by discarding or marking packets before the queue becomes too long.

RED's probabilistic algorithm aims to maintain flow fairness by identifying which packets to mark or reject while avoiding any one flow from dominating the system.

Jitter Control:

Variations in packet arrival timings within a network are referred to as jitter, and they can cause packet delays and degrade the quality of real-time applications like audio and video.

In order to lessen the impact of jitter on application performance, jitter control approaches work to minimize these differences and guarantee that packets reach their destination with constant timing.

Using buffering and packet scheduling algorithms to even out fluctuations in packet arrival times is a popular method of jitter control.

Before packets are forwarded to their destination, they are first briefly stored in buffers and then rearranged according to their sequence numbers or timestamps.

Algorithms for packet scheduling rank packets according to their timestamps or significance, guaranteeing that the packets with greater priority or more stringent timing requirements get sent.

Variations in packet arrival timings within a network are referred to as jitter, and they can cause packet delays and degrade the quality of real-time applications like audio and video.

In order to lessen the impact of jitter on application performance, jitter control approaches work to minimize these differences and guarantee that packets reach their destination with constant timing.

Using buffering and packet scheduling algorithms to even out fluctuations in packet arrival times is a popular method of jitter control.

Before packets are forwarded to their destination, they are first briefly stored in buffers and then rearranged according to their sequence numbers or timestamps.

Algorithms for packet scheduling rank packets according to their timestamps or significance, guaranteeing that the packets with greater priority or more stringent timing requirements get sent.

- **Overprovisioning, Buffering, Traffic Shaping, Leaky bucket, token bucket, Resource Reservation, Admission Control, Packet Scheduling**

Over Provisioning:

Over-provisioning is known as allocating more resources than are now needed to accommodate future growth or unforeseen spikes in traffic.

It offers a buffer to manage demand swings without sacrificing the calibre of the service.

In order to guarantee scalability and reliability, over-provisioning is frequently employed in network architecture, server capacity planning, and cloud computing.

Even though it can be expensive, over-provisioning aids in preserving service performance and availability amid spikes in traffic or periods of high demand.

Buffering:

When the rate of incoming traffic surpasses the rate of outgoing traffic, packets are temporarily stored in buffers and held during transmission.

Buffers mitigate the effects of congestion by mitigating changes in traffic flow.

Networking equipment like switches, routers, and network interface cards use buffers.

Managing algorithms and buffer sizes is essential for maximizing network efficiency and reducing latency.

Traffic Shaping:

Traffic shaping modifies the rate at which packets are transmitted in order to influence the flow of network traffic.

It facilitates equitable access to network resources, prioritizes important traffic, and controls bandwidth consumption.

Traffic priority, rate limitation, and queuing algorithms are examples of traffic-shaping systems.

Specific network requirements and traffic patterns are used to define traffic-shaping rules and quality of service (QoS) policies.

Leaky Bucket:

One traffic shaping technique used to regulate the outgoing traffic rate is the leaky bucket algorithm.

According to the leaky bucket concept, tokens are added to an imaginary bucket at a steady rate, and it has a fixed capacity.

Incoming packets must obtain tokens from the bucket before they may be sent.

Excess packets are either delayed or discarded if the bucket overflows.

The leaky bucket technique aids in traffic flow regulation and guards against data bursts overloading the network.

Token Bucket:

With greater traffic shaping flexibility, the token bucket algorithm improves on the leaky bucket method.

Tokens are added to a bucket at a steady rate in the token bucket concept.

Every token denotes authorization to send a specific quantity of data.

Before a packet can be transferred, it needs to obtain tokens from the bucket upon arrival.

The packet is either delayed or discarded if there are not enough tokens.

The token bucket method makes bursty traffic management and more precise control over traffic shaping possible.

Resource Reservation:

In order to meet certain traffic requirements, resource reservation entails pre-allocating network resources, such as bandwidth or buffer space.

Applications are able to request and reserve resources for their data flows through reservation protocols such as RSVP (Resource Reservation Protocol).

Resource reservations ensure that vital applications have the resources and service quality they need to achieve their goals.

By allocating resources to particular traffic patterns, it facilitates the effective use of resources and aids in preventing network congestion.

Admission Control:

Admission control techniques use the quality of service needs and available network resources to decide whether to accept or reject new traffic flows.

Admission control assesses if the network can handle the extra traffic without going against current service level agreements or QoS commitments before admitting a new flow.

In addition to preventing network congestion, admission management ensures that admitted traffic can be sufficiently served without compromising the performance of already-existing flows.

It is essential for preserving network stability, maximizing resource use, and achieving service-level goals.

Packet Scheduling:

Determining the sequence in which packets are transmitted from an output queue is known as packet scheduling.

Packets are prioritized by scheduling algorithms according to traffic class, quality of service needs, and packet priority.

First-in-first-out (FIFO), Weighted Fair Queuing (WFQ), and Priority Queuing (PQ) are examples of common scheduling algorithms.

Packet scheduling lowers packet latency, guarantees equitable access to network resources, and optimizes throughput for various kinds of traffic.

Maximizing network performance and providing users with a constant level of quality service is necessary.

9.2 Summary

- Discusses how addressing works at the transport layer and the various services and protocols provided.
- Provides an in-depth explanation of the services offered by TCP and UDP, along with detailed descriptions of their respective header formats.
- Examines the services the network layer provides in the OSI model, including routing, addressing, and packet forwarding.
- Covers various routing algorithms used in network layer protocols.
- Explains the fundamental characteristics of the Internet Protocol (IP), including its connectionless nature, packet forwarding, addressing, and header format.
- Provides a detailed description of IPv4 addressing and header format, highlighting key fields and their functions.
- Discusses the motivations behind IPv6, its expanded address space, simplified header format, enhanced security features, and support for auto-configuration.
- Explores the principles of congestion control and quality of service, emphasizing the importance of managing network congestion and ensuring consistent service delivery.
- Describes congestion control mechanisms in virtual-circuit subnets.
- Covers specific congestion control techniques in datagram subnets.

- Provides detailed explanations of various techniques and mechanisms used for congestion control, traffic management, and quality of service optimization in computer networks.

9.3 Keywords

- **QoS** - Quality of Service: A set of techniques and mechanisms used to manage network resources and ensure that certain traffic receives preferential treatment based on defined criteria such as latency, bandwidth, and reliability.
- **RSVP** - Resource Reservation Protocol: A communication protocol used to reserve network resources for specific traffic flows, ensuring quality of service guarantees and efficient resource utilization.
- **ECN** - Explicit Congestion Notification: A mechanism used by network devices to notify senders of congestion in the network, allowing them to adjust transmission rates and prevent packet loss.
- **FIFO** - First-In-First-Out: A queuing discipline where the first packet to enter a queue is the first to be transmitted, ensuring that packets are processed in the order they arrive.
- **WFQ** - Weighted Fair Queuing: A packet scheduling algorithm that allocates bandwidth fairly among different traffic flows while allowing certain flows to be prioritized based on assigned weights.
- **PR** - Priority Queuing: A packet scheduling algorithm that assigns different priority levels to packets and processes higher priority packets before lower priority ones, ensuring timely delivery of critical traffic.

9.4 Self-Assessment Questions

7 How does Explicit Congestion Notification (ECN) help manage network congestion and improve performance?

8 Compare and contrast FIFO, Weighted Fair Queuing (WFQ), and Priority Queuing (PQ) as packet scheduling algorithms.

9 Discuss the challenges and benefits of implementing over-provisioning in network design and management.

10 Explain the concept of traffic shaping and its role in controlling the flow of data packets in a network.

11 How do choke packets and load shedding contribute to congestion control in datagram subnets, and what are their respective advantages and limitations?

9.5 References / Reference Reading

- Michael A. Gallo, William M. Hancock, Computer Communications and Networking Technologies, CENGAGE learning.
- William Stallings, Data and Computer Communications, PHI
- Andrew S. Tanenbaum, Computer Networks, PHI.
- Behrouz A Forouzan, Data Communications and Networking, Mc-Graw Hill Education