KL (DEEMED TO BE UNIVERSITY)

CDOE
CENTER FOR DISTANCE AND ONLINE EDUCATION

MCA

COMPUTER NETWORKS AND COMMUNICATIONS

How to Use Self-Learning Material?

The pedagogy used to design this course is to enable the student to assimilate the concepts with ease. The course is divided into modules. Each module is categorically divided into units or chapters. Each unit has the following elements:

Table of Contents: Each unit has a well-defined table of contents. *For example: "1.1.1. (a)" should be read as "Module 1. Unit 1. Topic 1. (Sub-topic a)" and 1.2.3. (iii) should be read as "Module 1. Unit 2. Topic 3. (Sub-topic iii).*

Aim: It refers to the overall goal that can be achieved by going through the unit.

Instructional Objectives: These are behavioural objectives that describe intended learning and define what the unit intends to deliver.

Learning Outcomes: These are demonstrations of the learner's skills and experience sequences in learning, and refer to what you will be able to accomplish after going through the unit.

Self-Assessment Questions: These include a set of multiple-choice questions to be answered at the end of each topic.

Did You Know?: You will learn some interesting facts about a topic that will help you improve your knowledge. A unit can also contain Quiz, Case Study, Critical Learning Exercises, etc., as metacognitive scaffold for learning.

Summary: This includes brief statements or restatements of the main points of unit and summing up of the knowledge chunks in the unit.

Activity: It actively involves you through various assignments related to direct application of the knowledge gained from the unit. Activities can be both online and offline.

Bibliography: This is a list of books and articles written by a particular author on a particular subject referring to the unit's content.

e-References: This is a list of online resources, including academic e-Books and journal articles that provide reliable and accurate information on any topic.

Video Links: It has links to online videos that help you understand concepts from a variety of online resources.

LEADERSHIP KLEF

President
Er. Koneru Satyanarayana

Vice Chancellor
Dr. G. Pardha Saradhi Varma

Pro-Vice Chancellor
Dr. N. Venkatram

Registrar
Dr. K. Subbarao

CREDITS

Author
Chalamalasetty Sarvani

Director CDOE
C. Shanath Kumar

Instructional Designer
Nabina Das

Content Writer
K. Naga Durga

Graphic Designer
B. V. Satyanarayana

First Edition, 2023.

Author's Profile

Chalamalasetty Sarvani
Assistant Professor

Chalamalasetty Sarvani is an Assistant Professor at KL University, Vaddeswaram, with over eight years of teaching experience. She is pursuing a Ph.D. in Computer Science Engineering at Amrita Vishwa Vidyapeetham. Her expertise includes Cloud Computing, Machine Learning, and Artificial Intelligence, with several publications in reputable journals and conferences, including IEEE Xplore. Sarvani has authored books and holds a patent on AI-based renewable energy management. She has served in multiple roles as an alumni coordinator and accreditation contributor for NAAC and NBA. Her achievements include the "Best Teacher" award for 2021-22 and several reviewer roles for international conferences. She holds various certifications from Microsoft, AWS, Oracle, and Google. Sarvani is known for her problem-solving abilities, leadership skills, and dedication to academic growth.

Computer Networks

Course Description

The Computer Networks and Communications (CNC) course discusses various network fundamentals and technologies. It covers many topics, such as modern network functions, beginning with the essential concepts of network hardware and software and the widely used reference models, such as the OSI model and TCP/IP. Students will gain insight into how data is communicated over networks and explore the services that support Internet-based applications, such as email, web browsing, and file sharing.

The course introduces different transmission media types used to transfer data across networks. These include wireless technologies, which allow devices to communicate without physical connections and other technologies. Integrated Services Digital Network and (Asynchronous Transfer Mode) play a crucial role in data transmission in diverse types of networks. A vital aspect of this introduction is the focus on how data is controlled and managed as it travels through networks. The data link control mechanisms and error detection techniques will be explained through this course to ensure data accuracy. In the next stage, the course discusses standards and protocols that govern how networks are structured and managed. The protocols should be per the standards of IEEE, LANs, and MANs, which connect various networks to support better communication. To experience fast data transmission, the students should learn the concept of high-speed LANs.

Moving to the next section, the course deals with various steps in defining the network and offers several strategies for managing these networks. Students will be exposed to the technical aspects of routing algorithms, which determine the best path for data to travel across networks, and congestion control, which helps prevent network traffic from becoming too heavy and slowing down performance. The course also covers the network layer of the Internet, including the IP (Internet Protocol), which is central to how data is routed between devices. Students will learn about IP addressing, subnets, and other networking techniques to ensure smooth communication over different networks. The course also deals with the transport protocols, which enable the participants to transfer data over networks using TCP and UDP safely.

The course will explore how transport services are provided and the importance of Quality of Service (quality of service) models that ensure networks meet performance requirements. Network performance issues are discussed, which describe the effects of speed and reliability of network communication.

In the next section, the course describes various Internet protocols that support everyday activities, such as DNS (Domain Name System) for resolving website addresses, SNMP (Simple Network Management Protocol) for managing networks, and HTTP (Hypertext Transfer Protocol) for web browsing. Other protocols like FTP, TFTP, BOOTP, and email protocols are also explored. Apart from all these, the course discusses network security, which is essential. To have data security firewalls is

one of the main courses discussed in this course. Firewalls make the network detect threats and strive to protect the network. Specialised networks, including cellular, ad-hoc, mobile ad-hoc, and sensor networks, are also discussed, showing how networks adapt to different environments and needs.

The course **Computer Networks** has **five** modules.

MODULE 1

INTRODUCTION TO COMPUTER NETWORKS AND DATA COMMUNICATIONS

Introduction to Computer Networks: Introduction, Network Hardware, Network Software, Reference Models, Data Communication Services & Network Examples, Internet Applications, Data Communications: Transmission Media, Wireless Transmission, Multiplexing, Switching, Transmission in ISDN, Broad Band ISDN, ATM Network. Data Link Control, Error Detection & Correction, Sliding Window Protocols

MODULE 2

DATA COMMUNICATION AND NETWORKING

LANs & MANs: IEEE Standards for LANs & MANs-IEEE Standards 802.2, 802.3, 802.4, 802.5,802.6, High Speed LANs. Design Issues in Networks: Routing Algorithms, Congestion Control Algorithms, Network Layer on the Internet, IP Protocol, IP Address, Subnets, and Internetworking.

MODULE 3

INTERNET TRANSPORT PROTOCOLS AND NETWORK SERVICES

Internet Transport Protocols: Transport Service, Elements of Transport Protocols, TCP and UDP Protocols, Quality of Service Model, Best Effort Model, Network Performance Issues. Overview of DNS, SNMP, Electronic Mail, FTP, TFTP, BOOTP, HTTP Protocols, World Wide Web, and Firewalls.

MODULE 4

NETWORK DEVICES AND NETWORK TYPES

Network Devices: Overview of Repeaters, Bridges, Routers, Gateways, Multiprotocol Routers, routers, Hubs, Switches, Modems, Channel Service Unit CSU, Data Service Units DSU, NIC, Wireless Access Points, Transceivers, Firewalls, Proxies. Overview of Cellular Networks, Ad-hoc Networks, Mobile Ad hoc Networks, Sensor Networks

MODULE 5

NETWORKING SOLUTIONS USING ROUTING ALGORITHMS

Introduction and installation of Cisco packet tracer, peer-to-peer network using CPT, IP and MAC address in the computers using CPT, find Port Numbers/ Names, remove leading zeros from an IP address, data link layer character count framing method.

Table of Contents

COMPUTER NETWORKS

MODULE 1

Introduction to Computer Networks and Data Communications

Module Description

The module focuses on describing the fundamentals of computer networks. The section initially starts with the topics of network hardware and network software, which are essential for those looking for networking. After reviewing these, the modules also discuss basic concepts of networking, which help the students recognise network-based applications. This enables users to operate the network using different applications and modern technologies.

In the next section, the module discusses different network hardware and software types that allow smooth network transition by ensuring the highest accuracy. Reference models are one of the most significant topics this module covers, and the student will grasp the framework for how data moves over the networks through OSI and TCP/IP models. The module also explores data communication services and examples of networks we use daily, like LANs, WANs, and the Internet.

The module now discusses web browsing, email, and other cloud services, which are crucial when dealing with computer networks. Transferring data through different cables and signals is also explained, as it is a significant topic of this module. Multiplexing is discussed in this module to combine several signals. Switching, which directs the data to the correct destination, is also explained in this module.

This module will explain ISDN, Broadband ISDN, and ATM to ensure effective data transmission. The final topic is the data link layer, which ensures a smooth connection among two networks. Techniques like checksums and parity checks are used effectively to detect transmission errors. You will also learn about sliding window protocols, which manage data flow between devices to ensure that information is transmitted accurately and efficiently.

This module is divided into **three** units.

Unit 1.1 Introduction to Computer Networks
Unit 1.2 Data Communication Services and Transmission Media
Unit 1.3 Data Transmission Control and Reliability

MODULE 1

Introduction to Computer Networks and Data Communications

Unit 1

Introduction to Computer Networks

Unit Table of Contents

Unit 1.1 Introduction to Computer Networks

Aim

This unit explores the fundamental concepts of network hardware, software, and reference models in computer networks.

Instructional Objectives

This unit intends to:

- Explain the diverse types of network hardware and their roles in a network
- Describe the network software's functions and protocols' role in managing network communication
- Discuss the structure and functions of the OSI and TCP/IP models, comparing their layers and functionalities

Learning Outcomes

Upon completion of the unit, you will be able to:

- Develop an understanding of different network hardware components and their functions
- Explore the role of protocols in network communication
- Evaluate the differences between the OSI and TCP/IP models and identify their respective layers and functions

Introduction to Computer Networks

Computer networks are systems of interconnected computers that share resources and information. They can vary in scale from small local area networks (LANs) used in regional areas for small offices and home purposes. The vast wide-area networks (WANs) that span continents. The foremost aim of computer networking is to allow for data communication and resource sharing, such as file transfer, printer sharing, and internet access. Networks are integral to modern communication, enabling everything from email exchanges to real-time video conferencing and cloud computing services.

Various kinds of devices can be connected to a network:

- Desktop Computers
- Laptop
- Printer
- Scanner
- Personal digital assistants (PDA)
- Mobiles
- File and printing servers

Fig. 1: Computer networks

1.1.1 Network Hardware

Network hardware, often known as network devices, includes the physical devices required for communication and interaction between computers on a network. Critical components of network hardware are as follows:

- Network Interface Controller (NIC)
- Hub
- Switch
- Bridge
- Router
- Gateway
- Repeater
- CSU/DSU
- Modems

Network Interface Controller

- A circuit board inserted on a computer to connect to the network is called an NIC (network interface controller) card. It is also referred to as a network adapter or network interface card.
- A NIC card is necessary to connect computers to a network and enhance communication between data communication devices (DCE).
- NICs have electrical circuitry that complies with the physical layer, data link standards, and a port for attaching to the local area network (LAN) media.

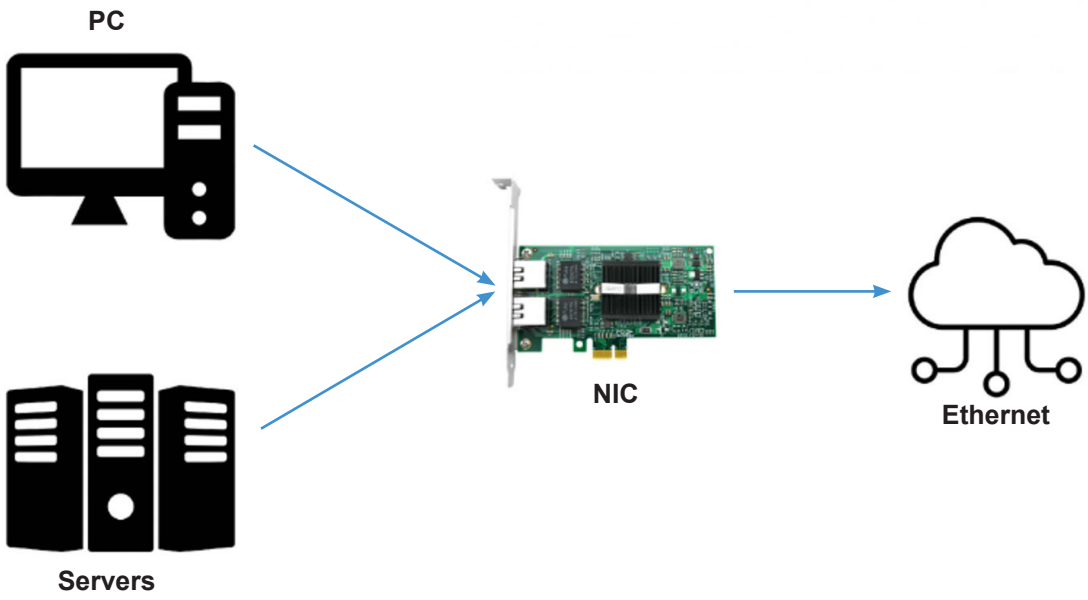


Fig. 2: Network Interface Controller

Hub: A hub joins wires from several branches, like the connector in a star topology that joins various stations. Although hubs cannot store data, they can deliver data packets to all connected devices.

Switch: A switch enables connections for devices like hubs and routers and supports restricted routing information for internal network nodes. It sent packets to the destination by recognising its hardware address. The data link layer section in the OSI Model will be responsible for making all the functionalities of the switches.

Bridge: A bridge is a type of network device used to divide a computer network into portions. In the OSI model, a bridge operates at layer two, or the data link layer. Its primary purpose is to verify the traffic of the incoming data and send it forward by filtering it.

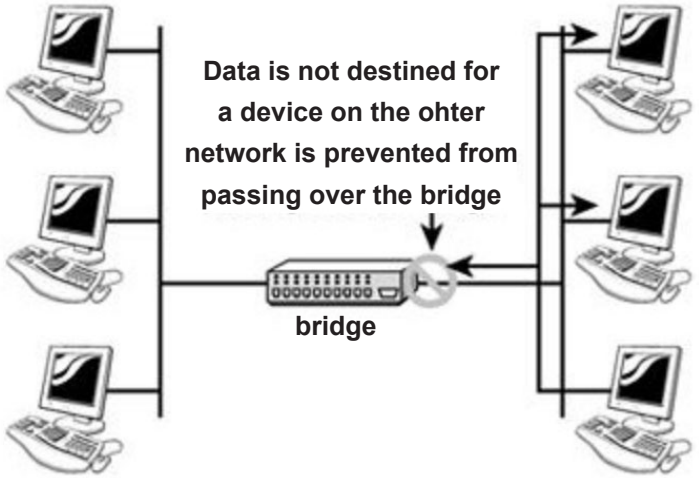


Fig. 3: Bridge

Router

- A router is a small piece of network hardware that moves packets between networks. It
- frequently has connections to two or more networks.
- To identify which port a packet will be sent out of when it arrives at a router port, the router
- checks the address information in the packet.
- A router assists in guiding data packets to their intended IP address

Gateways: A get gateway is commonly used to join two networks by using various transmission protocols. Hence, it acts as a telecommunications network. A gateway acts as a network's entry and exit point because all data must travel through or connect with it before being forwarded.

Repeater

- The repeater is responsible for retransmitting the signal that has been received. It will capture the signal when it is vital; it strictly avoids the chance of catching faint signals. Operating at the physical layer is a repeater.
- They do not even attempt to read the data frames. The repeater will send the data to each port multiple times. These are analogue gadgets that operate with connected signals.

CSU/DSU

- Channel Service Unit and Data Service Unit are both referred to as CSU/DSUs
- A router is connected to a digital circuit, such as a T1 or T3 line, using a CSU or DSU. Digital technology is responsible for operating the network, whereas analogue technology is responsible for transferring text data using phone lines.

Modem

- The term “modem” stands for modulator-demodulator. Data is transferred from one computer network to another through modems connected to telephone lines.
- Digital technology operates the computer network, whereas analogue technology transmits text messages through phone lines.

Self-Assessment Questions

1. Which of the following devices operates at the Data Link layer of the OSI model and is used to forward data based on MAC addresses?

   A). Hub
   B). Router
   C). Switch
   D). Modem

2. What is the primary function of a repeater in a network?

   A). Convert digital signals to analogue
   B). Filter and forward traffic to specific network segments
   C). Boost and retransmit signals to extend the network's range
   D). Route packets between different networks

3. Which network device acts as a network entry and exit point, allowing communication between two networks that use different protocols?

   A). Router
   B). Gateway
   C). Switch
   D). Bridge

1.1.2 Network Software

- Network software incorporates all the programs and protocols that enable transmission over a network.
- Data exchange and security measurements are two of network software's main aims, and they are often responsible for maintaining network operations efficiently.

Key Components of Network Software are as follows:

- Operating System Networking Capabilities
- Network Protocols
- Virtual LANs (VLANs)

Operating System Networking Capabilities: Modern operating systems such as Windows, Linux, macOS, Android, and iOS have built-in networking capabilities. These operating systems support essential network functionalities like TCP/IP stacks, ensuring devices can connect and communicate over various networks.

Network Protocols: Protocols are standardised rules that define how data is transmitted and received across a network. Key network protocols include:

- TCP/IP (Transmission Control Protocol/Internet Protocol)
- The TC_P/I model is universally used to detect errors from local networks. It is considered the most dependable model in which data packets are sent in the most secure form. The IP sends the data packets to the proper and accurate destination.
- TCP/IP Model Layers:
    - **Application Layer:** This layer provides network services directly to applications. Protocols include HTTP, FTP, SMTP, DNS, and TELNET.
    - **Transport Layer:** Ensures reliable communication between devices. TCP provides error checking and data integrity, while UDP offers a faster, connectionless service without error checking.
    - **Internet Layer:** This layer handles packet forwarding and routing. Protocols include IPv4 and IPv6, which manage IP addressing and routing.
    - **Link Layer:** The layer is responsible for the physical transmission of data over network media. It includes Ethernet and Wi-Fi protocols.
    - **HTTP/HTTPS (Hypertext Transfer Protocol/Secure):** HTTP transfers web pages over the Internet. HTTPS is the secure version of HTTP, encrypting data to protect sensitive information during transmission.

- **FTP (File Transfer Protocol):** FTP facilitates the transfer of files between computers over a network. FTP ensures easy access to the user for downloading or uploading their required files, even from a remote server.
- **SMTP (Simple Mail Transfer Protocol):** It transfers messages from email clients to the mail server and between mail servers.

Virtual Lans (VLANs): It allows for segmenting a physical network into smaller, isolated networks. The VLANs are responsible for ensuring security by removing the broadcast traffic. VLANs are typically used to reduce network congestion, improve security by isolating sensitive data, and manage network resources more efficiently.

By integrating these hardware and software components, computer networks can efficiently manage communication, resource sharing, and connectivity, forming the backbone of modern information technology infrastructure.

Self-Assessment Questions

4. Which of the following is a vital function of the Transport Layer in the TCP/IP model?

   A). Handling packet forwarding and routing
   B). Providing error checking and reliable data transmission
   C). Managing physical data transmission over network media
   D). Encrypting data for secure communication

5. What is the purpose of Virtual Local Area Networks (VLANs) in a network?

   A). To facilitate file transfer between computers
   B). To isolate sensitive data and reduce network congestion
   C). To enhance physical data transmission
   D). To route data between different networks

6. Which network protocol transfers web pages securely over the internet?

   A). FTP
   B). SMTP
   C). HTTP
   D). HTTP

1.1.3 Reference Models

In computer networks, reference models provide a conceptual framework for understanding and implementing network protocols and communication. There are two prominent models:

- OSI (Open Systems Interconnection) model
- TCP/IP (Transmission Control Protocol/Internet Protocol) model

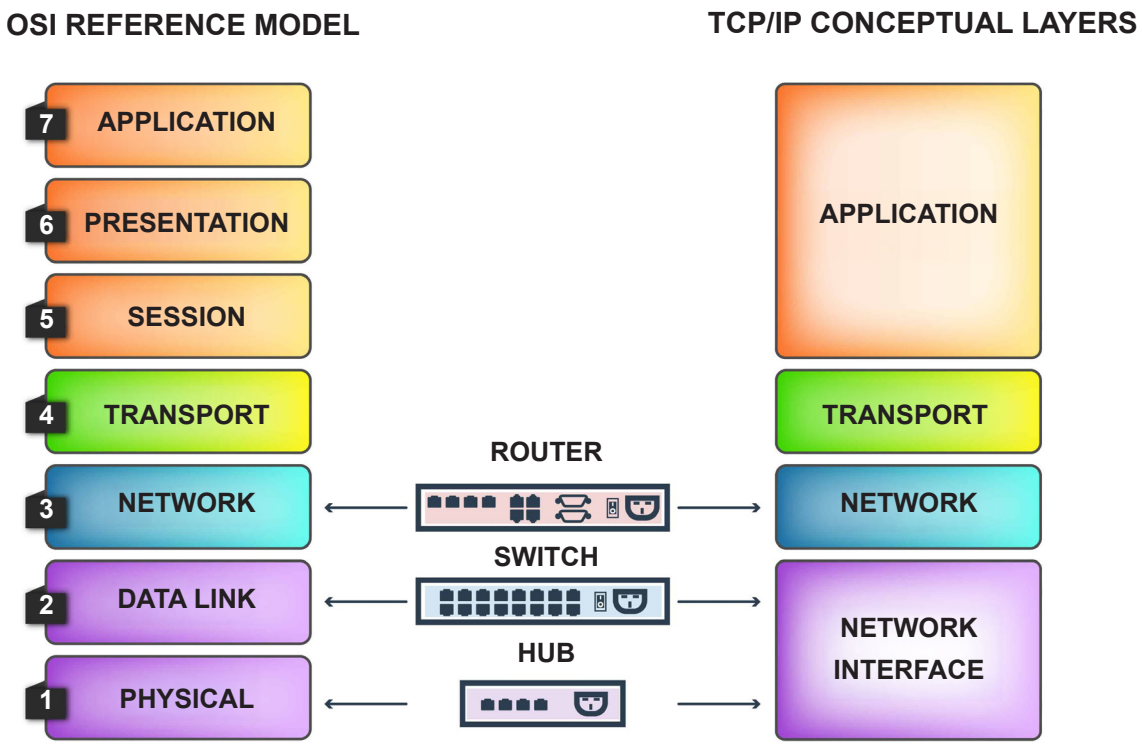


Fig. 4: Reference models

1.1.3.1 OSI Model

The OSI reference model and the TCP/IP conceptual layers show the network communication structure. The OSI model has seven layers, each representing distinct functions for transmitting data between devices, while the TCP/IP model has fewer layers, combining some of the OSI layers into broader categories. It also illustrates how network devices, such as routers, switches, and hubs, correspond to different layers in these models, highlighting their roles in data transmission.

The OSI (Open Systems Interconnection) model is a conceptual framework that explains how data is transferred over a network. It divides the communication process between two devices into seven layers, each with a specific function. These layers work together to ensure that data is sent and received accurately, from the physical transmission of bits (like 1s and 0s) through cables to how software applications interact.

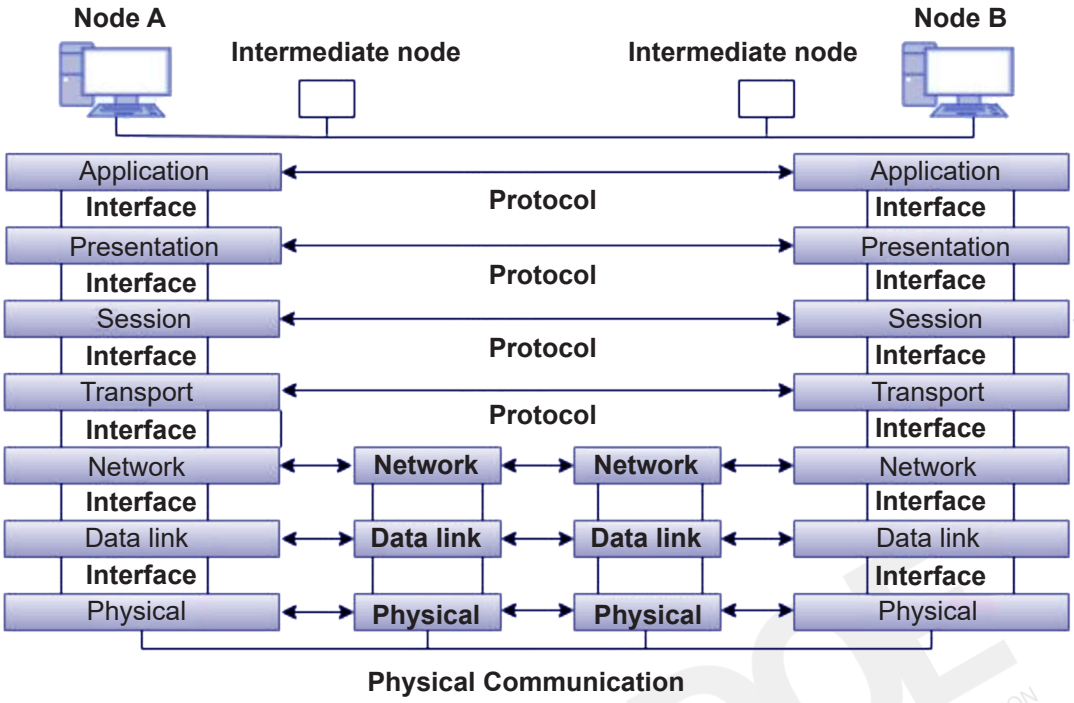


Fig. 5: Working of OSI Model

Two computers (Node A and Node B) are trying to communicate with each other over a network. They are interconnected by intermediate devices (routers, switches, etc.), and the communication process follows the OSI model is seven layers.

Each layer of the model has a specific role in ensuring that data is transmitted correctly from Node A to Node B.

Layers in OSI Model

- **Physical Layer (Layer 1):** This layer deals with the physical connection between devices. It involves the cables, switches, and signals used for data transmission. In the above diagram, data from Node A's physical layer is sent through the intermediate node's physical layer and reaches Node B's physical layer. It manages raw data transmission in the form of bits.
- **Data Link Layer (Layer 2):** This layer ensures data packets are transferred without errors. It manages error detection, frame formatting, and physical addressing. The data link layers of Node A, the intermediate nodes, and Node B ensure the data is appropriately framed and sent to the correct device.
- **Network Layer (Layer 3):** The layer determines the path the data takes across the network. It deals with logical addressing (like IP addresses) and routing. The network layers of the nodes and intermediate devices work together to find the most efficient path for the data to travel from Node A to Node B.

- **Transport Layer (Layer 4):** The transport layer ensures that data is delivered error-free and in the correct sequence. It manages flow control and error recovery. Node A's transport layer communicates with Node B to ensure the message is received and assembled correctly.
- **Session Layer (Layer 5):** This layer manages sessions between applications on different devices. It establishes, maintains, and terminates communication sessions. The session layers of both nodes manage the opening and closing of communication sessions.
- **Presentation Layer (Layer 6):** The presentation layer ensures that the data is in the correct format for the application. It manages data encryption, compression, and translation between different data formats. The presentation layers of Node A and Node B ensure the data is properly formatted and ready for use by the application layer.
- **Application Layer (Layer 7):** The topmost layer is responsible for the user-facing part of communication. It interacts directly with software applications like web browsers, email clients, etc. The application layers of Node A and Node B interact with the user applications (like web browsers or file-sharing apps) to send and receive data.
- **Communication Process (Node A to Node B):** When Node A wants to send data to Node B, the data passes down through the seven layers of Node A (from the application layer to the physical layer), through intermediate nodes (which handle the lower layers), and then back up through the layers of Node B (from physical to application). A specific protocol governs the communication process at each layer (as shown by the term "Protocol" between each layer in the diagram).

1.1.3.2 TCP/IP MODEL

The TCP/IP model (Transmission Control Protocol/Internet Protocol) is a simplified framework for understanding how data is transmitted over the Internet and other networks. It consists of four layers, each with specific roles in data communication. Unlike the OSI model, which has seven layers, the TCP/IP model focuses on how the Internet works, combining some OSI layers for practical purposes.

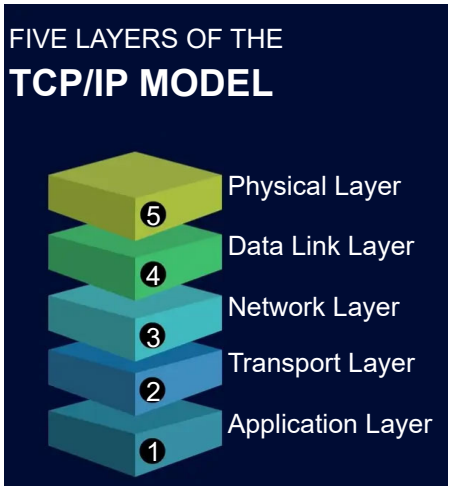


Fig. 6: Layers of TCP/IP Model

- **Data Link or Network Access Layer:** This layer mainly combines the data link and physical layers, which will be shown in the OSI model. It will work to transmit data through the available protocols.
- **Internet Layer:** This layer works to transmit data over networks logically. The main protocols residing at this layer are:
  - IP stands for Internet Protocol, which delivers the packets collected from the course host to the end host using the IP address in the packet headers.
  - IP has two versions: IPv4 and IPv6. Most websites currently use IPv4, but IPv6 is growing as the number of IPv4 addresses is limited compared to the number of users.
  - ICMP stands for Internet Control Message Protocol. It is encapsulated within IP datagrams and is responsible for providing hosts with information about network problems.
  - ARP stands for Address Resolution Protocol. Its job is to find a host's hardware address from a known IP address. ARP has several types: reverse ARP, Proxy ARP, Gratuitous ARP, and Inverse ARP.
- **Transport or Host-To-Host Layer:** This layer is analogous to the transport layer of the OSI model. It is responsible for end-to-end communication and error-free delivery of data. It shields the upper-layer applications from the complexities of data. The two main protocols present in this layer are:
  - **Transmission Control Protocol (TCP):** It is known to provide dependable and error-free communication between end systems. It performs data sequencing and segmentation. It also has an acknowledgement feature and controls data flow through a flow control mechanism. It is a highly effective protocol but has a lot of overhead due to such features. Increased overhead leads to increased cost.
  - **User Datagram Protocol (UDP):** On the other hand, it does not provide such features. It is the go-to protocol if your application does not require reliable transport, as it is very cost-effective. Unlike TCP, which is a connection-oriented protocol, UDP is connectionless.
- **Application Layer:** This layer performs the functions of the top three layers of the OSI model: Application, Presentation, and Session Layer. It is responsible for node-to-node communication and controls user-interface specifications. Some protocols in this layer are HTTP, HTTPS, FTP, TFTP, Telnet, SSH, SMTP, SNMP, NTP, DNS, DHCP, NFS, X Window, and LPD.
  - **HTTP and HTTPS:** HTTP stands for Hypertext transfer protocol. The World Wide Web uses it to manage communications between web browsers and servers. HTTPS stands for HTTP-Secure. It is a combination of HTTP with SSL (Secure Socket Layer). It is efficient in cases where the browser needs to fill out forms, sign in, authenticate, and conduct bank transactions.

- **SSH:** SSH stands for Secure Shell. It is terminal emulator software like Telnet. SSH is preferred because it can maintain an encrypted connection. It sets up a secure session over a TCP/IP connection.
- **NTP:** It stands for Network Time Protocol. It synchronises the clocks on our computer to one standard time source, which is especially useful in situations like bank transactions. Assume the following situation without NTP: Suppose you conduct a transaction where your computer reads the time at 2:30 PM while the server records it at 2:28 PM. The server can crash very severely if it is uncoordinated.

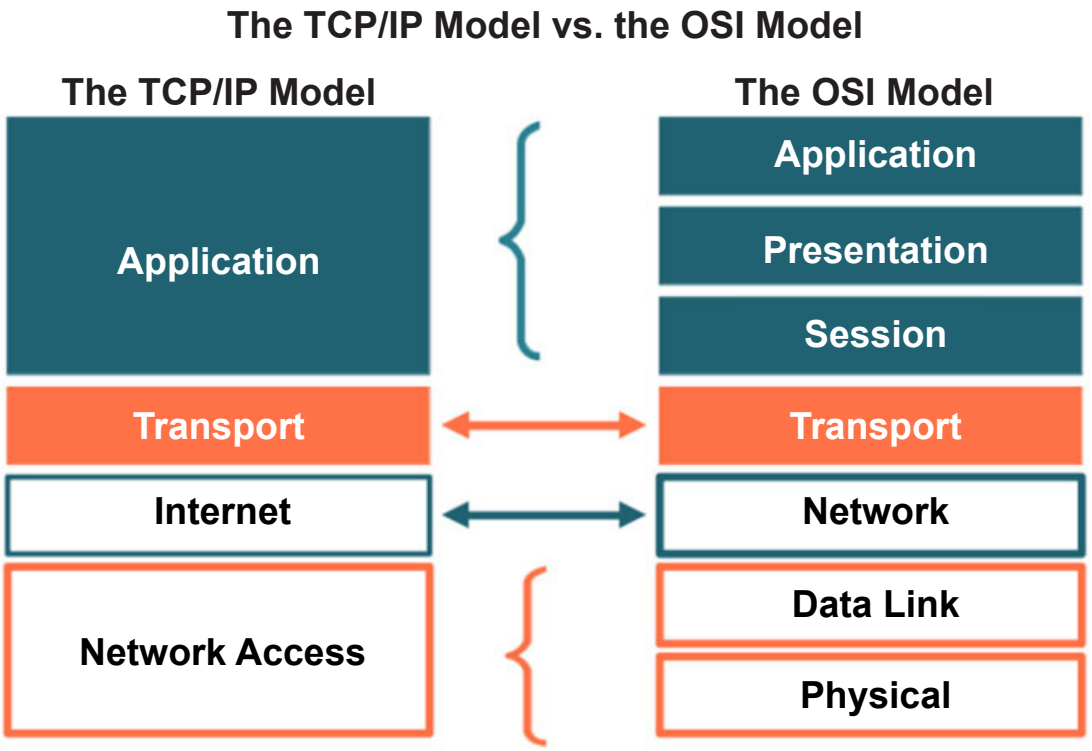


Fig. 7: OSI Model vs. TCP/IP Model

OSI Model	TCP/IP Model
It stands for open system interaction.	It stands for transmission control protection.
ISO has developed the OSI Model.	ARPANET developed it.
It is an independent standard and generic protocol used as a communication gateway between the network and the end user.	It consists of standard protocols that led to the development of the Internet. It is a communication protocol that provides a connection among hosts.
In the OSI model, the transport layer guarantees the delivery of the packets.	Although the transport layer does not guarantee packet delivery, it is still a dependable model.
This model is based on a vertical approach.	This model is based on a horizontal approach.
In this model, the session and presentation layers are separated, i.e., different.	In this model, the application layer includes the session and presentation layers.
It is also known as a reference model through which various networks are built. For example, the TCP/IP model is constructed from the OSI model.it is also referred to as a guidance tool.	It is an implemented OSI model.
In this model, the network layer provides both connection-oriented and connectionless services.	The network layer provides only connectionless services.
Protocols in the OSI model are hidden and can be easily replaced when any technology changes.	In this mode, the protocol cannot be easily replaced.
It consists of seven layers.	It consists of five layers.
The OSI model defines and properly distinguishes the services, protocols, and interfaces. It is protocol-independent.	The TCP/IP model properly separates services, protocols, and interfaces. It is protocol-dependent.
The usage of this model is shallow.	This model is universally used.
It standardises routers, motherboards, switches, and other hardware devices.	It does not provide standardisation for the devices. It provides a connection between the various computers.

Table 1: Comparison of OSI Model and TCP/IP Model

Self-Assessment Questions

7. Which OSI model layer is responsible for data encryption and formatting before transmission?

   A). Physical Layer
   B). Data Link Layer
   C). Presentation Layer
   D). Transport Layer

8. Which protocol operates at the Transport layer of the TCP/IP model to provide dependable, connection-oriented communication?

   A). IP
   B). HTTP
   C). UDP
   D). TCP

9. In the TCP/IP model, which layer is responsible for the logical addressing and routing of packets across the network?

   A). Application Layer
   B). Network Access Layer
   C). Internet Layer
   D). Transport Layer

1.1.4 Data Communication Services

Data communication services in computer networks are designed to facilitate data transfer between devices and ensure the effective operation of networked applications. These services are built on various protocols and technologies that address various aspects of data transmission, including reliability, security, and efficiency. Some Data communication services are as follows.

- **Email:** A service allowing users to send and receive digital messages online. Gmail, Outlook, and Yahoo Mail are some of the examples.
- **File Transfer Protocol (FTP):** This protocol transfers files between computers on a network. FileZilla and WinSCP are examples of it.
- **Voice over Internet Protocol (VoIP):** A service that allows users to make voice calls using a broadband internet connection instead of a regular phone line. Skype, Zoom, and Google Voice are some of its examples.
- **Instant Messaging:** A service that allows users to send and receive text messages in real-time, such as WhatsApp, Telegram, or Slack.
- **Video Conferencing:** A service that allows users to conduct live video meetings over the Internet through applications like Zoom, Microsoft Teams, and Google Meet.
- **Cloud Storage:** A service that allows users to store data on remote servers accessed via the Internet, such as Dropbox, Google Drive, or OneDrive.
- **Social Networking:** Platforms that enable users to create profiles, share information, and interact with others. Facebook, Twitter, and LinkedIn are some social networking platforms.
- **Web Browsing:** Accessing and viewing web pages on the internet through applications like Google Chrome, Mozilla Firefox, Safari etc.

Network Examples

- **Local Area Network (LAN):** A network that connects computers within a limited area such as a residence, school, or office building. For example, a network within a single office building will use this network.
- **Wide Area Network (WAN):** A telecommunications network that extends over a large geographical area for the primary purpose of computer networking. The internet is the best example of this network.
- **Metropolitan Area Network (MAN):** A network that spans a city or a large campus. A network covering a university campus is its best example.
- **Personal Area Network (PAN):** A network for interconnecting devices centred around a person's workspace. Examples include Bluetooth-connected devices such as smartphones, smartwatches, and laptops.

- **Virtual Private Network (VPN):** A secure network connection over a public network such as the Internet. Remote employees use corporate VPNs to access company resources securely.
- **Wireless Local Area Network (WLAN):** It is a network that allows devices to connect and communicate wirelessly within a limited area, typically using Wi-Fi technology. It includes Wi-Fi networks in homes, cafes, or offices.
- **Storage Area Network (SAN):** A network designed to manage large-scale data storage.
- Enterprise-level data centres will use these SANs to manage data.
- **Campus Area Network (CAN):** A network that connects multiple LANs within a limited geographical area, such as a university campus.

INTERNET-BASED APPLICATIONS:

- **Web Browsers:** Software used to access and view websites such as Google Chrome, Mozilla Firefox, and Safari.
- **Email Services:** Platforms for sending, receiving, and managing emails through applications like Gmail, Outlook, and Yahoo Mail.
- **Social Media Platforms:** Websites and applications that enable users to create and share content or participate in social networking, which includes platforms like Facebook, Twitter, and Instagram.
- **Search Engines:** Tools that allow users to search for information on the Internet, such as Google, Bing, and Yahoo Search.
- **Streaming Services:** Netflix, YouTube, and Spotify are platforms for watching videos, listening to music, and live-streaming content.
- **Cloud Storage Services:** These services allow users to store data on remote servers and access it online. Google Drive, Dropbox, and OneDrive are the best examples.
- **Online Shopping:** E-commerce websites where users can buy and sell goods and services. Amazon, Flipkart, Myntra, eBay, and Alibaba are some commonly used e-commerce websites.
- **Online Banking:** Digital platforms for managing bank accounts, transactions, and other financial services. PayPal, Chase Online, and Bank of America Online Banking are some banking institutions providing online banking services.
- **Collaboration Tools:** Applications that facilitate teamwork and project management over the Internet. Slack, Trello, and Asana are commonly used collaborative tools.
- **Online Education refers to platforms** that offer courses and educational content over the Internet. Coursera, Khan Academy, edX, Unacademy, and Vedantu are some education-provider platforms.
- **VoIP Services:** Applications for making voice calls over the Internet, such as Skype, Zoom, and Google Voice.

- **Instant Messaging Apps:** These are applications for sending and receiving instant messages. WhatsApp, Telegram, and Signal are some instant messaging applications.
- **Online Gaming:** Games played over the internet. Fortnite, World of Warcraft, League of Legends, etc., are examples.
- **Remote Desktop Applications:** Tools that allow users to access and control a computer remotely include TeamViewer, AnyDesk, and Microsoft Remote Desktop.
- **Content Management Systems (CMS):** Platforms used to create, manage, and modify digital content. WordPress, Joomla, and Drupal are examples.
- **File Sharing Services:** These are applications for sharing files over the internet. WeTransfer, Google Drive, and Dropbox are some commonly used sharing services.
- **Online Forums and Communities:** These are platforms for discussion and information sharing among users. Reddit, Stack Overflow, and Quora offer online forums and communities.
- **News Websites:** These are online platforms for accessing news and information, such as BBC News, CNN, and The New York Times.
- **Travel and Booking Services:** Websites for booking flights, hotels, and travel packages. By using Expedia, Booking.com, Airbnb, etc.
- **Health and Fitness Apps:** These applications provide health information, fitness tracking, and telemedicine services. MyFitnessPal, Fitbit, Teladoc, and more are some health apps.

Self-Assessment Questions

10. Which of the following is an example of a Voice over Internet Protocol (VoIP) service?

    A). Dropbox
    B). Google Meet
    C). Skype
    D). Facebook

11. What type of network is typically used to connect devices within a university campus?

    A). Wide Area Network (WAN)
    B). Personal Area Network (PAN)
    C). Campus Area Network (CAN)
    D). Storage Area Network (SAN)

12. Which platform is commonly used for storing and accessing data online through remote servers?

    A). Trello
    B). Google Drive
    C). TeamViewer
    D). WhatsApp

Summary

- Computer networks enable device connections for data sharing across LANs to WANs.
- NICs, hubs, routers, and modems ensure data transmission and connectivity.
- Network software, including protocols like TCP/IP, enables communication and management.
- The OSI model explains data transmission through seven layers, while the TCP/IP model simplifies it into four layers for internet communication.
- Switches and routers manage data flow and routing in networks, optimising performance.
- Firewalls and encryption provide security by controlling access and protecting data.
- Wireless technologies like Wi-Fi and Bluetooth enable wireless communication and device connectivity within networks.
- VLANs enhance network segmentation, and protocols like HTTP, FTP, and SMTP ensure reliable data exchange.

Terminal Questions

1. How does a computer network function, and what are its primary benefits for communication and resource sharing?
2. What roles do diverse network cables and connectors play in establishing reliable data transmission?
3. How do switches and routers contribute to data flow and management in small- and large-scale networks?
4. How do firewalls enhance network security, and how does encryption protect sensitive data?
5. How do wireless technologies like Wi-Fi and Bluetooth enable device connectivity and communication within networks?
6. What are the advantages and disadvantages of using wireless over wired networking technologies?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	C
2	C
3	B
4	B
5	B
6	D
7	C
8	D
9	C
10	C
11	C
12	B

Activity

Activity type: Online **Duration: 2 Days**

Propose how to set up the wireless network (Wi-Fi) for employees' devices. Ensure it is secure and does not interfere with the core wired network's performance.

Glossary

- Encryption: The process of converting data into a secure format to prevent unauthorised access during transmission.
- Ethernet: A standard wired networking technology used for local area networks, utilising cables for data transmission.
- Bandwidth: The maximum data transfer rate across a network, measured in bits per second (bps).
- Latency: The time delay between a data request and its delivery over a network, measured in milliseconds (ms).
- Proxy Server: An intermediary server that separates end users from the websites they browse, providing anonymity or security.
- Subnet Mask: A number that separates the network address from the host address in an IP address, used for network organisation.
- Topology: The arrangement or structure of a network, including star, mesh, bus, and ring topologies.
- Load Balancer: A device that distributes network traffic across multiple servers to ensure no single server becomes overwhelmed.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Network Hardware:** https://www.spiceworks.com/tech/networking/articles/what-is-network-hardware/
- **Network Software:** https://www.spiceworks.com/tech/networking/articles/what-is-network-software/

Video Links

Topic	Link
Introduction to Computer Networks	https://youtu.be/wXsgJPnr1nQ?si=nCJ-GX4XvWb0z-3t
OSI Model	https://youtu.be/vv4y_uOneC0?si=gqaQ2PnA-UH_VYjmW

Image Credits

Fig. 1: Computer networks	https://www.lifewire.com/thmb/9qDvxHNaoKaL2_N9Z0bF995Pl-s=/5671x4330/filters:no_upscale():-max_bytes(150000):strip_icc()/WirelessNet-work-5994852003f4020011db5333.jpg
Fig. 2: Network Interface Controller	https://www.ptbsb.id/wp-content/uploads/2024/02/What-is-a-Network-Interface-Card-scaled-1.jpg
Fig. 3: Bridge	https://www.elprocus.com/wp-content/uploads/bridge-in-computer-network.jpg
Fig. 4: Reference models	https://cdn.comparitech.com/wp-content/up-loads/2021/02/OSI-to-TCPIP-stack.jpg
Fig. 5: Working of OSI Model	https://www.tutorialride.com/images/computer-network/osi-model.jpeg
Fig. 6: Layers of TCP/IP Model	https://www.whatismyip.com/static/e3c2d375b219e64f67c8bc157b203f83/tcp-ip-model.webp
Fig. 7: OSI Model vs. TCP/IP Model	https://cheapsslsecurity.com/blog/wp-content/uploads/2022/06/tcp-ip-model-vs-osi-770x515.png

Keywords

- Network
- Router
- Switch
- Gateway
- Transmission
- Protocol

MODULE 1

Introduction to Computer Networks and Data Communications

Unit 2

Data Communication Services and Transmission Media

Unit Table of Contents

Unit 1.2 Data Communication Services and Transmission Media

Aim

This unit aims to explore the principles of data communication services, transmission media, and wireless transmission technologies.

Instructional Objectives

This unit intends to:

- Describe the distinct types of transmission media, including wired and wireless networks
- Discuss the functioning of various wireless transmission technologies
- Explain the concepts of multiplexing and switching

Learning Outcomes

Upon completion of the unit, you will be able to:

- Demonstrate the critical differences between wired and wireless transmission media
- Identify various wireless transmission technologies and their applications in real-world scenarios
- Explore the role of switching and multiplexing in computer networks.

1.2.1 Transmission Media

Computers and other telecommunications equipment use signals to represent data. Electromagnetic energy is used to send signals from one device to another. Magnetic signals move through a vacuum, the atmosphere, or other transmission mediums from one location to another (from source to receiver). Power, voice, and visible signals are all forms of electromagnetic energy (including electrical and magnetic fields), as are gamma rays, radio waves, UV light, and light in general.

The method by which we transfer our data from one location to another is known as a transmission medium. The first layer (physical layer) of the OSI seven-layer model for communication networks is dedicated to this medium. Transmission rate, cost and ease of installation, resistance to environmental conditions, and distances are the factors that must be considered while choosing a transmission medium.

Types of Transmission Medium

Transmission mediums are the paths through which data is transmitted in a network. They can be wired (like cables) or wireless (like radio waves), each with different speeds and reliability.

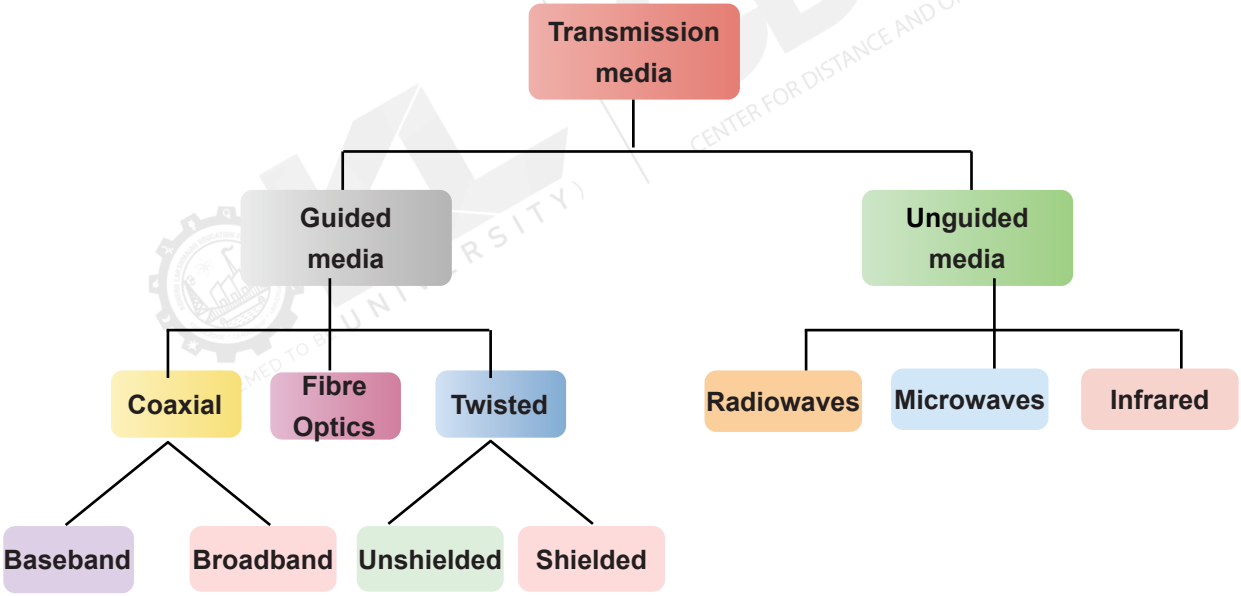


Fig. 1: Types of Transmission Media

1.2.1.1 Guided Media

It is a form of communication in which wire or cable confines signals to a particular path. Bounded/ Guided categories of mediums are discussed below.

- **Twisted Pair:** This cable is the most often used and the least expensive. It is portable, affordable, simple to install, and supports various networks. Its frequency range is 0 to 3.5 kHz. Typical attenuation is 0.2 dB/Km @ 1kHz. A 50 s/km delay is typical. The repeater distance is 2km. Unshielded twisted pairs and shielded twisted pairs are two types of twisted pairs.
    - **Unshielded Twisted Pair:** Compared to shielded twisted pair cable, which consists of two conductors, often copper, each with a distinct colour plastic insulator, it is the most prevalent form of communication. The purpose of coloured plastic insulation is identification. UTP cables consist of 2 or 4 pairs of twisted cable. Cable with two pair use RJ-11 connectors, and four pair cable use RJ-45 connector.

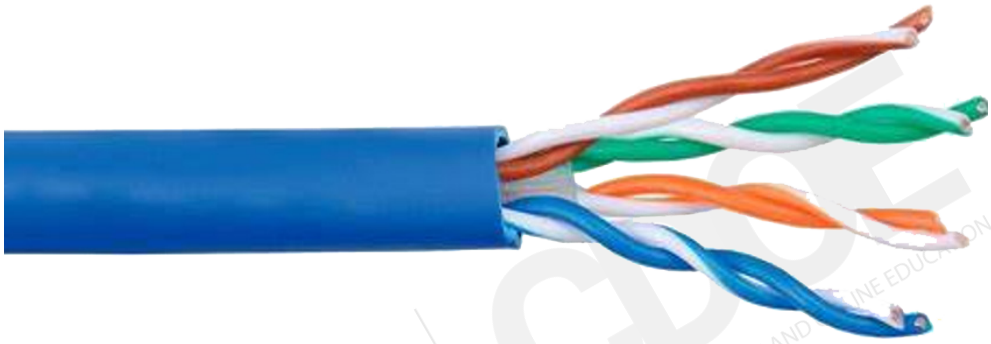


Fig. 2: Unshielded Twisted Pair

- **Shielded Twisted Pair Cable:** This cable has a metal foil or braided mesh covering that encases each pair of insulated conductors. The metal casing prevents electromagnetic noise penetration. Shielding also eliminates crosstalk. It has the same attenuation as an unshielded twisted pair. It is faster than unshielded and coaxial cable. It is more expensive than coaxial and unshielded twisted pair.

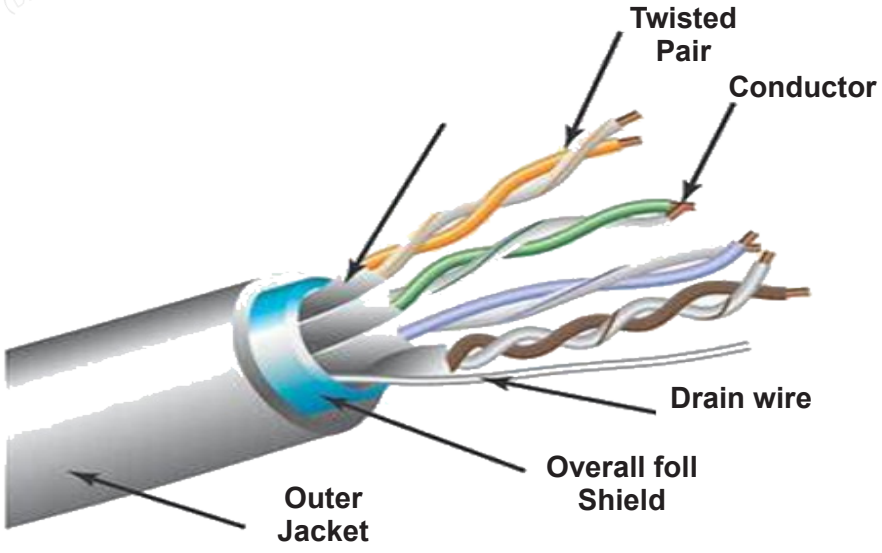


Fig. 3: Shielded Twisted Pair

- **Coaxial Cable:** Coaxial is called by this name because it contains two conductors that are parallel to each other. Copper is used in this as a centre conductor, which can be a solid wire or a standard one. It is surrounded by PVC installation, a sheath encased in an outer conductor of metal foil, braid, or both. Outer metallic wrapping is used as a shield against noise and as the second conductor which completes the circuit. The outer conductor is also encased in an insulating sheath. The outermost part is the plastic cover which protects the whole cable.

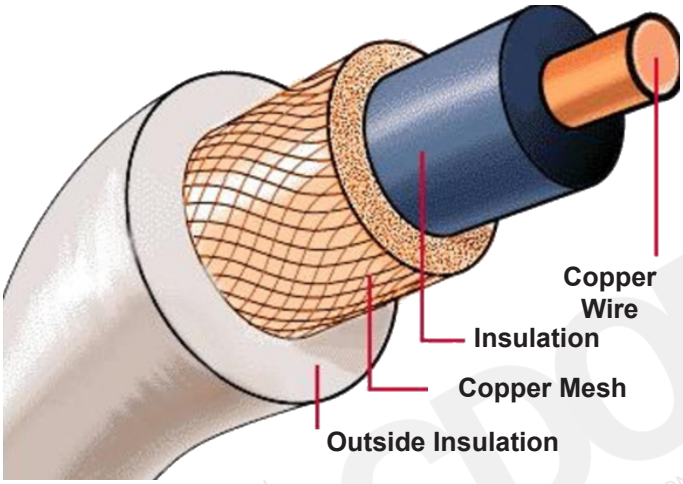


Fig. 4: Coaxial cable

- **Fibre Optic Cable:** These are like coaxial cables. They use electric signals to transmit data. At the centre is the glass core through which light propagates. The core of multimode fibres is fifty microns, and the thickness of single-mode fibres is 8 to 10 microns. The core in fibre optic cable is surrounded by glass cladding with a lower index of refraction than the core to keep all the light in the core. This is covered with a thin plastic jacket to protect the cladding. The fibres are grouped in bundles protected by an outer shield. Fiber optic cable has a bandwidth of more than 2 Gbps (Gigabytes per Second).

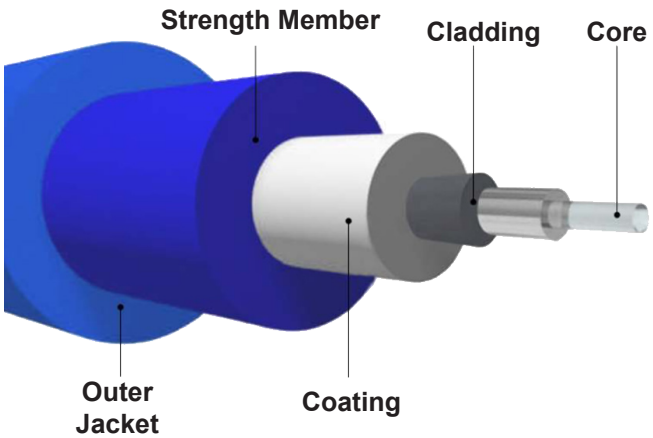


Fig. 5: Fibre optic cable

1.2.1.2 Unguided/Unbounded Transmission Media

Unguided or wireless media sends the data through air (or water), which is available to anyone with a device capable of receiving it. Radio Transmission and Microwave Transmission are two types of unguided/ unbounded media that are discussed below:

- **Radio Transmission:** Its frequency is between 10 kHz to 1GHz. It is simple to install and has high attenuation. These waves are used for multicast communications. Radio Transmission uses diverse types of propagation:
    - **Troposphere:** The lowest portion of Earth's atmosphere extending outward approximately thirty miles from the Earth's surface. Clouds, jet planes, and wind are found here.
    - **Ionosphere:** The layer of the atmosphere above the troposphere but below space. It contains electrically charged particles.
- **Microwave Transmission:** It travels at a higher frequency than radio waves. It requires the sender to be inside of the receiver. It operates in a system with a low gigahertz range. It is used for unicast communication. Terrestrial Microwave and Satellite Microwave are the two types of microwave transmission.

1.2.1.3 Wireless Transmission

Wireless transmission refers to the transfer of information between two or more points not connected by an electrical conductor. It encompasses a variety of technologies that use electromagnetic waves to communicate over the air.

Types of Wireless Transmission

- **Radio Frequency (RF):** Radio waves transmit data over long distances.

  Examples: AM/FM radio and two-way radios.
- **Microwave Transmission:** Uses microwave frequencies (1 GHz to 30 GHz) for high-speed data transmission over long distances.

  Examples: Satellite communication and point-to-point communication links.
- **Infrared (IR):** Uses infrared light to transmit data over short distances.

  Examples: Remote controls and IR communication between devices like printers and computers.
- **Bluetooth:** A short-range wireless technology for exchanging data between fixed and mobile devices.

  Examples: Wireless headphones, keyboards, and mice.
- **Wi-Fi:** A technology that allows devices to connect to a network wirelessly within a local area.

Examples: Home and office networks and public Wi-Fi hotspots.

- **Near Field Communication (NFC):** A short-range wireless communication technology for exchanging data between devices within a few centimetres.

  Examples: Contactless payments and NFC-enabled smartphones for data sharing.

- **Cellular Networks:** Networks of cell towers providing wide-area wireless coverage for mobile devices.

  Examples: mobile phones use 3G, 4G LTE, and 5G networks.

- **Zigbee:** A specification for a suite of high-level communication protocols using low-power digital radios.

  Examples: Smart home devices and industrial automation.

- **WiMAX:** A family of wireless broadband communication standards.

  Examples: Wireless internet service providers and long-range Wi-Fi.

- **Li-Fi:** Uses visible light communication (VLC) for high-speed data transmission.

  Examples: LED lighting systems for data communication and indoor networking.

Self-Assessment Questions

1. Which of the following transmission mediums is most used and least expensive for network communication?

   A). Twisted Pair Cable
   B). Coaxial Cable
   C). Fibre Optic Cable
   D). Microwave Transmission

2. What is the main advantage of a shielded twisted pair cable over an unshielded one?

   A). Higher bandwidth
   B). Lower cost
   C). Reduced electromagnetic interference
   D). Easier installation

3. Which wireless transmission technologies, such as contactless payments, are commonly used for short-range communication?

   A). Wi-Fi
   B). Zigbee
   C). Bluetooth
   D). NFC

1.2.2 Multiplexing

Multiplexing is a technique used in telecommunications and computer networks to combine multiple signals into one medium, transmitting multiple data streams simultaneously over a single communication channel. This optimises the use of available bandwidth and increases the efficiency of the transmission system.

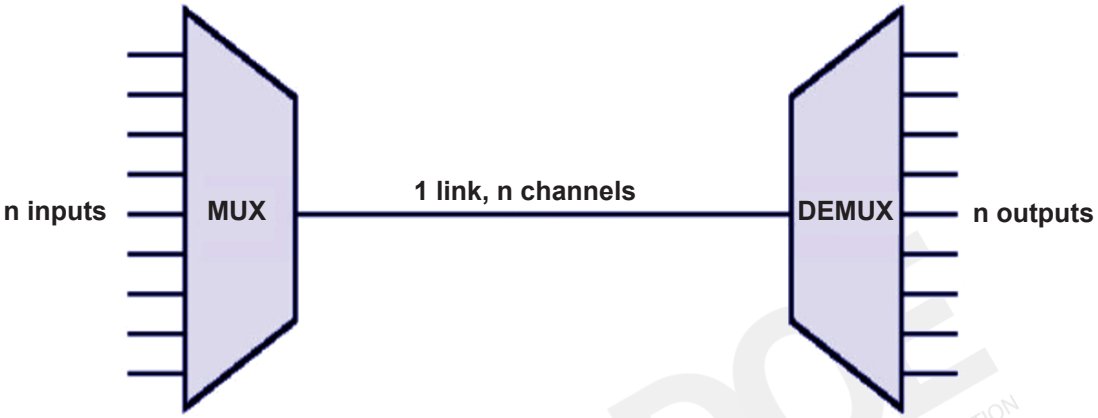


Fig. 6: Multiplexing

Types of Multiplexing

- **Frequency Division Multiplexing (FDM):** FDM works by dividing the available bandwidth of a communication channel into multiple frequency bands, each carrying a separate signal. Each signal modulates a different carrier frequency, allowing them to be transmitted simultaneously without interference.

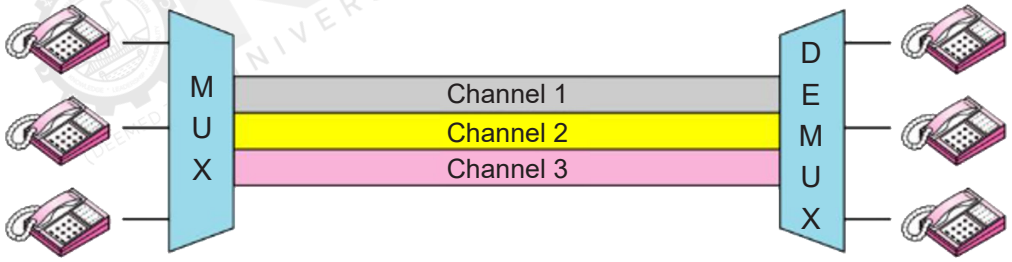


Fig. 7: Frequency Division Multiplexing

Examples: Traditional radio and television broadcasting, where different stations transmit at various frequencies. Cable television, where multiple TV channels are transmitted over a single coaxial cable.

- **Time Division Multiplexing (TDM):** TDM divides the communication channel into time slots and allocates each time slot to a different signal. Signals take turns using the channel, with each signal occupying the channel for a brief period sequentially.

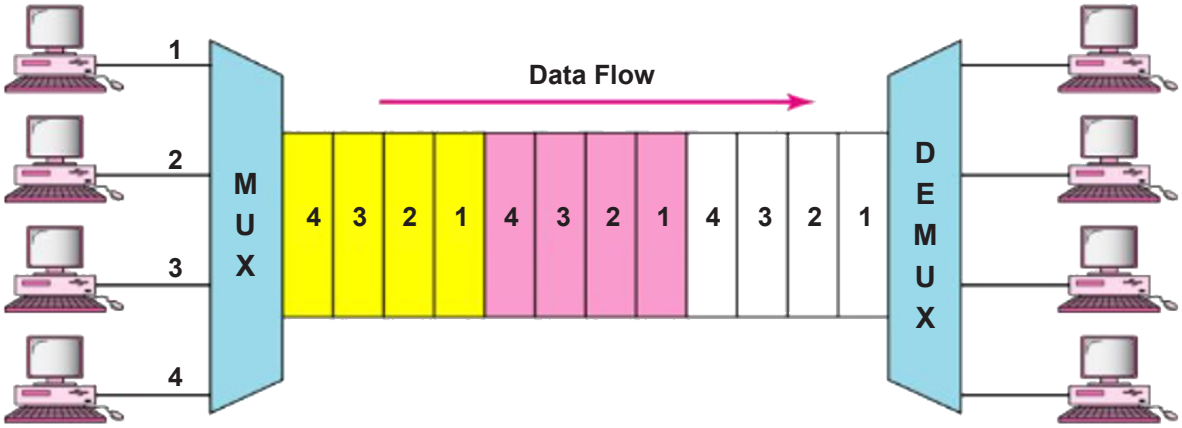


Fig. 8: Time Division Multiplexing

Examples: Digital telephony, where multiple phone calls are transmitted over the same wire by allocating time slots to each call. Synchronous Optical Networking (SONET) is used in fibre optic communication.

- **Wavelength Division Multiplexing (WDM):** WDM is like FDM but is used in fibre optic communications. It involves multiplexing light signals with different wavelengths (colours) onto a single fibre optic cable. significantly increases the data transmission capacity of the fibre.

  Examples: Fiber optic networks, where multiple data streams are transmitted using different wavelengths. Dense Wavelength Division Multiplexing (DWDM) allows even more channels to be multiplexed on a single fibre by closely spacing the wavelengths.

- **Code Division Multiplexing (CDM):** CDM assigns a unique code to each signal and combines them into one channel. Receivers use the code to extract the intended signal. This technique allows multiple signals to occupy the same bandwidth simultaneously.

  Examples: Code Division Multiple Access (CDMA) used in cellular networks. Spread spectrum technologies, where the signal is spread across a wider bandwidth.

- **Orthogonal Frequency Division Multiplexing (OFDM):** OFDM is a type of FDM in which the frequencies of the subcarriers are mathematically orthogonal, minimising interference between them. It divides the channel into multiple subchannels and simultaneously transmits parts of the signal.

  Examples: Wi-Fi (IEEE 802.11), LTE, and DVB-T (Digital Video Broadcasting - Terrestrial).

- **Space Division Multiplexing (SDM):** SDM involves transmitting separate signals in different spatial paths or physical channels. This can be achieved using multiple antennas (MIMO - Multiple Input, Multiple Output) or parallel cables/fibres.

  Examples: MIMO technology in wireless communication, used in modern Wi-Fi and 4G/5G networks. Parallel fibre optic cables in data centres.

Advantages of Multiplexing

- **Efficiency:** Increases the utilisation of the available bandwidth.
- **Cost-effectiveness:** Reduces the need for additional infrastructure by allowing multiple signals to share the same medium.
- **Scalability:** It makes expanding networks and accommodating more users or data streams easier.
- **Flexibility:** Supports various applications and services on the same infrastructure.

Challenges of Multiplexing

- **Interference:** Signals can interfere with each other if not effectively managed.
- **Complexity:** Multiplexing and demultiplexing require sophisticated technology and equipment.
- **Latency:** TDM can introduce delays due to the time-sharing nature of the technique.
- **Cost:** High initial setup cost for some multiplexing technologies, especially WDM in fibre optics.

Self-Assessment Questions

4. Which type of multiplexing divides a communication channel's available bandwidth into multiple frequency bands, each carrying a separate signal?

   A). Time Division Multiplexing (TDM)
   B). Frequency Division Multiplexing (FDM)
   C). Code Division Multiplexing (CDM)
   D). Wavelength Division Multiplexing (WDM)

5. Which type of multiplexing is used in fibre optic communications by multiplexing light signals with different wavelengths onto a single fibre optic cable?

   A). Time Division Multiplexing (TDM)
   B). Orthogonal Frequency Division Multiplexing (OFDM)
   C). Wavelength Division Multiplexing (WDM)
   D). Code Division Multiplexing (CDM)

6. Which multiplexing techniques assign a unique code to each signal, allowing multiple signals to occupy the same bandwidth simultaneously?

   A). Code Division Multiplexing (CDM)
   B). Frequency Division Multiplexing (FDM)
   C). Time Division Multiplexing (TDM)
   D). Space Division Multiplexing (SDM)

1.2.3 Switching

Switching is a fundamental concept in telecommunications and computer networks that involves directing data packets, voice calls, or other types of data from one point to another across a network. The primary goal of switching is to efficiently route data to its destination while optimising the use of network resources. Several switching techniques are suited for different network requirements and applications.

Types of Switching

- Circuit Switching
- Packet Switching
- Message Switching

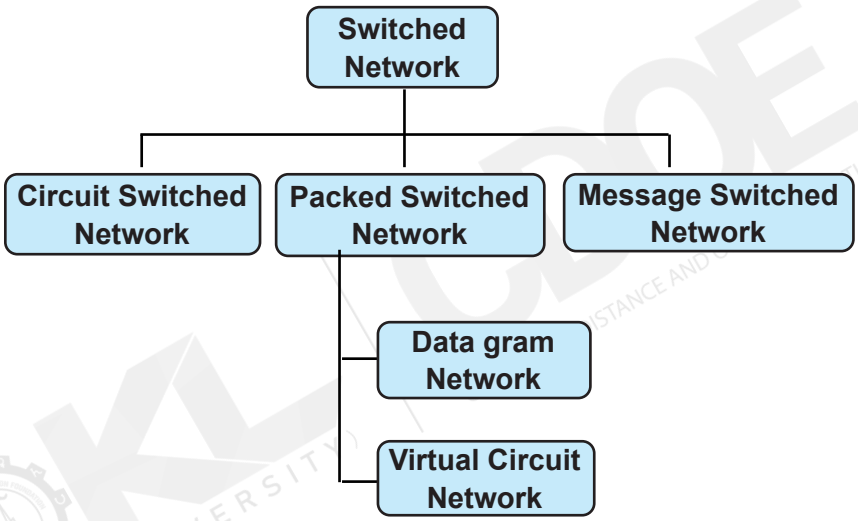


Fig. 9: Types of switching

- **Circuit Switching Model:** The circuit switching model is a telecommunications network model in which a dedicated physical path is established between two nodes for the duration of a communication session. This path is established through switches that direct the signal along a specific route. This model provides a reliable and secure connection, as the transmitted data will always follow the same path.
- **Packet Switching:** Packet switching is a method of data transmission in which data is broken into small chunks called packets, which are then sent over a network and reassembled at the destination. The packets may take different paths to the destination and can be routed around network congestion or faults. Packet switching is today's most common type of data transmission, with applications ranging from global communication networks to local area networks.
    - **Datagram Packet Switching:** In Datagram Packet switching, each data frame is taken as an individual entity and processed separately. No connection is established before data transmission occurs. Although this approach provides flexibility in data transfer, it may cause a loss of data frames or late delivery.

- **Virtual-Circuit Packet Switching:** In Virtual-Circuit Packet switching, a logical connection between the source and destination is made before transmitting any data. These logical connections are called virtual circuits. Each data frame follows these logical paths and provides a reliable way of transferring data with less chance of data loss.
- **Message Switching:** Message switching is a form of data transmission in which messages are stored and then forwarded from one node in a network to the next. It enables the network to route data around congested or failed parts by storing the message until a path is found. Message switching is much more dependable than circuit switching, as messages are only sent when the destination node is available.

Self-Assessment Questions

7. Which switching type involves establishing a dedicated physical path between two nodes for a communication session?

   A). Packet Switching
   B). Circuit Switching
   C). Message Switching
   D). Datagram Packet Switching

8. In which type of packet switching does each packet function as an individual entity and is processed separately without establishing a connection beforehand?

   A). Virtual-Circuit Packet Switching
   B). Datagram Packet Switching
   C). Circuit Switching
   D). Message Switching

9. Which switching technique involves storing a message at intermediate nodes before forwarding it to the destination, ensuring reliability when the destination is not immediately available?

   A). Circuit Switching
   B). Datagram Packet Switching
   C). Virtual-Circuit Packet Switching
   D). Message Switching

1.2.4 Transmission in ISDN

Integrated Services Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional public switched telephone network (PSTN) circuits. ISDN was developed to replace the analogue system with a more efficient and versatile digital one, offering better quality and higher speeds.

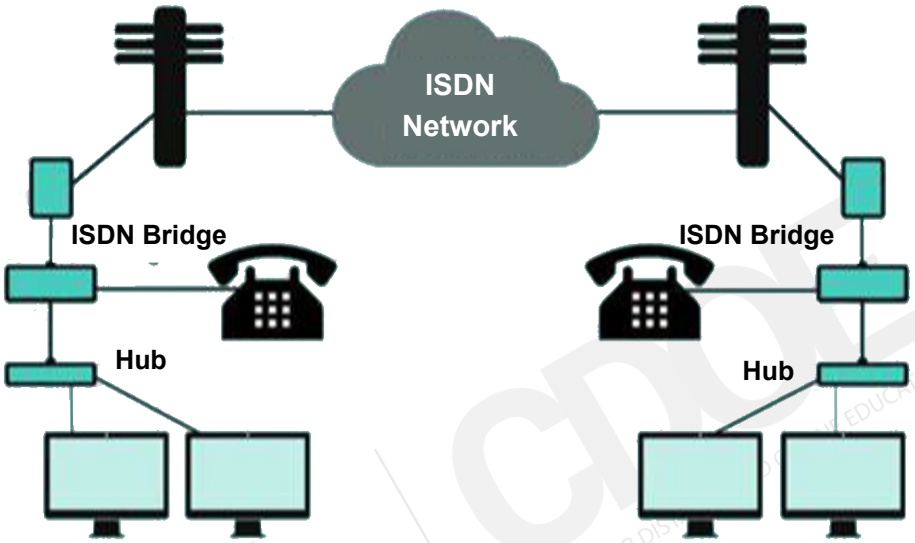


Fig. 10: Working of ISDN

Key Features of ISDN

- **Digital Transmission:** ISDN uses digital signals rather than analogue, providing more apparent voice quality and higher data rates.
- **Integration of Services:** It integrates multiple services (voice, data, video) into a single connection, allowing for simultaneous use of these services over a single line.
- **Faster Connection Setup:** ISDN offers speedier call setup times than traditional analogue lines, making it suitable for data transfer and business communications.
- **Higher Data Rates:** It supports higher data transmission rates than analogue modems, with Basic Rate Interface (BRI) providing up to 128 kbps and Primary Rate Interface (PRI) offering even higher speeds.

Broadband ISDN (B-ISDN)

Broadband ISDN (B-ISDN) was developed in the late 1980s and early 1990s to provide high-speed digital transmission for a wide range of services, including voice, data, and video, over a single integrated network. It aimed to support higher data rates than traditional narrowband ISDN, making it suitable for applications requiring substantial bandwidth.

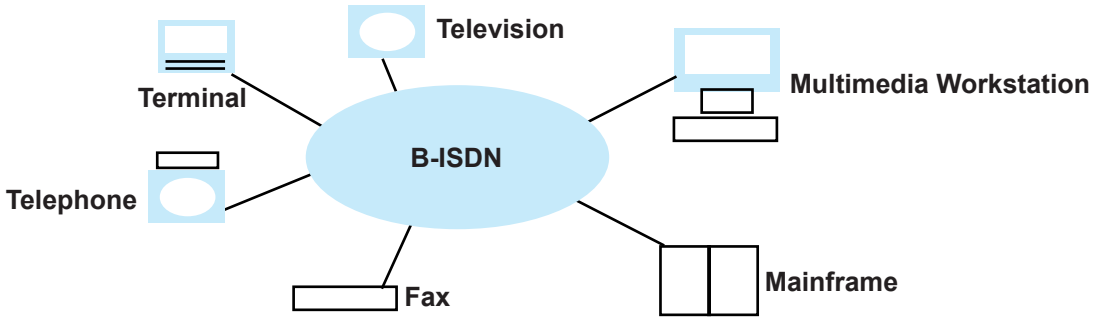


Fig. 11: Broadband ISDN

Key Features of Broadband ISDN

- **High Data Rates:** B-ISDN was designed to support data rates significantly higher than traditional ISDN, typically in the range of megabits per second (Mbps) to gigabits per second (Gbps).
- **Integrated Services:** It aimed to provide integrated digital services for voice, video, and data transmission over a single network infrastructure.
- **Asynchronous Transfer Mode (ATM):** ATM was the primary technology used in B-ISDN. It uses fixed-size cells (53 bytes) for data transmission, ensuring efficient and flexible handling of various types of traffic.
- **Fiber Optic Infrastructure:** B-ISDN relied heavily on fibre optic technology to achieve high data rates and support long-distance transmission.

B-ISDN vs. Traditional ISDN

- **Data Rates:** B-ISDN offers significantly higher data rates than traditional ISDN.
- **Technology:** B-ISDN relies on ATM and fibre optics, while traditional ISDN uses circuit switching and copper lines.
- **Services:** B-ISDN supports a broader range of services, including high-definition video and large-scale data transfer.

Self-Assessment Questions

10. What is one of the critical advantages of ISDN compared to traditional analogue systems?

    A). Integration of multiple services into a single connection
    B). Slower connection setup times
    C). Lower data transmission rates
    D). Only supports voice transmission

11. Which technology is primarily used in Broadband ISDN (B-ISDN) to manage several types of traffic efficiently?

    A). Circuit Switching
    B). Asynchronous Transfer Mode (ATM)
    C). Datagram Packet Switching
    D). Fibre Channel

12. What is a significant difference between B-ISDN and traditional ISDN?

    A). Traditional ISDN supports higher data rates
    B). B-ISDN relies on copper lines, while traditional ISDN uses fibre optics
    C). B-ISDN supports a broader range of services, including high-definition video
    D). Traditional ISDN uses ATM technology for data transmission

1.2.5 Asynchronous Transfer Mode (ATM) Network

Asynchronous Transfer Mode (ATM) is a high-speed networking standard designed for transmitting a wide range of digital data, including voice, video, and computer data, over a single network. ATM is based on cell switching and multiplexing, where data is divided into small, fixed-size cells for efficient and predictable transmission.

Key Features of ATM

- **Fixed-Size Cells:** ATM uses small, fixed-size cells of fifty-three bytes (5 bytes for the header and forty-eight bytes for the payload). The fixed cell size simplifies hardware design and enables fast switching.
- **High-Speed Transmission:** ATM supports high data rates, making it suitable for local and wide-area networks. Typical speeds range from 25 Mbps to several Gbps.
- **Quality of Service (quality of service):** ATMs provide various levels of quality of service to accommodate distinct types of traffic, such as real-time voice, video, and non-real-time data.
- **Scalability:** The architecture of ATM is scalable, supporting a range of speeds and network sizes.
- **Asynchronous Transmission:** Cells are transmitted asynchronously relative to one another, allowing efficient use of network resources.

Self-Assessment Questions

13. What is the size of an ATM cell used for data transmission?

    A). Sixty-four bytes
    B). Fifty-three bytes
    C). 128 bytes
    D). Thirty-two bytes

14. Which of the following is a crucial feature of ATM that allows it to manage diverse types of traffic, like real-time voice and video?

    A). Fixed transmission rates
    B). Quality of Service (quality of service)
    C). Variable-size cells
    D). Synchronous data transmission

Summary

- Data is transmitted using guided (wired) or unguided (wireless) mediums, with factors like transmission rate, cost, and distance affecting choice.
- Guided media includes twisted pair, coaxial, and fibre optic cables, each suited for specific network needs.
- Unguided media uses wireless transmission via radio and microwaves for multicast and unicast communication.
- Wireless transmission technologies like RF, Bluetooth, Wi-Fi, and cellular enable short- and long-range communication.
- Multiplexing combines signals over a single channel to optimise bandwidth, using techniques like Frequency, Time, Wavelength, and Code Division Multiplexing.
- Circuit switching uses dedicated paths, while packet switching sends data in packets, improving flexibility.
- Multiplexing can face issues like interference and latency but enhances network efficiency, cost-effectiveness, and scalability.

Terminal Questions

1. What are the critical differences between guided and unguided transmission media in performance and application?
2. How do fibre optic cables compare to coaxial and twisted pair cables regarding bandwidth, cost, and distance capabilities?
3. What are the main types of wireless transmission technologies, and how do they differ regarding range and data transmission rates?
4. Explain the concept of multiplexing and describe how Frequency Division and Time Division Multiplexing are used to optimise network bandwidth.
5. What are the primary differences between circuit and packet switching, and how do these techniques affect network performance?
6. What challenges are associated with multiplexing, and how can they impact the efficiency of a communication network?
7. In what ways does multiplexing enhance the scalability and cost-effectiveness of modern data and telecommunications systems?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	A
2	C
3	D
4	B
5	C
6	A
7	B
8	B
9	D
10	A
11	B
12	C
13	B
14	B

Activity

Activity type: Online **Duration: 2 Days**

Scenario

You are part of a network design team tasked with implementing a new communication system for a growing organisation. The company has multiple branches that require reliable communication to share data, collaborate on projects, and conduct meetings. The team must choose appropriate transmission media, decide on multiplexing techniques, and evaluate switching methods to ensure efficient data transmission across the network.

By referring to the given scenario, perform the following activity:

what recommendations would you provide to the organisation regarding future scalability and upgrades of their communication system

Glossary

- **Signal Attenuation:** The reduction in strength of a signal as it travels through a transmission medium, which can lead to loss of data quality.
- **Modulation:** The process of varying a carrier signal to transmit information, often used in radio and telecommunications.
- **Noise:** Unwanted electrical signals that interfere with the clarity of the transmitted data, potentially leading to errors.
- **Propagation Delay:** The time it takes for a signal to travel from the sender to the receiver can impact overall communication speed.
- **Throughput:** The actual rate of successful data transfer achieved over a network, often measured in bits per second, can be affected by several factors, including network congestion.
- **Interference:** Signal disruptions caused by overlapping frequencies or environmental factors can degrade the quality of wireless communication.
- **Latency :** The delay before a data transfer begins following an instruction for its transfer, often measured in milliseconds.
- **Transmission Rate:** The speed at which data is transmitted over a communication channel, affecting the performance and efficiency of the network.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Transmission Media:** https://www.geeksforgeeks.org/types-transmission-media/
- **Broadband ISDN:** https://www.tutorialspoint.com/what-is-bisdn-in-computer-network

Video Links

Topic	Link
Transmission Media	https://youtu.be/CX0kpovjVzg?si=n6B8FgXLIFx-PEMC
Transmission ISDN	https://youtu.be/a4E4fxU8IEE?si=sSw0_oY-8cN-sol4D

Image Credits

Fig. 1: Types of transmission media	https://th.bing.com/th/id/OIP.QMhc6k7oLR-rXiIXgpZvGWQAAAA?rs=1&pid=ImgDet-Main
Fig. 2: Unshielded twisted pair	https://th.bing.com/th/id/OIP.1btAPOHAI-0bOdNi5sXZyDQAAAA?rs=1&pid=ImgDet-Main
Fig. 3: Shielded twisted pair	https://www.dintek.com.tw/images/2023/06/30/twisted1.jphttps://th.bing.com/th/id/OIP.l3MsA2bO6uQNoB8ZpT0A-WAHaGs?rs=1&pid=ImgDetMain
Fig. 4: Coaxial cable	https://usercontent2.hubstatic.com/4889617.jpg
Fig. 5: Fibre optic cable	https://www.fastcabling.com/wp-content/uploads/2022/09/2-How-to-Choose-the-Right-Fiber-Optic-Cables.jpg
Fig. 6: Multiplexing	https://image1.slideserve.com/1910684/multiplexing1-l.jpg
Fig. 7: Frequency Division Multiplexing	https://image3.slideserve.com/6353491/frequency-division-multiplexing-l.jpg
Fig. 8: Time Division Multiplexing	https://image3.slideserve.com/6353491/time-division-multiplexing-l.jpg
Fig. 9: Types of switching	https://media.geeksforgeeks.org/wp-content/uploads/20230522105035/Types-of-switching.png
Fig. 10: Working of ISDN	https://th.bing.com/th/id/OIP._YT3M0ENzZ-WO2aX8BjZHwHaE7?rs=1&pid=ImgDetMain
Fig. 11: Broadband ISDN	https://pi4.informatik.uni-mannheim.de/pi4.data/content/courses/1996-ss/rn96/CN-Title/graphic/bisdnceb.gif

Keywords

- Electromagnetic signals
- Network communication
- Data transmission
- Wireless communication
- Radio Frequency (RF)
- Bluetooth
- Wi-Fi

MODULE 1

Introduction to Computer Networks and Data Communications

Unit 3

Data Transmission Control and Reliability

Unit Table of Contents

Unit 1.3 Data Transmission Control and Reliability

Aim

This unit aims to identify the functions of the Data Link Layer, Error Detection and Correction mechanisms, and the Sliding Window Protocol in ensuring reliable data transmission in computer networks.

Instructional Objectives

This unit intends to:

- Discuss the role of the Data Link Layer in network communication
- Define different types of error detection and correction techniques used in data transmission
- Explain how the Sliding Window Protocol ensures reliable delivery of frames across a network

Learning Outcomes

Upon completion of the unit, you will be able to:

- Identify the functions and responsibilities of the Data Link Layer in the OSI model
- Explain various methods used for detecting and correcting errors during data transmission
- Evaluate the effectiveness of the Sliding Window Protocol in managing data flow and handling lost or corrupted frame

1.3.1 Data Link Control

Data Link Control (DLC) is a layer in the OSI (Open Systems Interconnection) model responsible for ensuring reliable data transfer across a physical link. It is part of the Data Link Layer (Layer 2) and provides various mechanisms to manage data transmission between two devices over a network.

Critical Functions of Data Link Control

- **Framing:** DLC organises the data into frames, which are structured data units with a defined beginning and end. This lets the receiving device know where one frame ends and another begins.
- **Error Detection and Correction:** DLC includes mechanisms to detect errors that may occur during transmission. Standard methods include parity checks, cyclic redundancy checks (CRC), and checksums. If errors are detected, the DLC may request retransmission.
- **Flow Control:** Flow control mechanisms ensure the sender does not overwhelm the receiver with too much data too quickly. Techniques such as sliding windows and stop-and-wait are used to manage this.
- **Acknowledgement:** DLC protocols typically require the receiving device to return acknowledgements to the sender, confirming that frames were received correctly.
- **Addressing:** Each device on a network is identified by a unique address, often referred to as a MAC (Media Access Control) address. DLC ensures that frames are delivered to the correct device.
- **Medium Access Control (MAC):** In networks where multiple devices share the same communication medium, DLC provides rules for how devices take turns transmitting data to avoid collisions.

Common Data Link Protocols

- **Ethernet (IEEE 802.3):** Widely used in wired LANs.
- **Wi-Fi (IEEE 802.11):** Used for wireless networking.
- **PPP (Point-to-Point Protocol):** Used for direct communication between two network nodes.
- **HDLC (High-Level Data Link Control):** A bit-oriented protocol used for communication over point-to-point and multipoint links.

Self-Assessment Questions

1. Which of the following is a primary function of Data Link Control?

   A). Routing data between networks
   B). Error detection and correction
   C). Encrypting network traffic
   D). Managing user permissions

2. What method is commonly used by the Data Link Control layer to avoid collisions in networks where multiple devices share the same medium?

   A). Flow control
   B). Framing
   C). Medium Access Control (MAC)
   D). Routing

3. Which protocols operate at the Data Link Control layer?

   A). HTTP
   B). Ethernet (IEEE 802.3)
   C). IP (Internet Protocol)
   D). DNS

1.3.2 Error Detection and Correction

- Error is a condition when the receiver's information does not match the senders. Digital signals suffer from noise during transmission that can introduce errors in the binary bits travelling from sender to receiver.
- That means a 0 bit may change to 1, or a 1 bit may change to 0.
- Data (Implemented at the Data link layer or Transport Layer of the OSI Model) may get scrambled by noise or corrupted whenever a message is transmitted.
- To prevent such errors, error-detection codes are added as extra data to digital messages. This helps in detecting any errors that may have occurred during message transmission.

In Computer Networks, the errors can be classified into three types-

- Single-bit error
- Multiple-bits error
- Burst error

Single-Bit Error: A single-bit error occurs when one bit (i.e., a single binary digit) of a transmitted data unit is altered during transmission, resulting in an incorrect or corrupted data unit.

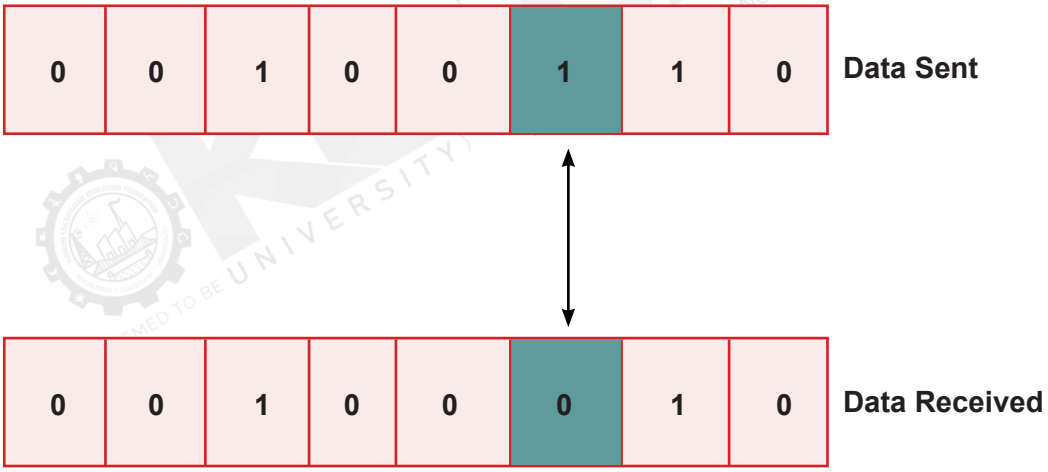


Fig. 1: Single-Bit Error

Multiple-Bits Error: Multiple-bit errors occur when two or more bits of a data sequence are changed during data transmission.

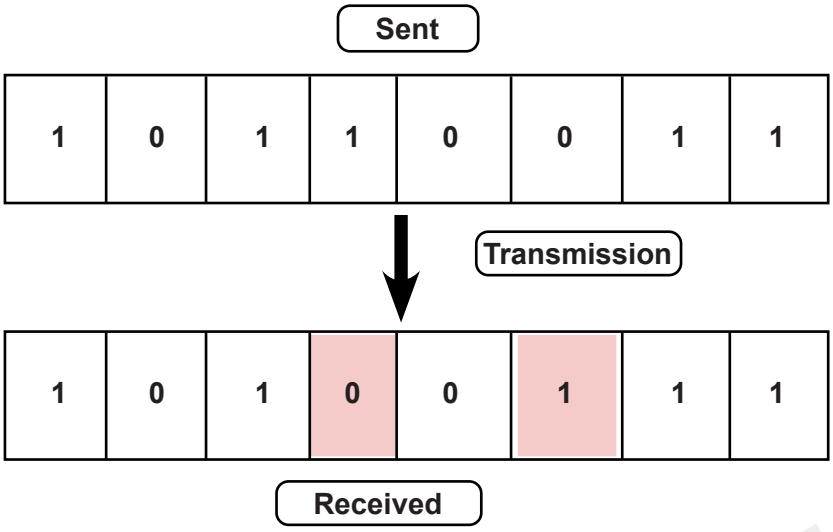


Fig. 2: Multiple-Bit Errors

Burst Error: Burst errors occur when more than one consecutive bit of a data sequence changes during data transmission. They can occur due to physical damage, like a scratch on a disc or a stroke of lightning in the case of wireless channels.

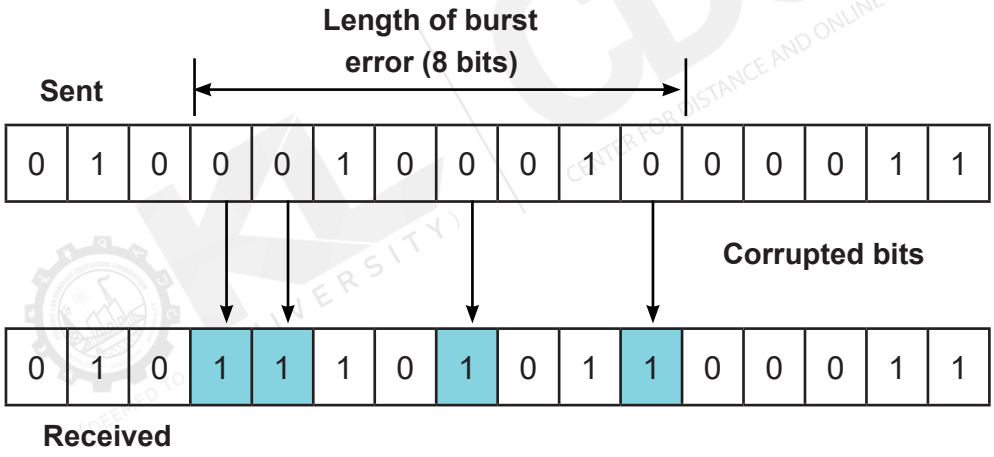


Fig. 3: Burst Error

Error Detection and error correction are the two types of error control mechanisms.

1.3.2.1 Error Detection Method

Introducing redundancy bits that provide additional information is a common technique to detect errors. Various techniques for error detection include:

- Simple Parity Check
- Two-Dimensional Parity Check
- Checksum
- Cyclic Redundancy Check (CRC)

Simple Parity Check: It is the simplest error detection method. It allows the user to add an extra bit to the data transmission. adding an extra bit is as follows:

- If the block has several ones oddly, then one should be added.
- If the block has several 1's in an even manner, then zero should be added.
- Finally, it displays all the numbers in even form. Hence, it will be called the even parity checking.

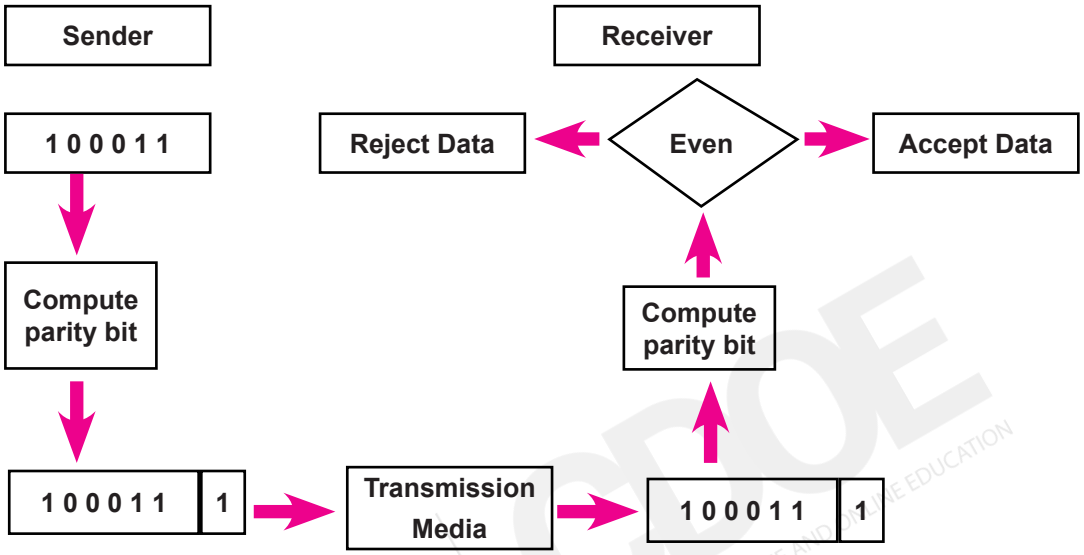


Fig. 4: Simple Parity Check

Simple parity checks have the following benefits:

- It is the most common method for detecting odd number errors.
- Single-bit errors can also be identified using this method.
- This is the fastest method for detecting errors due to less data processing and avoids communication delays.

Drawbacks of Simple Parity Check

- A single parity check cannot detect even the number of bit errors.
- For instance, 101010 is the data that needs to be sent. 1010101 is the codeword that was sent to the recipient (even parity was used). Assume that two of the codeword's bits flipped to 1111101 during transmission. The receiver makes the incorrect assumption that there is no error because the number of ones is even when they receive the codeword.

Two-Dimensional Parity Check: The data is arranged in a table using the Two-Dimensional Parity Check. Like a single-parity check, parity bits are calculated for each row. After splitting a block of bits into rows, the redundant row of bits is appended to the block. The parity bits obtained at the end will be compared to bits calculated from the received data.

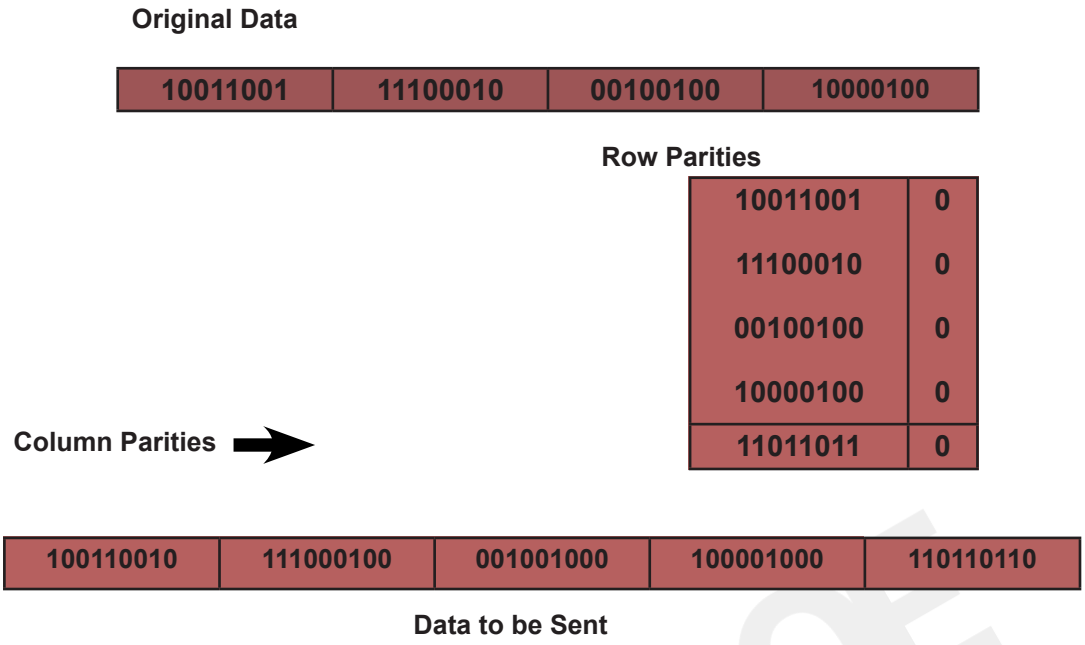


Fig. 5: Two-Dimensional Parity Check

Benefits

- It is famous for both the detection and correction of single-bit errors.
- When you investigate the matrix, two to three-bit errors will be found in any place in the matrix using this type of parity check.

Drawbacks

- If two bits in one data unit are corrupted, let's assume that two bits in the same location in another data unit will also be impacted.
- The error will then go undetected by the 2D Parity checker.
- This plan won't work if the parity component is off.

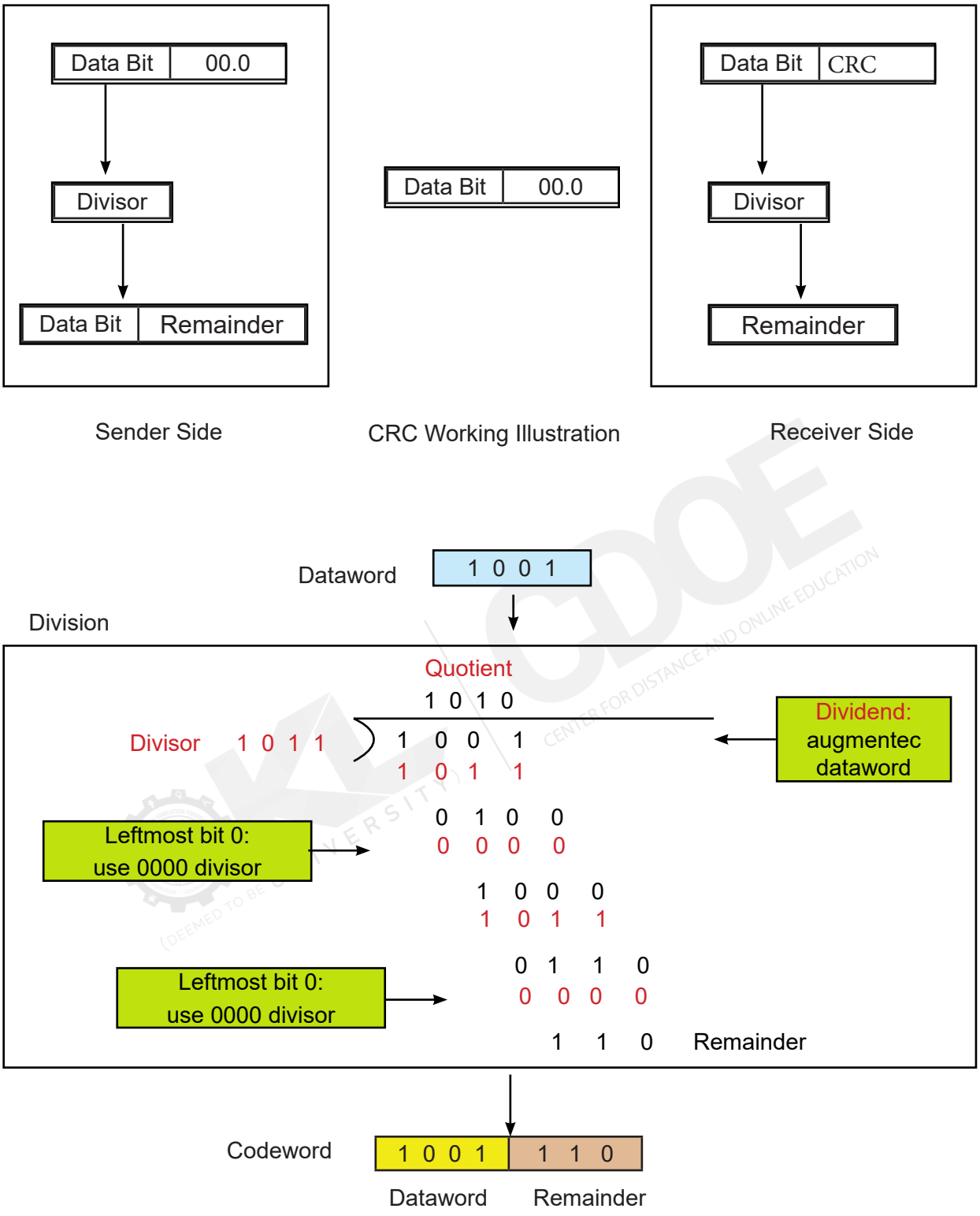
CRC Method: This is the method by which errors in the network will be detected while the process of transmission occurs. The checking will be done by applying the binary solution to the data that has been transmitted on the transmitter side and verifying using the same process on the recipient side.

The full form of CRC is as follows:

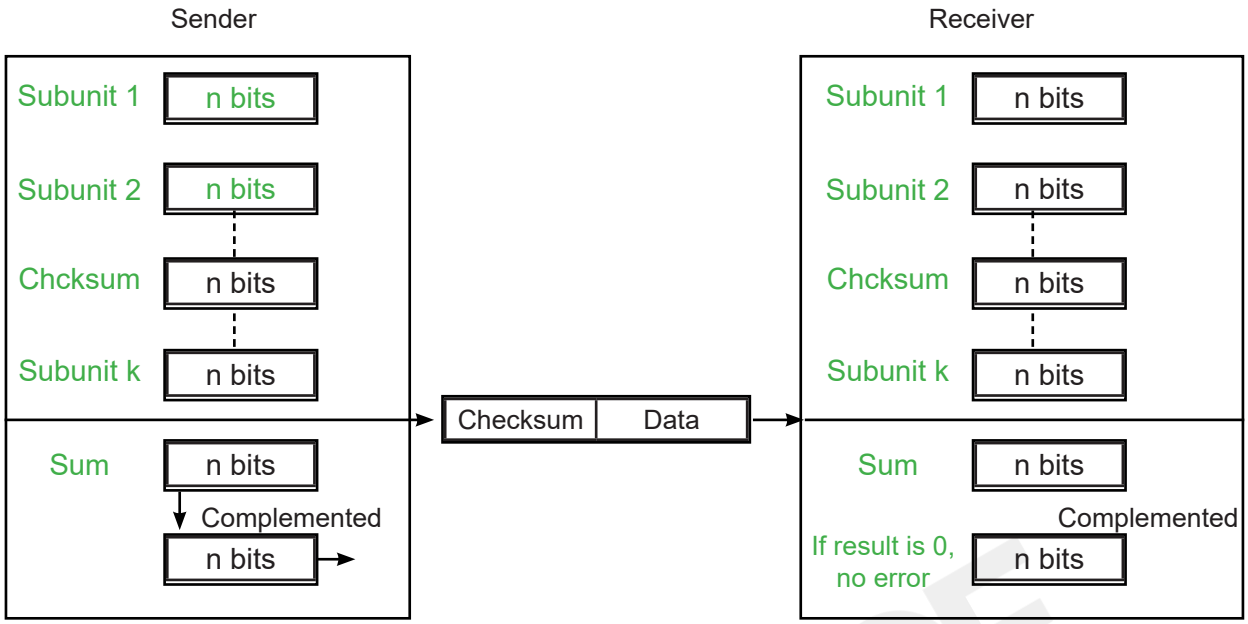
C=Check

R= Redundancy, which is used to recheck the method.

C- cyclic points, which are applied to the algorithmic formula.



Check Sum Method: The error detection method for upper-layer protocols is considered more reliable than LRC, VRC and CRC. This method makes use of a Checksum Generation on the Sender side and a Checksum Checker on the Receiver side



Original Data

10011001	11100010	00100100	10000100
1	2	3	4

k=4, m=8

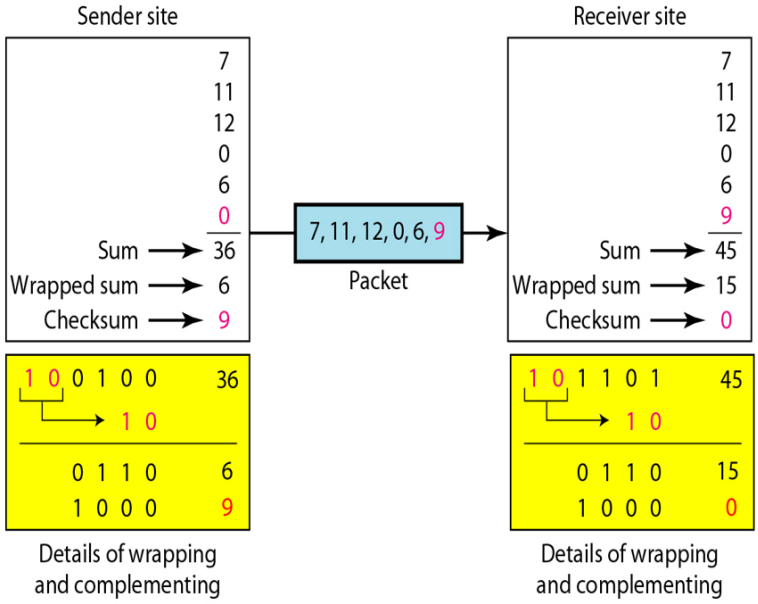
Sender

```
1        10011001
2        11100010
        (1)01111011
                 1
         01111100
3        00100100
         10100000
4        10000100
        (1)00100100
                 1
Sum:     00100101
CheckSum: 11011010
```

Reciever

```
1        10011001
2        11100010
        (1)01111011
                 1
         01111100
3        00100100
         10100000
4        10000100
        (1)00100100
                 1
         00100101
         11011010
Sum:     11111111
Complement:00000000
```

Conclusion: Accept Data



1.3.2.2 Error Correction

Once errors are detected in the network, the deviated bit sequence must be replaced with the right bit sequence so the receiver can accept and process the data. This method is called Error Correction.

This type of error can be corrected in two ways:

- After identifying the error, the recipient can send correspondence to request retransmission of the complete data unit. This process is called the backward error detection technique.
- This technique requires no effort and is free for wired transmissions. However, dealing with wireless transmission is expensive, so rather than using this method, one looks for a forward error detection method that offers auto-correcting codes for specific errors.

Self-Assessment Questions

4. Which error detection method adds a bit to ensure that the number of 1s is even or odd?

   A). Checksum
   B). Cyclic Redundancy Check (CRC)
   C). Simple Parity Check
   D). Two-Dimensional Parity Check

5. Which type of error occurs when two or more bits are altered during transmission?

   A). Single-bit error
   B). Burst error
   C). Multiple-bits error
   D). Parity error

6. In which error correction technique does the recipient request the retransmission of the complete data unit upon detecting an error?

   A). Forward error detection
   B). Backward error detection
   C). CRC method
   D). Checksum method

1.3.3 Sliding Window Protocol

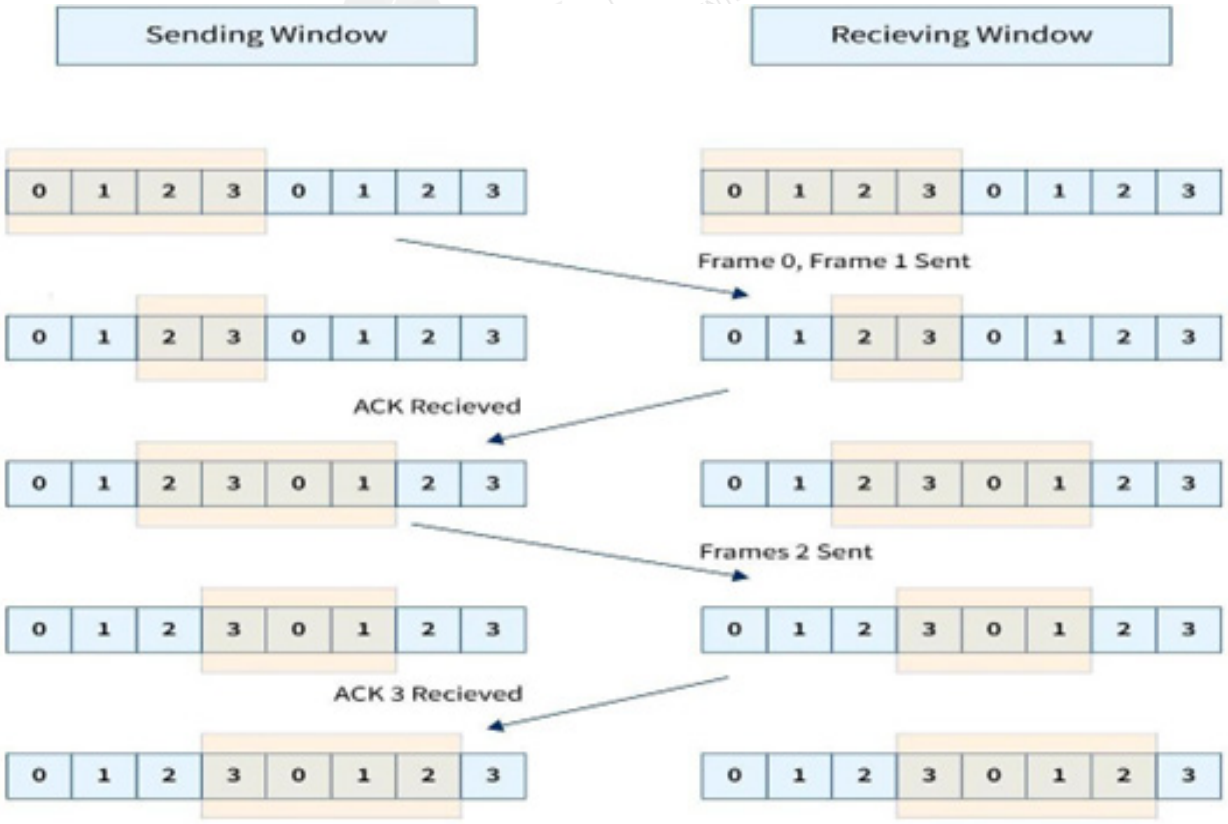
Sliding windows are a method of sending multiple frames at once. It manages data packets between the two devices, ensuring the delivery of data frames reliably and gradually.

- It's also found in TCP (Transmission Control Protocol).
- Each frame is sent from the sequence number using this technique.
- The sequence numbers are used on the receiving end to locate missing data.
- The sequence number is found to be used in the sliding window technique to avoid duplicate data.

Working Principle

- In these protocols, the sender's buffer is the sending window, and the receiver's is the receiving window.
- Assignment of sequence numbers to frames is between 0 and 2n-1 if the sequence number is an n-bit field. As a result, the sending window has a size of 2n-1. As a result, we choose an n-bit sequence number to accommodate a sending window size of 2n-1.
- Modulo-n is used to number the sequence numbers. If the sending window size is 3, the sequence numbers will be 0, 1, 2, 0, 1, 2, 0, 1, 2 and so on.

Let us take a simple example to understand how the sliding window protocol works.



Let us suppose that the sender's window size is four. The sequence number of the data frame will be in the range of 00 to (2N−1) (2N−1), i.e., 0, 1, 2, 3, 0, 1, 2, 3, and so on.
The steps of data transmission can be:

- The sender sends multiple frames.
- The receiver receives the frames and sends them back an ACK.
- Again, the sender sends the next frame.
- If the receiver does not send back an ACK in the specified time, then the sender sends back the frame as

The frame was either lost or damaged during the last transmission.

- This process continues until the receiver receives all the frames.
- The sliding window protocol is a valuable data link layer for sequential and reliable data frame delivery.
- The sliding window protocol is also used as the TCPor Transmission Control Protocol.
- Using the sliding window protocol, the sender can send multiple frames simultaneously.
- The sender associates a sequence number with the data frames so that the receiver can use this sequence number to arrange the frames in order if any were re-transmitted.
- The sequence number also helps the receiver identify the loss of damaged packets.
- When the receiver receives the frame, it returns an acknowledgement or ACK to the sender. The ACK lets the sender know that a particular frame was received correctly. There are two types of sliding window protocols: Go-Back-N ARQ and Selective Repeat ARQ.
- In the Go-Back-N ARQ, all the data frames starting from the lost frame are retransmitted, but in the Selective Repeat ARQ, we only resend the damaged or lost frames.
- In the Go-Back-N ARQ, the sender's window size is taken as N, but the receiver's window size is always one. Hence, the sender can send N data frames at a time, but the receiver can only receive one frame.
- In the Selective Repeat ARQ, the sender's window size is the same as that of the receiver, i.e., 2(m−1)2(m−1),
- where m is the number of bits used in the packet's header to express the packet's sequence number.

Self-Assessment Questions

7. What is the primary purpose of the sliding window protocol?

   A). Encrypting data before transmission
   B). Managing multiple frames sent between sender and receiver reliably
   C). Compressing data to save bandwidth
   D). Ensuring all frames are sent in parallel

8. What happens when a frame is lost or damaged during transmission in the Go-Back-N ARQ sliding window protocol?

   A). Only the lost frame is retransmitted
   B). All frames from the lost frame onward are retransmitted
   C). The sender stops sending any more frames
   D). The receiver corrects the lost frame automatically

9. What is the key difference between Go-Back-N ARQ and Selective Repeat ARQ in the sliding window protocol?

   A). Go-Back-N ARQ retransmits all frames after a lost frame, while Selective Repeat ARQ only retransmits the damaged or lost frames
   B). Go-Back-N ARQ is used for wireless networks, while Selective Repeat ARQ is used for wired networks
   C). Go-Back-N ARQ uses encryption, while Selective Repeat ARQ does not
   D). Selective Repeat ARQ retransmits all frames, while Go-Back-N ARQ retransmits only the lost frames

Summary

- Data Link Control (DLC) ensures reliable data transfer over a physical link by framing, error detection, flow control, and addressing.
- Single-bit, multiple-bit, and burst errors can occur during transmission and are detected using parity checks, CRC, and checksums.
- Simple parity checks can detect single-bit errors but struggle with even-number errors; two-dimensional parity adds extra error detection.
- The Cyclic Redundancy Check (CRC) method is widely used to detect errors by applying an algorithm at both sender and receiver ends.
- Error correction can occur through retransmission (backward) or auto-correction (forward) techniques.
- Sliding window protocols like Go-Back-N and Selective Repeat ensure reliable frame delivery, using sequence numbers and acknowledgements to detect lost frames.

Terminal Questions

1. What are Data Link Control's (DLC) key functions in ensuring reliable data transfer?
2. How does the sliding window protocol manage data transmission and ensure sequential delivery of frames?
3. What are the differences between single-bit, multiple-bit, and burst errors in data transmission?
4. How does the Cyclic Redundancy Check (CRC) method detect errors during data transmission?
5. What are the advantages and limitations of using simple parity checks for error detection?
6. How do Go-Back-N ARQ and Selective Repeat ARQ differ regarding retransmission in the sliding window protocol?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	C
3	B
4	C
5	C
6	B
7	B
8	B
9	A

Activity

Activity type: Online **Duration: 2 Days**

Scenario

Imagine you are part of a team managing data transmission between two networked devices in a large corporate environment. Recently, the network has experienced frequent transmission errors, leading to data corruption and communication delays. As part of the team, you are tasked with identifying and implementing mechanisms to improve the reliability of data transmission.

By referring to the given scenario, perform the following activity

What error detection and correction methods would you recommend ensuring data integrity during transmission, and why?

Glossary

- **Framing:** The process of dividing data into frames, discrete units with defined boundaries for transmission across a network.
- **Error Detection:** Techniques used to identify errors in data transmission, such as parity checks, checksums, and cyclic redundancy checks (CRC).
- **Flow Control:** Mechanisms, such as stop-and-wait and sliding window protocols, ensure the receiver transmits data at a manageable rate.
- **Acknowledgement (ACK):** The receiver sends signals to confirm the successful reception of data frames or packets.
- **Go-Back-N ARQ:** This is an error control protocol in which if a frame is lost or corrupted, the sender retransmits all frames starting from the lost one.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Error Detection and Correction:** https://www.geeksforgeeks.org/error-detection-in-computer-networks/
- **Sliding Window Protocol:** https://www.javatpoint.com/sliding-window-protocol

Video Links

Topic	Link
Error Detection and Correction	https://youtu.be/EMrY-8m8D1E?si=NbcPG6nHzcA9YjCt
Sliding Window Protocol	https://youtu.be/LnbvhoxHn8M?si=YhiAMTBm-JoWHAym6

Image Credits

Fig. 1: Single Bit Error	https://th.bing.com/th/id/R.730d2875f-d82ec613b5fe0c7368b-be97?rik=m%2bVZuJvkuk%2bx-rw&riu=http%3a%2f%2fecomputernotes.com%2fimages%2fSingle-bit-error.jpg&ehk=67wrPC%2bUys8yluwXihS%2b-4gDOVnIRdpafc7BhoSMVDYQ%3d&ris-l=&pid=ImgRaw&r=0&sres=1&sresct=1
Fig. 2: Multiple-Bit Errors	https://media.geeksforgeeks.org/wp-content/uploads/20230425113404/burst-error.png
Fig. 3: Burst Error	https://th.bing.com/th/id/R.4e1b68e4ad-f5ad54a7d5601ef1c25db3?rik=r9KNfjhN-JAVyeg&riu=http%3a%2f%2fwww.myread-ingroom.co.in%2fimages%2fstories%2f-docs%2fdcn%2fTypes+of+Errors_Burst+er-rors.JPG&ehk=Qg6JOrKsVfUSUjk8qH-GrIbnutTU5r%2fj6n7kE7jSzpEk%3d&ris-l=&pid=ImgRaw&r=0&sres=1&sresct=1
Fig. 4: Simple Parity Check	https://media.geeksforgeeks.org/wp-content/uploads/detect12.jpg
Fig. 5: Two-Dimensional Parity Check	https://th.bing.com/th/id/OIP.TSpnm8C5f_l1TaJGA6uOwAHaFE?rs=1&pid=ImgDet-Main
Fig. 6: CRC Method	https://www.knowelectronic.com/wp-content/uploads/2021/12/cyclic-redundancy-check-1024x442.png

Keywords

- Data Link Layer
- Burst Error
- Multiple-Bits Error
- Single-Bit Error
- Medium Access Control (MAC)
- Point-to-Point Protocol (PPP)
- High-Level Data Link Control (HDLC)

COMPUTER NETWORKS

MODULE 2

Data Communication and Networking

Module Description

The module discusses the standards involved in Local Area Networks (LANs) and Metropolitan Area Networks (MANs), as well as essential network design issues and protocols for internet communication. The first part focuses on the IEEE standards that govern LAN and MAN setups, which form the foundation of network communication in small to large-scale areas. You will explore standards such as IEEE 802.2, which defines Logical Link Control, IEEE 802.3 for Ethernet, IEEE 802.4 for Token Bus, IEEE 802.5 for Token Ring, and IEEE 802.6 for Metropolitan Area Networks using Distributed Queue Dual Bus (DQDB). Then, the module discusses high-speed LANs and high-speed network technology that supports faster data transfer and greater bandwidth.

The module discusses critical design issues for maintaining effective communication in the next part. In this section, you will learn the concepts of routing algorithms, which determine the process of delivering data packets within networks. You will also get a detailed explanation of different algorithms, such as static and dynamic routing, shortest path, distance vector, and link state algorithms.

In this section, the module focuses on maintaining effective internet-based communication and its role in the network. Then, it focuses on the Internet Protocol (IP), which enables data exchange between devices. This module also discusses IP addressing, IPv4, and IPv6 formats. Subnets, a crucial topic, are explained to aid effective network management by organising IP addresses. Finally, the concepts of internet working are presented, focusing on connecting several networks.

This module consists of **two** units.

Unit 2.1 Local and Metropolitan Networks
Unit 2.2 Network Design and Internet Protocol.

MODULE 2

Data Communication and Networking

Unit 1

Local and Metropolitan Area Networks

Unit Table of Contents

Unit 2.1 Local and Metropolitan Area Networks

Aim

This unit aims to explore the IEEE standards that enable structured, high-speed communication in local and metropolitan area networks.

Instructional Objectives

This unit intends to:

- Explain the role and impact of IEEE standards in the development of high-speed LAN technologies
- Describe the functions and advantages of different IEEE standards within LAN and MAN environments
- Discuss how these standards ensure reliable, high-speed data transmission across various network types

Learning Outcomes

Upon completion of the unit, you will be able to:

- Demonstrate an understanding of how IEEE standards support high-speed LAN and MAN connectivity
- Discuss and differentiate between the functions of IEEE standards, like Ethernet and Token-based protocols, in network performance
- Define the key features and purpose of IEEE standards within modern computer networks

2.1.1 IEEE Standards

The IEEE (Institute of Electrical and Electronics Engineers) standards for computer networks are a set of technical guidelines that help ensure different network devices (like routers, switches, and computers) can connect and work together smoothly. These standards define how data is transmitted across networks, such as Wi-Fi or Ethernet connections, and help ensure everything is compatible and reliable.

2.1.1.1 802.2 (Logical Link Control)

IEEE 802.2 is a standard developed by the Institute of Electrical and Electronics Engineers (IEEE). It defines computer networks' Logical Link Control (LLC) sublayer.

The functionality of IEEE 802.2 (Logical Link Control)

The primary function of IEEE 802.2 is to provide a consistent data transmission method across different types of networks by handling.

- Error control
- Flow control
- Framing.
- The LLC is one of the two sub-layers of the Data Link Layer (Layer 2) in the Open Systems Interconnection (OSI) model. It interfaces between the Medium Access Control (MAC) sub-layer and the Network Layer.

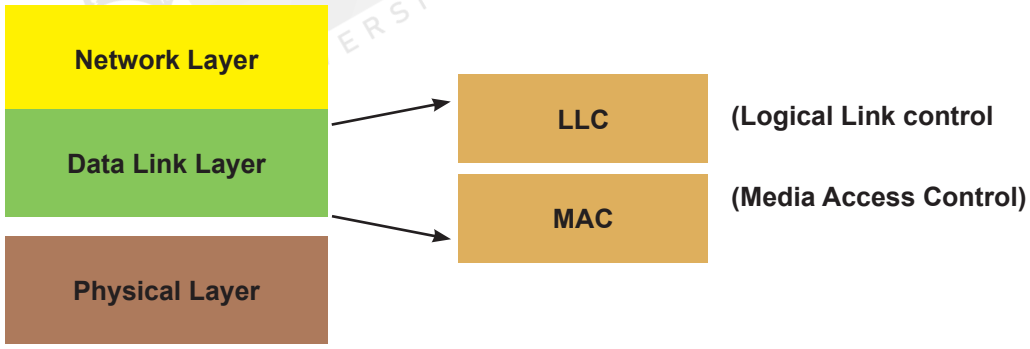


Fig. 1: Sublayers of Data Link Layer

- The LLC layer multiplexes the protocols over the MAC layer while sending and multiplexes the protocols while receiving them.
- The MAC address is defined as the Media Access Control address. It is a unique address allocated to the device's NIC. It is used to transmit data over Ethernet or Wi-Fi.

Functions of Logical Link Control

- **Multiplexing:** LLC's primary function is to multiplex protocols over the MAC layer during transmission. This allows several network protocols to operate simultaneously within a multipoint network over the same network medium.
- **De-multiplexing:** LLC de-multiplexes the protocols upon receiving data, ensuring each protocol gets the appropriate data.
- **Flow and Error Control:** LLC provides hop-to-hop flow and error control.
- **Frame Sequence Numbers:** It assigns frame sequence numbers to track acknowledgements in acknowledged services.

Services of Logical Link Control

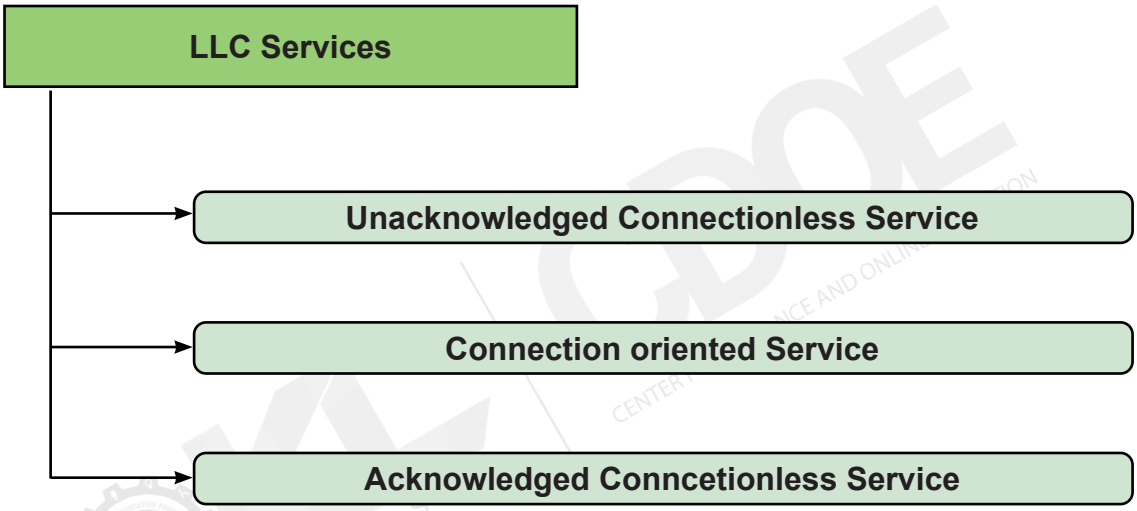


Fig. 2: Types of LLC Services

Unacknowledged Connectionless Service (LLC 1): The source machine sends or transmits data frames to the destination machine. However, in return, the destination machine does not acknowledge the source machine, so this service is known as unacknowledged. Along with this, there is no connection established between the source and destination machine,

Connection-Oriented Service (LLC 2): The source machine sends or transmits data frames to the destination machines, and in return, the destination machine provides an acknowledgement to the source machine, known as an acknowledged service. A connection is also established between the source and destination machine before data transfer. Therefore, it is known as a connection-oriented service.

Acknowledged Connectionless Service (LLC 3): The source machine sends or transmits data frames to the destination machines, and in return, the destination machine provides an acknowledgement to the source machine, so this service is known as an acknowledged service. Also, no connection has been established between the source and destination machine; therefore, it is known as a connectionless service.

2.1.1.2 802.3 (Ethernet)

Ethernet is a set of technologies and protocols used primarily in LANs. It was first standardised in the 1980s by the IEEE 802.3 standard, which defines the physical layer and the medium access control (MAC) sub-layer of the data link layer for wired Ethernet networks.

Ethernet is classified into two categories:

- **Classic Ethernet:** Classic Ethernet is the original form of Ethernet that provides data rates between 3 and 10 Mbps. The varieties are commonly referred to as 10BASE-X. Here, 10 is the maximum throughput, i.e., 10 Mbps, BASE denotes the use of baseband transmission, and X is the medium used.
- **Switched Ethernet:** Switched Ethernet uses switches to connect to the stations in the LAN. It replaces the repeaters used in classic Ethernet and allows full bandwidth utilisation.

Preamble	SFD	Destination Address	Source Address	Length	Data	CRC
7 Bytes	1 Byte	6 Bytes	6 Bytes	2 Bytes	46 - 1500 Bytes	4 Bytes

Fig. 3: IEEE 802.3 Frame Format

- **Preamble (7 bytes):** The frame begins with a preamble of 7 bytes (56 bits) of alternating 1s and 0s. The preamble allows devices on the network to synchronise their clocks before data transmission begins.
- **Start Frame Delimiter (SFD) (1 byte):** This 1-byte field marks the end of the preamble and the start of the actual Ethernet frame. The value of the SFD is always 10101011 in binary, which signals the beginning of the MAC addresses.
- **Destination MAC Address (6 bytes):** This field contains the destination device's 48-bit (6-byte) MAC address. It identifies the frame's intended recipient on the network.
- **Source MAC Address (6 bytes):** This field contains the source device's 48-bit (6-byte) MAC address, i.e., the device that sent the frame. It identifies the frame sender.
- **Length/Type (2 bytes):**
  - **Length:** In IEEE 802.3 frames, this field specifies the data size (payload) in bytes (ranging from 46 to 1500).
  - **Type:** In Ethernet II frames (an alternative format), this field indicates the protocol type carried in the payload (e.g., IPv4, IPv6).
- **Data/Payload (46 to 1500 bytes):** This field contains the transmitted data, such as an IP packet. The minimum size is forty-six bytes, and the maximum is 1500 bytes. If the data is less than 46 bytes, padding is added to meet the minimum size requirement.
- **Frame Check Sequence (FCS) (4 bytes):** The FCS is a 4-byte cyclic redundancy check (CRC) value used for error detection. The receiving device can verify the frame's integrity by checking for transmission errors. If errors are detected, the frame is discarded.

There are several versions of the IEEE 802.3 protocol. The most popular ones are

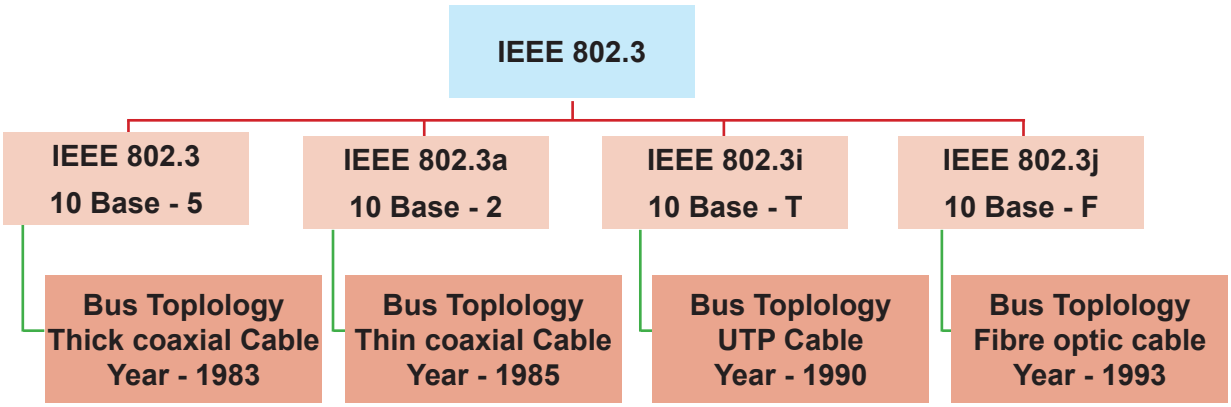


Fig. 4: Versions of IEEE 802.3

2.1.1.3 802.4 (Token Bus)

- The token bus is a popular standard for token-passing LANs. It was standardised by IEEE standard 802.4 and is used for industrial applications.
- In a token bus LAN, stations create a virtual ring, and tokens are then passed from one station to another using this virtual ring.
- Every station or node in the token bus network knows the address of its “left” and “right” station.
- A node or station can transmit data only when it holds a token. The workings of the Token Bus are like those of a token ring.

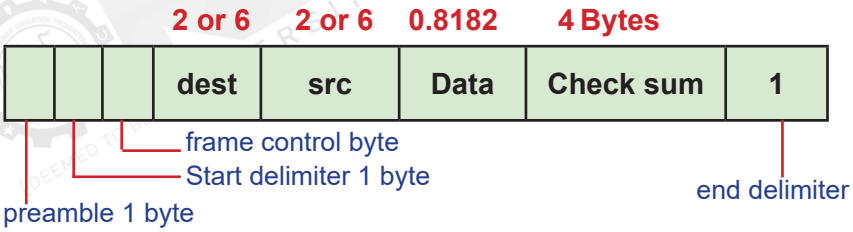


Fig. 5: Frame format of Token Bus

- **Preamble:** One byte for synchronisation.
- **Start Delimiter:** One byte that marks the beginning of the frame.
- **Frame Control:** One byte specifies the type of transmitted frame (e.g., data frame, token frame, or control frame).
- **Destination Address:** Two to six bytes that specify the address of the destination station.
- **Source Address:** Two to six bytes that specify the address of the source station.
- **Payload:** A variable length field that carries the data from the network layer.
- **Checksum:** Four-byte frame check sequence for error detection.
- **End Delimiter:** One byte that marks the end of the frame

Token Passing Mechanism in Token Bus

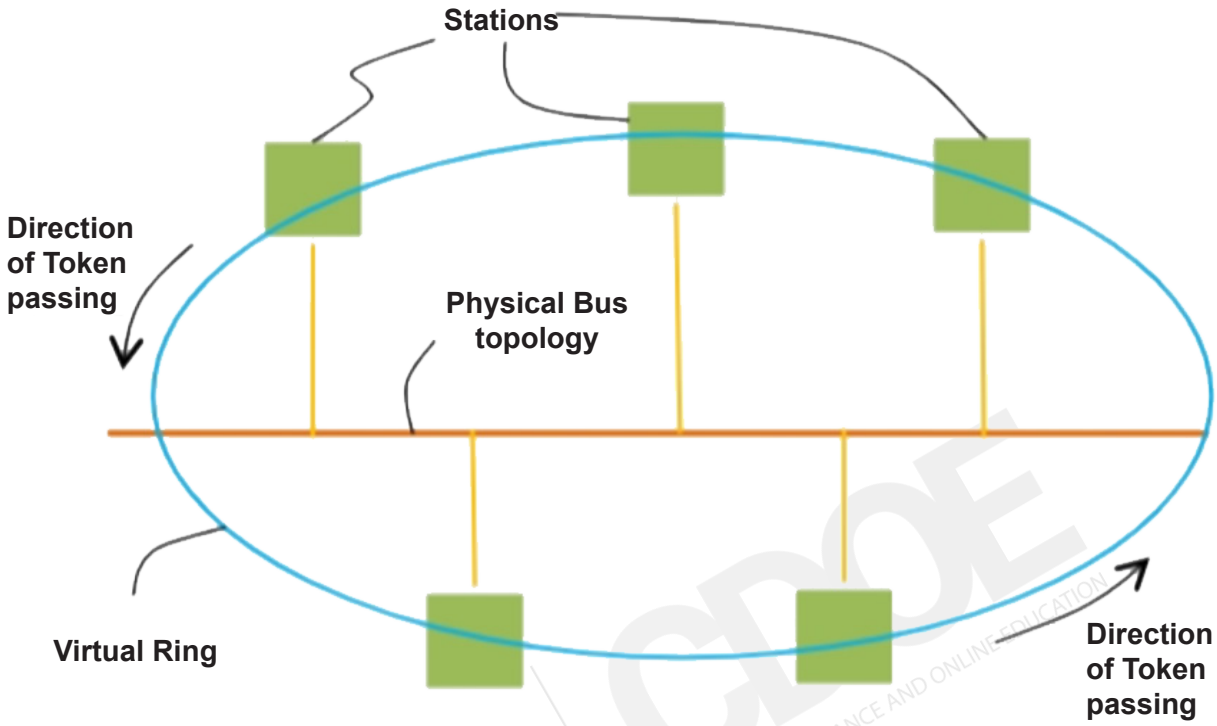


Fig. 6: Token Passing Mechanism

- A token is a small message circulating among the stations of a computer network that provides permission for transmission to the stations.
- If a station has data to transmit when it receives a token, it sends the data and then passes it to the next station; otherwise, it simply passes the token to the next station.
- The token is passed from one user to another in a sequence (clockwise or anticlockwise).
- The physical medium uses coaxial cables and has a bus or tree architecture.

Key Features

- Token Passing Mechanism: IEEE 802.4 uses a token-passing protocol, where a particular data packet, known as a token, circulates through the network. A device can only transmit data when it holds the token, ensuring that only one can transmit simultaneously, thereby avoiding collisions.
- Bus Topology: The standard defines a bus topology network, meaning all devices are connected to a shared communication medium (bus).
- Deterministic Access: The token-passing method provides deterministic access to the network, meaning that each device knows when it will have the opportunity to transmit data.

2.1.1.4 802.5 (Token Ring)

- Token ring (IEEE 802.5) is a communication protocol in a local area network (LAN) where all stations are connected in a ring topology and pass one or more tokens for channel acquisition.
- A token is a particular frame of three bytes circulating along the station ring. A station can send data frames only if it holds a token, which is released upon successful receipt of the data frame.

Differences Between Token Ring and Token Bus

Token Ring	Token Bus
The token is passed over the physical ring formed by the stations and the coaxial cable network.	The token is passed along the virtual ring of stations connected to a LAN.
The stations are connected by ring topology or sometimes star topology.	The underlying topology that connects the stations is either bus or tree topology.
It is defined by IEEE 802.5 standard.	It is defined by IEEE 802.4 standard.
The maximum time a token reaches a station can be calculated here.	It is not feasible to calculate the time token transfer.

Table 1: Differences between Token Ring and Token Bus

2.1.1.5 802.6 (MAN, DQDB)

IEEE 802.6 is a standard for a Metropolitan Area Network (MAN) known as the Distributed Queue Dual Bus (DQDB). It was developed by the Institute of Electrical and Electronics Engineers (IEEE) as part of its IEEE 802 series and focuses explicitly on networks that cover a city or large campus area.

Key Features of IEEE 802.6 (DQDB)

- **Dual Bus Architecture:** It uses two unidirectional buses (Bus A and Bus B) for network connectivity. Data can travel in opposite directions on these buses, enhancing redundancy and reliability.
- **Distributed Queueing**: The standard incorporates a distributed queueing mechanism, where each node on the network manages the queue for sending data. This ensures fair access to the network and minimises collisions.
- **High Data Rates**: IEEE 802.6 was designed to support high data rates, typically up to 155 Mbps, which was significant for its time.
- **Supports Multiple Services**: The standard can support various services, including data, voice, and video transmission, making it versatile for different applications.

- **Wide Area Coverage:** Unlike traditional LANs, which are limited to a smaller geographical area, IEEE 802.6 was designed to cover larger metropolitan regions, making it suitable for city-wide networks.
- **Connection-Oriented and Connectionless Services:** The standard supports connection-oriented services (such as those needed for voice and video) and connectionless services (such as standard data transmission).

Types of Networks

A network is categorised into one of the following categories based on the geographic area it serves:

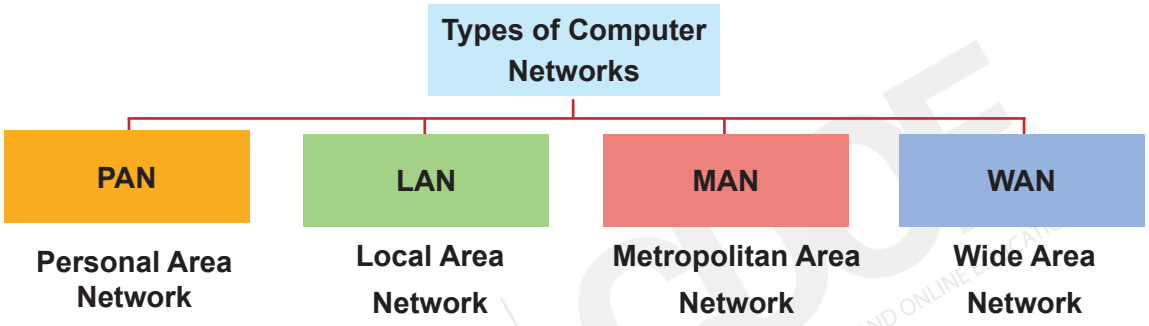


Fig. 7: Types of networks

Local Area Network (LAN): A LAN is a type of computer network that covers a limited geographical area, such as a home, office building, or campus. It is designed to facilitate communication and resource sharing between devices within the network, providing high-speed data transfer and local connectivity.

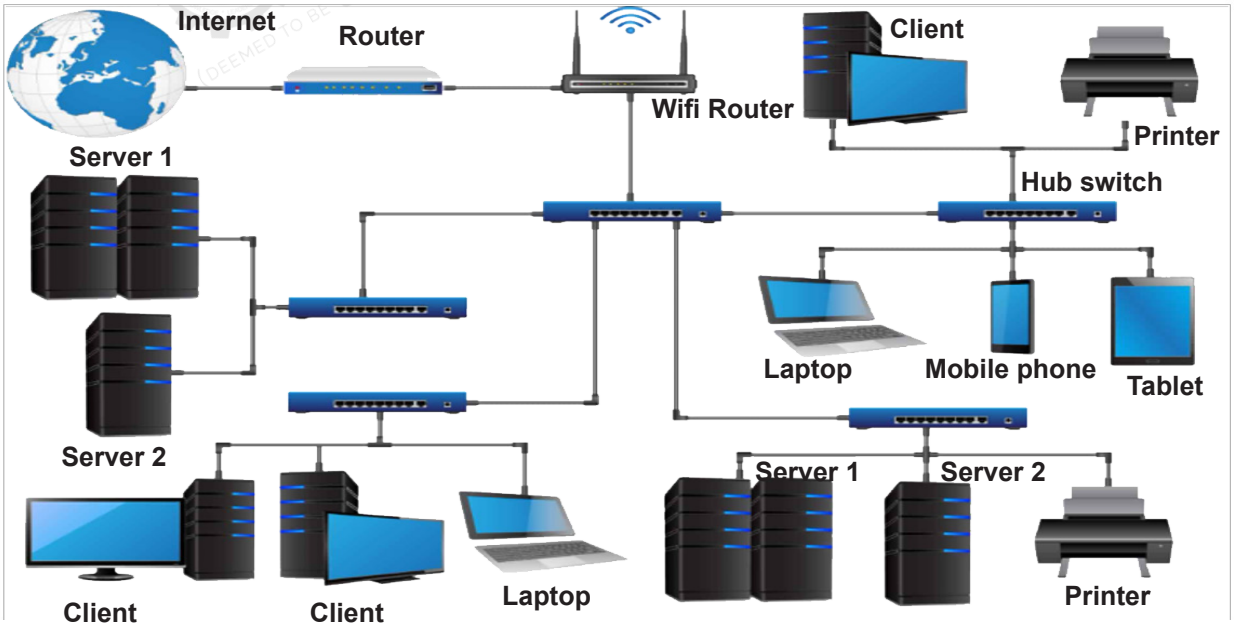


Fig. 8: Local Area Network

Metropolitan Area Network (MAN): A computer network spans a metropolitan area, connecting various locations within the city or urban area. It provides high-speed communication and data transfer capabilities, enabling organisations and individuals to share resources and access services across a larger geographic region.

Fig. 9: Metropolitan Area Network

Wide Area Network (WAN): It is a type of computer network that spans a large geographical area, often connecting multiple local area networks (LANs) across different locations. WANs utilize various technologies such as leased lines, satellites, or public networks to enable communication between geographically dispersed devices, facilitating data exchange and access to resources over long distances.

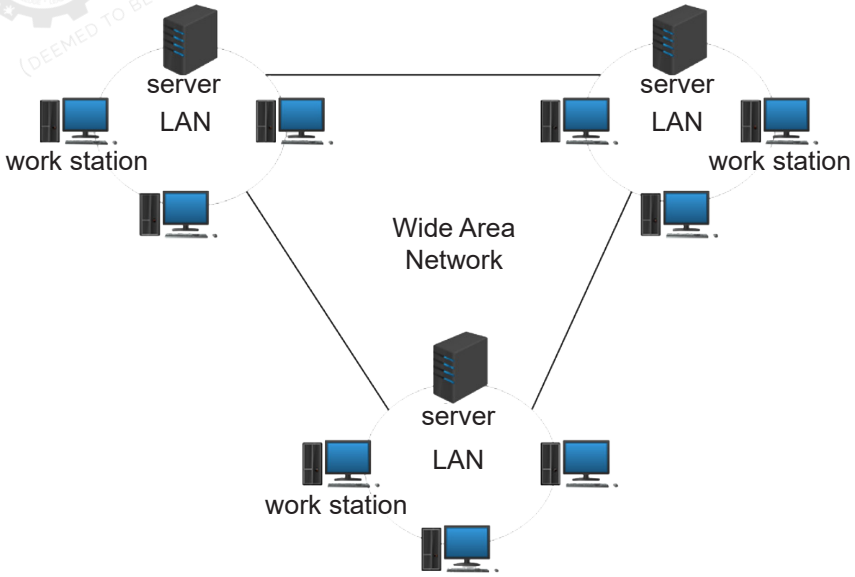


Fig. 10: Wide Area Network (WAN)

Personal Area Network (PAN): A personal area network (PAN) is a computer network designed specifically for an individual's personal use. It is often used to link devices such as cell phones, tablets, printers, PCs, and other digital devices inside an individual user's surroundings (typically within 10 metres or 33 feet). Personal Area Networks are used for personal purposes such as data sharing among devices within a 10-metre or 33-foot personal area network range. For example, if a computer is connected to a printer, scanner, and digital camera within 33 feet of each other, this is called a Personal Area Network.

Self-Assessment Questions

1. IEEE standards for computer networks help ensure:

   A). High-speed data transfer
   B). Compatibility and reliable connectivity
   C). Secure data transmission
   D). Efficient data storage

2. The main function of the IEEE 802.2 (Logical Link Control) standard is:

   A). Physical layer transmission
   B). Medium access control
   C). Consistent data transmission with error control and flow control
   D). IP address management

3. Which of the following is not a function of the Logical Link Control (LLC) layer?

   A). Multiplexing
   B). De-multiplexing
   C). Flow and error control
   D). IP Routing

4. In which IEEE 802.2 LLC service is a connection established before data transfer?

   A). Unacknowledged Connectionless Service (LLC 1)
   B). Acknowledged Connectionless Service (LLC 3)
   C). Connection-Oriented Service (LLC 2)
   D). All of the above

5. IEEE 802.3 standard refers to:

   A). Token Ring
   B). Ethernet
   C). Token Bus
   D). MAN

Self-Assessment Questions

6. The preamble in the IEEE 802.3 Ethernet frame is used for:

   A). Identifying the destination address
   B). Synchronizing clocks before data transmission
   C). Indicating the start of the frame
   D). Error detection

7. What is the purpose of the Frame Check Sequence (FCS) in IEEE 802.3?

   A). Address verification
   B). Data multiplexing
   C). Error detection
   D). Protocol selection

8. Which topology does the IEEE 802.4 (Token Bus) standard primarily use?

   A). Bus
   B). Star
   C). Ring
   D). Mesh

9. In a Token Bus network, a device can transmit data only when:

   A). It holds the token
   B). It receives an IP address
   C). It is the only device connected
   D). It is the first device in the network

10. The primary difference between Token Ring (IEEE 802.5) and Token Bus (IEEE 802.4) is:

    A). Token Ring uses star topology, while Token Bus uses ring topology.
    B). Token Ring passes the token over a physical ring, while Token Bus uses a virtual ring.
    C). Token Ring supports Ethernet, while Token Bus does not.
    D). Token Ring uses virtual connections, while Token Bus uses physical connections.

Self-Assessment Questions

11. The IEEE 802.6 standard is specifically designed for:

    A). Local Area Networks (LAN)
    B). Personal Area Networks (PAN)
    C). Metropolitan Area Networks (MAN)
    D). Wide Area Networks (WAN)

12. In IEEE 802.6 (DQDB), the “Dual Bus” architecture refers to:

    A). A single data path with backup
    B). Two unidirectional buses for network connectivity
    C). A token-passing mechanism
    D). Parallel network connections

13. Which type of network covers a limited geographical area like a home or office building?

    A). WAN
    B). LAN
    C). PAN
    D). MAN

14. A network used to connect devices in a metropolitan area, such as a city, is known as:

    A). LAN
    B). PAN
    C). MAN
    D). WAN

15. In IEEE 802.3 Ethernet, what does “BASE” refer to in “10BASE-T”?

    A). Baseband transmission
    B). Broadband transmission
    C). Banded transmission
    D). Binary transmission

2.1.2 High-Speed LANs

High-Speed Local Area Networks (LANs) are essential for modern computing environments where quick data transfer, low latency, and high reliability are critical. These networks are commonly found in businesses, academic institutions, and data centres where large volumes of data need to be moved quickly between devices within a localised area.

Key Components of High-Speed LANs

Ethernet Standards

- **Fast Ethernet (100 Mbps):** This early standard supported 100 Mbps, a significant upgrade over the original 10 Mbps Ethernet.
- **Gigabit Ethernet (1 Gbps):** A common standard today, Gigabit Ethernet supports 1 Gbps speeds and is suitable for most office environments.
- **10 Gigabit Ethernet (10 Gbps):** Used in environments that demand higher data throughput, such as data centres and high-performance computing clusters.
- **25, 40, 50, and 100 Gigabit Ethernet:** These standards are used in advanced networking scenarios, particularly in data centres and large-scale enterprise networks.

Fiber Optic Cabling

- **Single-Mode Fiber (SMF):** It is used for long-distance communication, often in high-speed networks spanning large areas like campuses or between data centres.
- **Multi-Mode Fiber (MMF):** Commonly used in shorter-distance applications within or between campus buildings.

Network Switches

- High-speed LANs rely on switches that support the necessary throughput, with ports capable of handling gigabit or multi-gigabit speeds.
- **Managed Switches:** These switches offer advanced features like Quality of Service (QoS), VLANs, and traffic management, which are essential for optimising network performance.

Wireless Networking (Wi-Fi)

- **Wi-Fi 6 (802.11ax):** The latest Wi-Fi standard offers increased capacity, efficiency, and data rates, making wireless networking more viable in high-speed LAN environments.
- **Wi-Fi 7 (802.11be):** An emerging standard offering even higher speeds and lower latency, further closing the gap between wired and wireless performance.

Design Issues in Networks

- Design issues in networks refer to the fundamental challenges and considerations that must be addressed when planning, developing, and maintaining a network.

- These issues determine how a network functions, performs, scales, and adapts to various conditions.
- Addressing these design issues ensures that the network meets the needs of its users and applications while being reliable, secure, and efficient.

Self-Assessment Questions

16. Which Ethernet standard is typically used in data centres and high-performance computing clusters to support high data throughput?

    A). Fast Ethernet (100 Mbps)
    B). Gigabit Ethernet (1 Gbps)
    C). 10 Gigabit Ethernet (10 Gbps)
    D). 100 Gigabit Ethernet

17. Which type of fibre optic cabling is commonly used for long-distance communication in high-speed networks, such as between data centres?

    A). Copper Cable
    B). Multi-Mode Fiber (MMF)
    C). Single-Mode Fiber (SMF)
    D). Coaxial Cable

18. Managed switches are essential in high-speed LANs because they offer features like:

    A). Faster data transfer rates
    B). Quality of Service (QoS), VLANs, and traffic management
    C). Higher durability in extreme conditions
    D). Lower power consumption

Summary

- IEEE Standards are the technical guidelines for device compatibility in networks.
- Logical link control handles multiplexing, de-multiplexing, flow control, and error control.
- Ethernet Frame Format includes fields like preamble, MAC addresses, and frame check sequences.
- A Token Bus Mechanism is a token that circulates for controlled transmission, reducing collisions.
- Local Area Network (LAN) Connects devices within a limited area, such as a building.
- Metropolitan Area Network (MAN) covers a larger urban area connecting various city locations.

Terminal Questions

1. What are the critical functions of the data link layer in network communication?
2. How does Ethernet ensure network compatibility and efficient data transmission?
3. What is the role of a token in token-passing protocols like Token Bus and Token Ring?
4. How do LAN, MAN, and WAN differ regarding range and applications?
5. What are the unique characteristics of a Metropolitan Area Network (MAN) compared to other network types?
6. How does the Personal Area Network (PAN) support connectivity between personal devices?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	C
3	D
4	C
5	B
6	B
7	C
8	A
9	A
10	B
11	C
12	B
13	B
14	C
15	A
16	C
17	C
18	B

Activity

Activity type: Online **Duration: 1 Week**

You are a network engineer at a company responsible for designing a network for a new office location. The office needs a reliable network setup that supports high-speed internet, secure data transfer, and connectivity across various departments. The office includes multiple floors, with a mix of personal workstations, shared resources (like printers and servers), and conference rooms. The network should support around 150 employees and must be scalable as the company plans to expand.

Based on the given scenario, outline the types of networks (LAN, MAN, WAN, or PAN) you would use within and for external communication with other branch offices. Justify your choices.

Glossary

- **OSI Model:** A conceptual framework that standardises the functions of a network into seven layers to guide interoperability and troubleshooting.
- **Encapsulation:** The process of wrapping data with protocol information at each OSI layer, transporting data across networks.
- **DNS (Domain Name System):** A hierarchical system that translates human-friendly domain names (like www.example.com) into IP addresses.
- **DHCP (Dynamic Host Configuration Protocol):** A protocol that automatically assigns IP addresses and other network configuration parameters to devices on a network.
- **Routing Protocol:** Routers use algorithms and protocols, such as OSPF or BGP, to determine the best path for data packets across networks.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **IEEE Standards in Computer Networks:** https://www.geeksforgeeks.org/difference-between-ieee-802-3-802-4-and-802-5/
- **High Speed LANs:** https://dl.acm.org/doi/pdf/10.1145/103724.103726

Video Links

Topic	Link
IEEE Standards in Computer Networks	https://youtu.be/3gOM7lPeqlY?si=ezcRbjM9llll5KQK
High-Speed LANs	https://youtu.be/u03RCIziXP8?si=Uf2XZenDsRE-bH-UU

Image Credits

Fig. 1: Sublayers of Data Link Layer	https://static.javatpoint.com/tutorial/computer-network/images/data-link-layer-in-osi-model2.png
Fig. 2: Types of LLC Services	https://media.geeksforgeeks.org/wp-content/uploads/20201005110740/erew12.png
Fig. 3: IEEE 802.3 Frame Format	https://media.geeksforgeeks.org/wp-content/uploads/IEEE-802.3-Ethernet-Frame-Format.png
Fig. 4: Versions of IEEE 802.3	https://www.tutorialspoint.com/assets/questions/media/23567/ieee_802_3.jpg
Fig. 5: Frame format of Token Bus	https://image.slidesharecdn.com/lecture21tokenbus-111030111849-phpapp01/95/token-bus-6-728.jpg?cb=1319973563
Fig. 6: Token Passing Mechanism	https://i1.wp.com/www.tutorialspoint.com/assets/questions/media/23100/token_passing_mechanism_token_bus.jpg
Fig. 7: Types of networks	https://1.bp.blogspot.com/-lojbssxrzOg/X1PLqfviT_I/AAAAAAAAAxU/03v3KLMfp8cGMZPq9gda4x1eICT-gZepCQCLcBGAsYHQ/s1600/Types%2Bof%2BComputer%2BNetworks%2B%2528www.tutorialsmate.com%2529.png
Fig. 8: Local Area Network	https://www.itechguides.com/wp-content/uploads/2020/06/local-area-network-concept-1920x1433.jpg
Fig. 9: Metropolitan Area Network	https://storage.icograms.com/templates/thumbnails/it-metropolitan-area-network.png
Fig. 10: Wide Area Network(WAN)	https://www.sangfor.com/sites/default/files/inline-images/example2.png

Keywords

- Packet Switching
- Subnet Masking
- Network Topology
- Firewall
- Throughput

MODULE 2

Data Communication and Networking

Unit 2

Network Design and Internet Protocol

Unit Table of Contents

Unit 2.2 Network Design and Internet Protocol

Aim

This unit aims to explore routing, congestion control, and the structure and function of the internet's network layer.

Instructional Objectives

This unit intends to:

- Discuss the primary design challenges in networking, such as routing and congestion control, that affect data flow and network efficiency
- Describe the role and structure of the network layer, emphasising the IP protocol, IP addressing, and subnetting
- Explain how internetworking supports connectivity and communication across different networks

Learning Outcomes

Upon completion of the unit, you will be able to:

- Compare fundamental network design concepts and the network layer components
- Assess the significance of routing, IP protocols, and subnetting in network management
- Analyse the critical elements of internetworking and their functions in connecting multiple networks

2.2.1 Routing Algorithms

Routing algorithms determine the paths that data packets travel through a network. These algorithms ensure efficient and reliable data transmission by selecting optimal routes from the source to the destination.

Classification of Routing Algorithms

- The routing algorithms can be classified as follows:
- Adaptive Algorithms
- Non-Adaptive Algorithms

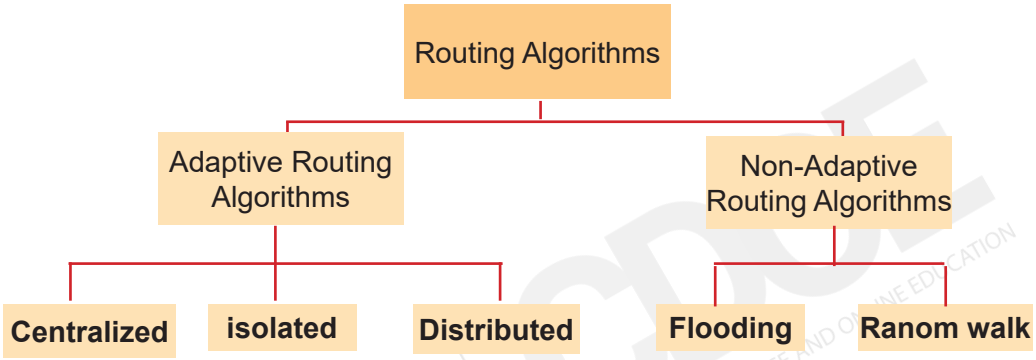


Fig. 1: Routing algorithms

2.2.1.1 Adaptive Routing algorithm

- An adaptive routing algorithm is also known as a dynamic routing algorithm.
- This algorithm makes the routing decisions based on the topology and network traffic.
- The main parameters related to this algorithm are hop count, distance and estimated transit time.
- An adaptive routing algorithm can be classified into three parts:
    - Centralized algorithm
    - Isolated algorithm
    - Distributed algorithm

Centralised Algorithm

- In this method, a centralised node has entire information about the network and makes all the routing decisions.
- The advantage of this is only one node is required to keep the information of the entire network and
- The disadvantage is that the entire network is done if the central node goes down. The link state algorithm is called a centralised algorithm since it knows the cost of each link in the network.

Isolated Algorithm

- In this method, each node makes its routing decisions using its information without seeking information from other nodes.
- The sending nodes don't have information about the status of a particular link.
- The disadvantage is that packets may be sent through a congested network, which may result in delays.
- Examples: Hot potato routing, and backward learning.

Distributed Algorithm

- In this method, the node receives information from its neighbours and decides whether to route the packets.
- A disadvantage is that the packet may be delayed if the intervals between receiving information and sending packets change.
- It is also a decentralised algorithm as it computes the least-cost path between source and destination.

2.2.1.2 Non-Adaptive Routing Algorithm

- Non-adaptive routing algorithms are also known as static routing algorithms.
- Static routing is a type of routing that does not change the route taken based on network conditions. This means that the same route is always taken,
- Static routing is usually used in small networks.
- One advantage of static routing is that it is simpler than adaptive routing. This is because there is no need to monitor and adjust the route based on changing conditions constantly. Further, these are classified as follows:
    - Flooding Algorithm
    - Random Walks Algorithm

Flooding Algorithm

When a packet must be sent to a destination computer, the source computer sends it to all its neighbours. The neighbours will then send the packet to their neighbours, and so on. This process is known as flooding.

Random Walks Algorithm

One of the most popular routing algorithms is the random walk algorithm. As its name suggests, this algorithm randomly selects a path for data to travel.

Self-Assessment Questions

1. Which of the following characteristics of an adaptive routing algorithm?

   A). Routes are fixed and do not change based on network conditions.
   B). Routing decisions are based on current network topology and traffic.
   C). It relies solely on a central node for routing information.
   D). Routing is based on a random path selection.

2. In which routing algorithm does each node independently make routing decisions based on its information without exchanging data with other nodes?

   A). Centralized algorithm
   B). Distributed algorithm
   C). Isolated algorithm
   D). Adaptive algorithm

3. What is a significant disadvantage of the flooding algorithm in non-adaptive routing?

   A). It uses a central node to make all routing decisions.
   B). It may create congestion due to excessive packet replication.
   C). It requires continuous updates on network conditions.
   D). It relies on information from neighbouring nodes.

2.2.2 Congestion Algorithm

Congestion control algorithms are network mechanisms that manage and alleviate congestion. Congestion occurs when too much data flows through the network, leading to delays, packet loss, and reduced performance. These algorithms help maintain efficient data transmission by regulating data flow, especially in high-traffic conditions.

Techniques of congestion control algorithms include:

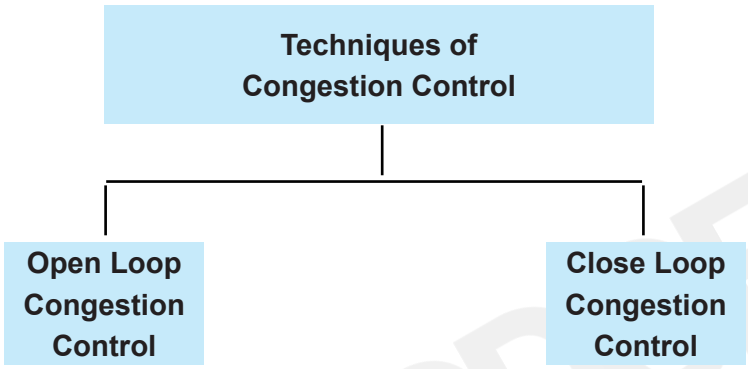


Fig. 2: Techniques of Congestion Control

- **Open-loop control (Prevention):** This approach focuses on preventing congestion before it occurs by designing the network and protocols to avoid overload. Examples include traffic shaping and admission control, which limit the amount of data entering the network.
- **Closed-Loop Control (Detection and Reaction):** Detects congestion after it occurs and adjusts the data flow accordingly. It often includes feedback mechanisms where the network informs sources to slow data transmission. Examples include:
    - **TCP Congestion Control:** Used widely in internet protocols, it adjusts the data transmission rate based on network feedback (e.g., reducing speed when packet loss occurs).
    - **Leaky Bucket:** Controls the data flow into the network constantly, smoothing outbursts.
    - **Token Bucket:** This type of storage allows for short data bursts but maintains control by requiring tokens for transmitting data packets.

Self-Assessment Questions

4. Which of the following is an example of an open-loop control technique for congestion prevention?

   A). TCP Congestion Control
   B). Leaky Bucket
   C). Traffic Shaping
   D). Token Bucket

5. In closed-loop congestion control, which algorithm allows for short data bursts by using tokens to regulate packet transmission?

   A). TCP Congestion Control
   B). Leaky Bucket
   C). Traffic Shaping
   D). Token Bucket

2.2.3 Network Layer on the Internet

- The network layer allows for connecting and transferring data packets between different devices or networks.
- The network layer is the third level (Layer 3) of the Open Systems Interconnection Model (OSI Model) and the layer that provides data routing paths for network communication.
- Data is transferred to the receiving device in packets via logical network paths in an ordered format controlled by the network layer.
- The network layer's primary responsibilities are logical connection setup, data forwarding, routing, and delivery error reporting.

2.2.3.1 IP Protocol

Internet Protocol (IP) is a foundational protocol governing routing and addressing data packets across the Internet. It provides a standardised set of rules and procedures for transmitting data between devices. IP assigns unique IP addresses to devices, breaks data into smaller packets, and ensures reliable delivery to the intended recipients.

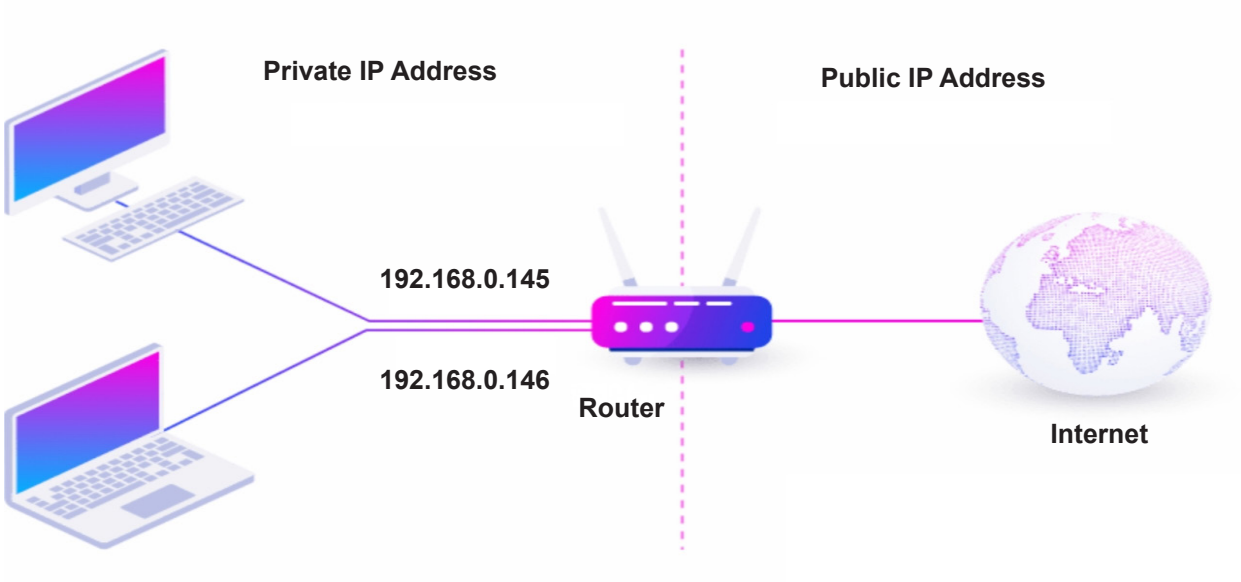


Fig. 3: Internet Protocol

- It transports packets from source to destination.
- A packet originating at a host on the home network must traverse four networks and many IP routers before reaching the company network on which the destination host is located.
- The Internet Protocol (IP) is a protocol, or set of rules, for routing and addressing packets of data
- Data traversing the Internet is divided into smaller pieces called packets.
- IP information is attached to each packet, which helps routers send packets to the right place.

2.2.3.2 IP Addresses

- An Internet Protocol (IP) address is the unique identifying number assigned to every device connected to the Internet.
- Typically assigned by an internet service provider (ISP).
- Using IP addresses, computers communicate over the internet or via local networks and share information with a specific location.

The primary purposes of an IP address in network communication are:

- **Identification:** Each device on a network is assigned an IP address, which uniquely identifies it. This ensures that data sent over the network reaches the correct destination.
- **Routing:** IP addresses help in directing data packets across networks. Routers use the destination IP address to determine the best path for forwarding the data from the source to the destination.
- **Facilitation of Communication:** IP addresses allow devices on different networks (e.g., between a computer and a web server) to communicate by establishing a connection and enabling data exchange.
- **Network Management:** IP addresses are also used for network administration, allowing tracking, monitoring, and controlling devices on a network.

Versions of IP Address

IPv4 (Internet Protocol version 4)

- It uses a 32-bit address format, typically expressed as four decimal numbers separated by dots (e.g., 192.168.0.1).
- It supports approximately 4.3 billion unique addresses.

IPV4 HEADER

The structure of an IPv4 header in network communications. Each part of the header has specific information that helps with routing and delivering data over the internet.

<table>
<tr><td>0</td><td>4</td><td>8</td><td colspan="2">16 19</td><td>31</td></tr>
<tr><td>Version</td><td>HL</td><td>Type of Service</td><td colspan="3">Total Length</td></tr>
<tr><td colspan="3">Identification</td><td>Flags</td><td colspan="2">Fragment Offset</td></tr>
<tr><td colspan="2">Time to Live</td><td>Protocol</td><td colspan="3">Header Checsum</td></tr>
<tr><td colspan="6">Source IP Address</td></tr>
<tr><td colspan="6">Destination IP Address</td></tr>
<tr><td colspan="5">Options</td><td>Padding</td></tr>
</table>

Fig. 4: IPV4 Header

- **Version:** Specifies the IP protocol version (usually IPv4 for this format).
- **IHL (Internet Header Length):** It indicates the header's length, which helps the receiver know where the data (payload) starts.
- **Type of Service (ToS):** This describes the quality of service for the packet and indicates priority or delay preferences.
- **Total Length:** The total size of the packet, including both header and data.
- **Identification:** Used for identifying fragments of the same packet if split across multiple packets.
- **Flags:** Control or indicate whether the packet can be fragmented or if it's the last fragment.
- **Fragment Offset:** Tells where this packet belongs in the sequence of fragments.
- **Time to Live (TTL):** Limits the packet's lifespan in the network. Each router reduces this by one; if it reaches zero, the packet is discarded.
- **Protocol:** Indicates the protocol used in the data part of the packet, like TCP or UDP.
- **Header Checksum:** Used to detect errors in the header for data integrity.
- **Source IP Address:** The IP address of the sender.
- **Destination IP Address:** The IP address of the receiver.
- **Options:** Additional options for advanced configurations are rarely used.
- **Padding:** Fills extra space if the header is not a multiple of 32 bits.

IPv6 (Internet Protocol version 6)

- It uses a 128-bit address format, typically expressed as eight groups of hexadecimal numbers separated by colons (e.g., 2001:0db8:8). It supports approximately 4.3 billion unique addresses. 5a3:0000:0000:8a2e:0370:7334).
- It supports a vastly more significant number of addresses, addressing the limitations of IPv4.

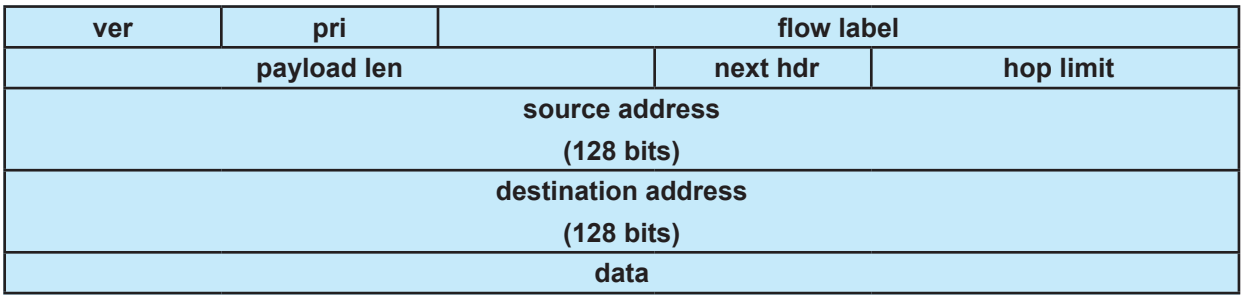


Fig. 5: IPV6 Header

The IPv6 header structure is used in IPv6, the newer version of the Internet Protocol. It organises essential information for sending data across networks.

- **Version:** Specifies the IP version, which is IPv6 for this header.
- **Priority/Traffic Class:** Indicates the packet's priority level, helping to manage network traffic and decide how packets are handled.
- **Flow Label:** Used to identify packets that need special handling, like real-time audio or video, so they can be processed more quickly.
- **Payload Length:** Shows the packet's data size (payload), excluding the header.
- **Next Header:** This points to the type of header that follows the IPv6 header, like the TCP or UDP header. It helps the receiver know how to process the packet.
- **Hop Limit:** Limits the packet's lifespan by counting the number of devices (like routers) it can pass through. Each device reduces this by one, and the packet is discarded if it reaches zero.
- **Source Address:** The sender's IP address, in 128-bit format (IPv6).
- **Destination Address:** The IP address of the receiver, also in 128-bit format.
- **Extension Headers:** Additional headers that provide extra options or features, like security or routing information.

Feature	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address comprising 4 fields separated by dots (.).	IPv6 is an alphanumeric address comprising 8 fields separated by colons (:).
Classes	IPv4 has 5 different classes of IP addresses: Class A, B, C, D, and E.	IPv6 does not contain classes of IP addresses.
Number of IP addresses	IPv4 has a limited number of IP addresses.	IPv6 has many IP addresses.
VLSM	IPv4 supports VLSM (Variable Length Subnet Mask), allowing for different sizes of subnets.	IPv6 does not support VLSM.
Address configuration	IPv4 supports manual and DHCP configuration.	IPv6 supports manual, DHCP, auto-configuration, and renumbering.
Address space	IPv4 generates 4 billion unique addresses.	IPv6 generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In IPv6, end-to-end connection integrity is achievable.
Security features	IPv4 security depends on applications and was not designed with security in mind.	IPv6 includes IPSEC, which was developed for security purposes.
Address representation	IPv4 addresses are represented in decimal format.	IPv6 addresses are represented in hexadecimal format.
Fragmentation	Fragmentation is done by both senders and routers in IPv4.	Fragmentation is done by senders only in IPv6.
Packet flow identification	IPv4 does not provide packet flow identification.	IPv6 uses a Flow Label field for packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 uses broadcasting.	IPv6 uses multicasting for efficient network operations.
Encryption and Authentication	IPv4 does not provide encryption and authentication.	IPv6 includes encryption and authentication.
Number of octets	IPv4 consists of 4 octets.	IPv6 consists of 8 fields, each containing 2 octets, totalling 16 octets.

Table 1: IPV4 vs. IPV6

Types of IP Address

Public IP Address:

- An IP address that is assigned to a device for direct communication over the internet.
- It allows devices to communicate with servers and devices outside their local network.

Private IP Address:

- An IP address is used within a private network (e.g., home or office) to allow devices to communicate with each other.
- It is not routable on the Internet and is used for internal network communication

Static IP Address:

- An IP address manually assigned to a device does not change.
- Often used for servers and devices that need a consistent IP address for reliable communication.

Dynamic IP Address:

- An IP address automatically assigned to a device by a DHCP (Dynamic Host Configuration Protocol) server and can change over time.
- Commonly used for general internet access where a constant IP address is unnecessary.

2.2.3.3 Subnets

A subnet (subnetwork) is an IP network's smaller, logical division. Subnetting helps organise a network into more manageable segments and can enhance security and performance. Key Concepts:

- **Subnet Mask:** Defines a subnet's range of IP addresses (e.g., 255.255.255.0).
- **CIDR Notation:** Classless Inter-Domain Routing (e.g., 192.168.1.0/24) specifies the IP range within a subnet.
- **Subnetting:** Dividing an extensive network into smaller subnets reduces congestion and isolates network segments.

Subnet Mask

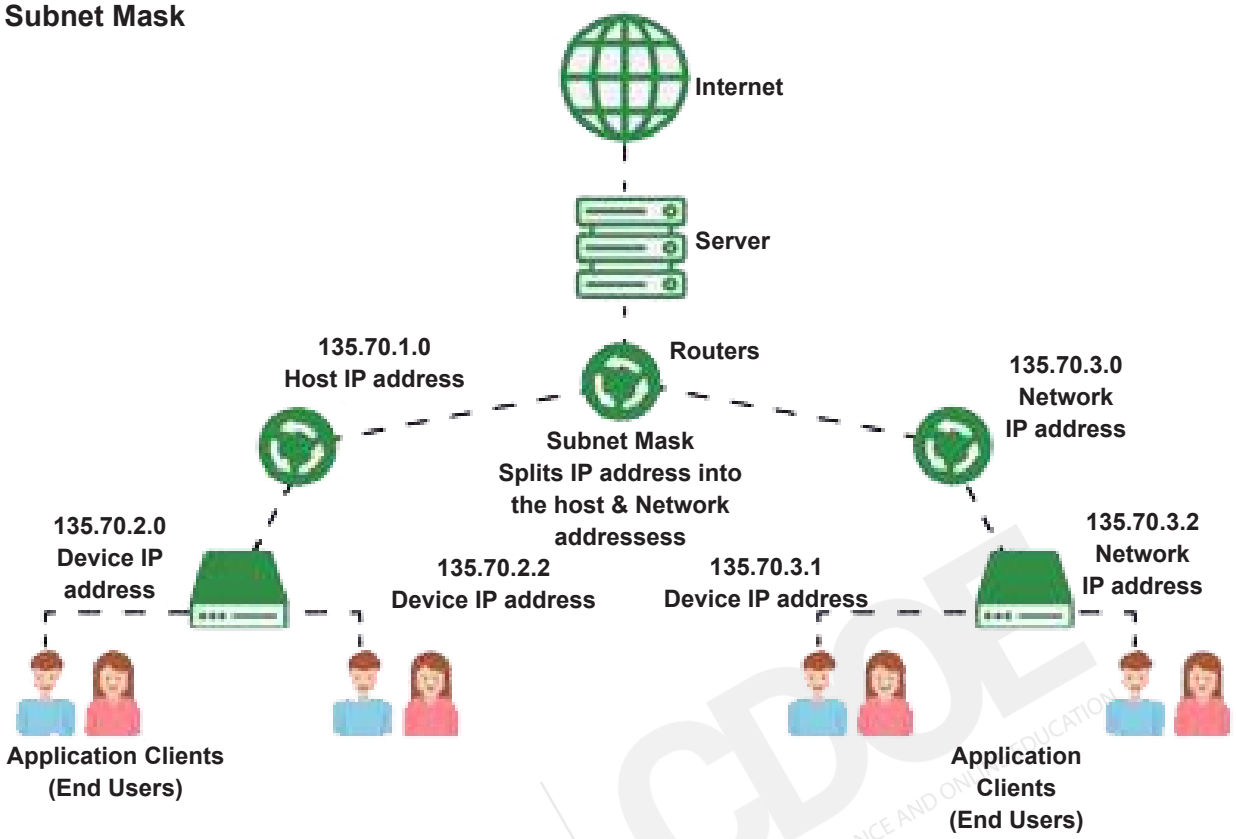


Fig. 6: Subnet Mask

- A Subnet Mask is used in networking to create multiple subnets. It divides the IP address into multiple parts that can be assigned to every computer.
- A Subnet Mask is created by Setting the Network bits to all “1” s and the Host bits to all “0” s.
- There are 4 octets in every IPV4 address having a Min value of 0 (decimal value of 00000000) and Max value of 255 (decimal value of 11111111)

Every IP address has 32 bits. There are different classes of IP addresses.

Class A: 8 bits (network id) 24 bits (Host id)

11111111.00000000.00000000.00000000, a subnet mask is 255.0.0.0

Class B: 16 bits (network id) 16 bits (Host id)

11111111.11111111.00000000.00000000 subnet mask is 255.255.0.0

Class C: 24 bits (network id) 8 bits (Host id)

11111111.11111111.11111111.00000000 subnet mask is 255.255.255.0

There are 256 IP addresses (0-255); from those, 2 IPs will be kept on hold. The “255” address is always assigned to a broadcast address, and the “0” address is always assigned to a network address. Neither can be assigned to hosts, as they are reserved for these purposes.

For example, a commonly used subnet mask is 255.255.255.0, which in binary is represented as: 11111111.11111111.11111111.00000000
For IP range,

- Class A IP address begins with 1 to 127.
- Class B IP address starts with 128 to 191.
- Class C IP address begins with 192 to 223.

You have an IP address of 192.168.1.10 with a subnet mask of 255.255.255.0. When you perform a bitwise AND operation between the IP address and the subnet mask, you get:

- IP address: 11000000.10101000.00000001.00001010
- Subnet mask: 11111111.11111111.11111111. 00000000
- Result: 11000000.10101000.00000001.00000000

The result reveals the network portion, 192.168.1.0, and the host portion, 0.

Uses of Subnetting

- It helps you to maximise IP addressing efficiency.
- Extend the life of IPV4.
- IPV4 Subnetting reduces network traffic by eliminating collision and broadcast traffic and thus improves overall performance.
- This method allows you to apply network security policies at the interconnection between subnets.
- Optimised IP network performance.

2.2.3.4 Internet working

Internetworking connects multiple networks or network segments to function as a large network. This connection is typically achieved through intermediary devices like routers and gateways. The term “internetworking” combines “inter” (between) and “networking,” reflecting the association between distinct networks.

Key Concepts:

- **Routers:** Devices that connect different networks and manage data traffic between them.
- **Gateways:** Devices that connect networks using different protocols, enabling communication between them.
- **Interconnecting Protocols:** Protocols like IP play a key role in enabling internetworking by providing a standard method for data exchange across diverse networks.

Types of Internetworks

- **Intranet:** A private network using IP-based tools (like web browsers) restricted to an organisation, usually protected from external access.
- **Extranet:** An extension of an intranet that provides limited access to external users or organisations, often used for business-to-business communication.
- **Internet:** The largest and most well-known example of internetworking, connecting millions of publics, private, governmental, and academic networks globally.

Self-Assessment Questions

6. Which OSI model layer is responsible for data routing paths for network communication?

A). Application Layer
B). Transport Layer
C). Network Layer
D). Data Link Layer

7. What is the primary purpose of an IP address in network communication?

A). To ensure data security
B). To uniquely identify devices on a network
C). To increase internet speed
D). To compress data packets

8. What type of IP address is assigned for internal network communication and is not routable on the internet?

A). Public IP Address
B). Private IP Address
C). Static IP Address
D). Dynamic IP Address

9. Which protocol version uses a 128-bit address format and supports many unique addresses?

A). IPv4
B). IPv5
C). IPv6
D). TCP

10. What does an IP header's "TTL" field represent?

A). Total Transfer Load
B). Time to Live
C). Transport Traffic Limit
D). Transmission Timeline

Self-Assessment Questions

11. In IPv4, which IP address class starts with a number between 1 and 127?

A). Class A
B). Class B
C). Class C
D). Class D

12. Which of the following is NOT a type of IP address?

A). Public IP Address
B). Private IP Address
C). Universal IP Address
D). Static IP Address

13. The IPv6 header does NOT include which of the following fields present in IPv4?

A). Version
B). Checksum
C). Source Address
D). Destination Address

14. Which of the following correctly represents an IPv6 address?

A). 192.168.0.1
B). 255.255.255.0
C). 2001:0db8:85a3:0000:0000:8a2e:0370:7334
D). 192.168.1.255

15. What does subnetting primarily help achieve in a network?

A). It increases the speed of data transfer.
B). It improves the efficiency of IP address allocation.
C). It enhances network hardware performance.
D). It changes the IP address format from IPv4 to IPv6.

Summary

- Routing algorithms determine optimal data paths, classified as adaptive (dynamic) and non-adaptive (static) algorithms.
- Adaptive routing dynamically adjusts routes based on network topology and traffic, including centralised, isolated, and distributed algorithms.
- Non-adaptive routing uses fixed paths, commonly in small networks, with methods like flooding and random walks.
- Congestion control algorithms use open-loop (prevention) and closed-loop (detection) techniques to manage data flow and reduce delays and losses.
- TCP congestion control, leaky bucket, and token bucket are key closed-loop techniques.
- The network layer (OSI Layer 3) handles data packet routing, forwarding, and error reporting, which is critical in IP protocol communication.
- IPv4 (32-bit) and IPv6 (128-bit) are IP versions, with IPv6 offering expanded addresses, improved security, and advanced routing.
- IP addresses are categorised into public, private, static, and dynamic types, essential for network communication and management.

Terminal Questions

1. What are the main differences between adaptive and non-adaptive routing algorithms, and how do they affect network performance?
2. How does congestion control contribute to network efficiency, and what are the roles of open-loop and closed-loop methods in managing congestion?
3. Explain the significance of TCP congestion control, leaky bucket, and token bucket techniques in ensuring smooth data transmission.
4. Describe the role of the network layer in the OSI model, particularly about routing and error handling.
5. Compare IPv4 and IPv6 regarding address structure, security features, and compatibility with modern network requirements.
6. How do public, private, static, and dynamic IP addresses function within networks, and what are their respective advantages and limitations?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	C
3	B
4	B
5	D
6	C
7	B
8	B
9	C
10	B
11	A
12	C
13	B
14	C
15	B

Activity

Activity type: Online **Duration: 1 week**

Imagine you are the network manager for a rapidly growing company with multiple office locations. As the company expands, network congestion increases, and you need to ensure reliable and efficient data communication between locations. Your current setup uses IPv4, static IPs for office locations, and a combination of adaptive and non-adaptive routing methods.

By referring to the above scenario, perform the given task.

Based on the high traffic levels, decide whether adaptive or non-adaptive routing algorithms would be more effective. Justify your choice by discussing how each algorithm would handle unexpected congestion or changing network paths.

Glossary

- **Traffic Management:** Controlling and optimizing network data flow to enhance performance and reduce congestion.
- **Dynamic Routing:** A routing method that automatically adjusts paths using routing protocols based on current network conditions.
- **Static Addressing:** This technique manually assigns a fixed IP address to a device, ensuring consistent connectivity.
- **Subnet:** A segmented portion of a more extensive network created to improve performance and security by dividing IP address space.
- **Address Configuration:** The process of assigning IP addresses and related settings to network devices for communication within a network.
- **Data Traversing:** Moving data packets through a network from the source to the destination, often following specific routing paths.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Routing Algorithm:** https://www.tutorialspoint.com/what-is-a-routing-algorithm-in-computer-network
- **Network Layer Protocol:** https://www.geeksforgeeks.org/network-layer-protocols/

Video Links

Topic	Link
Routing Algorithm	https://youtu.be/ET2W8DyA7zI?si=tpC1mUozLCOB-DbR
Network Layer Protocol	https://youtu.be/ly8ikWtAY7s?si=vjX7U8lYc9ngi-1JT

Image Credits

Fig. 1: Routing algorithms	https://scaler.com/topics/images/types-of-routing-algorithms-in-computer-networks.webp
Fig. 2: Techniques of Congestion Control	https://edukedar.com/wp-content/uploads/2021/09/techniques-of-congestion-control-1920x1080.jpg
Fig. 3: Internet Protocol	https://lh3.googleusercontent.com/-SkuXupnUtZ4/Y9VRa2fnHUI/AAAAAAAABkE/2bK4rbwpPYwN6a5I-jkF0m0l3ufG-cznPwCNcBGAsYHQ/s1280/IMG_ORG_1674924358104.jpeg
Fig. 4: IPV4 Header	https://image.slideserve.com/746067/ip-packet-header-6-l.jpg
Fig. 5: IPV6 Header	https://lh6.googleusercontent.com/proxy/IcyfHFK2ZDWBmg6nO0AS2pIZraCZZMBlV_sJw4E9h0dGyS3S2NNW6kEm7GWvPWy_1Jm5-dA7hSoDdrThsEoUY3LeWC0nDoeJVKln
Fig. 6: Subnet Mask	https://th.bing.com/th/id/OIP.yOFzRR4_Ia5P1UqCN-qOUQAAAA?rs=1&pid=ImgDetMain
Table 1: IPV4 vs. IPV6	Self-made

Keywords

- Routing
- Congestion
- Algorithms
- IP Addressing
- Network Protocols

COMPUTER NETWORKS

MODULE 3

Internet Transport Protocols and Network Services

Module Description

The module explores and discusses various protocols and services for Internet communication and data transfer. In the initial stage, the students will learn reliable data transmission services in the form of a transport layer. You will also learn about TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), understanding how each protocol supports data delivery and their specific applications across the network. After that, the module explores the concept of Quality of Service (QoS), which focuses on methods to prioritise and manage network traffic based on performance needs.

The best-effort model is covered by describing its approach to data delivery without guaranteed quality and discussing techniques to address common network performance issues like latency, congestion, and throughput. The module further explores essential network services and application-layer protocols that support internet functionality. now, you will be able to learn about the domain name system (DNS) to help change general domain names to IP addresses, thereby enabling the best possible web navigation. Students will also gain insights into the Simple Network Management Protocol (SNMP), vital for network monitoring and device management. After that, the module covers various protocols such as FTP, SMTP, POP3, and IMAP. These protocols are very helpful in making successful file transfers and helping to explore electronic mail through SMTP, POP3, and IMAP.

Specialised protocols such as BOOTP and TFTP are also explained in this module, which allows files to transfer more smoothly and efficiently. These protocols will help identify traffic and enable the user to experience a hassle-free network. Finally, the module covers the World Wide Web and how firewalls protect network security. You will be able to learn how to gather and access global information through the World Wide Web and how to protect your network through firewall applications.

This unit consists of **two** units.

Unit 3.1 Transport Protocols and Network Quality
Unit 3.2 Network Services and Application Protocols

MODULE 3

Internet Transport Protocols and Network Services

Unit 1

Transport Protocols and Network Quality

Unit Table of Contents

Unit 3.1 Transport Protocols and Network Quality

Aim

This unit aims to explore the fundamental transport protocols, TCP and UDP, and quality of services in prioritising network traffic.

Instructional Objectives

This unit intends to:

- Explain the purpose and characteristics of TCP and UDP protocols
- Define the concept of Quality of Service (QoS) in managing network resources
- Describe how the Best-effort model operates without guaranteed delivery
- Explore methods to mitigate network performance issues

Learning Outcomes

Upon completion of the unit, you will be able to:

- Evaluate the critical features of TCP and UDP in data transmission
- Assess the factors that affect the Quality of Service in networks
- Analyse common causes of network performance issues
- Demonstrate an understanding of techniques to optimise network performance

3.1.1 Transport Protocols

Internet transport protocols are critical components of the Internet's layered architecture, facilitating reliable and efficient data transmission between devices across networks. The two primary transport protocols in use today are:

- Transmission Control Protocol (TCP)
- User Datagram Protocol (UDP)

3.1.1.1 Transmission Control Protocol (TCP)

- A transport service is a function provided by transport layer protocols (such as TCP and UDP) that facilitate communication between network applications.
- It operates as an intermediary between the application and network layers, ensuring that data is correctly transmitted from the sender to the receiver across the internet or any network.
- The transport layer in the OSI model is responsible for end-to-end communication, error checking, and ensuring proper data delivery.

Key Features of TCP

- **A connection-oriented service:** It connects the communicating devices before transferring data, ensuring a reliable and orderly data exchange.
- **Reliable Delivery:** Ensures that all data is transmitted without errors, in the correct sequence, and with acknowledgment.
- **Flow Control:** Adjusts the data transmission rate so the sender does not overwhelm the receiver.
- **Congestion Control:** Regulates traffic to avoid overloading the network.
- **Error Detection and Correction:** Data corruption, loss, or duplication is detected and corrected using retransmissions.
- **Examples:** This protocol is used by applications that require guaranteed delivery, such as web browsing (HTTP/HTTPS), email (SMTP), and file transfer (FTP).

Elements of Transport Protocols: Transport protocols, such as TCP (Transmission Control Protocol) and UDP (User Datagram Protocol), are responsible for making reliable communication services over different network devices. These protocols contain several key elements that ensure the successful delivery of data across a network.

Critical Elements of Transport Protocols:

- **Segmentation & Reassembly:** This process breaks extensive data into smaller chunks for transmission and reassembles them at the receiver.

- **Multiplexing & Demultiplexing:** This method uses port numbers to send and receive data from multiple applications over a single network connection.
- **Connection Establishment & Termination:** For connection-oriented protocols (like TCP), a connection is set up before data transfer and terminated after.
- **Flow Control:** Manages the data transfer rate to prevent overwhelming the receiver (e.g., TCP's sliding window).
- **Error Detection & Correction:** Identifies and corrects transmission errors (e.g., TCP uses checksums and retransmission).
- **Reliability:** This will be helpful in making successful data delivery by using retransmissions and sequence numbers.
- **Congestion Control:** This is very helpful in preventing the overload on the network by reducing the transmission rate.
- **Port Numbers:** Identify specific applications or services (e.g., HTTP on port 80).
- **Timers:** Used for retransmissions and managing idle connections.
- **Connection Types:** TCP is connection-oriented (reliable); UDP is connectionless (fast but unreliable).

TCP Protocol

- TCP (Transmission Control Protocol) is a widely used transport layer protocol that ensures reliable, ordered, and error-checked data transmission between devices over a network.
- It is a connection-oriented protocol that establishes and maintains a connection until data exchange is complete.

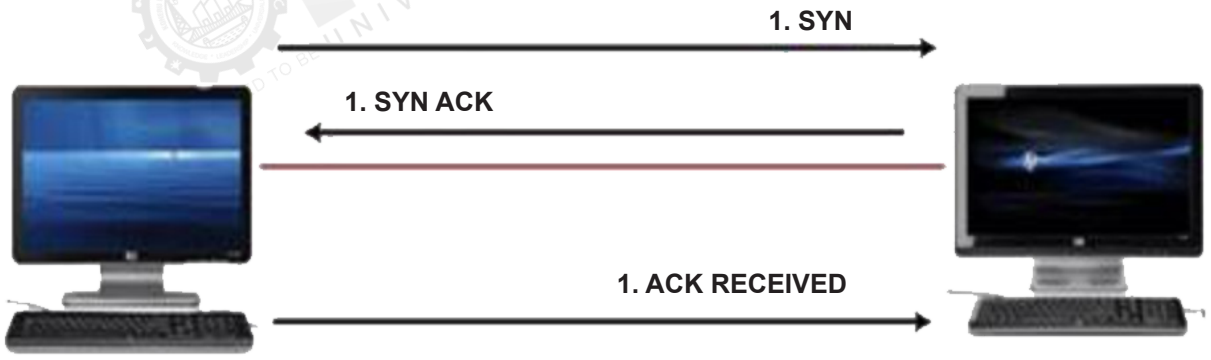


Fig. 1: Connection-Oriented Protocol

The above diagram explains the TCP three-way handshake. It is a method used by two devices (like computers) to establish a reliable connection over the internet.

- **SYN (Synchronise):** The computer on the left sends a "SYN" message to the computer on the right. This message is like saying, "Hello, I want to start a connection."

- **SYN-ACK (Synchronise-Acknowledge):** The computer on the right receives the SYN message and responds with a “SYN-ACK” message. This message means, “Hello, I got your request, and I agree to connect.”
- **ACK (Acknowledge):** The computer on the left receives the SYN-ACK message and sends back an “ACK” message, saying, “Thank you, I’m ready to communicate.”

After these three steps, a connection is established between the two computers, and they can start securely exchanging data.

3.1.1.2 User Datagram Protocol (UDP)

- UDP (User Datagram Protocol) is a simple, connectionless transport layer protocol that focuses on fast, efficient data transmission without guarantees of reliability or order.
- It is often used in scenarios where speed is more important than accuracy.

Key Features of UDP

- **Connectionless:** No connection setup; data is sent directly without prior communication between sender and receiver.
- **Unreliable Delivery:** This does not guarantee that data will arrive, be in order, or be error-free. There are no acknowledgments or retransmissions.
- **Low Overhead:** UDP is faster than TCP because it avoids the overhead of connection management, flow control, and error correction.
- **No Congestion Control:** Data is sent without regulating the rate, which could potentially overload the network.
- **Error Detection:** Different types of errors were detected by using the checksum method. However, the errors detected were not corrected using this method.

UDP Protocol

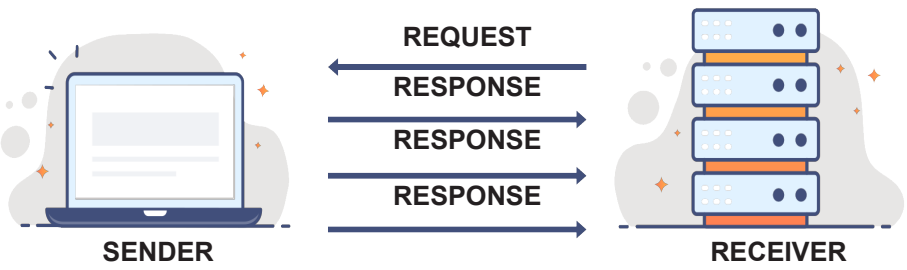


Fig. 2: UDP Protocol

This diagram explains the User Datagram Protocol (UDP), which is used to send data securely via the Internet. Unlike TCP, UDP is more straightforward and faster but does not guarantee that the data will reach the other side or arrive in the correct order. Here's a simple breakdown:

- **Request:** The "Sender" (like a computer) sends a request to the "Receiver" (like a server or group of servers) without checking if the receiver is ready or will respond.
- **Responses:** The receiver sends responses back to the sender. In UDP, multiple responses can be sent without any confirmation from the sender that each one was received.
- UDP has no handshake or error-checking process, so it's faster but less reliable.

Self-Assessment Questions

1. What is the primary difference between TCP and UDP regarding connection setup?

   A). TCP is connectionless, while UDP is connection oriented.
   B). TCP establishes a connection with a three-way handshake, while UDP does not establish a connection.
   C). Both TCP and UDP require a connection setup.
   D). UDP guarantees reliable data transmission, unlike TCP.

2. Which of the following best describes a scenario where UDP is preferable over TCP?

   A). Sending a large file that needs to be intact
   B). Online video streaming where speed is more critical than guaranteed delivery
   C). Web browsing, which requires ordered and reliable data
   D). Email transmission, where data integrity is essential

3. What feature of TCP helps prevent network overload by adjusting the data transmission rate?

   A). Error Detection
   B). Flow Control
   C). Multiplexing
   D). Congestion Control

3.1.2 Quality of Services and Best Effort Models

3.1.2.1 Quality of Service Model

- The quality of Service (QoS) model defines a network's ability to provide different priority levels or guarantees for specific types of traffic.
- It ensures critical data gets the resources it needs for optimal performance, particularly in networks with limited bandwidth or high traffic volumes.

Key Components of QoS

- **Traffic Classification**: Identifies and categorises data based on its priority. For example, real-time applications like VoIP and video conferencing are prioritised over bulk data transfers.
- **Traffic Shaping and Policing:**
  - **Shaping:** Regulates the flow of data to match available network capacity.
  - **Policing:** Enforces traffic limits, dropping or marking excess data.
  - **Priority Queuing:** Data is placed in queues based on priority, with higher-priority traffic sent first.
- **Bandwidth Reservation:** A minimum bandwidth for specific applications or traffic types (e.g., voice or video) is guaranteed.
- **Latency and Jitter Management:** Ensures low delay and consistent timing for real-time applications that need smooth, uninterrupted data delivery.

3.1.2.2 Best Effort Model

- The Best Effort model is an essential Quality of Service (QoS) approach to prioritisation or delivery guarantees.
- It provides no assurances regarding bandwidth, delay, jitter, or packet loss, meaning data is sent over the network, assuming it will eventually reach its destination, but without any guarantees.

Key Features of the Best Effort Model

- **No Prioritisation:** All data packets are handled similarly regardless of importance. There is no distinction between critical and non-critical traffic.
- **No Guarantees:** There are no guarantees for:
    - **Bandwidth:** Traffic may experience slowdowns or interruptions based on the overall network load.
    - **Latency and Jitter:** Delays and variations in delay are not managed.
    - **Packet Loss:** Some packets may be dropped during transmission, especially when the network is congested.

Simple and Scalable: It is easy to implement and requires minimal overhead, making it suitable for general internet traffic where service guarantees are not crucial.

Self-Assessment Questions

4. Which component of the Quality of Service (QoS) model is responsible for ensuring that high-priority traffic, like video conferencing, is transmitted first?

   A). Traffic Classification
   B). Traffic Shaping
   C). Priority Queuing
   D). Best Effort

5. In the Best Effort model, which of the following statements is true?

   A). Bandwidth is guaranteed for all traffic types.
   B). High-priority traffic is prioritised over other traffic.
   C). There are no guarantees for latency, jitter, or packet loss.
   D). Traffic shaping regulates data flow based on priority.

6. What is the Best Effort model's main advantage in network implementation?

   A). Simple and scalable, with minimal overhead.
   B). Provides bandwidth reservation for critical applications.
   C). Ensures consistent low latency for all types of traffic.
   D). Guarantees no packet loss across the network.

3.1.3 Network Performance Issues

- Network performance issues are problems that degrade data transmission quality, speed, and reliability across a network.
- These issues can significantly affect user experience, especially for real-time applications like video conferencing, VoIP, and online gaming.

Common Network Performance Issues:

1. Latency:

- **Definition:** The delay between sending and receiving data across the network.
- **Causes:** Long distances between devices, slow routers, inefficient routing paths, or network congestion.
- **Impact:** High latency affects real-time applications like video calls or gaming, causing noticeable delays.

2. Jitter:

- **Definition:** Variations in packet arrival times. Even if packets are sent regularly, they may arrive irregularly due to network fluctuations.
- **Causes:** Network congestion, improper queuing, or poor routing.
- **Impact:** Jitter can disrupt time-sensitive applications like VoIP, leading to choppy audio or video.

3. Packet Loss:

- **Definition:** Occurs when packets of data fail to reach their destination.
- **Causes:** Network congestion, faulty hardware, signal interference (in wireless networks), or overloaded routers.
- **Impact:** Causes degraded service, especially in real-time applications like streaming or online gaming. TCP will retransmit lost packets, adding delay.

4. Bandwidth Limitations:

- **Definition:** The maximum amount of data transmitted over a network in each time.
- **Causes:** Limited network infrastructure, oversubscription (too many users sharing the same

  bandwidth), or bottlenecks in the network path.
- **Impact:** Slow download/upload speeds, buffering in video streams, and lag in online activities.

5. Congestion:

- **Definition:** Occurs when the demand for network resources exceeds capacity, causing delays and packet loss.
- **Causes:** Too much data sent through the network, insufficient bandwidth, or inefficient routing.
- **Impact:** Slow response times, increased latency, and packet drops.

6. Network Interference (in wireless networks):

- **Definition:** Disruption caused by external signals that interfere with the network's operation.
- **Causes:** Physical obstacles, overlapping Wi-Fi channels, electromagnetic interference from other devices (e.g., microwaves, Bluetooth devices).
- **Impact:** Weak signals, slower connections, and packet loss.

7. Hardware Failures:

- **Definition:** Issues with networking equipment that can impair performance or cause downtime.
- **Causes:** Failing routers, switches, network cards, or cables.
- **Impact:** Slow or intermittent connectivity, dropped connections, or complete network outages.

8. DNS Issues:

- **Definition:** Problems with the Domain Name System (DNS), which translates domain names to IP addresses.
- **Causes:** Misconfigured DNS settings, DNS server outages, or slow DNS resolution times.
- **Impact:** Slow website loading times, inability to access certain websites, or complete loss of internet connectivity.

9. High CPU/Memory Usage on Network Devices:

- **Definition:** Overloaded network devices struggle to handle data efficiently.
- **Causes:** Too many processes or excessive data passing through a device.
- **Impact:** Reduced network performance, increased latency, and dropped connections.

Self-Assessment Questions

7. Which network performance issue is characterised by the delay between sending and receiving data across the network?

   A). Jitter
   B). Latency
   C). Bandwidth Limitation
   D). DNS Issue

8. What impact does packet loss typically have on real-time applications such as online gaming or video streaming?

   A). Increased download speed
   B). Choppy audio or video
   C). Faster data transmission
   D). Decreased CPU usage

9. Which of the following is a common cause of network interference in wireless networks?

   A). Inefficient routing
   B).
   C). Electromagnetic interference from other devices
   D). DNS misconfiguration

Summary

- Transport protocols like TCP and UDP are vital in managing data transmission. TCP ensures reliable connections, while UDP focuses on speed without reliability.
- TCP uses flow control, error detection, and congestion control to maintain data accuracy and prevent network overloads.
- UDP, unlike TCP, skips connection setup and error-checking, making it faster but less reliable for applications like streaming and gaming.
- Quality of Service (QoS) models manage network traffic by setting priorities, ensuring essential data like voice and video receive the necessary bandwidth, and reducing delays.
- Best Effort models offer no guarantees for data priority or quality, resulting in potential packet loss, latency, and inconsistency in traffic handling.
- Network performance issues, including latency, jitter, and packet loss, often result from congestion, bandwidth limits, or hardware failures and affect real-time applications.

Terminal Questions

1. How do TCP and UDP differ regarding reliability, connection setup, and data handling?
2. Explain the purpose of flow control and congestion control in TCP. Why are these features critical for maintaining network performance?
3. Identify and explain three common network performance issues.
4. How do these issues impact real-time VoIP and video conferencing applications?
5. What roles do error detection and correction play in TCP? Why does UDP omit this feature?
6. How do traffic shaping and policing contribute to Quality of Service (QoS) in a network?
7. Describe the consequences of high latency and jitter on user experience in online communication and gaming.
8. How do DNS issues affect network performance, and what are the potential causes and impacts of these problems?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	B
3	D
4	C
5	C
6	A
7	B
8	B
9	C

Activity

Activity type: Online **Duration: 1 Week**

You are a network engineer at a company responsible for designing a network for a new office location. The office needs a reliable network setup that supports high-speed internet, secure data transfer, and connectivity across various departments. The office includes multiple floors, with a mix of personal workstations, shared resources (like printers and servers), and conference rooms. The network should support around 150 employees and must be scalable as the company plans to expand.

Based on the given scenario, outline the types of networks (LAN, MAN, WAN, or PAN) you would use within and for external communication with other branch offices. Justify your choices.

Glossary

- **Transport Layer:** The fourth layer in the OSI model is responsible for end-to-end communication, data integrity, and error checking. It ensures data is reliably delivered between devices.
- **Error Detection and Correction:** Techniques used to identify and rectify data transmission errors, such as checksums and retransmissions, ensuring data integrity.
- **Segmentation and Reassembly:** The division of extensive data into smaller segments for transmission, which are then reassembled at the receiver for accurate data delivery.
- **Port Number:** A unique identifier assigned to specific applications or services (like HTTP or FTP), allowing correct data routing within a network.
- **Connectionless Protocol:** A protocol, like UDP, that sends data without first establishing a connection, trading reliability for faster, more efficient data transfer.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **TCP Protocol:** https://youtu.be/vKFLgmSC6do?si=1jS8rD16SOfV6Hm7
- **UDP Protocol:** https://www.geeksforgeeks.org/user-datagram-protocol-udp/

Video Links

Topic	Link
How TCP Works	https://youtu.be/vKFLgmSC6do?si=1jS8rD16SOfV6Hm7
User Datagram Protocol	https://youtu.be/HMKC3RSUuJg?si=ubrc4uHcs-4fEWYLa

Image Credits

Fig. 1: Connection-Oriented Protocol	https://th.bing.com/th/id/OIP.H2sAUIAZnqRNylgMA-T3oCAAAAA?rs=1&pid=ImgDetMain
Fig. 2: UDP Protocol	https://bunnyacademy.b-cdn.net/F7AJp-What-Is-UDP-how-does-it-work-and-what-are-its-benefits.png

Keywords

- Transport Protocols
- Congestion Control
- Retransmission
- Three-Way Handshake
- SYN
- ACK
- Bandwidth Reservation

MODULE 3

Internet Transport Protocols and Network Services

Unit 2

Network Services and Application Protocols

Unit Table of Contents

Unit 3.2 Network Services and Application Protocols

Aim

To explore the critical network services and application protocols that support communication, file transfer, and web security in networked environments.

Instructional Objectives

This unit intends to:

- Describe the purpose and function of network protocols and services like DNS, SNMP, and BOOTP
- Explain the role of file transfer and communication protocols, including FTP, TFTP, and email, in data exchange
- Discuss the importance of web protocols and security mechanisms, such as HTTP, the World Wide Web, and firewalls, in protecting and enabling internet access

Learning Outcomes

Upon completion of the unit, you will be able to:

- Explore the functionalities of DNS, SNMP, and BOOTP in managing network resources
- Identify the appropriate uses of FTP, TFTP, and email protocols in different data exchange scenarios
- Evaluate the significance of HTTP and the World Wide Web in facilitating online information sharing and access

3.2.1 Network Protocols and Services

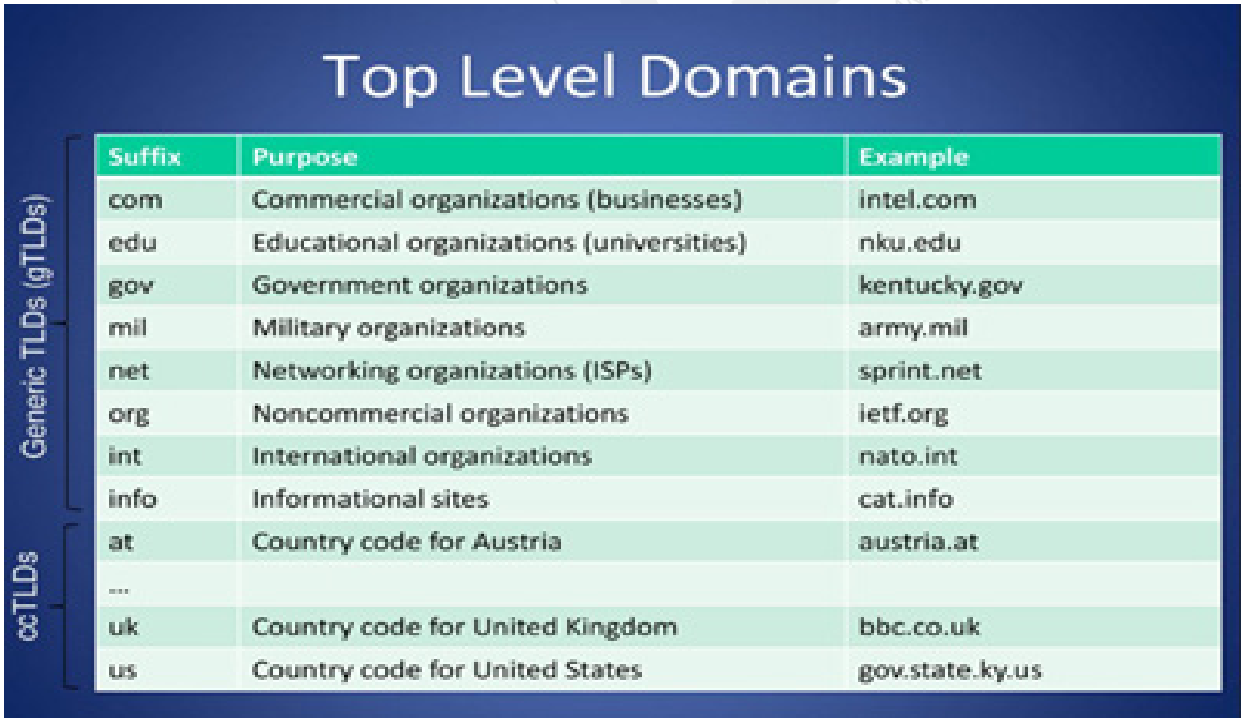
Network protocols and services allow computers to speak with each other through the network. Specific rules and processes enable computers to interact, such as connecting various devices, managing data, and striving to secure the data.

3.2.1.1 Domain Name System (DNS)

It was created in 1983 and has become a crucial Internet component. The development of the distributed database system and hierarchical domain-based naming scheme are the foundations of this DNS, which maps host names to IP addresses. Around 100 top-level domains are available on the Internet.

Domain: A domain is a subtree of the domain name space that consists of a group of hosts under the administrative control of a single entity, such as a company or a government agency.

- Each domain is subdivided into subdomains
- The leaves represent domains that have no subdomains
- A leaf domain may contain a single host or represent a company with thousands of hosts



Suffix	Purpose	Example
com	Commercial organizations (businesses)	intel.com
edu	Educational organizations (universities)	nku.edu
gov	Government organizations	kentucky.gov
mil	Military organizations	army.mil
net	Networking organizations (ISPs)	sprint.net
org	Noncommercial organizations	ietf.org
int	International organizations	nato.int
info	Informational sites	cat.info
at	Country code for Austria	austria.at
...		
uk	Country code for United Kingdom	bbc.co.uk
us	Country code for United States	gov.state.ky.us

Fig. 1: Top-level Domains

This chart shows different types of Top-Level Domains (TLDs), which are the last part of a website address, such as ".com" or ".edu". TLDs help categorise websites by their purpose or country. There are Generic TLDs (gTLDs) like ".com" for businesses, ".edu" for universities, ".gov" for government sites, and ".org" for non-profit organisations. Other TLDs, like ".int" and ".info", are used for international and informational sites. There are also Country Code TLDs (ccTLDs), such as ".uk" for the United Kingdom and ".us" for the United States, which indicate that a website is associated with a specific country. These TLDs help people quickly understand the type or origin of a website.

3.2.1.2 Simple Network Management Protocol (SNMP)

Simple Network Management Protocol (SNMP) is a popular protocol for controlling devices on an IP network. It allows network administrators to collect data from the network device, detect errors, and set preferences. SNMP also enables remote control of network hardware, like servers, routers, switches, printers, and other network-attached devices. In recent studies, the Internet Engineering Task Force declared that SNMP is part of the Internet Protocol Suite.

Key Concepts of SNMP:

- **Managers and Agents:**
    - **SNMP Manager:** A centralised system communicating with SNMP agents on network devices. The manager collects and analyses data, sends requests, and gets agent notifications.
    - **SNMP Agent:** A software component running on network devices (e.g., routers, switches, servers) that collects information about the device's status and configuration and responds to requests from the manager.
- **Management Information Base (MIB):** A database or schema that defines the structure of network information managed via SNMP. It contains descriptions of all manageable objects and their properties. Each object in the MIB has a unique Object Identifier (OID) used to identify and retrieve specific data from network devices.
- **Object Identifiers (OIDs):** Unique identifiers assigned to each object or data point that can be queried or managed via SNMP. OIDs are organised hierarchically, providing a way to identify each element in the MIB.
- **Communication Model:** SNMP communication is based on a client-server architecture, where the SNMP manager is the client that requests information, and SNMP agents are servers that provide information and send notifications.

3.2.1.3 BOOTP (BOOTSTRAP PROTOCOL)

BOOTP (Bootstrap Protocol) is a network protocol a client device uses to obtain configuration information, such as its IP address, default gateway, and server details, necessary to operate on an IP network. It was designed to support the diskless workstation in getting the data needed to communicate through a network.

Key Features of BOOTP:

- **Dynamic IP Address Assignment:** This feature eliminates the manual configuration required to obtain the IP address from the BOOTP server during bootup.
- **Network Configuration**: In addition to IP addresses, BOOTP can provide other network configuration parameters, such as the subnet mask, default gateway, and IP address of a TFTP server. These parameters can be used to download the boot image.
- **Use of UDP:** BOOTP is highly responsible for enabling active communication among clients and servers through the User Diagram Protocol. In general, messages are transmitted via 67 and 68 ports.
- **Static Configuration:** BOOTP uses static IP address mapping, in contrast to DHCP (Dynamic Host Configuration Protocol), which was created as an enhancement over BOOTP. This indicates that each device always receives the same IP address when it boots up because the server has a pre-configured table that correlates each client's hardware address (MAC address) with an IP address.

Self-Assessment Questions

1. Which of the following statements best describes the Domain Name System (DNS)?

   A). The system maps host names to IP addresses and organises domains hierarchically.
   B). It is a protocol used for remote control of network devices.
   C). It is an email protocol that handles incoming mail.
   D). It is a protocol for transferring files over the network.

2. In the Simple Network Management Protocol (SNMP), what is the role of the Management Information Base (MIB)?

   A). It stores and manages email messages.
   B). It defines the structure of network information managed by SNMP and contains descriptions of all manageable objects.
   C). It allows direct communication between email servers.
   D). It serves as a storage for transferred files.

3. Which BOOTP (Bootstrap Protocol) feature distinguishes it from DHCP?

   A). BOOTP dynamically assigns IP addresses to devices each time they boot up.
   B). BOOTP uses static IP address mapping, where each device receives the same IP address on every boot.
   C). BOOTP communicates over TCP protocol.
   D). BOOTP only provides the IP address without other network configuration details

3.2.2 File Transfer and Communication Protocols

File Transfer and Communication Protocols are essential for sharing files and messages across a network. These protocols help users send and receive data, making communicating and exchanging information between devices easy.

3.2.2.1 File Transfer Protocol (FTP)

- One of the most frequent tasks anticipated in a networking or internetworking environment is file transfers between computers.
- The standard method for copying a file from one host to another that TCP/IP offers is called File Transfer Protocol (FTP).
- FTP differs from other client/server applications in establishing two connections between the hosts. One connection is used for data transfer, and the other is for controlling information.

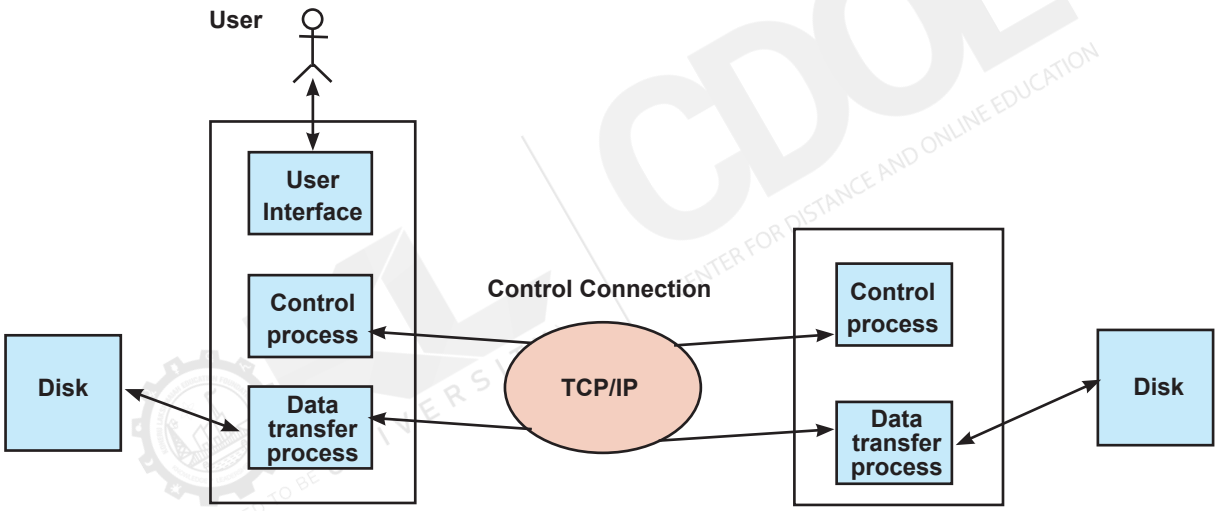


Fig. 2: File Tranfer Protocol

- The entire interactive FTP session is spent with the control connection active. For every transferred file, the data connection is opened and then closed.

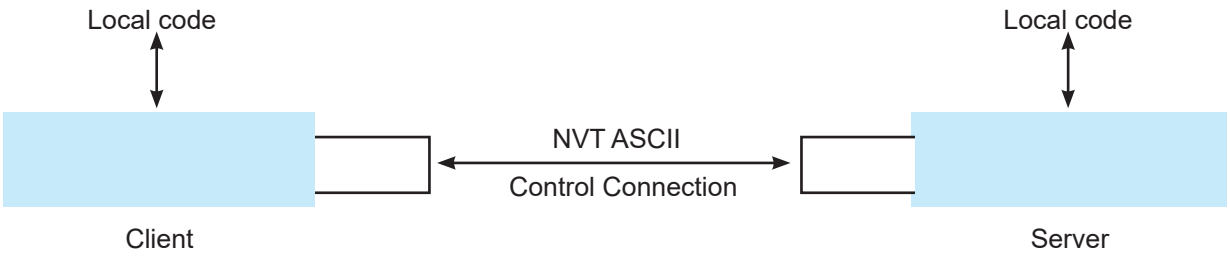


Fig. 3: Control Connection

File transfer in FTP means one of three things:

- Copying the file from the server to the client side will be called aft/e in FTP.
- A file must be copied from the client to the server. We call this storing aft/e. It is carried out under the supervision of the STOR command.
- The server must send the client a list of file or directory names.
- The LIST command oversees this process. The directory names in the list of files are considered files across FTP, and these files are transmitted through the data link.
- Three communication characteristics, such as file type, data structure, and transmission mode, are specified to address the heterogeneity issue.

3.2.2.2 Trivial File Transfer Protocol (TFTP)

The trivial file transfer protocol (TFTP) is appropriate for applications that don't need intricate FTP procedures and don't have enough RAM or ROM to support them.

The main features of TFTP are:

- TFTP works on the principle of client-side server.
- It uses a Well-known UDP port number 69 for the TFTP server.
- TFTP is an unsecured protocol.
- TFTP does not support authentication.
- Every TFTP data unit has a sequence number.
- Each data unit is individually acknowledged. After receiving the acknowledgment, the following data unit is sent.
- Error recovery occurs by retransmission after timeout.

TFTP Operation

- The client sends a read or write request at the server's UDP Port69
- The server accepts the request by sending a data message in case of the read request.
- The server accepts the request by sending acknowledgment in case of a write request.
- In either scenario, the server chooses a UDP port for additional communication and sends the client its initial response on that port.
- Every data message has a fixed data block size of 512 octets and is acknowledged separately.
- The session ends when a data block with fewer than 512 octets or the final data block containing EDF is used.
- Retransmission following a timeout is used for error recovery.

- After the time out, the sender repeats the message if the TFTP message is lost and no response is expected. The final acknowledgement is repeated following a timeout if the subsequent data message is not received after acknowledgement.

3.2.2.3 Electronic Email

Electronic Mail (Email) is a method of exchanging digital messages over the Internet. It is one of the most popular Internet services and offers a quick and easy way to share files, send and receive messages, and communicate with people worldwide.

Critical Components of Email:

- **Email Client: An application** allows users to manage data and send, read, and write emails without hassle. Microsoft Outlook and Mozilla Thunderbird are examples. Yahoo Mail, Gmail, etc., are regarded as web-based email clients.
- **Mail Server:** A computer system stores and manages email messages. Email sending, receiving, and mail servers handle delivery. There are two main types:
    - **Incoming Mail Server:** This server retrieves emails. POP3 (Post Office Protocol 3) and IMAP (Internet Message Access Protocol) are standard protocols.
    - **Outgoing Mail Server:** Handle sending emails. The SMTP (Simple Mail Transfer Protocol) sends outgoing mail.
- **Email Address:** A unique identifier for each user, consisting of a local part (username), the “@” symbol, and a domain part (e.g., username@example.com). The local part specifies the user, while the domain specifies the server that hosts the email.

Self-Assessment Questions

4. What is a critical difference between FTP and TFTP?

   A). FTP uses a single connection, while TFTP uses two connections.
   B). FTP requires authentication, while TFTP does not.
   C). TFTP uses TCP, while FTP uses UDP.
   D). FTP is used for file transfers within a single system only.

5. Which protocol is used by an email client to send outgoing emails?

   A). IMAP
   B). POP3
   C). SMTP
   D). FTP

6. What is the role of the control connection in FTP?

   A). It transfers files between the client and server.
   B). It maintains the interactive session and handles commands.
   C). It encrypts data during transfer.
   D). It manages error recovery by retransmitting lost data.

3.2.3 Web and Security Protocols

Web and security protocols are guidelines designed to help protect data when it is shared online. They guarantee that data is transmitted and received securely between users and websites.

3.2.3.1 Hypertext Transfer Protocol (HTTP)

HTTP (Hypertext Transfer Protocol) is an application layer protocol used for transmitting hypermedia documents, such as HTML. It is the foundation of any data exchange on the World Wide Web and is responsible for facilitating communication between web servers and clients (such as browsers). HTTP is a stateless protocol, meaning that user session data is not stored, and the server handles each client request separately. As time moved, HTTP has evolved to increase its efficiency and offered more secure networks by creating different versions such as HTTP/1.0, HTTP/1.1, etc.

Key Features of HTTP:

- **Request-Response Model:** A client submits a request to a server via HTTP, and the server either provides the requested resource or an error message in response.
- **Stateless:** The HTTP protocol is stateless, so the request made by the user every time will be independent and will not keep track of the requests made last time. Cookies, tokens, or session IDs can all be used to control sessions.
- **Layered over TCP/IP:** The foundation for HTTP was the TCP/IP protocol, which allows the dependable transfer of data through the Internet.
- **Methods (Verbs):** Several methods (also known as verbs) that specify the desired action to be performed are defined by HTTP. The most popular techniques consist of:
    - **GET:** This method allows users to request data directly from the server. It is considered the most secure method, which means the state of the resource remains unchanged.
    - **POST:** This sends data to a server and can modify the resource's state. It is often used for submitting forms or uploading files.
    - **PUT:** Updates an existing resource and creates it if it does not exist.
    - **DELETE:** Deletes are sources that focus on deleting the data as per the user's requests.
    - **HEAD:** It offers the same things as the source GET. The only difference is it only looks for the resource headers, and the head will not ask the body.
    - **OPTIONS:** It outlines the target resource's communication options.
    - **PATCH:** Partially updates an existing resource.

- **Headers:** HTTP headers are key-value pairs in requests and responses. They convey additional information, such as content type, length, authorisation credentials, caching instructions, etc.
- **HTTP Status Codes:** HTTP responses include status codes to indicate the result of the request:
    - **1xx (Informational):** Request received; the process is continuing.
    - **2xx (Successful):** the request from the user ID was received and accepted. (e.g., 200 0K)
    - **3xx (Redirection):** Further action must be taken to complete the request (e.g., 301 Moved Permanently, 302 Found).
    - **4xx (Client Error):** The request contains incorrect syntax or cannot be fulfilled (e.g., 400 Bad Request, 404 Not Found).
    - **5xx (Server Error):** The request was valid, but the server failed to fulfil it. (e.g., 500 Internal Server Error).

3.2.3.2 World Wide Web (WWW)

The World Wide Web (WWW), often simply referred to as the Web, is a system of interlinked hypertext documents and multimedia content that can be accessed via the Internet. Founded by Sir Tim Berners-Lee in 1989, the Web allows users to access information from anywhere in the world, provided they have a device with an Internet connection. The Web has radically altered how people communicate, interact with digital content, and obtain information.

Key Concepts of the World Wide Web:

- **Web Pages and Websites:**
    - **Web Pages:** Individual documents that contain text, images, videos, or links. Each web page is identified by a URL (Uniform Resource Locator).
    - **Websites:** Collections of related groups of linked webpages that are housed on the same domain.
- **Hypertext and Hyperlinks:** Hypertext is the foundation of the Web; it is text that links to other documents or other texts. Hyperlinks are clickable references that connect web pages, enabling easy navigation across related content.
- **Web Browser:** A web browser is software that enables users to access and interact with the World Wide Web. Popular browsers include Google Chrome, Mozilla Firefox, Microsoft Edge, Safari, and Opera. Browsers interpret the code (HTML, CSS, JavaScript) and display web content.
- **HTTP/HTTPS Protocols:** Web pages are transferred between servers and clients using HTTP (Hypertext Transfer Protocol) and HTTPS (Hypertext Transfer Protocol Secure) application-layer protocols. HTTPS adds a layer of security to ensure data privacy and integrity.

- **URLs (Uniform Resource Locators):** Resources on the Internet can be found using URLs. They usually contain the protocol.
- **HTML, CSS, and JavaScript:**
    - **HTML (Hypertext Markup Language):** It is the standard language used to create webpages. HTML uses tags to organise the page's content.
    - **CSS (Cascading Style Sheets):** A language for stylesheets that manage web pages' layouts, colours, and fonts.
    - **JavaScript:** A programming language that gives web pages dynamic behaviour and interactivity.

3.2.3.3 Firewalls

A firewall is a security device that monitors and controls the network traffic. By using some security rules, it will detect the threats that are coming to the network. The firewall was designed to provide a barrier among trusted networks to prevent threats from coming to the network. It restricts the data loss by preventing the unauthorised access to the network. It will also focus on minimising cyberattacks and strive for data integrity.

Key Functions of Firewalls:

- **Traffic Filtering:** The firewalls continuously check for threats coming from and leaving the network. They allow only legitimate traffic to pass through the network. They evaluate packets based on IP addresses, ports, and protocols according to security rules.
- **Access Control:** Firewalls enforce access control policies by allowing or blocking specific IP addresses, domains, or users. Unauthorised access is strictly prevented.
- **Monitoring and Logging:** Firewalls maintain network activity logs and generate alerts for suspicious activity. This helps monitor network security and identify potential threats.
- **Network Address Translation (NAT):** Firewalls often perform NAT, which allows multiple devices on a private network to connect to external networks through a single public IP address, thereby enhancing security and conserving IP addresses.
- **Virtual Private Network (VPN) Support:** Firewalls often support VPN functionality, enabling encrypted communication over the internet for secure remote access.

Self-Assessment Questions

7. Which of the following HTTP methods is used to retrieve data from a server without modifying the resource's state?

   A). POST
   B). PUT
   C). DELETE
   D). GET

8. What is the primary purpose of a firewall in network security?

   A). To allow all network traffic without restrictions
   B). To monitor and control network traffic based on security rules
   C). To provide web access to users
   D). To store user session data

9. Which protocol adds a security layer to HTTP to ensure data privacy and integrity?

   A). HTTPS
   B). TCP
   C). FTP
   D). SMTP

Summary

- Network protocols establish standards for device communication, enabling seamless data sharing and management across diverse systems.
- Key protocols like DNS, FTP, HTTP, and SNMP play foundational roles in translating names to IPs, transferring files, connecting devices, and managing network resources.
- Email protocols support global digital communication, enabling reliable message transmission, retrieval, and storage across networked servers and clients.
- Simplified protocols, such as TFTP, offer lightweight options for data transfer, especially where resources are limited or advanced security features are not necessary.
- The structure and functioning of the World Wide Web rely on interconnected hypertext documents, with browsers and hyperlinks providing intuitive navigation of vast digital information.
- Security and management protocols ensure the stability and reliability of the internet by managing data flows and controlling access within the network.

Terminal Questions

1. How do different network protocols contribute to seamless communication across global networks, and why is standardisation important in this context?
2. What role does DNS play in internet navigation, and how would the absence of DNS affect users and organisations?
3. In what scenarios would FTP be preferable to HTTP or HTTPS for file transfers, and what are the primary considerations when choosing between them?
4. How do email protocols like SMTP, POP3, and IMAP work together to enable email transmission, and what are the unique advantages of each protocol?
5. Why might a network administrator choose TFTP over FTP, and what are the potential security implications of this choice?
6. What is the relationship between HTTP and the World Wide Web, and how does this protocol impact web browsing experiences for users?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	A
2	B
3	C
4	B
5	C
6	B
7	D
8	B
9	A

Activity

Activity type: Offline **Duration: 2 Days**

Imagine you are a network engineer for a company that recently expanded to two new international branches. Your team ensures seamless communication across all locations, secure data transfer for company files, and efficient email communication between employees globally. You are also responsible for monitoring network health and managing network security.

Based on the given scenario, perform the given activity.

Decide which protocols (such as FTP, SFTP, or HTTPS) would be most suitable for securely transferring sensitive company documents. Explain your choice and any trade-offs.

Glossary

- **TFTP (Trivial File Transfer Protocol):** It is a lightweight protocol for transferring files without authentication, primarily in LAN environments.
- **Packet:** A small unit of data transmitted over a network. Each packet contains a portion of the data and header information such as source, destination, and error-checking data.
- **Bandwidth:** The maximum data transfer rate across a given network path, typically measured in bits per second (bps). It determines how much data can be sent or received in a fixed amount of time.
- **Latency:** The time delay from the source sending data to the receiving destination. Lower latency is critical in applications requiring real-time data, such as video conferencing.
- **Encryption:** Encoding data to prevent unauthorised access, ensuring that only authorised parties can decipher the transmitted information. Used widely in secure protocols like HTTPS.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Network Protocols:** https://www.techtarget.com/searchnetworking/feature/12-common-network-protocols-and-their-functions-explained
- **World Wide Web:** https://www.geeksforgeeks.org/world-wide-web-www/

Video Links

Topic	Link
Network Protocols	https://youtu.be/E5bSumTAHZE?si=RcLnwruY9LpcdF-j
World Wide Web	https://youtu.be/J8hzJxb0rpc?si=mjTKOvJmiGrAT-m1l

Image Credits

Fig. 1: Top-level Domains	https://slideplayer.com/slide/13633278/83/images/8/Top+Level+Domains+Suffix+Purpose+Example+com.jpg
Fig. 2: File Transfer Protocol	https://techbriefly.com/wp-content/uploads/2021/07/ftp1.jpg
Fig. 3: Control Connection	https://th.bing.com/th/id/R.3604030dfcec2eed3ab71b51e6d32937?rik=DpIMEUaXM8Ucqg&riu=http%3a%2f%2fecomputernotes.com%2fimages%2fControl-Connection.jpg&ehk=wVmktwfKrCOo6eSJQ5Z6B8C8bahOGPK9BAsbNFXrvKc%3d&risl=&pid=ImgRaw&r=0

Keywords

- Protocol Stack
- Routing Table
- Proxy Server
- HTTP
- Network Topology
- Port Forwarding

COMPUTER NETWORKS

MODULE 4

Network Devices and Network Types

Module Description

This module focuses on various network devices and essential types of networks, focusing on how they facilitate data transmission, connectivity, and network security. Initially, the module discusses network devices, which are crucial in modern communication systems. Repeaters increase signals to cover long distances, while Bridges connect multiple networks, allowing data to pass selectively based on MAC addresses. Coming to the routers direct the packets of data to the networks by using their IP addresses. In Gateways, link networks with different protocols, translating data as needed. Multiprotocol routers offer high flexibility to routers when communicating with multiple protocols simultaneously.

Hubs distribute data across a network, though they lack data filtering, while Switches are more advanced, directing data only to intended devices, improving efficiency. Modems enable digital data transmission over telephone lines, and Channel Service Units (CSUs) and Data Service Units (DSUs) are crucial for interfacing with digital and leased lines. The Network Interface Card (NIC) allows devices to connect to a network physically or wirelessly. Wireless Access Points extend wireless coverage, enabling seamless device connectivity. Transceivers are used to combine the functions of transmitter and receiver, which makes the data conversion more flexible.

The module also discusses how firewalls and proxies add layers of security, controlling data flow and filtering potentially harmful content. Various types of networks are discussed in this section. Cellular Networks rely on cellular towers for mobile communication, which is vital for mobile devices. Ad-hoc Networks establish direct device-to-device communication without a central router, offering flexibility in temporary setups. Mobile Ad-hoc Networks (MANETs) are specialised for mobile devices in dynamic environments, adjusting to changing device positions. Lastly, Sensor Networks use distributed sensors for data collection, often in environmental monitoring.

This module consists of **two** units.

Unit 4.1 Network Devices
Unit 4.2 Types of Networks

MODULE 4

Network Devices and Network Types

Unit 1

Network Devices

Unit Table of Contents

Unit 4.1 Transport Protocols and Network Quality

Aim

To provide a vision of basic, advanced, and specialised network devices, focusing on their roles in network connectivity, interconnection, and data conversion.

Instructional Objectives

This unit intends to:

- Explain the purpose and functionality of essential connectivity
- Explore the role of advanced interconnection devices, including bridges, routers, multiprotocol routers, and CSU/DSU, in network infrastructure
- Describe the function of access and conversion devices and their data conversion roles in managing network traffic

Learning Outcomes

Upon completion of the unit, you will be able to:

- Identify the different types of network devices and their specific purposes within a network
- Explore the function and significance of interconnection devices in enabling whole network communication
- Evaluate the effectiveness of various access and conversion devices in meeting network requirements

4.1.1 Basic Connectivity Devices

In computer networks, connectivity devices are hardware components that help computers and other devices communicate so that data can flow across the network. Devices controlling and guiding data flow in various ways include hubs, switches, routers, and access points. Hubs are essential devices that connect multiple computers in a network but don't filter data. Switches are smarter than hubs and can direct data to specific devices. Routers connect different networks, like your home network, to the internet, while access points enable wireless connections for devices in a network. These devices work together to make network communication fast and efficient.

4.1.1.1 Repeaters

- Electronic devices that receive signals and transmit them again are called repeaters.
- It captures the signal before it deteriorates or becomes too faint.
- It regenerates the bit and transmits the signal after being refreshed. Operating at the physical layer is a repeater.
- They don't even attempt to read the data frames. It ensures that data is sent out on each port multiple times. These are analogue gadgets that operate with connected signals.

4.1.1.2 Hubs

- A hub is typically a multiport repeater. Similar to the connector in a star topology that connects different stations, a hub connects wires from multiple branches.

Types of Hubs

- **Active Hub:** This device enhances, cleans, and relays network signals with its own power source, acting as a wiring centre and repeater to increase node distance.
- **Passive Hub:** Simply transports signals without boosting or cleaning them, so it doesn't extend node distance.
- **Intelligent Hub:** Functions like an active hub with added remote management for port setup and traffic monitoring.

4.1.1.3 Switches

- Switches offer more inventive functionality than hubs. This multiport gadget improves network efficiency.
- A switch enables connections for devices like hubs and routers and supports restricted routing information for internal network nodes.
- Switches typically can send incoming packets to the correct destination by understanding their hardware address.

- The OSI model's Data Link layer represents the switch's functionality. A multilayer switch can operate at the OSI's network and data connection layers, acting as both a switch and a router.
- Switches differ in their capabilities. Here are three types based on their capabilities:
    - Unmanaged
    - Managed
    - Smart or intelligent switches

Functionality of Network Switch

When a device is connected to a switch, the switch recognises the media access control (MAC) address, a code built into the device's network interface card (NIC).

- The switch employs the MAC address to determine which associated device is sending outgoing packets and where to deliver incoming packets.
- When a packet of data is transmitted from one device to another, the switch receives it and determines what to do by looking at the header.
- Once the destination address is matched, the switch routes the packet through the appropriate ports that link to the destination devices.
- Switches can operate at Layer 3, which is necessary for them to support virtual LANs (VLAN), which are logical network segments that can span subnets

4.1.1.4 Modems

- Modem: Short for modulator-demodulator, it transfers data between networks via telephone lines.
- Modems convert digital computer data to analogue for phone lines and back to digital.
- It converts digital signals to analogue at the transmitting end.
- It converts analogue signals back to digital at the receiving end.
- Transforms analogue signals into digital signals for the receiving computer to process.

Types of Modems

Categorisation is usually based on the following basic modem features:

- Directional capacity: Half duplex modem and full duplex modem.
- Connection to the line: 2-wire modem and 4-wire modem.
- Transmission mode: Asynchronous modem and synchronous modem.

Half Duplex

- A half duplex modem allows for one-way transmission only.
- If the modem detects a carrier on the line, it informs the DTE by sending a control signal to its digital interface of the incoming carrier.

Full Duplex

- Transmission in both directions can happen simultaneously using a full duplex modem.
- Consequently, the line has two carriers—one sending data and the other receiving it.

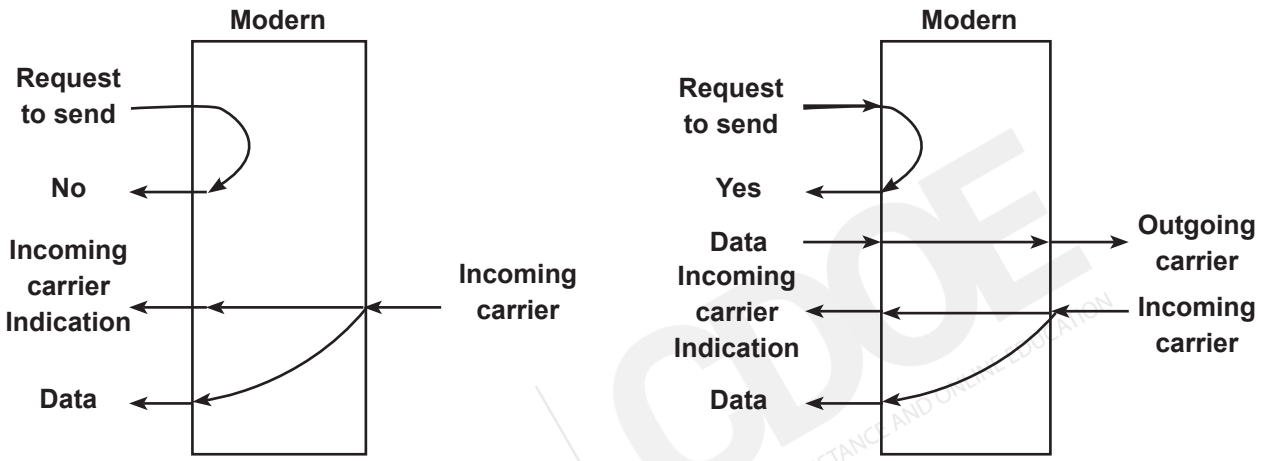


Fig. 1: Half Duplex and Full Duplex Modem's

2-Wire Modem

- Incoming and outgoing carriers use the same pair of wires with 2-wire modems.
- Since just one pair of wires is extended to the subscriber's location, leased 2-wire connections are typically less expensive than 4-wire connections.
- The telephone exchange-based data link is likewise a 2-wire connection.
- Creating half-duplex transmission with 2-wire modems is simple and uses the same frequency for incoming and outgoing carriers.
- For a full duplex mode of operation, two transmission channels are required: one for the transmit direction and the other for the receive direction.

4-Wire Modem

- A 2-wire or 4-wire connection to the transmission medium is possible for the line interface of the modem.
- One pair of wires in a 4-wire connection is used for the incoming carrier, and the other is utilised for the outgoing carrier.
- On a 4-wire connection, full duplex and half duplex data transmission modalities are both feasible.

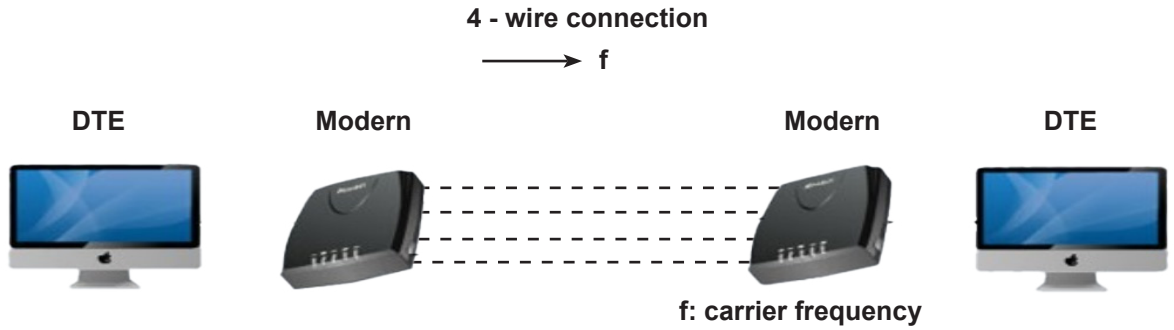


Fig. 2: 4–Wire Modem

Asynchronous Modem

- Asynchronous modems can handle start and stop bits in data bytes.
- The modem and the DTE do not use a separate timing signal or clock.
- The internal timing pulses are repeatedly synchronised to the start pulse's leading edge.

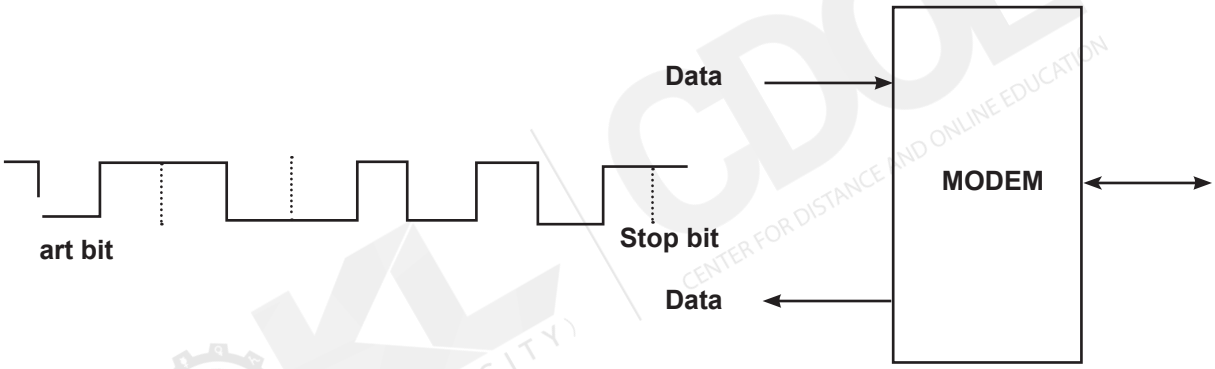


Fig. 3: Asynchronous Modem

Synchronous Modem

- A clock signal is necessary for synchronous modems to manage a constant stream of data bits.
- The clock signal and the data bits are always in sync.
- The transmitting and receiving of data bits use different clocks.
- For synchronous data bit transfer, the DTE can use its internal clock to supply the modem with it.

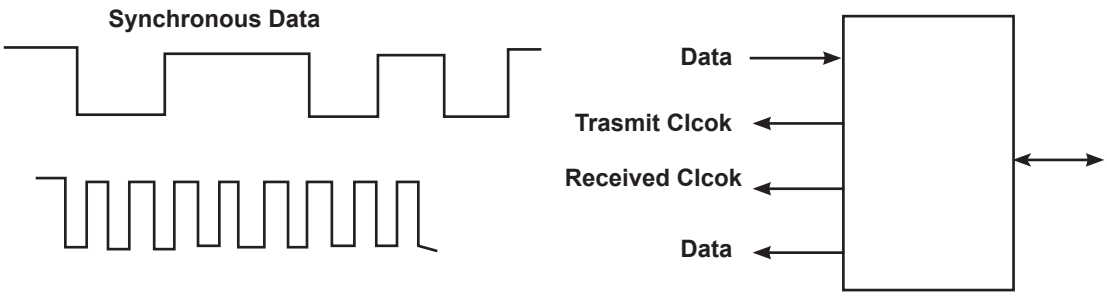


Fig. 4: Synchronous Modem

Self-Assessment Questions

1. What function does an active hub perform in a network?

   A). Transports signals without boosting
   B). Enhances, cleans, and relays network signals with its power source
   C). Provides wireless connectivity
   D). Only monitors traffic

2. Which type of modem allows for two-way data transmission at the same time?

   A). Half duplex modem
   B). Asynchronous modem
   C). Full duplex modem
   D). 2-wire modem

3. At which OSI layer do switches primarily operate?

   A). Physical layer
   B). Data Link layer
   C). Network layer
   D). Transport layer

4.1.2 Advanced Network Interconnection Devices

4.1.2.1 Bridges

- A bridge in a computer network is one type of network device used to divide a network into portions.
- In the OSI model, a bridge operates at layer 2, or the data link layer.
- Examining incoming traffic to determine whether to filter it or forward it is the primary purpose of the bridge.

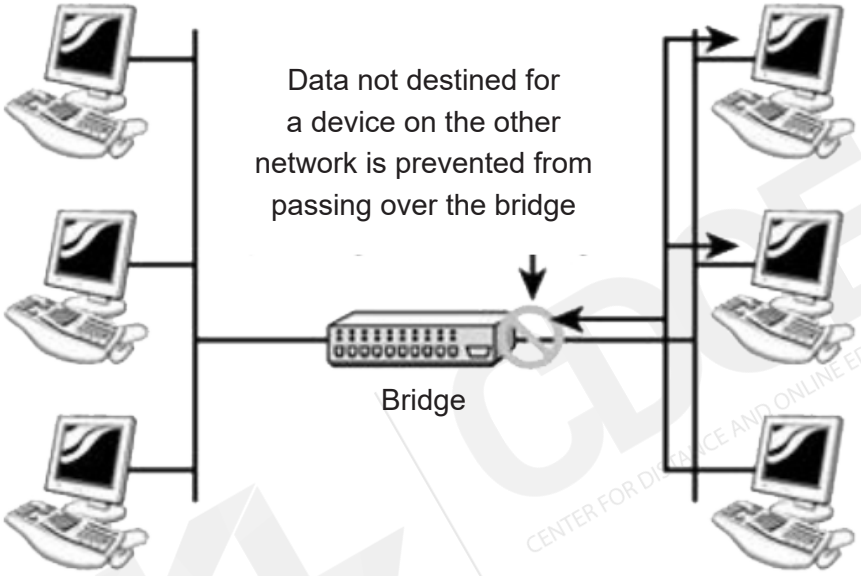


Fig. 5: Bridge

4.1.2.2 Routers & Multiprotocol Routers

- A router is a network hardware device used to transfer packets between networks. It frequently has connections to two or more networks.
- The router checks the address information in a packet to identify which port it will be sent out of when it arrives at a router port.
- A router assists in guiding data packets to their intended IP address. Different types of routers exist, including wireless routers, wired routers, core routers, and edge routers.

Multiprotocol Routers

- A Multiprotocol Router is a network device capable of supporting multiple network protocols and routing data between different types of networks.
- Because they can function with various network standards, these routers enable smooth communication between LANs (Local Area Networks), WANs (Wide Area Networks), and the Internet.

4.1.2.3 Channel and Data Service Units (CSU & DSU)

- Channel Service Unit and Data Service Unit are both referred to as CSU/DSUs
- A router is connected to a digital circuit, such as a T1 or T3 line, using a CSU or DSU, a digital interface device.
- The CSU/DSU likewise provides signal timing for communication between these devices.

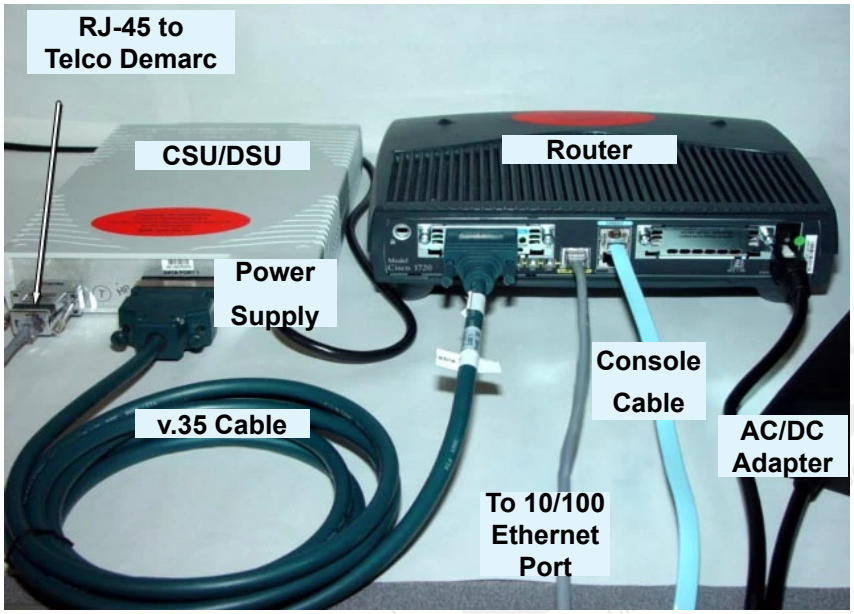


Fig. 6: CSU/DSU

The above image shows a network setup with a CSU/DSU and a router connected by various cables. The CSU/DSU is linked to a telecommunications line via an RJ-45 cable and powered by a separate power supply. A v.35 cable connects the CSU/DSU to the router, which also has a console cable, an Ethernet cable for network access, and an AC/DC power adapter. Each labelled component highlights how these devices work together to establish and manage network connections.

Self-Assessment Questions

4. What is the primary purpose of a bridge in a computer network?

   A). To divide a network into smaller segments and filter traffic
   B). To transfer data packets across multiple networks
   C). To convert digital signals to analogue signals
   D). To act as a wireless access point for network devices

5. What type of router can support various network protocols and enable communication between different types of networks?

   A). Edge Router
   B). Core Router
   C). Multiprotocol Router
   D). Wireless Router

6. Which device connects a router to a digital circuit, such as a T1 or T3 line, and provides signal timing for communication?

   A). Bridge
   B). Router
   C). CSU/DSU
   D). Switch

4.1.3 Access and Conversion Devices

Access and conversion devices are essential tools in networking that enable different types of connections and signal transformations to ensure smooth communication across networks.

4.1.3.1 Gateways

- A gateway is a telecommunications network node connecting two networks using different transmission protocols.
- A gateway acts as a network's entry and exit point because all data must travel through it or connect with it before being forwarded.
- Generally, the gateways are protocol converters that operate on any open systems interconnection (OSI) model layer and allow interoperability between two protocols.

4.1.3.2 Network Interface Cards

- A circuit board inserted into a computer to connect to the network is called an NIC (network interface controller) card. It is also referred to as a network adapter or network interface card.
- A NIC card is necessary to connect computers to a network and enhance communication between data communication devices (DCE).
- NICs have electrical circuitry that complies with the physical layer and data link standards and a port for attaching to the local area network (LAN) media.

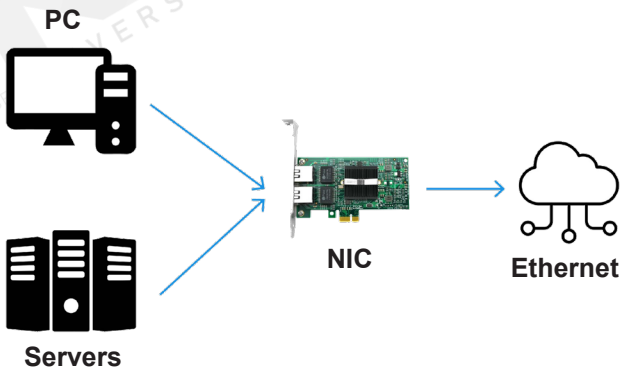


Fig. 7: Network Interface Card (NIC)

Components of a NIC Card

- Controller
- Boot ROM
- NIC port for the cable/transceiver
- BUS interface
- LED indicators
- Profile bracket

Functions of NIC

- It functions as a translator, assisting in converting data into digital signals.
- Network cards offer both wired and wireless connection options.
- In between the computer and the data network, it serves as middleware
- This network card utilises the OSI model's physical and data link layers.
- Signal transmission occurs at the physical layer, whereas data packet transfer occurs at the network layer.

The network interface card will work in two different segments.

- **Wired Network Connectivity:** In a wired network, an Ethernet cable is linked to the motherboard's network port. It allows direct connection to hubs or switches. The MAC address is used to share data or resources.
- **Wireless Network Connectivity:** Establish communication between numerous devices, a central hub, and switches using radio waves or a wireless medium.

Installing of Network Interface Card: Below is the procedure for installing a NIC Card, which stands for Network Interface Card. As its name suggests, this card is found on a computer's motherboard and is used to connect to the Internet.

- Step 1: Shut down Windows, turn off the computer and unplug it.
- Step 2: Remove the cover from your computer.
- Step 3: Find an unused expansion slot inside the computer.
- Step 4: Remove the metal slot protector from the back of the computer's chassis
- Step 5: Insert the network interface card into the slot.
- Step 6: Secure the network interface card.
- Step 7: Put the computer's case back together.
- Step 8: Plug in the computer and turn it back on.

Self-Assessment Questions

7. What is the primary role of a gateway in a network?

   A). To act as a firewall for network security
   B). To join two networks using different transmission protocols
   C). To connect multiple devices within a local network
   D). To convert digital signals into analogue signals

8. Which layer(s) of the OSI model does a Network Interface Card (NIC) primarily operate on?

   A). Physical and Data Link layers
   B). Network and Application layers
   C). Session and Transport layers
   D). Data Link and Network layers

9. How does a Network Interface Card (NIC) establish connectivity in a wireless network setup?

   A). Using an Ethernet cable
   B). Through direct MAC address sharing
   C). By using radio waves or a wireless medium
   D). By connecting to the computer's USB port

Summary

- Connectivity devices like hubs, switches, routers, and access points enable efficient communication in computer networks by guiding data flow.
- Repeaters boost signals before they weaken, while hubs connect multiple devices but don't filter data.
- Switches direct data to specific devices using MAC addresses, improving network efficiency, and operating at multiple OSI layers.
- Modems convert digital signals to analogue for phone lines and vice versa, with various types based on directionality, wiring, and transmission mode.
- Advanced devices like bridges, routers, and CSU/DSUs manage data flow across network segments, protocols, and digital circuits.
- Gateways and NICs facilitate connectivity and protocol conversion, ensuring interoperability between network systems.

Terminal Questions

1. What are the primary functions of connectivity devices like hubs, switches, and routers in a computer network?
2. How does a repeater differ from a hub, and in what situations is each device typically used?
3. Explain the different types of hubs (active, passive, and intelligent) and their roles in network connectivity.
4. Describe how a switch uses a device's MAC address to direct data traffic. How does this improve network efficiency compared to a hub?
5. What are the differences between a half duplex and a full duplex modem? Provide an example of when each type might be used.
6. How do synchronous and asynchronous modems differ regarding data transmission timing? Which applications are best suited for each type?
7. What are CSU/DSU devices, and how do they help connect routers to digital circuits like T1 or T3 lines?
8. Describe the role of gateways in networking and explain how they enable communication between networks with different protocols.
9. What is a Network Interface Card (NIC) and its key components? How does it facilitate communication between a computer and a network?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	C
3	B
4	A
5	C
6	C
7	B
8	A
9	C

Activity

Activity type: Online **Duration: 2 Days**

Scenario:

Imagine you're a network administrator for a recently expanded small company that needs an upgraded network infrastructure to support its growing team and devices. Your role involves assessing the current setup, identifying the proper devices, and ensuring smooth data flow across the network.

By referring to the above scenario, perform the following activity.

Analyse the company's existing network setup, consisting of a primary hub and outdated devices. Determine which devices (switches, routers, access points, and repeaters) should be added or replaced to improve network efficiency, reliability, and speed.

Glossary

- **Modulation:** The process of converting digital data into an analogue signal for transmission over media that only supports analogue signals, typically used by modems.
- **Intelligent Hub:** A type of hub that functions similarly to an active hub but includes remote management features, allowing for port configuration and traffic monitoring. MAC Address: A unique identifier assigned to a network interface card (NIC) that switches use to determine the destination of data packets within a network.
- **T1 Line:** A high-speed digital transmission line used to provide dedicated internet access or private network connections, supporting data rates up to 1.544 Mbps.
- **T3 Line:** A faster digital transmission line that provides higher bandwidth, supporting data rates up to 44.736 Mbps, typically used for large-scale data transmission.
- **RJ-45 Cable:** A cable used for Ethernet connections, typically used to connect routers, switches, or computers in local area networks (LANs).
- **Protocol Converter:** A device that translates communication protocols between two networks, enabling interoperability.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Network Protocols and Services:** https://itexamanswers.net/ccna-cyber-ops-version-1-1-chapter-4-network-protocols-and-services.html
- **Network Interface card:** https://www.tutorialspoint.com/what-is-network-interface-card-nic

Video Links

Topic	Link
Network Protocols and Services	https://youtu.be/E5bSumTAHZE?si=le71KtmYjNeZZYao
Network Interface card	https://youtu.be/m9evUZtkEAc?si=vhbCfuMoO-J9EOM7R

Image Credits

Fig. 1: Half Duplex and Full Duplex Modem's	https://www.differencebetween.info/sites/default/files/images/Duplexmodem.jpg
Fig. 2: 4–Wire Modem	https://2.bp.blogspot.com/-gmCduMVIv_s/WE-f7oaS6Z7I/AAAAAAAAB8c/w_IT5FdIceclejayTQxrCx_fgdWoY3tZACLcB/s1600/4-wire.jpg
Fig. 3: Asynchronous Modem	https://ecomputernotes.com/images/Asynchronous-Modem.jpg
Fig. 4: Synchronous Modem	https://th.bing.com/th/id/R.99c204632d-ffd45225fc409d340603a2?rik=%2f-Pu%2bS1GoCK%2fk1Q&riu=http%3a%2f%2fecom-puternotes.com%2fimages%2fSynchronous-Modem.jpg&ehk=MJFcJDKnXp9DrcIvnkMM6ckvoAYQME%2f-gD5r0zhTkDEs%3d&risl=&pid=ImgRaw&r=0
Fig. 5: Bridge	https://www.elprocus.com/wp-content/uploads/bridge-in-computer-network.jpg
Fig. 6: CSU/DSU	https://vignette3.wikia.nocookie.net/dotw/images/3/36/Dsu-router-connection.jpg/revision/latest?cb=20140424034824
Fig. 7: Network Interface Card (NIC)	https://www.voltrium.com.sg/en/wp-content/uploads/2022/09/What-is-a-Network-Interface-Card-scaled.jpg

Keywords

- Active Hub
- Routing Table
- IP Address
- Edge Router
- Network Adapter
- Expansion Slot
- Single Transmission

MODULE 4

Network Devices and Network Types

Unit 2

Types of Networks

Unit Table of Contents

Unit 4.2 Types of Networks

Aim

To introduce to learners key network devices, security components, and various network types and their applications.

Instructional Objectives

This unit intends to:

- Explain the functions and importance of network devices such as Wireless Access Points, Transceivers, Firewalls, and Proxies
- Describe the fundamental characteristics and architecture of cellular networks
- Explore the key concepts of Ad-hoc Networks and Mobile Ad-hoc Networks (MANETs)
- Outline the structure, purpose, and uses of Sensor Networks

Learning Outcomes

Upon completion of the unit, you will be able to:

- Differentiate between various network devices and security components
- Discuss the operational mechanisms of cellular and ad-hoc network types
- Evaluate the effectiveness of Mobile Ad-hoc Networks in different environments
- Demonstrate an understanding of the applications and benefits of Sensor Networks in modern communication

4.2.1 Network Devices and Security Components

A network can be connected, managed, and protected with network devices and security components. Data can move safely between various network parts by routers, firewalls, and access points.

4.2.1.1 Wireless Access Points

- A networking device known as a Wireless Access Point (WAP) enables wireless devices to join a wired network via Wi-Fi or similar protocols.
- WAPs serve as a central hub in a wireless network, extending the reach of a wired network and enabling wireless communication for mobile devices such as laptops, smartphones, and IoT devices.

Key Functions of Wireless Access Points:

- **Wireless Connectivity:** WAPs allow wireless devices to join a network, usually through Wi-Fi. They transform a router's or switch's wired signal into a wireless one.
- **Extending Network Coverage:** WAPs can expand the coverage area of an existing wireless network, providing wireless access in areas where the signal from the main router might be weak or non-existent.
- **Network Bridging:** WAPs can also bridge various network segments to facilitate communication between wireless networks.
- **Managing Multiple Devices:** Access points can distribute the load and effectively manage network traffic by supporting numerous simultaneous connections from different wireless devices.

4.2.1.2 Transceivers

- A transceiver is an electronic gadget that combines a transmitter and receiver into one unit.
- Transceivers are vital in many communication systems because they primarily send and receive signals.
- Transceivers are frequently used in wired and wireless communication networks, such as Ethernet, fibre optics, and radio communication systems.

Key Functions:

- **Transmission:** The transceiver sends data in the form of signals, converting information into a suitable format for transmission (e.g., converting digital data into radio signals or light pulses).
- **Reception:** It receives incoming signals, decodes them, and converts them back into a format usable by the connected system (e.g., converting radio signals or light pulses into digital data).

- **Signal Conversion:** Transceivers can also modulate and demodulate signals in specific systems, converting between various signal types (electrical to optical).

4.2.1.3 Firewalls

A security system is a tool that monitors and regulates all network traffic, both inbound and outbound, based on predetermined rules. It is a barrier to keeping networks and PCs safe from online threats and illegal access.

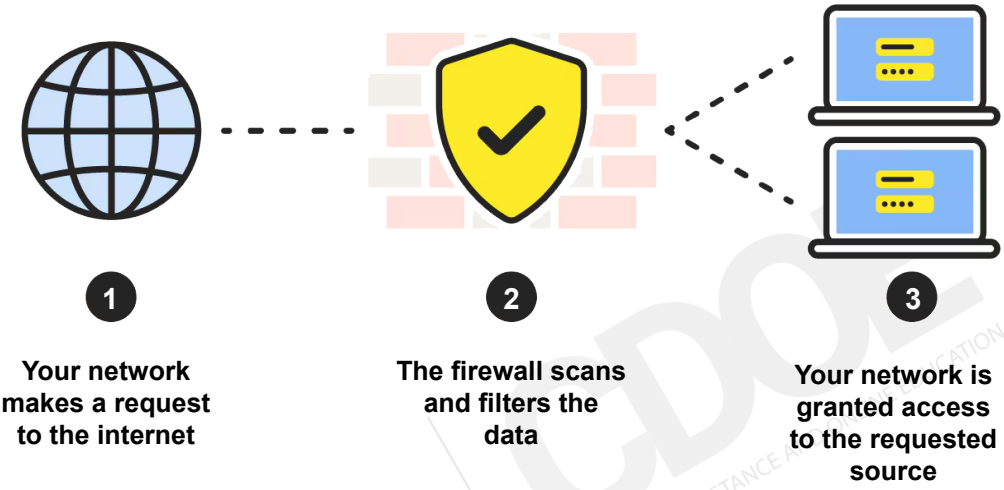


Fig. 1: Working of a firewall

There are three types of firewalls:

1. Network-based firewalls
2. Application firewalls, and
3. Proxy server firewalls

Network-Based Firewall: Network traffic is routed by a network-based security system. Packets in the TCP/IP protocol stack are routed based on network rules that are either administrator-defined or defaulted. Network-based firewalls come in two varieties:

- **Stateless Packet Filtering Firewalls:** These firewalls are used when packet sessions are absent. They lack source logging, packet inspection, learning, and validation capabilities and need manual parameter inputs. As a result, malicious IP addresses may not be the source of security threats. A stateless firewall also prevents more complex packet sessions from passing through.
- **Stateful Inspection Firewalls:** These firewalls expedite packet processing using tables and active sessions. When evaluating a packet that is not part of the table, new connection rules are applied. Two drawbacks of stateful firewalls are that they can bottleneck traffic and are process intensive. DDOS and MITM attacks are, therefore, feasible.

Application Firewall: The TCP/IP stack is used by an application firewall, also known as an application layer firewall, to filter and intercept all packets of traffic going to and coming from apps. It goes further than that, though. Additionally, this firewall regulates how particular applications on a network or server run files and code. This implies that an intruder cannot execute malicious code if they manage to get inside. Three categories of application firewalls exist:

- **Passive App Firewalls:** These firewalls inspect all incoming traffic against known vulnerabilities but do not deny traffic even if a potential attack is found.
- **Active App Firewalls:** These firewalls inspect all incoming traffic against known vulnerabilities. Only the traffic found to be “clean” will pass to the application.
- **Web App Firewalls:** These WAFs filter, monitor, and block traffic specifically to/from web applications.

4.2.1.4 Proxies

A proxy server is protocol-aware and acts as an entry point between networks. It responds to input packets and blocks other packets. It caches, filters, logs, and controls traffic from devices to keep networks secure. Its single-entry point allows organisations to assess threats, implement attack and error detection, and perform validity checks. These proxy servers are the most secure type of firewall, as they filter packets through a protected proxy server before traffic reaches the network perimeter. The above-and-beyond security capabilities of proxy servers include:

- **Deep packet inspection, which searches for:**
    - Signatures of malware
    - Outgoing, sensitive data
    - Restricted content
- **Sandboxing:** This benefits your network by allowing threats to “play out” in an isolated environment.
- **Traffic validation:** It uses administrative tools to validate traffic from recognised sources.

Key Functions of Proxies:

- **Anonymity:** Users who are worried about their privacy while using geo-restricted content will use proxy servers to hide their IP address.
- **Content Filtering:** Organisations frequently use proxy servers to restrict access to websites or categories of content. Restricting inappropriate or non-work-related content is a frequent practice in businesses and schools.
- **Improved Security:** These Proxy Servers are more helpful in enhancing security by monitoring and filtering threats to the network. They can block malware, phishing attempts, and other security threats.

- **Bandwidth Saving and Caching:** Proxies can cache frequently requested content, so if several users ask for the same thing, the proxy can provide it from its cache rather than constantly retrieving it from the internet. As a result, load times are improved, and less bandwidth is used.
- **Access Control:** Proxies can be configured to enforce access policies, allowing administrators to control which users or devices can access specific resources or websites.

Self-Assessment Questions

1. Which of the following is a primary function of a Wireless Access Point (WAP)?

A). Encrypting data packets
B). Extending network coverage
C). Monitoring network traffic for security threats
D). Converting analogue signals to digital signals

2. Which type of firewall inspects packets and creates a session table for active connections, allowing more secure and efficient traffic handling?

A). Stateless Packet Filtering Firewall
B). Network-Based Firewall
C). Stateful Inspection Firewall
D). Web Application Firewall

3. What are the primary benefits of using a proxy server?

A). Providing anonymity by hiding users' IP addresses
B). Blocking all incoming and outgoing traffic
C). Modulating wireless signal strength
D). Converting digital data into optical signals

4.2.2 Overview of Network Types

Network types refer to diverse ways computers and devices connect and communicate.

4.2.2.1 Cellular Networks

- Cellular networks are wireless communication networks, enabling more devices to communicate even when they are far apart.
- They create smaller areas known as cells, each serviced by a base station or cell tower.

Key Components of Cellular Networks:

- **Cell Towers (Base Stations):** Every network cell has a cell tower connecting to nearby mobile devices. The tower transmits and receives radio signals, linking users to the network.
- **Mobile Devices:** Mobile devices connect to the nearest cell tower using radio signals. This ensures a smooth connection between the cells without interruptions.
- The network facilitates **smooth handoffs between cells**, enabling continuous service, and these devices are mobile.
- **Core Network:** This network is the most important cellular network and is responsible for routing calls, messages, and data. It connects to external networks like the Internet and other telecommunications systems. Components include the Mobile Switching Centre (MSC), Gateway GPRS Support Node (GGSN), and Home Location Register (HLR), which manage user information, connections, and data transmission.
- **Frequency Bands:** Cellular networks transmit data using specific radio frequencies. Different generations of networks (e.g., 3G, 4G, 5G) use different frequency bands, allowing multiple devices to communicate simultaneously without interference.
- **Cells:** The entire network is divided into cells, each covered by a cell tower. These cells are typically hexagonal and allow for efficient reuse of frequencies across the network, enabling scalability.

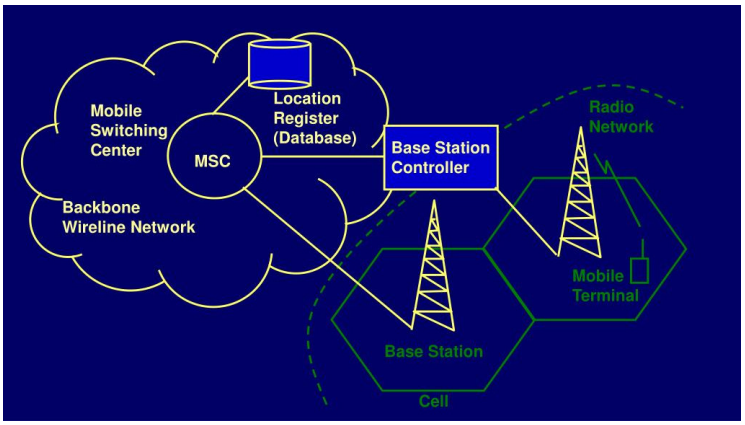


Fig. 2: Cellular Network Architecture

By segmenting the region into tiny units known as “cells,” cellular network architecture enables mobile devices to communicate over vast areas. Each cell has a base station or mobile tower that connects to neighbouring mobile phones for data and calls to move throughout the network. The Mobile Switching Centre (MSC), towers are connected to a central hub that routes data and calls to the appropriate network locations. Additionally, the network links to other networks, like the Internet or other phone networks, enabling communication outside the local area. This structure lets users move between cells without losing connection, as the call or data session is automatically transferred to the next tower when they move out of range.

4.2.2.2 Ad-hoc Networks

- Ad-hoc Networks are decentralised wireless networks that allow devices to communicate directly with each other without relying on pre-existing infrastructure like routers, base stations, or access points.
- Each network device, or node, acts as a client and a router, forwarding data to other devices. Ad-hoc networks are helpful when traditional networking infrastructure is unavailable or impractical.

Key Features of Ad-hoc Networks:

- **Infrastructure-less:** Ad-hoc networks do not rely on fixed infrastructure like cell towers or access points. Instead, they are formed dynamically when devices come into range and communicate directly.
- **Decentralised:** Control is not centralised. Every network device functions independently and transfers data between nodes.
- **Self-Organising:** The network is extremely flexible and adaptive because it automatically forms and adapts according to device availability and movement.
- **Dynamic Topology:** The network’s topology changes as devices move in and out of range. Nodes may leave the network, new nodes may join, and connections can be reestablished or rerouted.
- **Multi-hop Communication:** When two devices are out of direct communication range, data is passed through intermediate nodes (multi-hop) to reach its destination.

4.2.2.3 Mobile Ad-hoc Networks

- Mobile Ad-hoc Networks (MANETs) are decentralised, infrastructure-less wireless networks where mobile devices communicate directly. In MANETs, each device (node) acts as a host and a router, forwarding data to other nodes and enabling communication across the network.
- MANETs’ dynamic and self-organising characteristics enable their rapid deployment in locations where conventional networking infrastructure is either unobtainable or impractical.

Key characteristics

- **Infrastructure-less:** Unlike traditional networks, MANETs do not rely on pre-existing infrastructure like routers, access points, or base stations.
- **Dynamic Topology:** The network's topology constantly changes as nodes come into and leave range. To ensure constant communication, the network must update its routes.
- **Multi-hop Communication:** If two devices are not in direct communication range, data can be transmitted via intermediary nodes. Because of this, MANETs can communicate with devices that are not near one another.
- **Self-Healing:** MANETs can recover from node or link failures. If a node moves out of range or a link breaks, the network automatically reroutes data to ensure continuous communication.
- **Decentralised:** There is no central authority in charge of running the network. Because each node oversees data forwarding and routing, MANETs are incredibly adaptable and durable when centralised control is impractical.
- **Autonomy and Scalability:** MANETs can be installed in both small and large settings because of their high scalability. Every device is a router, allowing the network to expand dynamically as new nodes are added.

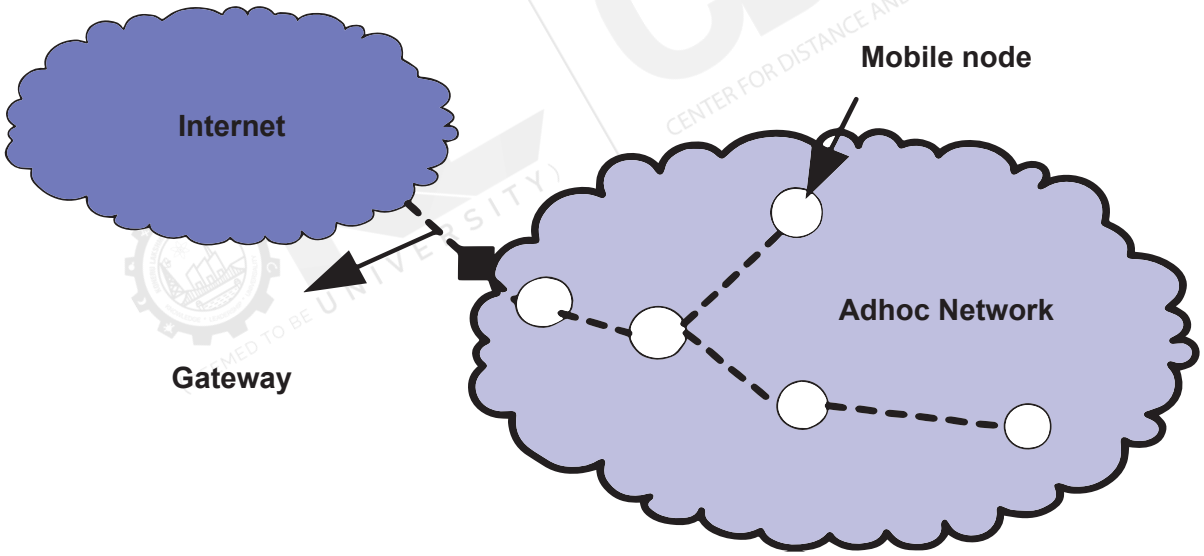


Fig. 3: Ad-hoc network with mobile nodes

Without a fixed infrastructure, such as a router, this diagram illustrates an ad hoc network with mobile nodes or devices that can connect directly to one another. The flexible network is formed by the dashed lines connecting the mobile nodes, showing they can communicate wirelessly. By connecting the ad hoc network to the external Internet, a gateway can also connect the network to the Internet. This setup allows devices in the ad hoc network and internet resources to communicate.

Self-Assessment Questions

4. What is a vital characteristic of a cellular network that enables devices to maintain continuous communication while moving across different areas?

   A). Multi-hop Communication
   B). Self-Healing
   C). Decentralised control
   D). Handoff between cells

5. What feature allows an ad hoc network to function without relying on fixed infrastructure, such as routers or access points?

   A). Centralised control
   B). Infrastructure-less setup
   C). Core Network
   D). Frequency Bands

6. In a Mobile Ad-hoc Network (MANET), if two devices are not within direct communication range, how can they still communicate?

   A). Using cell towers
   B). Through an internet connection
   C). Via multi-hop communication
   D). By establishing a core network

4.2.3 Sensor Networks

Wireless Sensor Networks (WSNs) are a type of ad hoc network made up of tiny, independent devices called sensors that track environmental or physical parameters like temperature, humidity, vibration, pressure, or motion to monitor large-scale environments without the need for infrastructure.

Key Components of Sensor Networks:

1. **Sensor Nodes:** Each node consists of sensors, a processor, a communication module, and a power source (usually batteries). These nodes collect data from the environment and transmit it to a base station or other nodes in the network.
2. **Sink Node (Base Station):** A sink node, or base station, acts as a central hub where sensor data is collected, processed, and transmitted to the user or external network. The base station is often connected to more robust systems for data analysis.
3. **Communication Module:** A multi-hop network is established by each sensor node wirelessly connecting to nearby nodes.
4. **Power Source:** Typically, sensor nodes run on batteries, so network longevity depends on energy efficiency. Some networks may employ energy-harvesting methods or solar power to increase node lifespan.
5. **Processor and Memory:** Each node has a microcontroller or processor to process the data collected by the sensors. Memory stores data temporarily before it is transmitted.

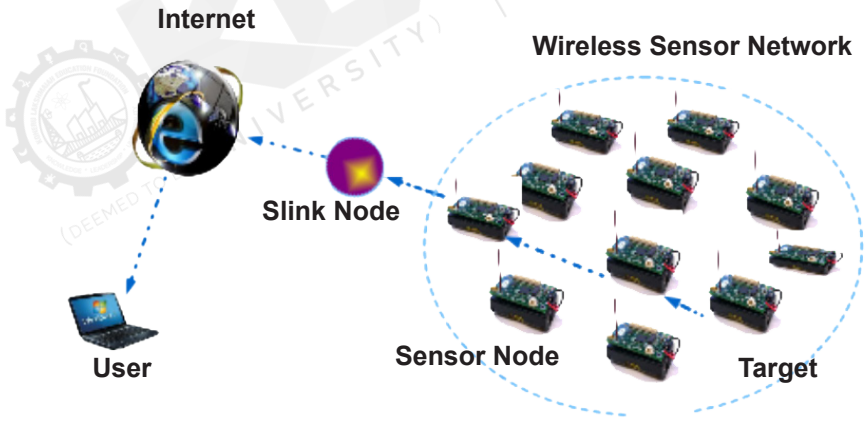


Fig. 4: Wireless Sensor Network

The wireless sensor network (WSN) consists of multiple sensor nodes that gather data from their surroundings, such as temperature, humidity, or movement. The sink node communicates with these sensors, a central device that collects data from the network's sensor nodes. The data can then be sent to a user who can view and track it remotely after the sink node connects to the internet. This configuration makes real-time monitoring and control of the sensor data possible, which uses an internet-enabled device to provide helpful information for applications like environmental monitoring, smart cities, and industrial automation.

Self-Assessment Questions

7. What is the primary role of a sensor node in a Wireless Sensor Network (WSN)?

   A). To collect environmental data and transmit it within the network
   B). To act as a central hub for data collection
   C). To provide power to the entire network
   D). To connect directly to the internet

8. In a Wireless Sensor Network, what is the primary function of the sink node (base station)?

   A). To serve as the power source for all sensor nodes
   B). To control the sensor nodes directly
   C). To store all data permanently
   D). To process and transmit collected data to the user or external network

9. What power source is typically used for sensor nodes in a Wireless Sensor Network?

   A). Batteries, sometimes with energy-harvesting methods
   B). Solar power only
   C). Wired electricity
   D). Centralised power grid

Summary

- Network devices like routers, firewalls, and proxies are vital for managing connections and ensuring secure data transmission.
- Wireless Access Points (WAPs) provide wireless connectivity, bridging wired networks and enabling multi-device access.
- Transceivers enable the sending and receiving of signals in networks, which is essential for wired and wireless communication.
- Firewalls control network traffic and protect against threats, with various types offering different levels of inspection.
- Proxies filter and secure traffic, improve network performance and provide anonymity and access control.
- Cellular and ad-hoc networks allow device communication, with cellular networks using towers and ad-hoc networks enabling direct device links.

Terminal Questions

1. Explain the role of a Wireless Access Point (WAP) in a network. How does it extend the coverage and facilitate communication between devices?
2. Describe the functions of a transceiver in communication systems. How does it handle both the transmission and reception of signals?
3. Differentiate between stateful and stateless firewalls. What are the main advantages and disadvantages of each?
4. What are the key functions of a proxy server in network security, and how does it enhance privacy and security for users?
5. What are the main components of a cellular network, and how do they work together to ensure continuous service across different areas?
6. Discuss the characteristics of Mobile Ad-hoc Networks (MANETs). How do they differ from traditional networks, and what are their advantages in terms of flexibility and scalability?

Answer Keys

Self-Assessment Questions	
Question No.	**Answers**
1	B
2	C
3	A
4	D
5	B
6	C
7	A
8	D
9	A

Activity

Activity type: Online **Duration: 2 Days**

Scenario:

You have been hired as the network administrator for a newly established bright office. The office has multiple wireless devices (laptops, smartphones, IoT devices like bright lights, thermostats, security cameras, and printers) that must be connected to the corporate network. Your task is to set up the network and implement security measures to ensure its safety and efficiency.

Based on the given scenario, perform the following activity

Choose the appropriate type of firewall (Stateful vs. Stateless) and justify your decision based on the network's needs.

Glossary

- **Transceiver:** A device that transmits and receives communication signals, often used in networking to convert and send signals over a medium (like fibre or copper cables).
- **Proxy Server:** A server that acts as an intermediary for client requests seeking resources from other servers, often used for security, caching, and content filtering.
- **Network Segmentation:** Dividing a computer network into sub-networks to improve performance and security by isolating network parts.
- **VPN (Virtual Private Network):** A secure network connection encrypts data and allows remote users or networks to connect securely to the leading network.
- **Intrusion Detection System (IDS):** A security system to detect unauthorised access or abnormal activity on a network or device.
- **Intrusion Prevention System (IPS):** A security system that not only detects threats but also takes action to prevent them by blocking or alerting administrators.

Bibliography

Textbooks

- Tanenbaum, S. (2022). *Computer Networks*. Delhi, India: Pearson Education.
- Peterson, L. L., & Davie, B. S. (2021). *Computer networks* (6th ed.). Oxford, England: Morgan Kaufmann.

Bibliography

External Resources

- Tanenbaum, A. S., & Wetherall, D. J. (2010). *Computer Networks* (5th ed.). Upper Saddle River, NJ: Pearson.
- Singh, B. (2014). *Data Communications and Computer Networks* (4th ed.). Delhi, India: PHI Learning.

e-References

- **Cellular Networks:** https://www.geeksforgeeks.org/cellular-networks/
- **Mobile Ad-hoc Network:** https://www.geeksforgeeks.org/introduction-of-mobile-ad-hoc-network-manet/

Video Links

Topic	Link
Ad-hoc Sensor Network	https://youtu.be/ycaz99NogS4?si=-IZVD5aAaUjuDCgz
Firewalls	https://youtu.be/9GZlVOafYTg?si=zVTVZEN-hWX-004MZ

Image Credits

Fig. 1: Working of a firewall	https://us.norton.com/content/dam/blogs/images/norton/am/how-a-firewall-works.png
Fig. 2: Cellular Network Architecture	https://image2.slideserve.com/4410446/cellular-network-architecture-l.jpg
Fig. 3: Ad-hoc network with mobile nodes	https://www.researchgate.net/publication/46093654/figure/fig9/AS:670711450439701@1536921479617/Mobile-Ad-Hoc-network-connected-with-Internet.png
Fig. 4: Wireless Sensor Network	https://th.bing.com/th/id/R.382a29b601c3d2ee0a66d4edb74015c3?rik=AuK8%2fJT0YJ39ww&riu=http%3a%2f%2fmicrocontrollerslab.com%2fwp-content%2fuploads%2f2015%2f08%2fWIRELESS-SENSOR-NETWORKS.png&ehk=WwpwuBOGqUB7IUCCbiVEW6KLb0VmbPq10Dmp9yRTFDc%3d&risl=&pid=ImgRaw&r=0

Keywords

- Encryption
- Two-factor authentication
- Access Control List
- NAT (Network Address Translation)
- DHCP (Dynamic Host Configuration Protocol)

MODULE 5

Networking Solutions using Routing Algorithms

Unit 1

Foundations of Network Routing and Simulation with Cisco Packet Tracer

Unit Table of Contents

Unit 5.1 Foundations of Network Routing and Simulation with Cisco Packet Tracer

Aim

This unit aims to provide a comprehensive overview of the installation and application of the Cisco Packet Tracer.

Instructional Objectives

This unit intends to:

- Explain the essential functions and installation process of the Cisco Packet Tracer and create a peer-to-peer network simulation
- Demonstrate the configuration of IP and MAC addresses, identification of port numbers, and application of data link layer framing methods in Cisco Packet Tracer

Learning Outcomes

Upon completion of the unit, you will be able to:

- Explore the configured IP and MAC addresses in a peer-to-peer network simulation within Cisco Packet Tracer
- Identify and apply port numbers and data link layer framing methods, including the character count framing method, in a simulated network environment

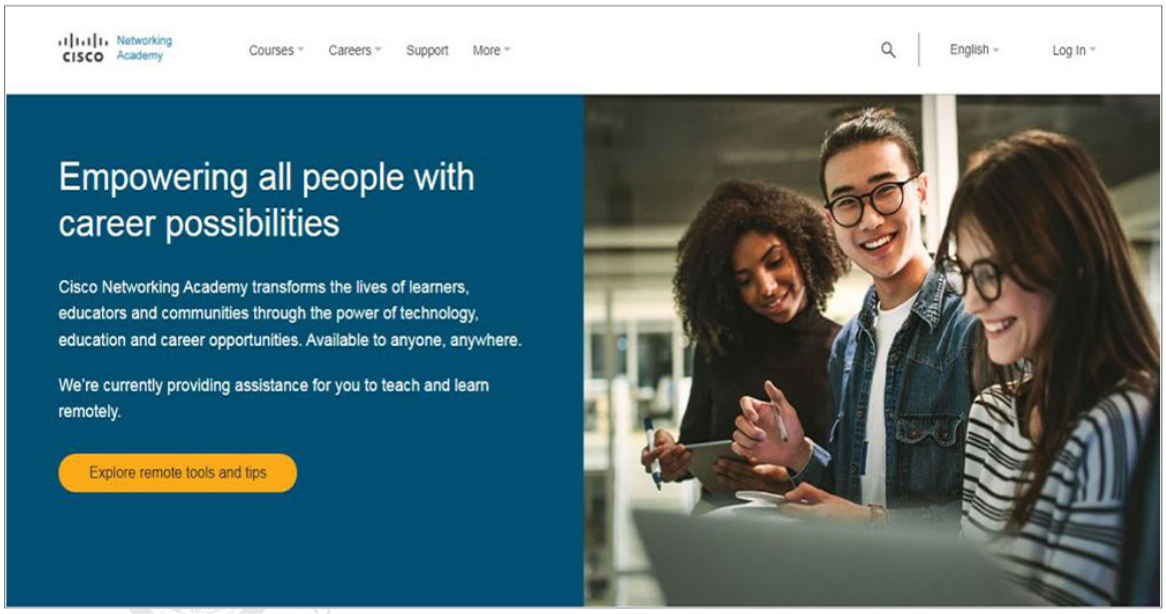
5.1.1 Introduction and Installation of Cisco Packet Tracer

Packet Tracer is a computer program developed by Cisco Corporation to facilitate network simulations, helping users fluently grasp networking and cybersecurity concepts. It's freely available for various operating systems such as macOS, Windows, and Linux. The software features a user-friendly interface, making it simple to use.

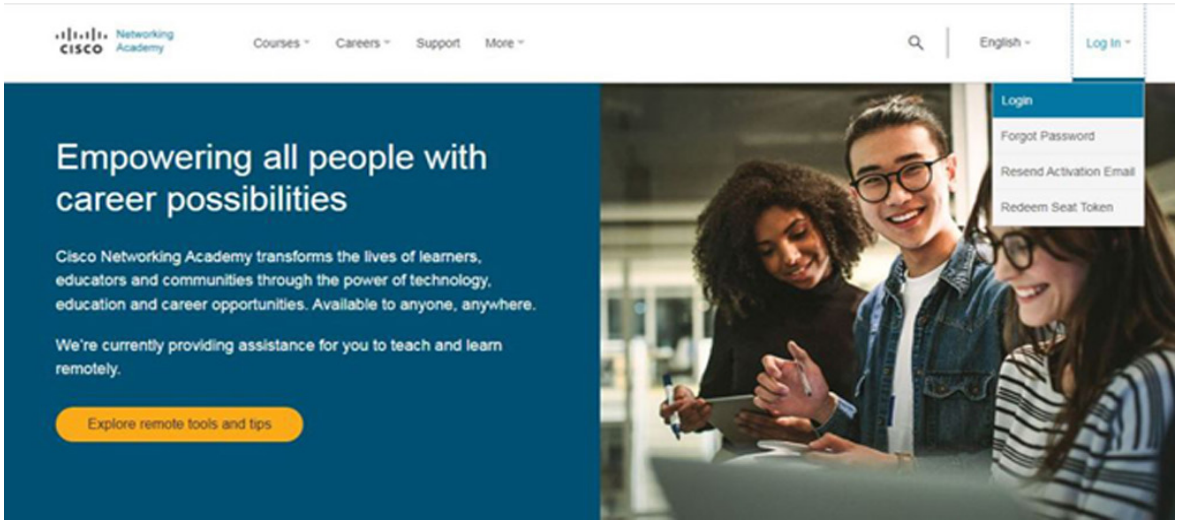
Installing Packet Tracer on Windows

Follow the below procedure to install Packet Tracer on Windows

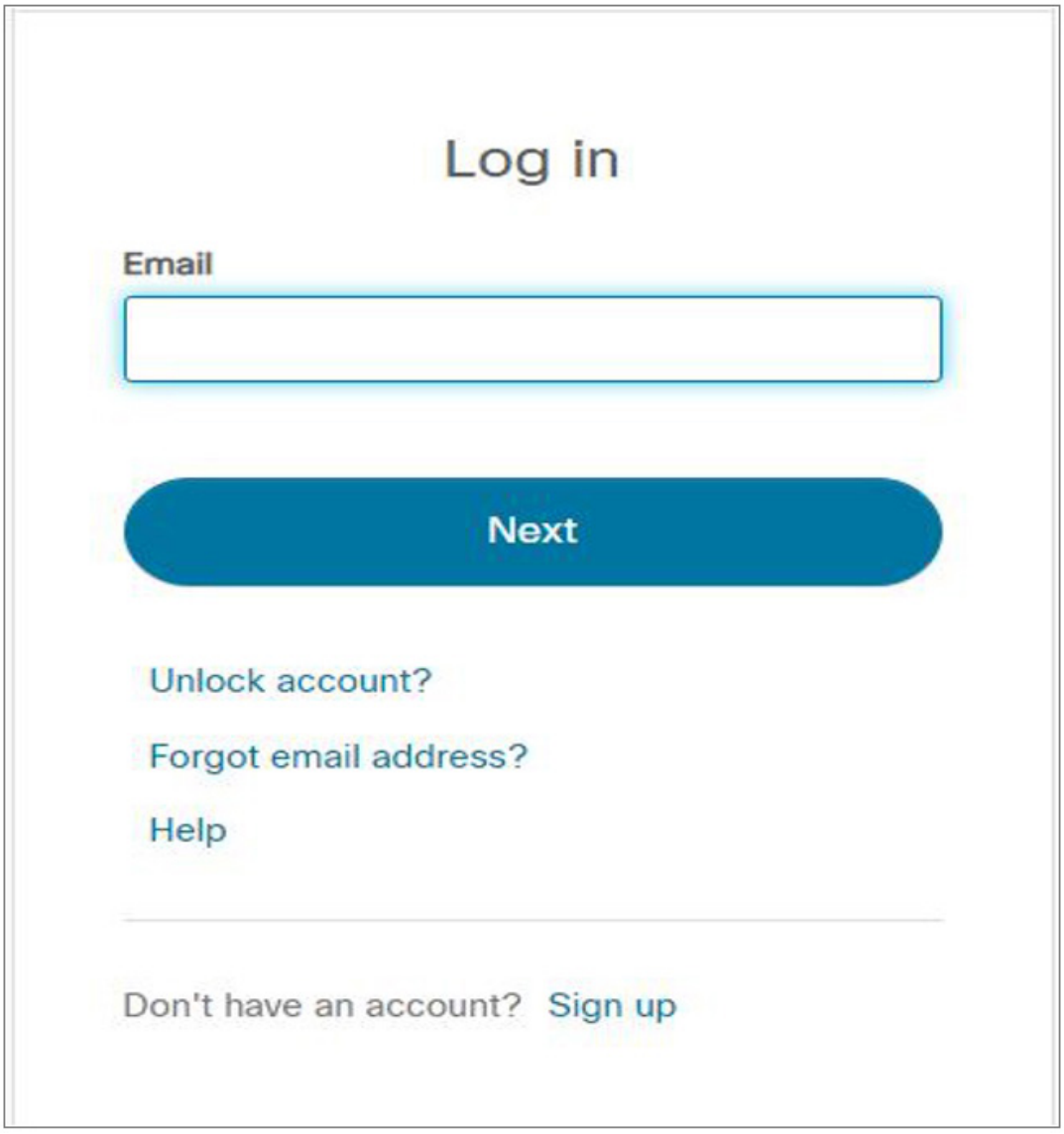
Step 1: Visit the official website of Netacad using any web browser.



Step 2: Press the login button and select the log-in option.

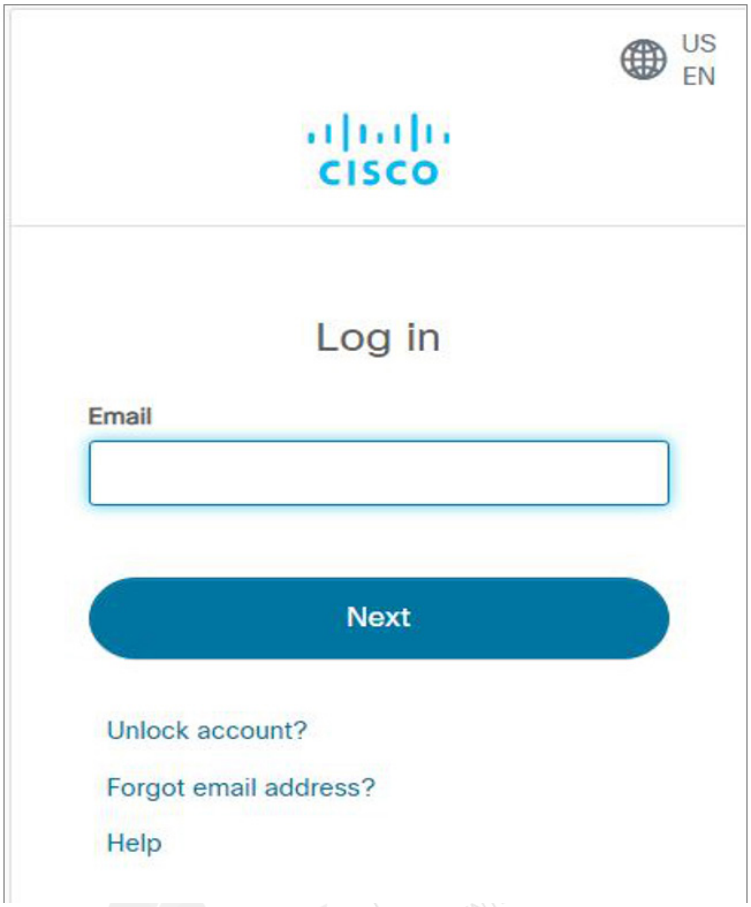


Step 3: Next screen will appear, click on the sign- up option.

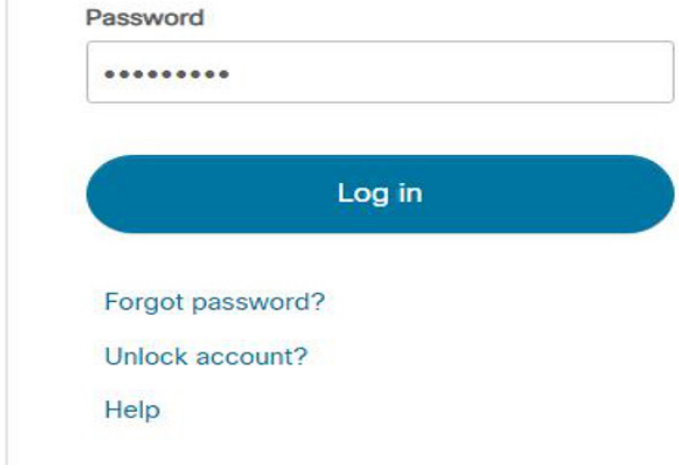


Step 4: The next screen will appear and will ask for email, password and other simple details, fill them and click on Register.

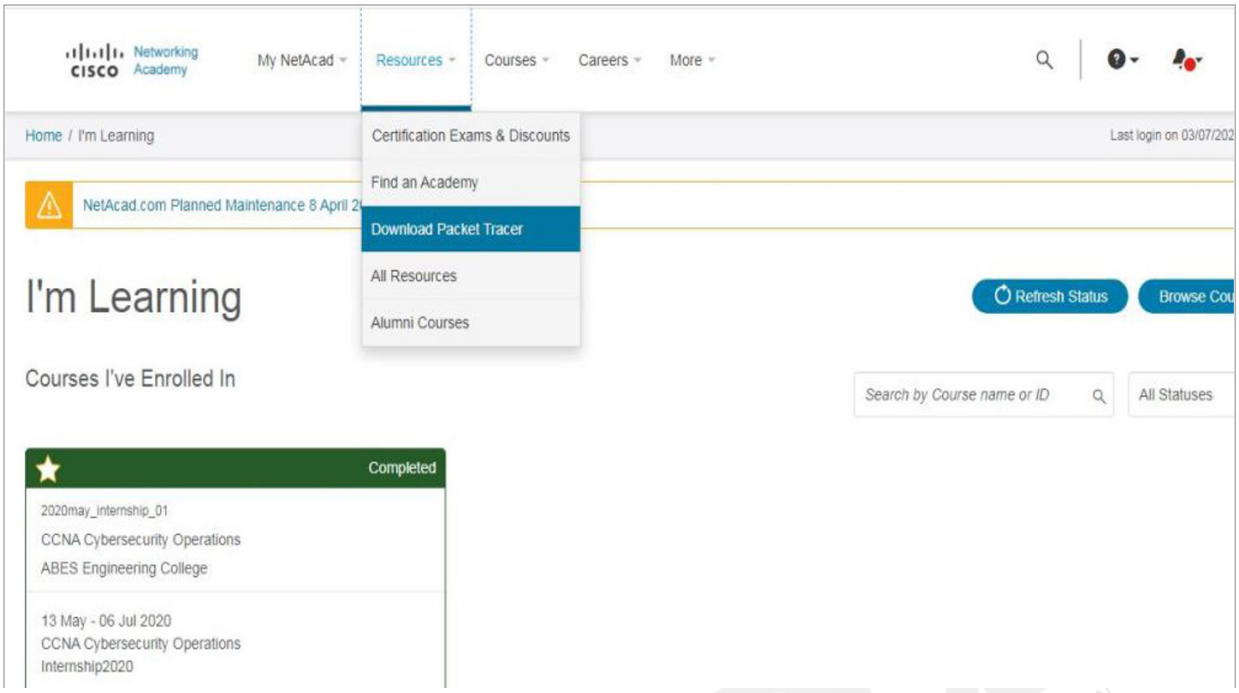
Step 5: Now the login screen appears again so fill in the Email id.



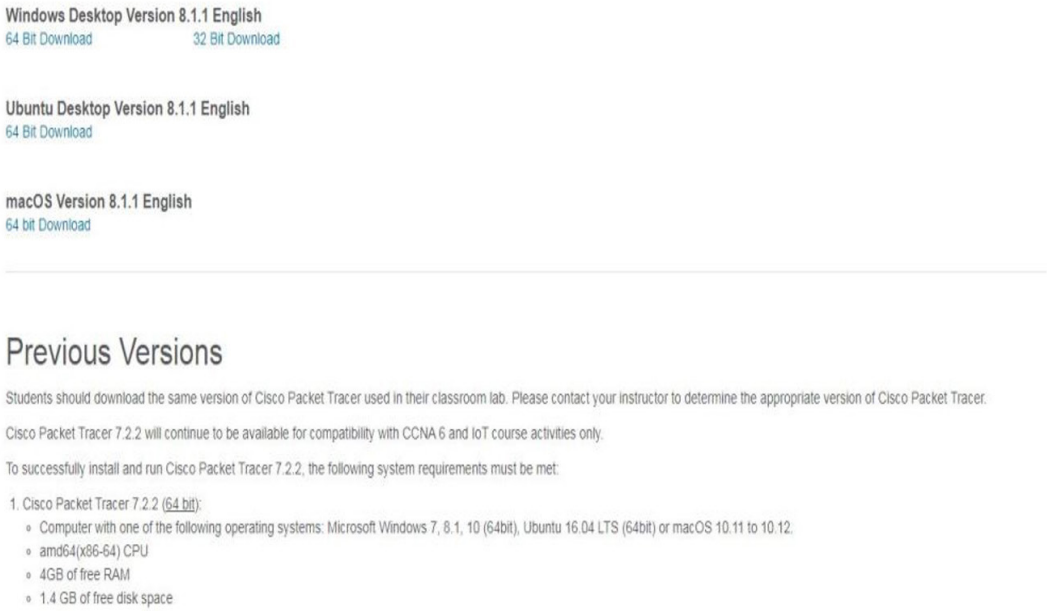
Step 6: On the coming screen enter the password and press the Login button.



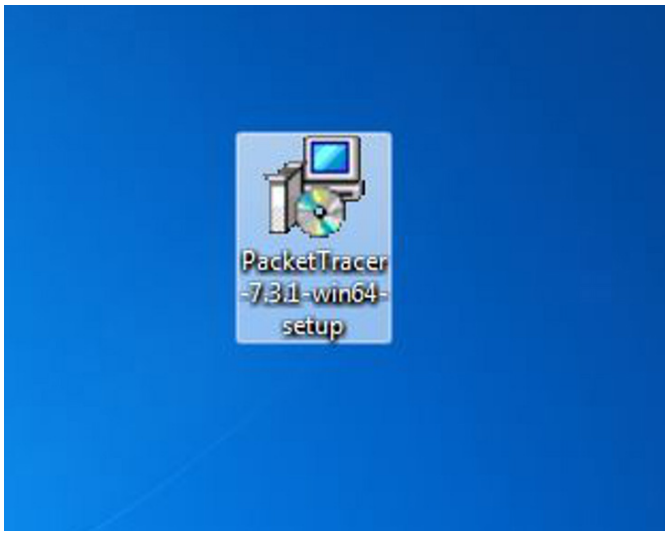
Step 7: The Dashboard will initialize, now click on Resources and choose the Download Packet Tracer Option.



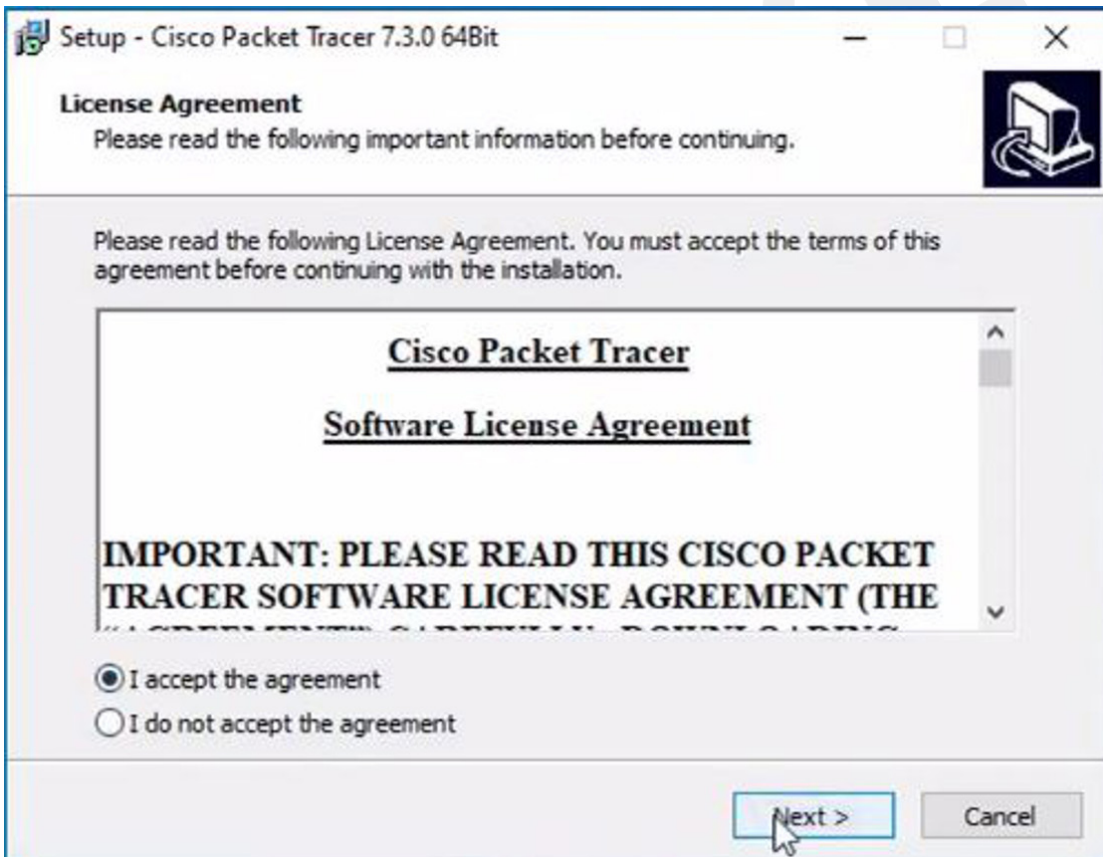
Step 8: On the coming web page choose the operating system to download the packet tracer. Downloading will start automatically.



Step 9: Check for the executable file in your system and run it.

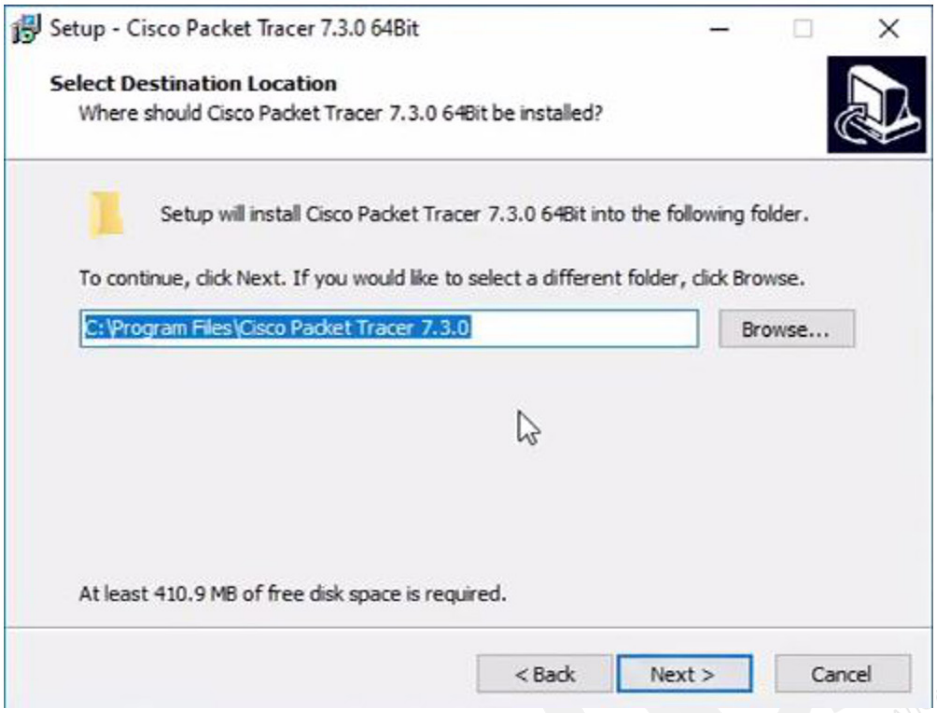


Step 10: The next screen is of License Agreement so Click on I accept the license.

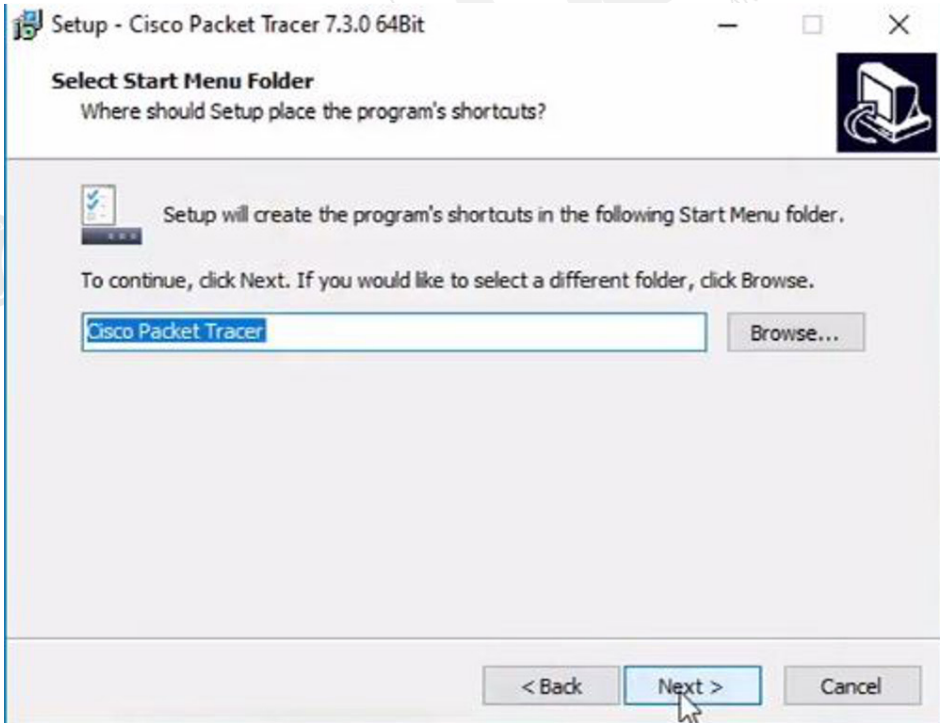


Step 11: Choose the installing location which has sufficient space.

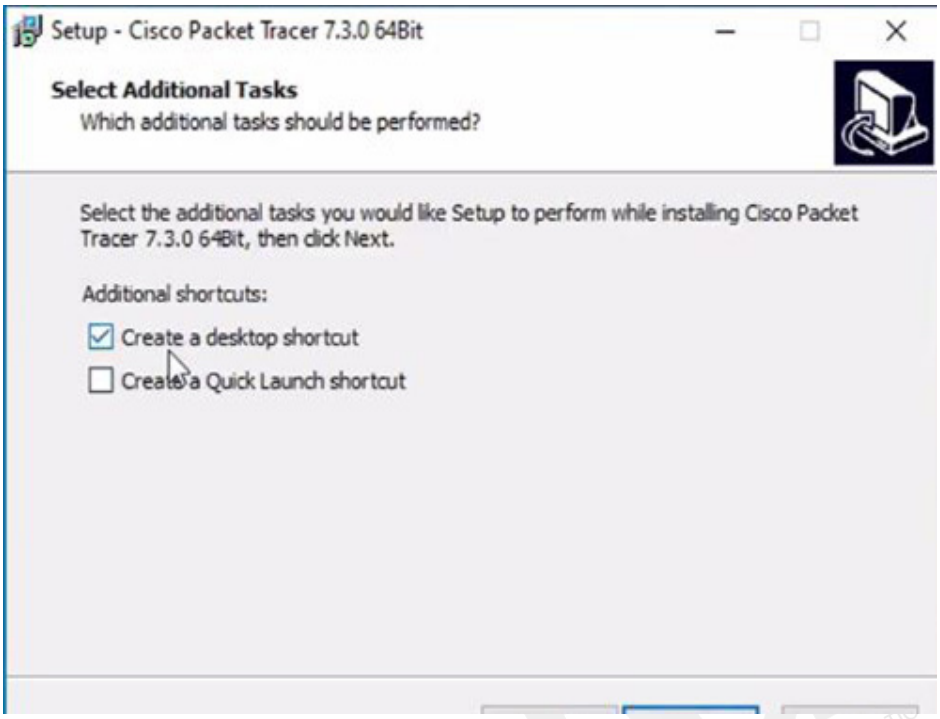
Step 10 Step 11 Step 12 Step 13 Step 14 Step 15 Step 16 Step 17 Step 18



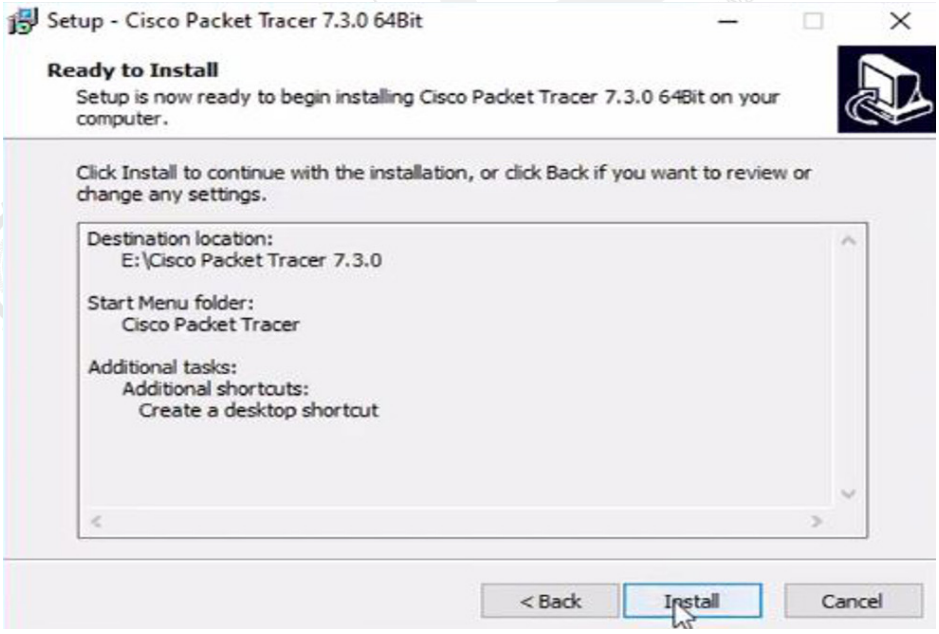
Step 12: Select the start menu folder and click the Next button.



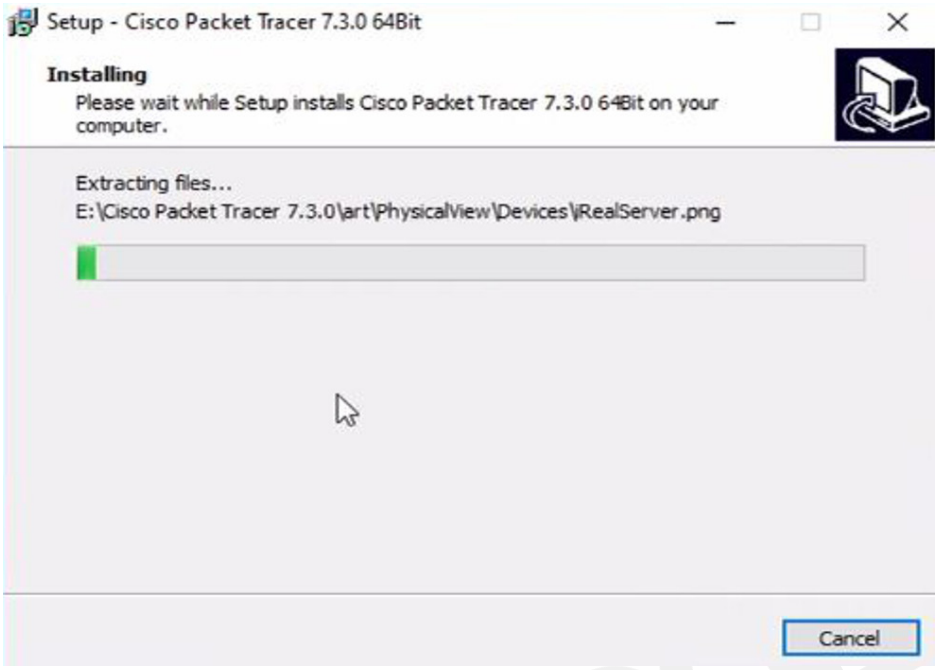
Step 13: Check the box for creating a desktop icon and click on the Next button.



Step 14: Now packet tracer is ready to install so click on the Install button.



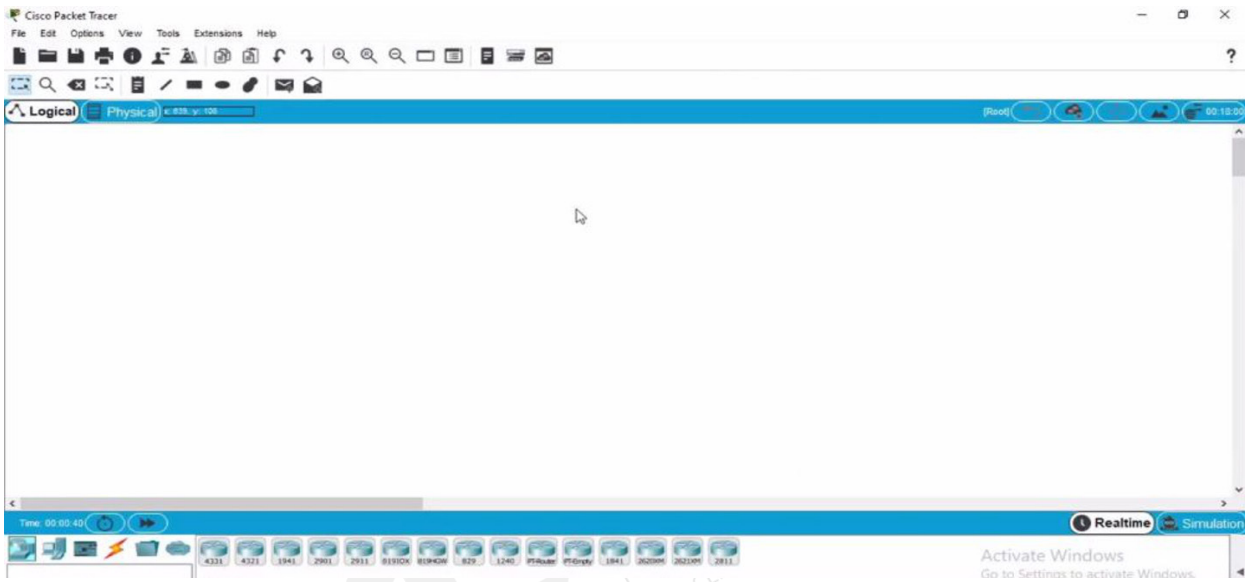
Step 15: The installation process will start and will hardly take a minute.



Step 16: Click on the Finish button to complete the installation

Step 17: An icon is created on the desktop so run it.

Step 18: The interface is initialized and the software is ready to use.



You have successfully installed packet tracer on your Windows System.

5.1.2 Application using Cisco Packet Tracer.

Peer-to-Peer Network Using Cpt

The procedure to create a peer-to-peer network using Cisco Packet Tracer(CPT)

Step 1: Open the Cisco Packet Tracer

- Launch the Cisco Packet Tracer on your computer.

Step 2: Add Devices to the Workspace

- From the device list at the bottom of the interface, select End Devices.
- Drag and drop two PCs(PC- 0 and PC- 1) onto the workspace.

Step 3: Connect the PCs

- Select the Connections option(lightning bolt icon) from the device list.
- Choose the Copper Straight Through Cable.
- Click on PC- 0, select the FastEthernet0 interface, and also click on PC- 1, selecting its FastEthernet0 interface as well. This connects the two PCs.

Step 4: Configure IP Addresses

- Click on PC- 0, also choose the Desktop tab, and select IP Configuration.
    - Set the IP Address to 192.168.1.1 and the Subnet Mask to 255.255.255.0.
- Repeat the same steps for PC-1
    - Set the IP Address to 192.168.1.2 and the Subnet Mask to 255.255.255.0.

Step 5: Test Network Connectivity

- Click on PC- 0, go to the Desktop tab, and open the Command Prompt.
- Type the command ping 192.168.1.2
- If the setup is correct, you should see successful replies from PC- 1, confirming that the two PCs can communicate.

Step 6: (Optional)Use Simulation Mode

- To view how the packets are transferred between the devices, you can switch to Simulation Mode(by clicking the clock symbol on the bottom-right).
- Generate traffic(like a ping command) to observe the packet flow in real-time.

Step 7: Save Your Project

- Save your project by going to File> Save As to retain your peer- to- peer network setup.

This process establishes a simple peer- to- peer network between two PCs in CPT.

Ip and Mac Address in the Computers Using CPT

To find and configure the IP address and MAC address on computers using Cisco Packet Tracer(CPT), follow these steps

Step 1: Open Cisco Packet Tracer and Add a computer

- Launch the Cisco Packet Tracer and drag a PC (computer) from the End Devices section to the workspace.

Step 2: Assign an IP Address to the PC

1. Click on the PC (e.g., PC- 0) in the workspace.
2. Go to the Desktop tab at the top of the pop-up window.
3. Select IP Configuration.
4. Under IP Configuration, you can assign
    - IP Address Enter an IP address like 192.168.1.10.
    - Subnet Mask generally 255.255.255.0.
    - Default Gateway If you are using a router in the network, enter its IP, like 192.168.1.1. still, you can leave it blank for peer-to-peer networks, If not.

Example configuration

- IP Address 192.168.1.10
- Subnet Mask 255.255.255.0
- Default Gateway 192.168.1.1

Step 3: View the MAC Address of the PC

To find the MAC address of the PC

1. Click on the PC again and go to the Desktop tab.
2. Select Command Prompt.
3. In the command prompt, type ipconfig all

This command will display both the IP and MAC addresses (referred to as" Physical Address").

The MAC address will look something like this: 00D0. BA89.AC34.

Step 4: Save Your Configuration

- • After setting up the IP address, close the configuration window.
- • If you want to save your project, go to File> Save As and save the configuration.

By following these steps, you can configure and view the IP and MAC addresses on a computer within the Cisco Packet Tracer.

FIND PORT NUMBERS/NAMES

To find the port numbers and their corresponding names, Python provides a module called socket that can be used to look up port numbers for common services. This module includes a method called getservbyname to get the port number for a service name, and getservbyport to find the service name by the port number.

Key Points:

- **Service Name to Port**: The getservbyname function can retrieve the port number corresponding to a given service name.
- **Port to Service Name**: The getservbyport function can retrieve the service name for a given port number.
- **Commonly Used Ports**: The program can display standard port numbers for services like HTTP, FTP, SSH, etc.

Python Program to Find Port Numbers/Names

```
import socket

def find_port_by_service(service_name):
    try:
        # Get port number by service name
        port = socket.getservbyname(service_name)
        return f"Service: {service_name}, Port: {port}"
    except OSError:
        return f"Service {service_name} not found"

def find_service_by_port(port_number):
    try:
        # Get service name by port number
        service = socket.getservbyport(port_number)
        return f"Port: {port_number}, Service: {service}"
    except OSError:
        return f"Port {port_number} not found"

# Example usage
service_name = "http"
port_number = 80

print(find_port_by_service(service_name))
print(find_service_by_port(port_number))
```

How it Works:

1. **Finding Port by Service Name**: The getservbyname method is used to look up the port number for a specific service name(e.g.," http" for HTTP).
2. **Finding Service by Port Number**: The getservbyport method is used to find the service associated with a particular port number(e.g., port 80 for HTTP).
3. **Handling Errors**: If an invalid service name or port number is provided, an error message is returned to indicate that the service or port couldn't be found.

Example:

Input 1:

Service: http

Output 1:

Service: http, Port: 80

Input 2:

Port: 80

Output 2:

Port: 80, Service: http

Conclusion:

This Python program demonstrates how to use the socket module to find port numbers corresponding to service names and vice versa. It handles successful lookups and errors, ensuring that users can easily identify services by port numbers or vice versa. This system is useful for network programming and understanding standard service ports.

REMOVE LEADING ZEROS FROM AN IP ADDRESS

To remove leading zeros from an IP address, we can split it into four octets, remove any leading zeros from each octet, and then combine them back together. The code below demonstrates how to do this efficiently in Python.

Key Points:

- **Splitting the IP Address**: The IP address is split into octets using the split (“.”) system.
- **Removing Leading Zeros**: Each octet is converted to an integer to remove any leading zeros and converted back to a string to preserve the correct IP format.
- **Rejoining the Octets**: The cleaned woodwinds are joined back together using join (“.”), forming the final IP address without any leading zeros.

Python Program to Remove Leading Zeros from an IP Address:

```
def remove_leading_zeros(ip_address):
    # Split the IP address into its four octets
    octets = ip_address.split(“.”)

    # Remove leading zeros from each octet by converting it to an integer and back to a string
    octets_no_zeros = [str(int(octet)) for octet in octets]
```

```
    # Join the cleaned octets back into a single IP address string
    cleaned_ip = ".".join(octets_no_zeros)

    return cleaned_ip

# Example usage
ip = "192.168.001.010"
cleaned_ip = remove_leading_zeros(ip)
print(f"Original IP: {ip}")
print(f"Cleaned IP: {cleaned_ip}")
```

How it Works:

1. **Splitting the IP Address**: The IP address is first split into four octets using the split (".") method.
2. **Removing Leading Zeros**: Each octet is converted to an integer to remove leading zeros and converted back to a string to maintain the proper IP format.
3. **Rejoining the Octets**: After removing the leading zeros, the cleaned octets are joined back into a single IP address using join (".").

Example:

Input:
Original IP: 192.168.001.010

Output:
Cleaned IP: 192.168.1.10

Conclusion:

This Python program efficiently removes leading zeros from each octet of an IP address by converting the octets to integers and back to strings. This system ensures that each octet is correctly formatted without any unnecessary leading zeros, making it practical for validating and processing IP addresses.

DATA LINK LAYER CHARACTER COUNT FRAMING METHOD

The Character Count Framing Method is used in the Data Link Layer of the OSI (Open Systems Interconnection) model to frame data for transmission. This method involves specifying the number of characters or bytes contained in a frame at the beginning of the frame itself. The idea is to prefix each frame (or block of data) with a count of the total characters in that frame, including the count itself. This count helps the receiver to identify where each frame starts and ends, enabling proper data transmission and reception.

Key Points:

- The first byte of the frame contains the number of characters in the frame.
- Each frame is distinct and is preceded by its length information.
- This method is simple but can be prone to synchronisation issues if the character count is corrupted during transmission.

Python Program for Character Count Framing:

This program prompts the stoner to input a payload, which is also processed by the Character Count Framing Method. A space separates each frame(word) in the payload, and the program outputs the frame prefixed by its character count.

```
print('Separate frames in payload are by space')

while True:
    # Prompt the user to enter the payload and split it into frames
    s = input('Enter payload:\n').split()

    # Initialize an empty string to store the framed output
    si = ''

    # Iterate over each frame (word) in the payload
    for x in s:
        # Prepend the length of the frame plus one to include the count itself
        x = str(len(x) + 1) + x
        # Append the frame with the character count to the output string
        si += x

    # Print the concatenated result, which is the payload with character count framing
    print(si)
```

How it Works:

1. **Input**: The user inputs a payload containing multiple frames (words) separated by spaces.
2. **Processing**:
   - Each word is treated as a frame.
   - The length of each frame (word) is calculated, and the result is increased by 1 (to account for the character count itself).
   - The count is then prepended to the word.
3. **Output**: The program outputs a single string with each frame prefixed by its character count.

Example:

Input 1:
Enter payload:
hello

Output 1:
6hello
Here, the frame “hello” has 5 characters, and the length of the frame is 6 (count includes the length field itself). So, the output is “6hello”.

Input 2:
Enter payload:
data structures and algorithms

Output 2:
5data11structures4and11algorithms

- “data” has 4 characters, so it becomes “5data”.
- “structures” has 10 characters, so it becomes “11structures”.
- “and” has 3 characters, becoming “4and”.
- “algorithms” has 10 characters, becoming “11algorithms”.

Conclusion:

This program demonstrates the Character Count Framing Method by taking a payload, calculating the length of each frame, and adding the character count to the beginning of each frame. The result is a string where each frame is easily identified by its length, making it easier to transmit and process on the receiver’s end.

Introduction and installation of Cisco packet tracer, peer-to-peer network using CPT, IP and MAC address in the computers using CPT, finding Port Numbers/ Names, removing leading zeros from an IP address, and data link layer character count framing method.

Keywords

- Cisco Packet Tracer
- Network Simulation
- Peer-to-Peer Network
- IP Configuration
- MAC Address
- Port Numbers
- Data Link Layer
- Character Count Framing
- Python Program

COMPUTER NETWORKS AND COMMUNICATIONS

KL UNIVERSITY (DEEMED TO BE UNIVERSITY)
CDOE CENTER FOR DISTANCE AND ONLINE EDUCATION

https://kluonline.edu.in/

supportcdoe@kluniveristy.in