GOVERNMENT POLLYTECHNIC, NAYAGARH

PREPARED BY :- TANMAY NATH MISHRA

SUB :- COMPUTER NETWORK SYSTEM

CHAPTER 1: INTRODUCTION TO COMPUTER NETWORKS

Introduction to Computer Networks

A computer network is a collection of interconnected computing devices that communicate with one another to share data, resources, and services. These devices include computers, servers, printers, routers, and mobile devices connected through wired or wireless communication links. Networks enable efficient information exchange using standard communication protocols and help reduce resource duplication. They play a crucial role in modern digital infrastructure by supporting communication, collaboration, and centralized data management. Networks can range from small home networks to large global systems like the Internet. An office network where employees share files and printers is a common example.

Applications and Advantages of Networks

Computer networks are widely used in business, education, healthcare, banking, and entertainment. They enable services such as email, video conferencing, online banking, cloud computing, and remote access. One major advantage of networks is resource sharing, which allows multiple users to share hardware, software, and data. Networks improve reliability through backups and redundancy, reduce costs, and enable centralized control of information. They also increase productivity and support global communication. Online banking systems are a practical example of network applications.

Types of Networks (LAN, MAN, WAN, PAN)

Networks are classified based on their geographical coverage. A Local Area Network (LAN) covers a small area such as a home or office and offers high-speed communication. A Metropolitan Area Network (MAN) spans a city and connects multiple LANs. A Wide Area Network (WAN) covers large areas such as countries or continents, with the Internet being the largest WAN. A Personal Area Network (PAN) connects personal devices over a short range using technologies like Bluetooth. Each type serves specific communication needs.

Network Models

Network models provide a structured framework for understanding how data is transmitted across networks. They divide communication into layers, with each layer performing specific functions. This layered approach simplifies design, development, and troubleshooting. Network models also ensure interoperability between devices from different vendors. The

OSI and TCP/IP models are the most widely known network models. These models are conceptual and help explain the flow of data in a network.

CHAPTER 2: OSI AND TCP/IP MODELS

OSI Reference Model – Overview

The OSI (Open Systems Interconnection) Reference Model was developed by ISO to standardize network communication. It consists of seven layers, each responsible for a specific task in the data communication process. The OSI model separates hardware and software functions and helps in understanding complex networking concepts. Although it is not directly implemented, it is widely used for learning and troubleshooting. By isolating network functions into layers, problems can be identified and resolved efficiently.

OSI Model Layers 1–3

The first three layers of the OSI model are the Physical, Data Link, and Network layers. The Physical layer deals with the transmission of raw bits and defines cables, connectors, and signalling methods. The Data Link layer ensures reliable communication between adjacent devices through framing, error detection, and flow control. It also handles MAC addressing. The Network layer manages logical addressing and routing, enabling data packets to travel across interconnected networks. Routers operate at this layer.

OSI Model Layers 4–7

Layers four to seven handle end-to-end communication and user interaction. The Transport layer ensures reliable delivery through segmentation, error control, and flow control. The Session layer manages sessions between applications. The Presentation layer handles data formatting, compression, and encryption. The Application layer provides services directly to users, such as email, file transfer, and web access. Applications like web browsers operate at this layer.

TCP/IP Model and Comparison with OSI

The TCP/IP model is a practical networking model used on the Internet. It consists of four layers: Application, Transport, Internet, and Network Access. Unlike OSI, TCP/IP combines multiple OSI layers into fewer layers. The Application layer includes OSI's Application, Presentation, and Session layers. TCP/IP is widely implemented, while OSI is mainly used for conceptual understanding and troubleshooting.

CHAPTER 3: TRANSMISSION MEDIA

Transmission Media – Principles and Issues

Transmission media are the paths through which data travels from sender to receiver. They are classified into guided (wired) and unguided (wireless) media. Important factors affecting transmission include bandwidth, noise, attenuation, interference, cost, and security. The selection of transmission media depends on distance, speed, and application requirements. Wired media offer better security, while wireless media provide mobility. Fiber optic cables are preferred for high-speed, long-distance communication.

Coaxial Cable

Coaxial cable consists of a central conductor surrounded by insulation and a metallic shield. It provides better noise immunity than twisted pair cables and supports moderate bandwidth. Coaxial cables are commonly used in cable television and broadband Internet. Although durable, they are bulky and expensive compared to modern alternatives. Their use in LANs has declined with the rise of Ethernet and fiber optics.

UTP and STP Cables

Unshielded Twisted Pair (UTP) and Shielded Twisted Pair (STP) cables are widely used in Ethernet networks. UTP cables are inexpensive, flexible, and easy to install, making them popular for LANs. STP cables include shielding to reduce electromagnetic interference. Both support high-speed data transmission but have distance limitations. Cat6 UTP cables are commonly used in modern networks.

Fiber Optic Cable – Single Mode and Multimode

Fiber optic cables transmit data as light signals and offer very high bandwidth and security. Single-mode fiber supports long-distance communication and is used in backbone networks. Multimode fiber is suitable for shorter distances, such as within buildings. Fiber optics are immune to electromagnetic interference and difficult to tap. Despite high installation costs, they are essential for high-speed internet infrastructure.

Wireless Media – HF, VHF, UHF

Wireless communication uses electromagnetic waves to transmit data without cables. HF waves support long-distance communication, VHF is used for TV and FM radio, and UHF is used in mobile communication. Wireless media allow mobility and easy deployment but are vulnerable to interference and security threats. Bandwidth and range vary based on frequency. Radio broadcasting is a common example.

Microwave and Ku Band

Microwave communication uses high-frequency waves and requires a clear line of sight. It supports high data rates and is used for long-distance terrestrial communication. Ku band is used in satellite communication and television broadcasting. Weather conditions such as rain can affect signal quality. These technologies are widely used despite their higher setup costs.

CHAPTER 4: WIRELESS AND MOBILE NETWORKS

WiFi Standards (802.11 a/b/g/n/ac)

WiFi standards defined by IEEE 802.11 enable wireless LAN communication. Different standards operate at 2.4 GHz and 5 GHz frequencies and offer varying speeds. 802.11b provides low speed, while 802.11a and g offer higher speeds. 802.11n introduced MIMO technology, and 802.11ac provides very high throughput. These standards are widely used in homes and offices.

Cellular Data – 2G, 3G, 4G, 5G

Cellular networks have evolved to support increasing data demands. 2G focuses on voice communication, 3G supports mobile internet, 4G provides high-speed data, and 5G offers ultra-low latency and very high speeds. Each generation improves efficiency and performance. Cellular networks are essential for mobile communication and IoT applications.

CHAPTER 5: NETWORK TOPOLOGIES

Bus and Star Topologies

Bus topology uses a single backbone cable shared by all devices, making it simple but vulnerable to failure. Star topology connects devices to a central hub or switch, improving performance and management. Failure of one device does not affect others, but hub failure can disrupt the network. Star topology is widely used in LANs.

Ring, Mesh, Tree, and Hybrid Topologies

Ring topology connects devices in a circular path, while mesh topology provides multiple paths for reliability. Tree topology supports hierarchical structures, and hybrid topology combines multiple topologies. Each topology has advantages and limitations related to cost, scalability, and reliability. Hybrid networks are common in large organizations.

CHAPTER 6: DATA LINK LAYER

Data Link Layer – Functions and Design Issues

The Data Link layer ensures reliable communication between adjacent nodes. It performs framing, error detection, error correction, and flow control. It also manages MAC addressing

and media access control. Design issues include efficient framing and error-handling techniques. Ethernet is a popular Data Link layer protocol.

Framing, Error Control, and Flow Control

Framing divides data into manageable units. Error control detects and corrects transmission errors using CRC and checksums. Flow control regulates data transmission to prevent receiver overload. Techniques like Stop-and-Wait and Sliding Window ensure reliable communication.

Ethernet Protocol

Ethernet is defined by IEEE 802.3 and is the most widely used LAN technology. It uses MAC addresses and supports high data rates. Modern Ethernet networks use switches and full-duplex communication. Ethernet is scalable, reliable, and cost-effective.

WLAN Protocol

WLAN protocols defined by IEEE 802.11 enable wireless LAN communication. They use CSMA/CA to avoid collisions and rely on access points. WLANs support mobility but are affected by interference. Security is provided through WPA and WPA2.

Bluetooth, Switching Techniques, and VLAN

Bluetooth supports short-range personal area networking. Switching techniques include circuit and packet switching. VLANs logically divide a physical network into multiple virtual networks, improving security and efficiency.

CHAPTER 7: NETWORK LAYER

Network Layer – Functions and Design Issues

The Network layer handles routing, logical addressing, packet forwarding, and congestion control. It enables internetworking using IP addresses. Routers operate at this layer to determine optimal paths.

IPv4 Addressing

IPv4 uses 32-bit addresses written in dotted decimal format. Due to limited address space, techniques like NAT and subnetting are used. IPv4 is still widely used.

IPv6 Addressing

IPv6 uses 128-bit addresses and provides a vast address space. It supports auto-configuration and improved security. IPv6 is designed for future internet growth.

Routing Principles

Routing selects the best path for data packets using routing tables and metrics. It can be static or dynamic. Efficient routing ensures optimal network performance.

Distance Vector Routing Algorithm

Distance vector routing shares routing tables with neighbors and uses the Bellman-Ford algorithm. It is simple but slow and prone to routing loops.

Link State Routing Algorithm

Link state routing uses network topology information and Dijkstra's algorithm. It converges quickly and is suitable for large networks.

RIP Protocol

RIP is a distance vector protocol using hop count as a metric. It is simple but not scalable and mainly used in small networks.

OSPF Protocol

OSPF is a link state protocol that supports large networks. It uses cost as a metric and converges quickly, making it widely used in enterprises.

CHAPTER 8: TRANSPORT AND APPLICATION LAYERS

Transport Layer – Functions and Design Issues

The Transport layer provides end-to-end communication, segmentation, error control, and flow control. It ensures reliable or best-effort delivery using TCP or UDP.

UDP Protocol

UDP is connectionless and fast but unreliable. It is used in applications where speed is more important than accuracy, such as streaming.

TCP Protocol

TCP provides reliable, ordered, and error-free data delivery. It uses acknowledgments and congestion control. TCP is used for file transfer and email.

TCP vs UDP

TCP is reliable but slower, while UDP is fast but unreliable. The choice depends on application requirements.

Application Layer – Overview and Design Issues

The Application layer provides services such as email, file transfer, and web access. Design issues include scalability, performance, and security.

DNS

DNS converts domain names into IP addresses and uses a hierarchical structure. It is essential for internet operation.

DHCP

DHCP automatically assigns IP addresses and network parameters, simplifying network administration.

SNMP

SNMP monitors and manages network devices by collecting performance and fault information.

FTP and TFTP

FTP supports secure and reliable file transfer, while TFTP is simpler and used for booting and updates.

SMTP

SMTP is used to send emails between mail servers and works with POP or IMAP for retrieval.

World Wide Web (WWW)

The WWW uses HTTP/HTTPS and enables access to multimedia content through browsers.

Telnet and SSH

Telnet provides remote access but is insecure, while SSH offers encrypted and secure remote login.

CHAPTER 9: NETWORK DEVICES

Network Interface Card (NIC) and Hub

NIC enables devices to connect to networks and provides a MAC address. Hubs broadcast data to all devices and are now obsolete.

Switch Types, Router, Access Point, and WLC

Switches forward frames intelligently, routers forward packets between networks, access points provide wireless connectivity, and WLCs manage multiple access points in enterprise networks.