SUDDHANANDA SCHOOL OF MANAGEMENT&

COMPUTER SCIENCE

LECTURE NOTES ON

COMPUTER NETWORKS (MCPC1002)

UNIT – I

INTRODUCTION TO COMPUTER NETWORKS AND NETWORK MODELS:

INTRODUCTION TO COMPUTER NETWORKS:

A computer network is a collection of interconnected computers and devices that communicate with each other to share resources, data, and services.

The connection may be established using:

- Wired media
- Wireless media

The main purpose of networking is:

- Communication
- Resource sharing
- Information exchange

Definition

A computer network is a system in which multiple computers are connected together through communication channels to exchange information and share resources.

Examples of Computer Networks

1. Internet
2. Mobile networks
3. Banking networks
4. Railway reservation systems
5. Office LAN networks
6. Wi-Fi networks

NEED FOR COMPUTER NETWORKS

Computer networks are essential because they provide:

1. Resource Sharing
2. File Sharing
3. Communication
4. Centralized Management

5. Internet Access
6. Remote Access

ADVANTAGES OF COMPUTER NETWORKS

1. Resource Sharing

Devices like printers, scanners, and storage can be shared.

2. Fast Communication

Emails and messages can be sent instantly.

3. Cost Reduction

Hardware and software resources can be shared.

4. Data Sharing

Users can access shared files and databases.

5. Reliability

Backup systems improve reliability.

6. Remote Access

Users can access systems remotely.

DISADVANTAGES OF COMPUTER NETWORKS

1. Security threats
2. Virus attacks
3. High setup cost
4. Network failure affects communication
5. Requires skilled administration

TYPES OF COMPUTER NETWORKS

Networks are classified according to geographical area.

1. LAN (Local Area Network)

A LAN covers a small geographical area.

Examples:

- School
- Office
- Laboratory

Features:

- High speed
- Low cost
- Privately owned

Advantages of LAN

1. Fast communication
2. Easy file sharing
3. Low maintenance cost

2. MAN (Metropolitan Area Network)

A MAN covers a city or metropolitan area.

Examples:

- Cable TV network
- City-wide internet network

Features:

- Larger than LAN
- High speed communication

3. WAN (Wide Area Network)

A WAN covers very large geographical areas.

Examples:

- Internet
- Banking networks

Features:

- Uses satellite communication
- Connects different countries

Difference Between LAN, MAN and WAN

Feature	LAN	MAN	WAN
Area Covered	Small	City	Large
Speed	High	Medium	Lower
Cost	Low	Medium	High
Ownership	Private	Public/Private	Public

NETWORK TOPOLOGIES

Topology refers to physical arrangement of computers in a network.

TYPES OF TOPOLOGY

1. Bus Topology
2. Star Topology

3. Ring Topology
4. Mesh Topology
5. Tree Topology

1. Bus Topology

All devices connect to a single communication cable called bus.

Advantages:

- Easy installation
- Low cost

Disadvantages:

- Cable failure affects entire network

2. Star Topology

All devices connect to central hub or switch.

Advantages:

- Easy troubleshooting
- Better performance

Disadvantages:

- Hub failure affects network

3. Ring Topology

Each device connects to next device forming ring structure.

Advantages:

- Equal access

Disadvantages:

- Failure affects communication

4. Mesh Topology

Every node connects to every other node.

Advantages:

- High reliability

Disadvantages:

- Expensive

5. Tree Topology

Combination of star and bus topology.

Advantages:

- Scalable

Disadvantages:

- Complex structure

NETWORK DEVICES

1. Hub

A hub broadcasts data to all devices.

Works at:

- Physical layer

2. Switch

A switch sends data only to destination device.

Advantages:

- Faster than hub
- Reduces traffic

3. Router

Connects different networks.

Functions:

- Packet forwarding
- Routing

4. Bridge

Connects similar LAN segments.

5. Repeater

Regenerates weak signals.

6. Gateway

Connects different protocols and networks.

NETWORK MODELS

Two important models:

1. OSI Model
2. TCP/IP Model

OSI REFERENCE MODEL

OSI stands for:

- Open Systems Interconnection

Developed by:

- ISO (International Organization for Standardization)

It contains seven layers.

Layers of OSI Model

Layer Number	Layer Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network
2	Data Link
1	Physical

1. Physical Layer

Responsible for transmission of raw bits.

Functions:

- Electrical signals
- Cables
- Connectors

Devices:

- Hub
- Repeater

2. Data Link Layer

Provides error-free transmission.

Functions:

- Framing
- Error detection
- Flow control

Devices:

- Switch
- Bridge

3. Network Layer

Responsible for routing.

Functions:

- Logical addressing

- Path selection

Device:

- Router

Protocols:

- IP

4. Transport Layer

Provides reliable communication.

Functions:

- Segmentation
- Error recovery
- Flow control

Protocols:

- TCP
- UDP

5. Session Layer

Manages communication sessions.

Functions:

- Session establishment
- Synchronization

6. Presentation Layer

Responsible for:

- Encryption
- Compression
- Data formatting

7. Application Layer

Closest to user.

Functions:

- Email
- File transfer
- Web browsing

Protocols:

- HTTP
- FTP
- SMTP

TCP/IP MODEL

TCP/IP model is practical model used in Internet.

Layers of TCP/IP Model

Layer	Functions
Application	User services
Transport	Reliable delivery
Internet	Routing
Network Access	Physical transmission

Difference Between OSI and TCP/IP

OSI Model	TCP/IP Model
7 Layers	4 Layers
Theoretical	Practical
ISO Standard	Internet Standard

TRANSMISSION MEDIA

Communication channel used for data transmission.

TYPES OF TRANSMISSION MEDIA

1. Guided Media
2. Unguided Media

GUIDED MEDIA

Uses physical cables.

Types:

1. Twisted Pair Cable
2. Coaxial Cable
3. Optical Fiber

1. Twisted Pair Cable

Two insulated copper wires twisted together.

Advantages:

- Cheap
- Easy installation

Disadvantages:

- Noise interference

2. Coaxial Cable

Contains central conductor surrounded by insulation.

Advantages:

- Better shielding

3. Optical Fiber

Uses light signals.

Advantages:

- Very high speed
- Secure communication

Disadvantages:

- Expensive

UNGUIDED MEDIA

Wireless communication.

Types:

1. Radio Waves
2. Microwaves
3. Infrared

DATA COMMUNICATION MODES

1. Simplex

One-way communication.

Example:

- Keyboard to computer

2. Half Duplex

Two-way but one at a time.

Example:

- Walkie-talkie

3. Full Duplex

Both directions simultaneously.

Example:

- Telephone

NETWORK PROTOCOLS

Protocols are communication rules.

Examples:

- HTTP
- FTP
- TCP
- IP
- SMTP

INTERNET PROTOCOL (IP)

Provides logical addressing.

Functions:

- Addressing
- Routing

TCP (Transmission Control Protocol)

Provides reliable transmission.

Features:

- Error checking
- Acknowledgment

UDP (User Datagram Protocol)

Fast but unreliable protocol.

Used in:

- Video streaming
- Gaming

DOMAIN NAME SYSTEM (DNS)

Converts domain names into IP addresses.

Example:

- google.com → IP address

CLIENT SERVER MODEL

Client requests services.

Server provides services.

Example:

- Web browser and web server

PEER TO PEER NETWORK

All computers have equal responsibility.

Example:

- File sharing systems

APPLICATIONS OF COMPUTER NETWORKS

1. Online Banking
2. E-commerce
3. Cloud Computing
4. Video Conferencing
5. E-learning
6. Social Media
7. Remote Working

SECURITY ISSUES IN NETWORKS

1. Hacking
2. Virus attacks
3. Data theft
4. Unauthorized access

NETWORK SECURITY METHODS

1. Firewall
2. Antivirus
3. Encryption
4. Authentication

Conclusion :

Computer networks play a major role in modern communication systems. Networking enables efficient data sharing, communication, and resource utilization. Concepts such as:

- Network models
- Topologies
- Protocols
- Transmission media

form the foundation of advanced networking technologies and Internet communication systems.

UNIT – II

DATA LINK LAYER, ERROR DETECTION AND MAC PROTOCOLS:

INTRODUCTION TO DATA LINK LAYER

The Data Link Layer is the second layer of the OSI model. It is responsible for reliable transmission of data between two directly connected devices.

This layer converts raw bits received from the Physical Layer into frames and ensures error-free communication.

Position of Data Link Layer in OSI Model

Layer	Name
7	Application
6	Presentation

Layer	Name
5	Session
4	Transport
3	Network
2	Data Link Layer
1	Physical Layer

FUNCTIONS OF DATA LINK LAYER

The main functions are:

1. Framing
2. Error Control
3. Flow Control
4. Physical Addressing
5. Access Control
6. Reliable Data Transfer

1. Framing

The Data Link Layer divides raw bit stream into manageable units called frames.

A frame contains:

- Header
- Data
- Trailer

Advantages of Framing

1. Easy error detection
2. Organized transmission
3. Efficient communication

Types of Framing

1. Character Count
2. Byte Stuffing
3. Bit Stuffing

Character Count Method

The first field specifies number of characters in frame.

Disadvantage:

- If count field becomes corrupted, synchronization problem occurs.

Byte Stuffing

Special characters indicate start and end of frame.

If same character appears in data, extra escape character is inserted.

Bit Stuffing

Used in bit-oriented protocols.

A 0 bit is inserted after five consecutive 1s.

2. Physical Addressing

The Data Link Layer adds physical address (MAC address) to frames.

MAC address uniquely identifies devices in LAN.

Example:

- 00:1A:2B:3C:4D:5E

3. Error Control

Errors may occur during transmission due to:

- Noise
- Signal distortion
- Interference

Error control mechanisms detect and correct errors.

TYPES OF ERRORS

1. Single Bit Error

Only one bit changes during transmission.

Example:

- Sent → 101100
- Received → 101000

2. Burst Error

Multiple bits change.

More common in networks.

ERROR DETECTION METHODS

1. Parity Check

Simplest method.

Extra parity bit added.

Two types:

- Even parity

- Odd parity

Even Parity

Total number of 1s should be even.

Example:

- Data = 1011
- Number of 1s = 3

Add parity bit = 1

Final data:

- 10111

Now total 1s = 4 (even)

Advantages

1. Simple implementation
2. Low cost

Disadvantages

1. Cannot detect multiple errors

2. Checksum Method

Data divided into equal segments.

Binary addition performed.

Complement of sum transmitted.

Receiver verifies checksum.

Used in:

- TCP/IP protocols

Steps of Checksum

1. Divide data into segments
2. Add segments
3. Take complement
4. Send checksum

3. Cyclic Redundancy Check (CRC)

Most powerful error detection technique.

Widely used in:

- Networks
- Digital communication
- Storage devices

CRC Process

1. Sender and receiver agree on generator polynomial.
2. Data appended with zeros.
3. Binary division performed.
4. Remainder transmitted as CRC bits.

CRC Formula

CRC=Remainder\ after\ modulo\ 2\ division

Advantages of CRC

1. Detects burst errors
2. Highly reliable
3. Widely used

Disadvantages

1. Complex implementation

ERROR CORRECTION

Error correction means detecting and correcting errors automatically.

HAMMING CODE

Hamming code is widely used error correction technique.

It can:

- Detect errors
- Correct single-bit errors

Hamming Distance

Number of differing bits between two code words.

Formula:

d(x,y)

FLOW CONTROL

Flow control manages transmission speed between sender and receiver.

Purpose:

- Prevent data loss
- Avoid receiver overload

TYPES OF FLOW CONTROL

1. Stop-and-Wait Protocol
2. Sliding Window Protocol

1. Stop-and-Wait Protocol

Sender sends one frame and waits for acknowledgment.

If ACK received:

- Next frame sent

Otherwise:

- Frame retransmitted

Advantages

1. Simple
2. Reliable

Disadvantages

1. Slow performance

2. Sliding Window Protocol

Multiple frames can be transmitted before receiving acknowledgment.

Improves efficiency.

Advantages

1. Better bandwidth utilization
2. Faster communication

Disadvantages

1. More complex

NOISY CHANNEL PROTOCOLS

Communication channels containing transmission errors are called noisy channels.

Protocols used:

1. Stop-and-Wait ARQ
2. Go-Back-N ARQ
3. Selective Repeat ARQ

STOP-AND-WAIT ARQ

ARQ stands for:

- Automatic Repeat Request

Sender waits for ACK.

If timeout occurs:

- Retransmission happens

GO-BACK-N ARQ

Sender transmits multiple frames.

If one frame lost:

- All subsequent frames retransmitted.

Advantages

1. Efficient transmission

Disadvantages

1. Wastage of bandwidth

SELECTIVE REPEAT ARQ

Only erroneous frame retransmitted.

More efficient than Go-Back-N.

Advantages

1. Better performance
2. Reduced retransmission

Disadvantages

1. Complex implementation

MAC (MEDIA ACCESS CONTROL)

MAC controls access to shared communication medium.

Main objective:

- Avoid collision

CHANNEL ALLOCATION PROBLEMS

When multiple devices share same medium:

- Collision may occur

MAC protocols solve this issue.

TYPES OF MAC PROTOCOLS

1. Random Access Protocols
2. Controlled Access Protocols
3. Channelization Protocols

RANDOM ACCESS PROTOCOLS

Devices transmit whenever channel becomes free.

1. ALOHA

Earliest random access protocol.

Two types:

1. Pure ALOHA
2. Slotted ALOHA

Pure ALOHA

Stations transmit anytime.

If collision occurs:

- Retransmission happens

Efficiency:

18.4%

Slotted ALOHA

Time divided into slots.

Transmission only at beginning of slot.

Efficiency:

36.8%

CSMA (Carrier Sense Multiple Access)

Before transmission:

- Device senses channel

If channel busy:

- Wait

If free:

- Transmit

Types of CSMA

1. 1-Persistent CSMA
2. Non-Persistent CSMA
3. p-Persistent CSMA

CSMA/CD

Carrier Sense Multiple Access with Collision Detection.

Used in:

- Ethernet

Working:

1. Sense channel
2. Transmit frame
3. Detect collision
4. Stop transmission
5. Retransmit later

Advantages

1. Efficient
2. Reduces collisions

CSMA/CA

Carrier Sense Multiple Access with Collision Avoidance.

Used in:

- Wireless LAN

CONTROLLED ACCESS PROTOCOLS

Transmission controlled systematically.

Types:

1. Reservation
2. Polling
3. Token Passing

TOKEN PASSING

A special frame called token circulates.

Only token holder can transmit.

Advantages:

- No collision

Disadvantages:

- Token loss affects communication

ETHERNET

Most widely used LAN technology.

Developed by:

- Xerox

Uses:

- CSMA/CD

FEATURES OF ETHERNET

1. High speed
2. Low cost
3. Reliable communication

ETHERNET FRAME FORMAT

Contains:

1. Preamble
2. Source Address
3. Destination Address
4. Data
5. CRC

SWITCHING

Switching transfers data from source to destination.

TYPES OF SWITCHING

1. Circuit Switching
2. Message Switching
3. Packet Switching

1. Circuit Switching

Dedicated communication path established.

Example:

- Telephone network

Advantages:

- Reliable

Disadvantages:

- Expensive

2. Message Switching

Entire message transmitted at once.

Store-and-forward technique used.

3. Packet Switching

Message divided into packets.

Widely used in Internet.

Advantages:

1. Efficient
2. Fast communication

Difference Between Circuit and Packet Switching

Circuit Switching	**Packet Switching**
Dedicated path	No dedicated path
Expensive	Cost effective
Continuous connection	Data divided into packets

LOCAL AREA NETWORK (LAN)

A LAN connects computers within small area.

Examples:

- Office

- College
- Laboratory

WIRELESS LAN

Wireless communication using Wi-Fi.

Advantages:

1. Mobility
2. Easy installation

Disadvantages:

1. Security issues

IEEE STANDARDS

IEEE develops networking standards.

Examples:

- IEEE 802.3 → Ethernet
- IEEE 802.11 → Wi-Fi

APPLICATIONS OF DATA LINK LAYER

1. Error-free communication
2. Network reliability
3. Data framing
4. MAC addressing
5. Wireless communication

REAL LIFE APPLICATIONS

1. Wi-Fi communication
2. Ethernet networks
3. Mobile communication
4. Internet browsing
5. Data transfer systems

Conclusion:

The Data Link Layer is responsible for reliable node-to-node communication. Important concepts such as:

- Error detection
- Flow control
- Framing
- MAC protocols
- Ethernet

- Switching

play a major role in efficient network communication.

Protocols like:

- CSMA/CD
- CRC
- Sliding Window

are widely used in modern computer networks to ensure fast and reliable data transfer.

UNIT – III

NETWORK LAYER AND ROUTING:

INTRODUCTION TO NETWORK LAYER

The Network Layer is the third layer of the OSI reference model. It is responsible for transferring data packets from source to destination across multiple networks.

The main function of this layer is:

- Routing
- Logical addressing
- Path determination
- Packet forwarding

The Network Layer ensures that data reaches the correct destination even if sender and receiver are connected through different networks.

Position of Network Layer in OSI Model

Layer Number	Layer Name
7	Application
6	Presentation
5	Session
4	Transport
3	Network Layer

Layer Number	Layer Name
2	Data Link Layer
1	Physical Layer

FUNCTIONS OF NETWORK LAYER

The major functions are:

1. Logical Addressing
2. Routing
3. Packet Forwarding
4. Internetworking
5. Congestion Control
6. Fragmentation and Reassembly

1. Logical Addressing

Each device in a network is identified using an IP address.

Logical addressing helps:

- Identify sender and receiver
- Route packets correctly

Example:

- IPv4 Address → 192.168.1.1

2. Routing

Routing means selecting the best path for packet transmission from source to destination.

Routers perform routing operations.

3. Packet Forwarding

Routers receive packets and forward them to next network.

4. Internetworking

The Network Layer connects different networks together.

Example:

- LAN connected to Internet

5. Congestion Control

Controls excessive traffic in network.

6. Fragmentation

Large packets are divided into smaller packets for transmission.

At destination:

- Reassembly occurs

INTERNET PROTOCOL (IP)

IP stands for:

- Internet Protocol

It is the most important protocol of Network Layer.

Functions:

1. Addressing
2. Routing
3. Packet delivery

Characteristics of IP

1. Connectionless
2. Unreliable
3. Best-effort delivery

TYPES OF IP ADDRESS

1. IPv4
2. IPv6

IPv4 ADDRESS

IPv4 uses:

- 32-bit addressing

Representation:

- Decimal format

Example:

- 192.168.1.10

Structure of IPv4 Address

32\ bits=4\ octets

Each octet:

- 8 bits

Advantages of IPv4

1. Simple implementation
2. Widely supported

Limitations of IPv4

1. Limited addresses
2. Security issues

IPv6 ADDRESS

IPv6 introduced to solve IPv4 limitations.

Uses:

- 128-bit addresses

Example:

- 2001:0db8:85a3::8a2e:0370:7334

Advantages of IPv6

1. Huge address space
2. Better security
3. Faster routing

Difference Between IPv4 and IPv6

IPv4	IPv6
32-bit	128-bit
Limited addresses	Large address space
Decimal notation	Hexadecimal notation

IP ADDRESS CLASSES

IPv4 addresses divided into classes.

Class A

Range:

- 1 to 126

Used for:

- Large organizations

Class B

Range:

- 128 to 191

Used for:

- Medium networks

Class C

Range:

- 192 to 223

Used for:

- Small networks

Class D

Used for:

- Multicasting

Class E

Used for:

- Research purposes

SUBNETTING

Subnetting divides one network into smaller networks.

Purpose:

1. Efficient address utilization
2. Better management
3. Improved security

Subnet Mask

Used to identify:

- Network portion
- Host portion

Example:

- 255.255.255.0

ROUTERS

A router is a networking device used to connect multiple networks.

Functions:

1. Packet forwarding
2. Routing
3. Path selection

ROUTING

Routing determines optimal path between source and destination.

TYPES OF ROUTING

1. Static Routing
2. Dynamic Routing

1. Static Routing

Routes manually configured.

Advantages:

1. Secure
2. Simple for small networks

Disadvantages:

1. Difficult for large networks

2. Dynamic Routing

Routes automatically updated.

Advantages:

1. Automatic adaptation
2. Efficient for large networks

Disadvantages:

1. More complex

ROUTING ALGORITHMS

Routing algorithms help select best path.

Types:

1. Distance Vector Routing
2. Link State Routing

DISTANCE VECTOR ROUTING

Each router shares routing table with neighbors.

Uses:

- Bellman-Ford Algorithm

Features

1. Simple implementation
2. Periodic updates

Advantages

1. Easy configuration

Disadvantages

1. Slow convergence

LINK STATE ROUTING

Each router builds complete network topology.

Uses:

- Dijkstra Algorithm

Advantages

1. Fast convergence
2. Accurate routing

Disadvantages

1. Complex implementation

SHORTEST PATH ALGORITHM

Used to determine shortest route.

Most common:

- Dijkstra Algorithm

Dijkstra Algorithm

Finds shortest path from source node to all other nodes.

Applications:

1. GPS systems
2. Internet routing
3. Network optimization

ROUTING TABLE

A routing table stores routing information.

Contains:

1. Destination network
2. Next hop
3. Metric
4. Interface

CONGESTION CONTROL

Congestion occurs when network traffic becomes excessive.

Results:

1. Packet loss
2. Delay
3. Reduced performance

Causes of Congestion

1. High traffic
2. Limited bandwidth
3. Slow routers

Congestion Control Techniques

1. Traffic shaping
2. Queue management
3. Load balancing

TRAFFIC SHAPING

Controls data transmission rate.

Types:

1. Leaky Bucket Algorithm
2. Token Bucket Algorithm

Leaky Bucket Algorithm

Data transmitted at constant rate.

Advantages:

1. Smooth traffic flow

Disadvantages:

1. Packet loss possible

Token Bucket Algorithm

Tokens generated periodically.

Allows burst traffic transmission.

Advantages:

1. Flexible traffic handling

INTERNET CONTROL MESSAGE PROTOCOL (ICMP)

ICMP reports errors and network information.

Functions:

1. Error reporting
2. Diagnostic tools

Examples of ICMP Messages

1. Destination unreachable
2. Time exceeded
3. Echo request/reply

PING COMMAND

Uses ICMP.

Purpose:

- Test connectivity between devices.

TRACEROUTE

Shows path taken by packets.

Used for:

- Network troubleshooting

ADDRESS RESOLUTION PROTOCOL (ARP)

ARP converts IP address into MAC address.

Working of ARP

1. Sender broadcasts ARP request.
2. Target device replies with MAC address.

Reverse ARP (RARP)

Converts MAC address into IP address.

DHCP (Dynamic Host Configuration Protocol)

Automatically assigns IP addresses.

Advantages:

1. Reduces manual configuration
2. Simplifies management

NETWORK ADDRESS TRANSLATION (NAT)

NAT converts private IP addresses into public IP addresses.

Purpose:

1. Address conservation
2. Security enhancement

TYPES OF NAT

1. Static NAT
2. Dynamic NAT
3. PAT (Port Address Translation)

FIREWALL

A firewall protects network from unauthorized access.

Functions:

1. Traffic filtering
2. Security monitoring

TYPES OF FIREWALL

1. Packet Filtering Firewall
2. Proxy Firewall
3. Stateful Firewall

VIRTUAL PRIVATE NETWORK (VPN)

VPN creates secure communication tunnel over Internet.

Advantages:

1. Privacy
2. Security
3. Remote access

MOBILE IP

Allows mobile users to move across networks without changing IP address.

QUALITY OF SERVICE (QoS)

QoS ensures better performance for important applications.

Used in:

1. Video conferencing
2. Online gaming
3. Voice calls

MULTICASTING

One sender transmits data to multiple receivers simultaneously.

Applications:

1. Online classes
2. Video streaming

UNICAST, BROADCAST AND MULTICAST

Type	Description
Unicast	One to one
Broadcast	One to all
Multicast	One to many

APPLICATIONS OF NETWORK LAYER

1. Internet communication
2. Online banking
3. GPS navigation
4. Cloud computing
5. Mobile communication
6. Video conferencing

REAL LIFE EXAMPLES

Application	Use of Network Layer
Google Maps	Routing

Application	Use of Network Layer
Internet Browsing	IP addressing
WhatsApp Calls	Packet delivery
Online Games	Congestion control

ADVANTAGES OF NETWORK LAYER

1. Efficient routing
2. Supports internetworking
3. Provides logical addressing
4. Reduces network congestion

DISADVANTAGES

1. Complex routing algorithms
2. Congestion issues
3. Delay in packet delivery

Conclusion:

The Network Layer plays an important role in data communication across multiple interconnected networks. Concepts such as:

- IP addressing
- Routing
- Congestion control
- ARP
- ICMP
- DHCP
- NAT

form the foundation of Internet communication and modern networking systems.

Efficient routing and packet forwarding ensure reliable communication in:

- Computer networks
- Mobile networks
- Cloud systems
- Internet services

UNIT – IV

TRANSPORT LAYER, APPLICATION LAYER AND NETWORK SECURITY:

INTRODUCTION TO TRANSPORT LAYER

The Transport Layer is the fourth layer of the OSI reference model. It is responsible for end-to-end communication between source and destination systems.

The Transport Layer ensures:

- Reliable communication
- Error recovery
- Flow control
- Data segmentation

It acts as a bridge between:

- Upper layers
  and
- Lower layers

Position of Transport Layer in OSI Model

Layer Number	Layer Name
7	Application
6	Presentation
5	Session
4	Transport Layer
3	Network Layer
2	Data Link Layer
1	Physical Layer

FUNCTIONS OF TRANSPORT LAYER

The major functions are:

1. Process-to-Process Delivery
2. Segmentation and Reassembly

3. Error Control
4. Flow Control
5. Multiplexing
6. Connection Control

1. Process-to-Process Delivery

The Transport Layer delivers data from one application process to another.

Example:

- Browser to Web Server
- Email Client to Mail Server

2. Segmentation and Reassembly

Large data is divided into smaller segments before transmission.

At destination:

- Segments are reassembled.

3. Error Control

Transport Layer ensures reliable data transfer by:

- Detecting errors
- Retransmitting lost packets

4. Flow Control

Controls data transmission speed between sender and receiver.

Purpose:

- Prevent receiver overload

5. Multiplexing

Multiple applications can use network simultaneously.

Example:

- Email
- Web browsing
- Video streaming

all can run together.

6. Connection Control

Transport Layer can provide:

1. Connection-oriented communication
2. Connectionless communication

TRANSPORT LAYER PROTOCOLS

Two important protocols:

1. TCP
2. UDP

TRANSMISSION CONTROL PROTOCOL (TCP)

TCP stands for:

- Transmission Control Protocol

It is:

- Reliable
- Connection-oriented

TCP ensures:

- Ordered delivery
- Error-free transmission

FEATURES OF TCP

1. Reliable communication
2. Error checking
3. Flow control
4. Congestion control
5. Acknowledgment mechanism

TCP HEADER FORMAT

TCP header contains:

1. Source Port Number
2. Destination Port Number
3. Sequence Number
4. Acknowledgment Number
5. Window Size
6. Checksum

TCP CONNECTION ESTABLISHMENT

TCP uses:

- Three-Way Handshake

THREE-WAY HANDSHAKE

Steps:

1. SYN
2. SYN-ACK
3. ACK

This establishes reliable connection.

Working of Three-Way Handshake

Step 1

Client sends:

- SYN message

Step 2

Server replies:

- SYN + ACK

Step 3

Client sends:

- ACK

Connection established successfully.

Advantages of TCP

1. Reliable communication
2. Error recovery
3. Ordered delivery
4. Secure transmission

Disadvantages of TCP

1. Slower speed
2. High overhead

USER DATAGRAM PROTOCOL (UDP)

UDP stands for:

- User Datagram Protocol

It is:

- Connectionless
- Unreliable

UDP provides fast communication.

FEATURES OF UDP

1. Fast transmission
2. Low overhead
3. No acknowledgment
4. No retransmission

Advantages of UDP

1. Faster communication
2. Suitable for real-time applications

Disadvantages of UDP

1. No guarantee of delivery
2. Possible packet loss

APPLICATIONS OF UDP

1. Online gaming
2. Video conferencing
3. Live streaming
4. DNS services

DIFFERENCE BETWEEN TCP AND UDP

TCP	UDP
Connection-oriented	Connectionless
Reliable	Unreliable
Slower	Faster
Error checking available	Limited error checking
Used in web browsing	Used in streaming

PORT NUMBERS

Ports identify applications running on systems.

Examples:

- HTTP → Port 80
- HTTPS → Port 443
- FTP → Port 21

SOCKETS

A socket is an endpoint of communication.

Combination of:

- IP Address
- Port Number

FLOW CONTROL IN TRANSPORT LAYER

Flow control prevents sender from overwhelming receiver.

TCP uses:

- Sliding Window Protocol

Sliding Window Concept

Multiple packets transmitted before acknowledgment.

Advantages:

1. Better efficiency
2. Higher throughput

CONGESTION CONTROL

Congestion occurs when network traffic exceeds capacity.

Results:

1. Packet loss
2. Delay
3. Reduced performance

Congestion Control Techniques

1. Slow Start
2. Congestion Avoidance
3. Fast Retransmit
4. Fast Recovery

APPLICATION LAYER

The Application Layer is the topmost layer of OSI model.

It provides services directly to users.

FUNCTIONS OF APPLICATION LAYER

1. File transfer
2. Email services
3. Web services
4. Remote login
5. Network management

APPLICATION LAYER PROTOCOLS

Important protocols:

1. HTTP
2. HTTPS
3. FTP
4. SMTP
5. POP3
6. IMAP
7. DNS
8. TELNET
9. SSH

HYPERTEXT TRANSFER PROTOCOL (HTTP)

HTTP is used for:

- Web browsing

Features:

1. Client-server model
2. Stateless protocol

HTTPS

Secure version of HTTP.

Uses:

- SSL/TLS encryption

Advantages:

1. Secure communication
2. Data privacy

FILE TRANSFER PROTOCOL (FTP)

FTP transfers files between systems.

Functions:

1. Upload files
2. Download files

Advantages

1. Fast file transfer

Disadvantages

1. Less secure without encryption

SIMPLE MAIL TRANSFER PROTOCOL (SMTP)

SMTP is used for:

- Sending emails

POST OFFICE PROTOCOL (POP3)

POP3 retrieves emails from mail server.

INTERNET MESSAGE ACCESS PROTOCOL (IMAP)

IMAP allows email access from multiple devices.

DOMAIN NAME SYSTEM (DNS)

DNS converts domain names into IP addresses.

Example:

- www.google.com → IP address

TELNET

Used for remote login.

Disadvantage:

- Insecure communication

SECURE SHELL (SSH)

Secure remote login protocol.

Advantages:

1. Encryption
2. Secure communication

NETWORK SECURITY

Network security protects systems and data from unauthorized access and attacks.

OBJECTIVES OF NETWORK SECURITY

1. Confidentiality
2. Integrity
3. Availability
4. Authentication
5. Authorization

1. Confidentiality

Only authorized users can access data.

2. Integrity

Data should not be modified illegally.

3. Availability

Resources should remain available to authorized users.

TYPES OF NETWORK ATTACKS

1. Passive Attacks
2. Active Attacks

PASSIVE ATTACKS

Attacker monitors communication without altering data.

Examples:

1. Eavesdropping
2. Traffic analysis

ACTIVE ATTACKS

Attacker modifies or damages data.

Examples:

1. Virus attacks
2. Hacking
3. Denial of Service

MALWARE

Malicious software designed to damage systems.

Types:

1. Virus
2. Worm
3. Trojan Horse
4. Spyware
5. Ransomware

1. VIRUS

Attaches itself to files and spreads.

Effects:

- Corrupt files
- Slow system

2. WORM

Self-replicating malware spreading through networks.

3. TROJAN HORSE

Malicious software disguised as useful software.

4. SPYWARE

Secretly collects user information.

5. RANSOMWARE

Locks files and demands payment.

FIREWALL

Firewall monitors incoming and outgoing traffic.

Functions:

1. Blocks unauthorized access
2. Protects internal network

TYPES OF FIREWALL

1. Packet Filtering Firewall
2. Proxy Firewall
3. Stateful Inspection Firewall

ENCRYPTION

Encryption converts plain text into unreadable form.

Purpose:

- Data security

TYPES OF ENCRYPTION

1. Symmetric Encryption
2. Asymmetric Encryption

SYMMETRIC ENCRYPTION

Same key used for:

- Encryption
- Decryption

Example:

- AES

ASYMMETRIC ENCRYPTION

Uses:

- Public key
- Private key

Example:

- RSA

DIGITAL SIGNATURE

Used to verify:

1. Authenticity
2. Integrity

AUTHENTICATION

Verifies identity of users.

Methods:

1. Password
2. OTP
3. Biometrics

VIRTUAL PRIVATE NETWORK (VPN)

VPN creates secure communication tunnel.

Advantages:

1. Privacy
2. Secure remote access

CYBER SECURITY THREATS

1. Phishing
2. Hacking
3. Identity theft
4. Data leakage

PREVENTION METHODS

1. Strong passwords
2. Antivirus software
3. Firewall usage
4. Software updates
5. Data encryption

CLOUD NETWORKING

Cloud networking provides services over Internet.

Examples:

1. Google Drive
2. AWS
3. Microsoft Azure

INTERNET OF THINGS (IoT)

IoT connects smart devices through Internet.

Examples:

1. Smart home
2. Smart watch
3. Smart vehicles

APPLICATIONS OF COMPUTER NETWORKS

1. Online Banking
2. E-commerce
3. Cloud Computing
4. Social Media
5. Online Education
6. Video Conferencing
7. Remote Working

REAL LIFE EXAMPLES

Application	Network Usage
Gmail	SMTP, IMAP
Google Chrome	HTTP/HTTPS
WhatsApp	TCP/UDP
Zoom	UDP
Online Shopping	HTTPS

ADVANTAGES OF TRANSPORT AND APPLICATION LAYERS

1. Reliable communication
2. Fast data transfer
3. Secure communication
4. Efficient application services

DISADVANTAGES

1. Security threats
2. Congestion issues
3. Packet loss in UDP

Conclusion:

The Transport Layer and Application Layer are essential components of computer networks. Protocols such as:

- TCP
- UDP
- HTTP
- FTP
- SMTP
- DNS

enable reliable and efficient communication across the Internet.

Network security mechanisms such as:

- Firewalls
- Encryption
- VPN
- Authentication

help protect networks from cyber threats and unauthorized access.

These concepts form the foundation of:

- Internet communication
- Online services
- Cloud computing
- Modern cybersecurity systems

UNIT – V

WIRELESS NETWORKS, MOBILE COMPUTING AND NETWORK MANAGEMENT:

INTRODUCTION TO WIRELESS NETWORKS

A wireless network is a communication network in which devices communicate without using physical cables.

Wireless communication uses:

- Radio waves
- Microwaves
- Infrared signals

Wireless networks allow users to access data and internet services from different locations without wired connections.

NEED FOR WIRELESS NETWORKS

Wireless networks are important because they provide:

1. Mobility
2. Flexibility
3. Easy installation
4. Cost reduction
5. Remote communication

ADVANTAGES OF WIRELESS NETWORKS

1. Easy mobility
2. Quick installation
3. No cable requirement
4. Flexible communication
5. Supports portable devices

DISADVANTAGES OF WIRELESS NETWORKS

1. Security issues
2. Signal interference
3. Lower speed than wired networks
4. Limited range

TYPES OF WIRELESS NETWORKS

Wireless networks are classified according to coverage area.

1. WLAN (Wireless Local Area Network)

A WLAN covers small geographical area using Wi-Fi.

Examples:

- Home Wi-Fi
- Office Wi-Fi

Features of WLAN

1. Wireless communication
2. Uses access points
3. Supports mobility

Advantages

1. Easy installation
2. Portable connectivity

Disadvantages

1. Security vulnerabilities

2. WMAN (Wireless Metropolitan Area Network)

Covers city-wide area.

Example:

- WiMAX

3. WWAN (Wireless Wide Area Network)

Covers large geographical regions.

Examples:

- Mobile communication networks
- Cellular networks

WI-FI TECHNOLOGY

Wi-Fi stands for:

- Wireless Fidelity

It is based on:

- IEEE 802.11 standard

Wi-Fi allows wireless internet access.

COMPONENTS OF WI-FI NETWORK

1. Access Point (AP)
2. Wireless Router
3. Wireless Adapter
4. Client Devices

ACCESS POINT (AP)

An access point connects wireless devices to wired network.

Functions:

1. Signal transmission
2. Device communication

IEEE 802.11 STANDARDS

Standard	Speed
802.11a	54 Mbps
802.11b	11 Mbps
802.11g	54 Mbps
802.11n	600 Mbps
802.11ac	Higher speed

BLUETOOTH

Bluetooth is short-range wireless communication technology.

Used for:

- File sharing
- Wireless headphones
- Smart devices

FEATURES OF BLUETOOTH

1. Low power consumption
2. Short range communication
3. Easy connectivity

Advantages

1. Low cost
2. Portable communication

Disadvantages

1. Limited range
2. Lower speed

INFRARED COMMUNICATION

Uses infrared light signals for communication.

Applications:

1. Remote controls
2. Wireless keyboards

CELLULAR NETWORKS

Cellular networks support mobile communication using cells.

Each area is divided into small regions called:

- Cells

Each cell contains:

- Base station

GENERATIONS OF MOBILE NETWORKS

1. 1G
2. 2G
3. 3G
4. 4G
5. 5G

1G TECHNOLOGY

First generation mobile communication.

Features:

- Analog communication
- Voice calls only

Limitations

1. Poor quality
2. Low security

2G TECHNOLOGY

Digital communication introduced.

Features:

1. SMS services
2. Better voice quality

3G TECHNOLOGY

Introduced mobile internet.

Features:

1. Video calling
2. Faster internet

4G TECHNOLOGY

High-speed internet communication.

Features:

1. HD video streaming
2. Online gaming
3. VoLTE support

5G TECHNOLOGY

Latest wireless communication technology.

Features:

1. Very high speed
2. Low latency
3. Massive device connectivity

Advantages of 5G

1. Faster downloads
2. Smart city support
3. Better IoT communication

MOBILE COMPUTING

Mobile computing allows users to access information while moving.

It combines:

1. Mobile devices
2. Wireless communication
3. Internet services

COMPONENTS OF MOBILE COMPUTING

1. Mobile Hardware
2. Mobile Software
3. Mobile Communication

MOBILE DEVICES

Examples:

1. Smartphones
2. Tablets
3. Laptops
4. Smart watches

FEATURES OF MOBILE COMPUTING

1. Portability
2. Mobility
3. Connectivity
4. Flexibility

APPLICATIONS OF MOBILE COMPUTING

1. Mobile banking
2. E-commerce
3. GPS navigation

4. Online learning
5. Video conferencing
6. Social media

MOBILE IP

Mobile IP allows users to move across networks while maintaining same IP address.

Components of Mobile IP

1. Mobile Node
2. Home Agent
3. Foreign Agent

Advantages of Mobile IP

1. Continuous connectivity
2. Mobility support

HANDOFF IN MOBILE NETWORKS

Handoff means transferring communication from one base station to another.

TYPES OF HANDOFF

1. Hard Handoff
2. Soft Handoff

Hard Handoff

Old connection terminated before new connection established.

Soft Handoff

New connection established before old connection disconnected.

SATELLITE COMMUNICATION

Communication through artificial satellites.

Used in:

1. Television broadcasting
2. GPS systems
3. Weather forecasting

TYPES OF SATELLITES

1. GEO (Geostationary Earth Orbit)
2. MEO (Medium Earth Orbit)
3. LEO (Low Earth Orbit)

Advantages of Satellite Communication

1. Global coverage
2. Long-distance communication

Disadvantages

1. High cost
2. Signal delay

SENSOR NETWORKS

Sensor networks consist of interconnected sensor devices.

Applications:

1. Environmental monitoring
2. Healthcare
3. Military systems

INTERNET OF THINGS (IoT)

IoT connects physical devices through internet.

Examples:

1. Smart homes
2. Smart cars
3. Smart appliances

FEATURES OF IoT

1. Automation
2. Real-time monitoring
3. Remote control

Advantages of IoT

1. Improved efficiency
2. Better monitoring
3. Reduced human effort

NETWORK MANAGEMENT

Network management refers to administration and maintenance of computer networks.

OBJECTIVES OF NETWORK MANAGEMENT

1. Performance monitoring
2. Fault detection
3. Security management
4. Resource management

FUNCTIONS OF NETWORK MANAGEMENT

1. Configuration Management

2. Fault Management
3. Accounting Management
4. Performance Management
5. Security Management

1. Configuration Management

Manages network devices and configurations.

2. Fault Management

Detects and resolves network problems.

3. Accounting Management

Tracks resource usage.

4. Performance Management

Monitors network efficiency.

5. Security Management

Protects network from threats.

SNMP (Simple Network Management Protocol)

SNMP is widely used network management protocol.

Functions:

1. Monitoring devices
2. Managing network traffic

Components of SNMP

1. SNMP Manager
2. SNMP Agent
3. Management Information Base (MIB)

NETWORK MONITORING TOOLS

1. Wireshark
2. Nagios
3. SolarWinds
4. PRTG Network Monitor

QUALITY OF SERVICE (QoS)

QoS ensures better performance for important applications.

Applications:

1. Video conferencing
2. VoIP calls
3. Online gaming

CLOUD COMPUTING

Cloud computing provides services over internet.

Types:

1. Public Cloud
2. Private Cloud
3. Hybrid Cloud

Advantages of Cloud Computing

1. Scalability
2. Cost reduction
3. Remote access

NETWORK VIRTUALIZATION

Virtualization creates virtual network resources.

Advantages:

1. Efficient resource utilization
2. Flexibility

CYBER SECURITY IN WIRELESS NETWORKS

Wireless networks face security threats such as:

1. Unauthorized access
2. Data interception
3. Malware attacks

SECURITY METHODS

1. WPA/WPA2 Encryption
2. Firewall
3. VPN
4. Authentication

VPN (Virtual Private Network)

VPN creates secure communication tunnel over internet.

Advantages:

1. Data privacy
2. Secure remote access

WIRELESS SENSOR NETWORK (WSN)

WSN contains distributed sensor nodes.

Applications:

1. Industrial monitoring

2. Disaster management
3. Agriculture

GREEN NETWORKING

Green networking reduces energy consumption in networks.

Advantages:

1. Energy saving
2. Environmental protection

APPLICATIONS OF WIRELESS NETWORKS

1. Mobile communication
2. Smart cities
3. Online education
4. Healthcare systems
5. E-commerce
6. GPS navigation

REAL LIFE EXAMPLES

Technology	Application
Wi-Fi	Internet access
Bluetooth	Wireless headphones
5G	Smart communication
IoT	Smart home
GPS	Navigation system

ADVANTAGES OF MOBILE COMPUTING

1. Anywhere access
2. Real-time communication
3. Improved productivity
4. Better flexibility

DISADVANTAGES

1. Security threats
2. Battery limitations
3. Signal interference

FUTURE OF WIRELESS NETWORKS

Future wireless technologies will focus on:

1. Faster communication
2. Smart automation
3. AI integration
4. Smart transportation
5. Advanced IoT systems

Conclusion :

Wireless networking and mobile computing have transformed modern communication systems. Technologies such as:

- Wi-Fi
- Bluetooth
- Mobile IP
- IoT
- 5G

play a major role in today's digital world.

Network management techniques ensure:

- Efficient communication
- Better security
- High performance
- Reliable connectivity

These concepts are widely used in:

- Smart devices
- Cloud systems
- Mobile applications
- Industrial automation
- Modern communication networks