AS PER THE LATEST SYLLABUS PRESCRIBED BY THE STATE BOARD OF TECHNICAL EDUCATION & TRAINING, ANDHRA PRADESH

AS PER C-20

COMPUTER NETWORKS

For **CM.E.** Second Year, IV Semester

B. SINDHU

Senior Lecturer

Dept.of Computer Engineering

FALCON PUBLISHERS

Turrebaz Khan Road, First Floor, Pushpanjali Complex,

Opp : Osmania Medical College, **KOTHI,** Hyderabad - 500 095

Phone No : 040-66132366 - 24615141

E-mail : falconpublishers77@gmail.com - **Website :** falconpublishers.com

SYLLABUS

Subject : Computer Networks

Subject Code : CM-405

Periods/Week : 05

Total No. of Periods : 75

Marks of FA : 20

Marks of SA : 80

S.No.	Major Topics	No. of Periods	CO's Mapped
1.	Introduction to Networks	15	CO1, CO2
2.	LAN components, Devices, tools, and Network Topologies	15	CO3
3.	Network Addressing and sub-netting	15	CO3, CO4, CO6
4.	Networks protocols and management	20	CO3, CO5, CO6
5.	Basic Network administration	10	CO6
	Total Periods	**75**	

LEARNING OUTCOMES

1.0 Introduction to Computer Networks.

1.1 Describe the Overview of Networking.

1.2 Discuss the Need and importance of Networking.

1.3 Classification and features of Networks–LAN, MAN,WAN

1.4 Importance of Wi-Fi, Bluetooth

1.5 List the Hardware and Software Components.

1.6 Explain Various Network Communication Standards.

1.7 Explain the OSI Reference Model with its architecture and layer functions.

1.8 Explain the functions of each layer of TCP/IP Reference Model

1.9 Compare TCP/IP and OSI reference models.

2.0 Network components, devices, tools, and Network Topologies.

2.1 Discuss the need and importance of LAN Cables, Connectors, wireless network adapter

2.2 Explain about LAN Cables

- 2.2.1 Coaxial Cables,
- 2.2.2 Twisted-Pair Cables(Shielded, Unshielded)
- 2.2.3 Optical Fibre Cables,

2.3 Explain about LAN Connectors.

- 2.3.1 Registered Jack(RJ)-45
- 2.3.2 Straight Tip (ST)
- 2.3.3 Subscriber Connector (SC)0
- 2.3.4 Lucent Connector (LC)

2.4 Explain about LAN Devices

- 2.4.1 Repeaters
- 2.4.2 Hubs
- 2.4.3 Switches
- 2.4.4 Network Interface Cards(NICs)
- 2.4.5 Routers (CISCO, DAX, Etc.)
- 2.4.6 Modem (56 KBPS Internal or External, ADSLModems.)
- 2.4.7 Gateways

2.5 Explain about Wireless network adapter

2.6 List and Explain the Functions of LAN Tools

- 2.6.1 Anti-Magnetic mat
- 2.6.2 Anti-Magnetic Gloves
- 2.6.3 Crimping Tool
- 2.6.4 Cable Tester
- 2.6.5 Cutter
- 2.6.6 Loop back plug
- 2.6.7 Toner probe
- 2.6.8 Punch down tool
- 2.6.9 Protocol analyzer
- 2.6.10 Multi meter

2.7 Explain about Topologies with their merits and de-merits

2.7.1 Bus

2.7.2 Ring

2.7.3 Star

2.7.4 Mesh

2.7.5 Hybrid Topologies

3.0 Network Addressing and sub-netting

3.1 Introduction to Network Addressing

3.2 Explain TCP/IP Addressing Scheme

3.3 List and describe the Components of IP Address

3.4 List and explain IP Address Classes

3.5 Define subnet and describe the necessity of sub-netting

3.6 Illustrate sub-netting

3.7 Explain sub-netting with a simple example

3.8 List the Advantages and disadvantages of sub netting

3.9 Describe the Internet Protocol Addressings

3.9.1 IPv4

3.9.2 IPv6

3.10 Statetheneed for IPv6.

3.11 Explain about Classful addressing and classless addressing inIPv4.

3.12 Describe Internet protocol version-6 (IPv6) addressing.

4.0 Networks protocols and management

4.1 Describe need of protocols in computer networks

4.2 Explain the protocols

4.2.1 Hyper Text Transfer Protocol(HTTP)

4.2.2 File Transfer Protocol(FTP)

4.2.3 Simple Mail Transfer Protocol(SMTP)

4.2.4 Address Resolution Protocol(ARP)

4.2.5 Reverse Address Resolution Protocol(RARP)

4.2.6 Telnet

4.3 Describe Simple Network Management Protocol(SNMP)

4.4 Explain about working of SNMP.

4.5 Explain about DHCP, DNS

4.6 Explain the Overview of Network Management.

4.7 Explain Network Monitoring and Troubleshooting.

4.8 Explain about Remote Monitoring (RMON).

5.0 Basic Network administration

5.1 Explain about Network administration.

5.2 Describe the need of Network Administration.

5.3 Responsibilities of Network Administrator.

5.4 Discuss User & Group Managements.

5.5 Analyze the working of Device Manager

5.6 Analyze Verification & Managing Ports.

5.7 Explain the procedure of Installing, Managing & Configuration of Printers,

5.8 Demonstrate Disk Management Tools & Tasks

5.9 Describe File Systems Management.

5.10 Demonstrate on NTFS (File and Folder) & Share Permissions.

MODEL BLUE PRINT

S.No.	Chapter/Unit title	No. of Periods	Weightage of Marks	Marks Wise Distribution				Question Wise Distribution			
				R	U	Ap	An	R	U	Ap	An
1.	Introduction to Networks	15	14	8	6			1	2		
2.	LAN components, Devices, Tools, and Network Topologies	15	14	6	8			2	1		
3.	Network Addressing and Sub-netting	15	14		3	11	*		1	2	*
4.	Network Protocols and Management	20	14	3	8	3	*	1	1	1	*
5.	Basic Networks and Administration	10	14		6	8	*		2	1	*
	Total	75	70 + 10*	17	31	22	10*	4	7	4	1

Note :

Part-C : 10 marks single analytical question may be chosen from any one of starred chapters.

CONTENTS

CHAPTER · 1 — 1.1 – 1.12

INTRODUCTION TO NETWORKS

1.1 OVERVIEW OF NETWORKING 2

1.2 NEED AND IMPORTANCE OF NETWORKING 2

1.3 CLASSIFICATIONS AND FEATURES OF NETWORKS 3

1.4 IMPORTANCE OF WI-FI, BLUETOOTH 4

1.5 HARDWARE AND SOFTWARE COMPONENTS 5

1.6 VARIOUS NETWORK COMMUNICATION STANDARDS 5

1.7 OSI REFERENCE MODEL WITH ITS ARCHITECTURE AND LAYER FUNCTIONS 6

1.8 FUNCTIONS OF EACH LAYER OF TCP/IP REFERENCE MODE 8

1.9 TCP/IP AND OSI REFERENCE MODELS 10

- *Review Questions* *11*

CHAPTER-2 — 2.1 – 2.18

LAN COMPONENTS, DEVICES, TOOLS AND NETWORK TOPOLOGIES

2.1 NEED AND IMPORTANCE OF LAN CABLES, CONNECTORS, WIRELESS NETWORK ADAPTER 2

2.2 LAN CABLES 2

2.2.1 Coaxial Cables *2*

2.2.2 Twisted-Pair Cables *3*

2.2.3 Optical Fibre Cable *4*

2.3 LAN CONNECTORS 4

2.3.1 Registered Jack (RJ)-45 ..... *4*

2.3.2 Straight Tip (ST) *5*

2.3.3 Subscriber Connector (SC) *5*

2.3.4 Lucent Connector (LC) *5*

2.4 LAN DEVICES 5

2.4.1 Repeaters 5

2.4.2 Hubs 6

2.4.3 Switches 6

2.4.4 Network Interface Cards (NICs) 7

2.4.5 Routers (CISCO, DAX) 7

2.4.6 Modem (56 kbps Internal or External ADSL Modems) 8

2.4.7 Gateways 9

2.5 WIRELESS NETWORK ADAPTER 9

2.6 FUNCTIONS OF LAN TOOLS 10

2.6.1 Anti-Magnetic Mat 10

2.6.2. Anti-Magnetic Gloves 10

2.6.3 Crimping Tool 10

2.6.4 Cable Tester 10

2.6.5 Cutter 11

2.6.6 Loop Backplug 11

2.6.7 Tonerprobe 11

2.6.8 Punch down Tool 11

2.6.9 Protocol Analyser 11

2.6.10 Multimeter 11

2.7 TOPOLOGIES WITH THEIR MERITS AND DE-MERITS 12

2.7.1 BUS Topology 12

2.7.2 RING Topology 13

2.7.3 Star Topology 14

2.7.4 Mesh Topology 15

2.7.5 Hybrid Topology 16

- **Review Questions** **18**

CHAPTER-3 3.1 – 3.24

NETWORK ADDRESSING AND SUB-NETTING

3.1 INTRODUCTION TO NETWORK ADDRESSING 2

3.2 TCP/IP ADDRESSING SCHEME 2

3.3 COMPONENTS OF IP ADDRESS 3

3.4 IP ADDRESS CLASSES 3

3.5 SUBNET AND THE NECESSITY OF SUB-NETTING 5

3.6 SUB-NETTING WITH A SIMPLE EXAMPLE 6

3.7 ADVANTAGES AND DISADVANTAGES OF SUBNETTING 11

3.8 INTERNET PROTOCOL ADDRESSINGS 12

3.8.1 IPV4 12

3.8.2 IPV6 12

3.9 NEED FOR IPV6 13

3.10 CLASSFUL ADDRESSING AND CLASSLESS ADDRESSING IN IPV4 13

3.11 INTERNET PROTOCOL VERSION-6 (IPV6) ADDRESSING 17

- REVIEW QUESTIONS 23

CHAPTER-4 4.1 – 4.18

NETWORKS PROTOCOLS AND MANAGEMENT

4.1 NEED OF PROTOCOLS IN COMPUTER NETWORKS 2

4.2 PROTOCOLS 2

4.2.1 Hyper Text Transfer Protocol (HTTP) 2

4.2.2 File TransferProtocol (FTP) 3

4.2.3 Simple Mail Transfer Protocol (SMTP) 3

4.2.4 Address Resolution Protocol (ARP) 4

4.2.5 Reverse Address Resolution Protocol (RARP) 5

4.2.6 Telnet 5

4.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP) 6

4.4	WORKING OF SNMP	.....	8
4.5	DHCP, DNS	.....	10
4.6	OVERVIEW OF NETWORK MANAGEMENT	.....	10
4.7	NETWORK MONITORING AND TROUBLESHOOTING	.....	11
4.8	REMOTE MONITORING (RMON)	.....	17
	• *Review Questions*	.....	*18*

CHAPTER-5 5.1 – 5.18

BASIC NETWORK ADMINISTRATION

5.1	NETWORK ADMINISTRATION	.....	2
5.2	NEED OF NETWORK ADMINISTRATION	.....	2
5.3	RESPONSIBILITIES OF NETWORK ADMINISTRATOR	.....	3
5.4	USER AND GROUP MANAGEMENTS	.....	3
5.5	WORKING OF DEVICE MANAGER	.....	4
5.6	VERIFICATION AND MANAGING PORTS	.....	4
5.7	PROCEDURE OF INSTALLING, MANAGING AND CONFIGURATION OF PRINTERS	.....	5
5.8	DISK MANAGEMENT TOOLS AND TASKS	.....	7
5.9	FILE SYSTEMS MANAGEMENT	.....	10
5.10	NTFS (FILE AND FOLDER) AND SHARE PERMISSIONS	.....	14
	• *Review Questions*	.....	*18*

MODEL PAPERS 1 - 4

QUESTION PAPER (JUNE/JULY-2022) 5 - 6

Chapter-1

INTRODUCTION TO NETWORKS

CHAPTER OUTLINE

1.1 Overview of Networking 2

1.2 Need and Importance of Networking 2

1.3 Classifications and Features of Networks 3

1.4 Importance of Wi-Fi, Bluetooth 4

1.5 Hardware and Software Components 5

1.6 Various Network Communication Standards 5

1.7 OSI Reference Model with its Architecture and Layer Functions 6

1.8 Functions of each Layer of TCP/IP Reference Model 8

1.9 TCP/IP and OSI Reference Models 10

1.1 OVERVIEW OF NETWORKING

A network consists of two (or) more computers that are linked in order to share resources (such as printers and CDs), exchange files (or) allow electronic communications.

The computers on a network may be linked through cables, telephone lines, radio waves, satellites (or) infrared light beams. Network computer devices that originate, route and terminate the data are called ***network nodes.***

Nodes can include hosts such as personal computers, phones, servers as well as networking hardware. Two such devices can be said to be networked together when one device is able to exchange information with the other device, whether (or) not they have a direct connection to each other.

1.2 NEED AND IMPORTANCE OF NETWORKING

Computer networks support applications such as access to the World Wide Web, shared use of application and storage servers, printers, and fax machines, and use of email and instant messaging applications.

Computer networks help users on the network to share the resources and in communication. Can you imagine a world now without emails, online newspapers, blogs, chat and the other services offered by the internet?

The following are the important uses and benefits of a computer network :

1. **File Sharing :** Networking of computers helps the network users to share data files.
2. **Hardware Sharing :** Users can share devices such as printers, scanners, CD-ROM drives, hard drives etc., Without computer networks, device sharing is not possible.

3. **Application Sharing :** Applications can be shared over the network and this allows implementing client/server applications

4. **User Communication :** Networks allow users to communicate using e-mail, news groups and video conferencing etc.,

5. **Network Gaming :** A lot of network games are available, which allow multi-users to play from different locations.

6. **Voice Over IP (VoIP) :** Voice over Internet Protocol (IP) is a revolutionary change in telecommunication which allows to send telephone calls (voice data) using standard Internet Protocol (IP) rather than by traditional PSTN.

1.3 CLASSIFICATIONS AND FEATURES OF NETWORKS

S.No.	Key	LAN	MAN	WAN
1.	Definition	LAN stands for Local Area Network	MAN stands for Metropolitan Area Network	WAN stands for Wide Area Network.
2.	Ownership	LAN is often owned by private organizations.	MAN ownership can be private (or) public.	WAN ownership can be private (or) public.
3.	Speed	LAN speed is quiet high.	MAN speed is average.	WAN speed is lower than that of LAN.
4.	Delay	Network Propagation delay is short in LAN.	Network Propagation delay is moderate in MAN.	Network Propagation delay is longer in WAN.
5.	Congestion	LAN has low congestion as compared to WAN.	MAN has higher congestion than LAN.	WAN has higher congestion than both MAN and LAN.
6.	Fault Tolerance	Fault tolerance of LAN is higher than WAN.	Fault tolerance of MAN is lower than LAN.	Fault tolerance of WAN is lower than both LAN and MAN.

7.	Maintenance	Designing and maintaining LAN is easy and less costly than WAN.	Designing and maintaining WAN is complex and more costly than LAN.	Designing and maintaining WAN is complex and more costly than both LAN and MAN.

1.4 IMPORTANCE OF WI-FI, BLUETOOTH

Wi-Fi stands for Wireless Fidelity, It is one of the important technologies of the computer networking. It allows the users to connect to the internet without wires, It allows the router to be cordless also, The network is connected through an access point for internet. Wi-Fi is used for different purposes such as data transmission and wireless communication, With using a Wi-Fi connection whenever possible will most often result in faster, more reliable internet access, and it is cheap. Wi-Fi allows wireless connection for up to 20 meters. Wi-Fi is used for free at restaurants (or) coffee houses, It sends out Data to LAN and WAN network and these networks allow any connection without using cords, You can take your laptop where ever you want with the option of having a wireless connection with the help of the routers and the adapters.

Bluetooth technology is a standardized short-range wireless communication technology that uses a low-power radio frequency at low cost, It is interoperable and it sucks up very little energy, It is a special wireless communication system that allows completely different electronic devices to communicate with each other, Most new vehicles come with Bluetooth connectivity. Smart phones use Bluetooth technology to communicate with other devices and portable personal computers (or) laptops are the first ones to use Bluetooth technology. Bluetooth can work between any two enabled devices and does not require additional network equipment such as routers (or) modems, so it is a popular choice for

sending data between mobile electronics over close ranges. You can make your cell phone, laptop, PDA and car stereo communicate to each other with Bluetooth wireless technology, You can link your devices without the cables and you can move with your network easily as Bluetooths transmission range is about 30 feet.

1.5 HARDWARE AND SOFTWARE COMPONENTS

Both hardware and software components are used to create a computer network.

The Hardware Components are :

1. Cable for interconnection.
2. Network Cards / Network Adapters.
3. Client computer.
4. Server computer.
5. Repeater.
6. Hub.
7. Gateway.
8. Dial-up Internet Connection.
9. ISP Account.

The software needed is a Network Operating System (NOS)

1.6 VARIOUS NETWORK COMMUNICATION STANDARDS

The primary reason for standards is to ensure that hardware and software produced by different vendors can work together. Without networking standards, it would be difficult if not impossible to develop networks that easily share information. The use of standards makes it much easier to develop software and hardware that link different networks because software and hardware can be developed one layer at a time.

There are Two Types of Standards :

1. Formal, and
2. De facto.

1. **Formal :** A formal standard is developed by an official industry (or) government body. For example, there are formal standards for applications such as Web browsers (**Eg** : HTTP, HTML), for network layer software (**Eg** : IP), data link layer software (**Eg** : Ethernet IEEE 802.3), and for physical hardware (**Eg** : V.90 modems). Formal standards typically take several years to develop, during which time technology changes, making them less useful.

2. **De Facto :** De facto standards are those that emerge in the marketplace and are supported by several vendors but have no official standing. For example, Microsoft Windows is a product of one company and has not been formally recognized by any standards organization, yet it is a de facto standard. In the communications industry, de facto standards often become formal standards once they have been widely accepted. The formal standardization process has three stages : specification, identification of choices and acceptance. The specification stage consists of developing a nomenclature and identifying the problems to be addressed. In the identification of choices stage, those working on the standard identify the various solutions and choose the optimum solution from among the alternatives.

1.7 OSI REFERENCE MODEL WITH ITS ARCHITECTURE AND LAYER FUNCTIONS

Virtually all networks today are based on the Open Systems Interconnection (OSI) standard. OSI was developed in 1984 by the International Organization for Standardization (ISO), a global federation of national standards organizations representing approximately 130 countries. The core of this

standard is the OSI Reference Model, a set of seven layers that define the different stages that data must go through to travel from one device to another over a network.

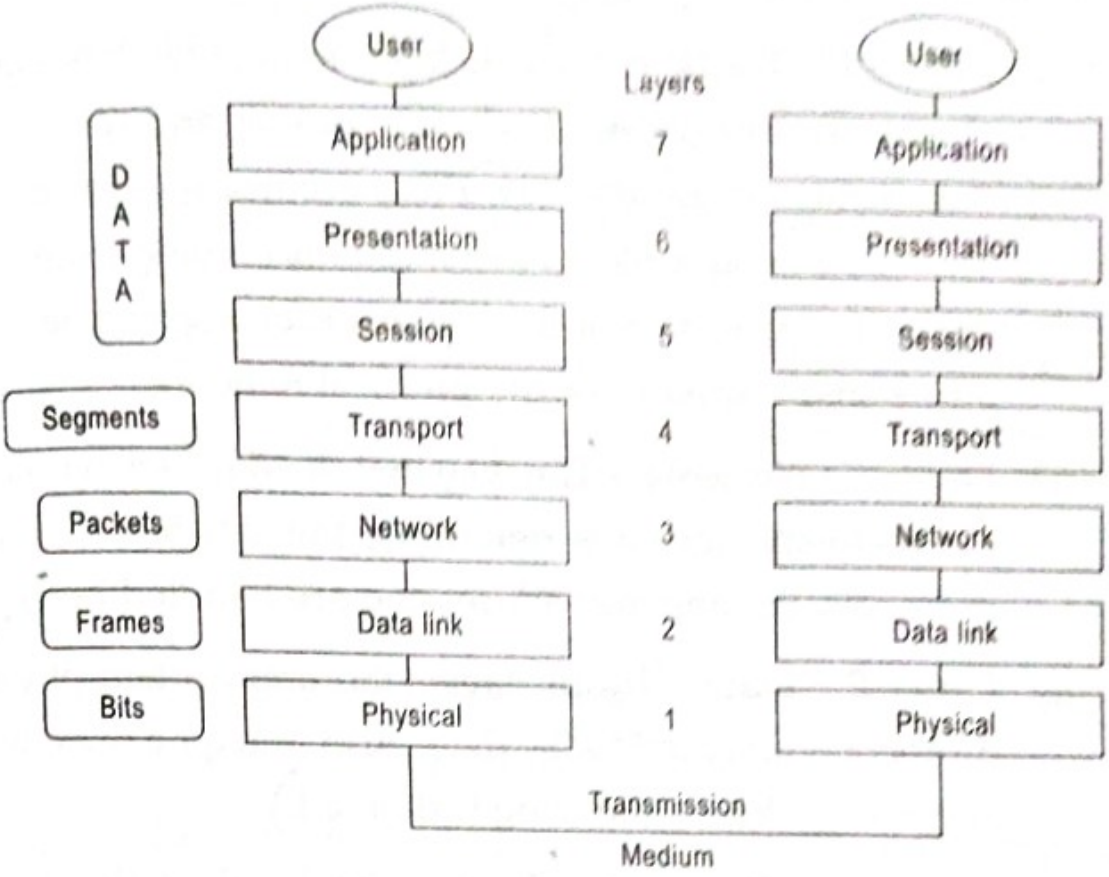


FIG 1.1 :

Think of the seven layers as the assembly line in the computer. At each layer, certain things happen to the data that prepare it for the next layer. The seven layers, which separate into two sets, They are :

1. Application Set :

***(i) Layer-7* : Application** - This is the layer that actually interacts with the operating system (or) application whenever the user chooses to transfer files, read messages (or) performs other network-related activities.

***(ii) Layer-6* : Presentation** - Layer 6 takes the data provided by the Application layer and converts it into a standard format that the other layers can understand.

(iii) ***Layer-5*** **: Session** - Layer 5 establishes, maintains and ends communication with the receiving device.

2. **Transport Set :**

(i) ***Layer-4*** **: Transport** - This layer maintains flow control of data and provides for error checking and recovery of data between the devices. Flow control means that the Transport layer looks to see if data is coming from more than one application and integrates each application's data into a single stream for the physical network.

(ii) ***Layer-3*** **: Network** - The way that the data will be sent to the recipient device is determined in this layer. Logical protocols, routing and addressing are handled here.

(iii) ***Layer-2*** **: Data** - In this layer, the appropriate physical protocol is assigned to the data. Also, the type of network and the packet sequencing is defined.

(iv) ***Layer-1*** **: Physical** - This is the level of the actual hardware. It defines the physical characteristics of the network such as connections, voltage levels and timing.

The OSI Reference Model is just a guideline. Actual protocol stacks often combine one (or) more of the OSI layers into a single layer.

1.8 FUNCTIONS OF EACH LAYER OF TCP/IP REFERENCE MODE

TCP/IP that is transmission control protocol and the internet protocol was developed by Department of Defence's Project Research Agency (ARPA, later DARPA) under the project of network interconnection.

Originally it was created to connect military networks together, later it was used by government agencies and universities. It is robust to failures and flexible to diverse networks. Most widely

used protocol for interconnecting computers and it is the protocol of the internet.

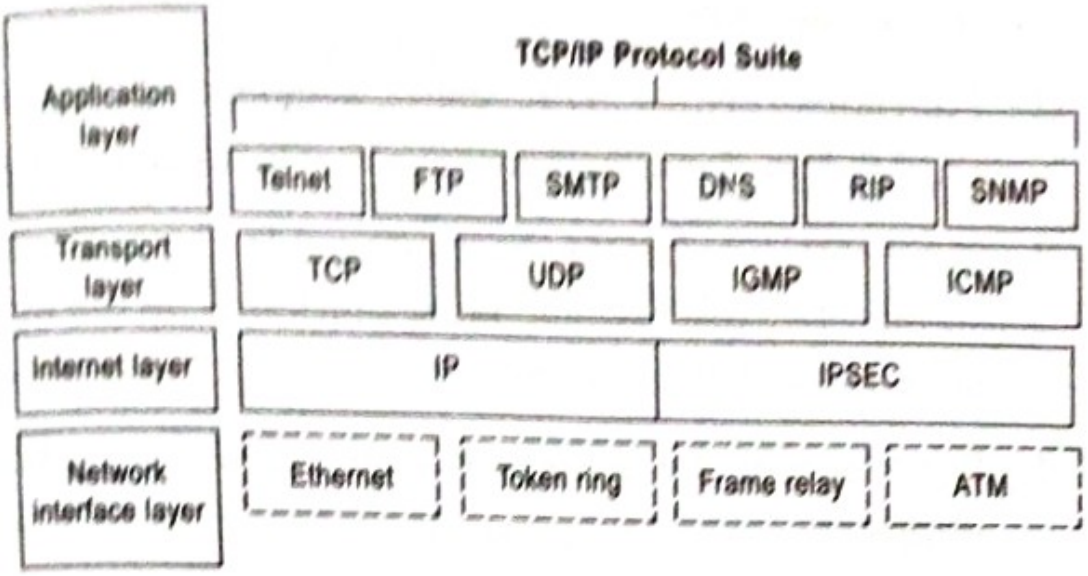


Fig 1.2 :

Layer-1 : Host-to-network Layer

1. Lowest layer of the all.
2. Protocol is used to connect the host, so that the packets can be sent over it.
3. Varies host to host and network to network.

Layer-2 : Internet layer

1. Selection of a packet switching network which is based on a connectionless internetwork layer is called a ***internet layer.***
2. It the layer which holds the whole architecture together.
3. It allows the host to insert the packets.
4. It helps the packet to travel independently to the destination.
5. Order in which packets are received is different from the way they are sent.
6. IP (internet protocol) is used in this layer.

Layer-3 : Transport Layer

1. It decides if data transmission should be on parallel path (or) single path.
2. Functions such as multiplexing, segmenting (or) splitting on the data done by layer four that is transport layer.
3. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.
4. Functions of the transport layer are same as the OSI model.
5. Transport layer also arrange the packets sent in sequence.

Layer-4 : Application Layer

1. Protocols used in this layer are high level protocols such as TELNET, FTP (file transfer protocol) etc.,

1.8 TCP/IP AND OSI REFERENCE MODELS

S.No.		TCP/IP Model	OSI Model
1.	Stand for	Transmission control Protocol/Internet protocol.	Open system Interconnect.
2.	Meaning	It is a client server model used for transmission of data over the internet.	It is a theoretical model which is used for computing system.
3.	Number of	4 Layers.	7 Layers.
4.	Developed by	Department of Defence (DOD).	ISO (International Standard Organization.
5.	Tangible	Yes.	No.
6.	Usage	Mostly used.	Never used.
7.	Type of Approach	Horizontal approach.	Vertical approach.

Part-A

1. What is the need of networking ?
2. If networking couldn't exist what could be the scenario ? Good (or) bad ?
3. Explain the importance of networking of computers.
4. What is that which distinguishes between LAN, MAN and WAN ?
5. What is a LAN ?
6. What is the importance of MAN ?
7. What is the need of WAN ?
8. What is the importance of Bluetooth ?
9. Differentiate between software component and hardware component.
10. Diagrammatically represent OSI reference model.
11. Compare TCP/IP and OSI models on any 4 points.

Part-B

1. Classify LAN, MAN and WAN according to their features and concepts.
2. Give the importance of WAN, Bluetooth and Wi-Fi.
3. List the important software and hardware components of a computer with their need.
4. Explain various network communication standards.
5. Explain the working of OSI model with help of a diagram.
6. Explain TCP/IP reference model
7. Compare the working of OSI and TCP/IP reference models.

Chapter-2

LAN COMPONENTS, DEVICES, TOOLS, AND NETWORK TOPOLOGIES.

CHAPTER OUTLINE

2.1 Need and Importance of LAN Cables, Connectors, Wireless Network Adapter 2

2.2 LAN Cables 2

2.3 Lan Connectors 4

2.4 Lan Devices 5

2.5 Wireless Network Adapter 9

2.6 Functions of LAN Tools 10

2.7 Topologies with their Merits and De-merits 12

2.1 NEED AND IMPORTANCE OF LAN CABLES, CONNECTORS, WIRELESS NETWORK ADAPTER

LAN cables are heart of the network which carry the data signals from one terminal to the other. LAN connectors whether Ethernet, coaxial, wireless (or) otherwise are the primary interface between modern computers, local network connections, and ultimately the Internet. A LAN cable is used for connecting to computers and hardware to form a LAN. LAN is a Local Area Network of devices and which help connect the network together. LAN's can be huge in size (MAN or WAN). Ethernet cables are everywhere. They are the workhorses of the wired network world. These cables are vital when creating a home (or) business network (or) establishing internet connections.

2.2 LAN CABLES

2.2.1 *Coaxial Cables*

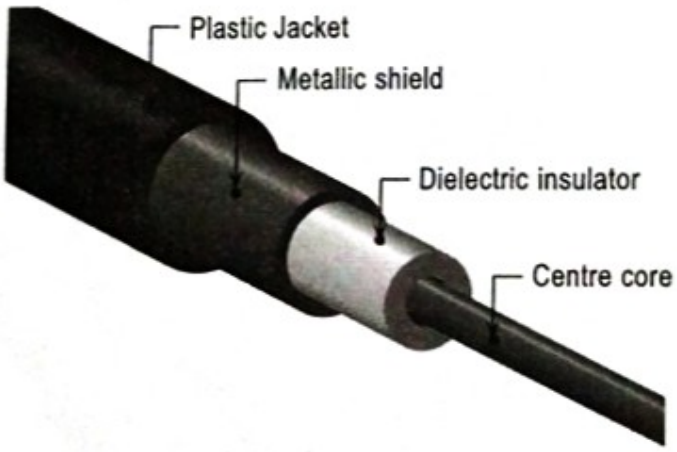


FIG 2.1 : Coaxial Cable

Coaxial cable (or) **Coax** is a type of cable that has an inner conductor surrounded by a tubular insulating layer, surrounded by a tubular conducting shield. Many coaxial cables also have an insulating outer sheath (or) jacket. The term coaxial comes from the inner conductor and the outer shield sharing a

geometric axis. Coaxial cable was invented by English engineer and mathematician Oliver Heaviside. Coaxial cable differs from other shielded cable used for carrying lower-frequency signals, such as audio signals.

2.2.2 *Twisted-Pair Cables*

Twisted pair cabling is a type of wiring in which two conductors of a single circuit are twisted together for the purposes of cancelling out electromagnetic interference (EMI) from external sources; for instance, electromagnetic radiation from unshielded twisted pair (UTP) cables, and cros stalk between neighbouring pairs. It was invented by Alexander Graham Bell. There are two twisted pair types: shielded and unshielded. Shielded Twisted Pair (STP) has a fine wire mesh surrounding the wires to protect the transmission; Unshielded Twisted Pair (UTP) does not. Shielded cable is used in older telephone networks, network, and data communications to reduce outside interference.

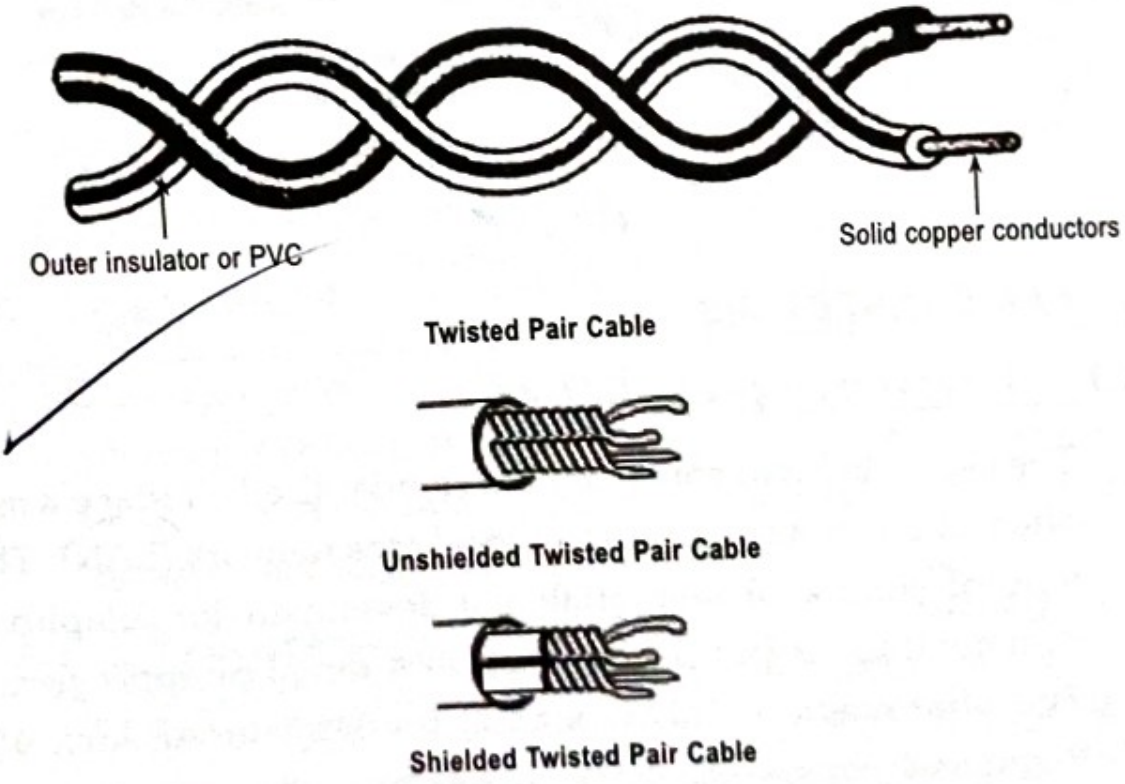


FIG 2.2 :

2.2.3 *Optical Fibre Cable*

Fibre Optic communication is a method of transmitting information from one place to another by sending pulses of light through an optical fiber. The light forms an electromagnetic carrier wave that is modulated to carry information. First developed in the 1970s, fiber-optic communication systems have revolutionized the telecommunications industry and have played a major role. Because of its advantages over electrical transmission, optical fibers have largely replaced copper wire communications in core networks in the developed world. Optical fiber is used by many telecommunications companies to transmit telephone signals, Internet communication and cable television signals.

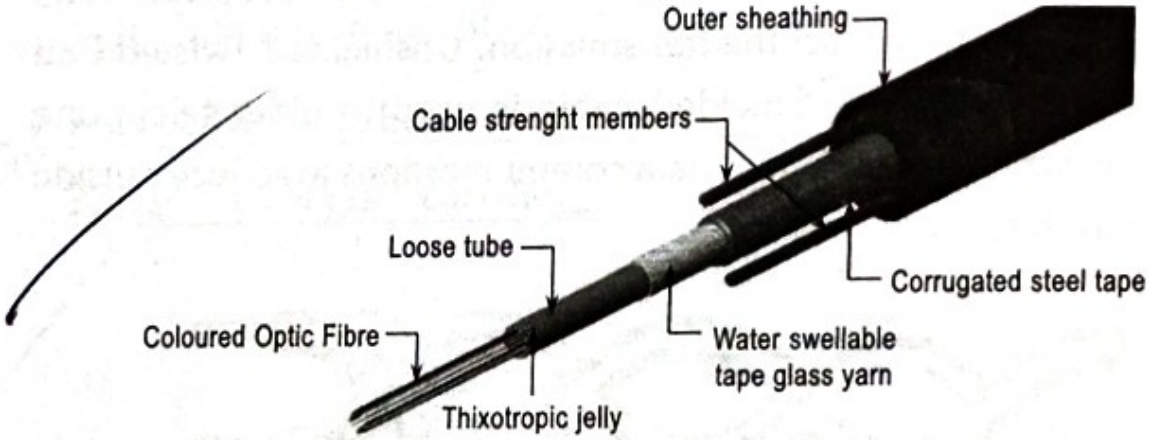


FIG 2.3

2.3 LAN CONNECTORS

2.3.1 *Registered Jack (RJ)-45*

The eight-pin RJ45 connector is a standardised interface which often connects a computer to a local area network (LAN). This type of connector was originally developed for telephone communications but is now used in a range of applications. The abbreviation, RJ45, stands for Registered Jack-45. Registered jack specifications are related to the wiring patterns of the jacks, rather than their physical characteristics. The term

RJ45 has also come to refer to a range of connectors for Ethernet jacks. An 8 Position/8 Contact connector, called **an 8P8C**, is a modular connector for telecommunication cables. It is also informally referred to as an **RJ45.**

2.3.2 *Straight Tip (ST)*

(Straight Tip connector) A fiber-optic cable connector that uses a bayonet plug and socket. It was the first de facto standard connector for most commercial wiring. For bi-directional transmission, two fiber cables and two ST connectors are used.

2.3.3 *Subscriber Connector (SC)*

SC. (Standard Connector, Subscriber Connector) A fiber-optic cable connector that uses a push-pull latching mechanism similar to common audio and video cables. For bi-directional transmission, two fiber cables and two SC connectors (Dual SC) are used.

2.3.4 *Lucent Connector (LC)*

LC (or) lucent connector is a small form factor Fiber optic connector.

It uses a 1.25 mm ceramic Ferrule with good performance and is favored for single mode.

2.4 LAN DEVICES

LAN device is a device directly connected to a local area network. Devices on the same LAN can usually access the same resources, share files and access the Internet through the same access point, like a router.

2.4.1 *Repeaters*

In digital communication systems, a repeater is a device that receives a digital signal on an electromagnetic (or) optical transmission medium and regenerates the signal along the next

leg of the medium. In electromagnetic media, repeaters overcome the attenuation caused by free-space electromagnetic-field divergence (or) cable loss. A series of repeaters make possible the extension of a signal over a distance. Repeaters remove the unwanted noise in an incoming signal. Unlike an analog signal, the original digital signal, even if weak (or) distorted, can be clearly perceived and restored. With analog transmission, signals are re-strengthened with amplifiers which unfortunately also amplify noise as well as information. Because digital signals depend on the presence (or) absence of voltage, they tend to dissipate more quickly than analog signals and need more frequent repeating.

2.4.2 *Hubs*

Hub is a place of convergence where data arrives from one (or) more directions and is forwarded out in one (or) more other directions. A hub usually includes a switch of some kind. (And a product that is called a ***"switch"*** could usually be considered a hub as well.) The distinction seems to be that the hub is the place where data comes together and the switch is what determines how and where data is forwarded from the place where data comes together. Regarded in its switching aspects, a hub can also include a router. As a network product, a hub may include a group of modem cards for dial-in users, a gateway card for connections to a local area network (for example, an Ethernet or a token ring), and a connection to a line.

2.4.3 *Switches*

A switch is a device that channels incoming data from any of multiple input ports to the specific output port that will take the data toward its intended destination. In the traditional circuit-switched telephone network, one (or) more switches are used to set up a dedicated though temporary connection

(or) circuit for an exchange between two (or) more parties. On an Ethernet local area network (LAN), a switch determines from the physical device (Media Access Control or MAC) address in each incoming message frame which output port to forward it to and out of. In a wide area packet-switched network such as the Internet, a switch determines from the IP address in each packet which output port to use for the next part of its trip to the intended destination.

In the Open Systems Interconnection (OSI) communications model, a switch performs the Layer 2 (or) Data-link layer function. That is, it simply looks at each packet (or) data unit and determines from a physical address (the "MAC address") which device a data unit is intended for and switches it out toward that device. However, in wide area networks such as the Internet, the destination address requires a look-up in a routing table by a device known as a ***router.*** Some newer switches also perform routing functions (Layer 3 or the Network layer functions in OSI) and are sometimes called ***IP switches.***

2.4.4 *Network Interface Cards (NICs)*

A network interface card (NIC) is a circuit board (or) card that is installed in a computer so that it can be connected to a network. A network interface card provides the computer with a dedicated, full-time connection to a network. Personal computers and workstations on a local area network (LAN) typically contain a network interface card specifically designed for the LAN transmission technology.

2.4.5 *Routers (CISCO, DAX)*

Routers are networking devices operating at layer 3 (or) a network layer of the OSI model. They are responsible for receiving, analysing, and forwarding data packets among the connected computer networks. When a data packet arrives,

the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

Features of Routers :

1. A router is a layer 3 (or) network layer device.
2. It connects different networks together and sends data packets from one network to another.
3. A router can be used both in LANs (Local Area Networks) and WANs (Wide Area Networks).
4. It transfers data in the form of IP packets. In order to transmit data, it uses IP address mentioned in the destination field of the IP packet.
5. Routers have a routing table in it that is refreshed periodically according to the changes in the network. In order to transmit data packets, it consults the table and uses a routing protocol.

2.4.6 *Modem (56 kbps Internal or External ADSL Modems)*

A modem is a network device that both modulates and demodulates analog carrier signals (called ***sine waves***) for encoding and decoding digital information for processing. Modems accomplish both of these tasks simultaneously and for this reason, the term modem is a combination of "modulate" and "demodulate." The most common use for modems is for both sending and receiving of the digital information between personal computers. This information used to be transmitted over telephone lines using V.92, the last dial-up standard, to an analog modem that would convert the signal back to a digital format for a computer to read.

2.4.7 Gateways

A gateway is a network node that forms a passage between two networks operating with different transmission protocols. The most common type of gateways, the network gateway operates at layer 3, i.e., network layer of the OSI (open systems interconnection) model. However, depending upon the functionality, a gateway can operate at any of the seven layers of OSI model. It acts as the entry exit point for a network since all traffic that flows across the networks should pass through the gateway. Only the internal traffic between the nodes of a LAN does not pass through the gateway. On basis of direction of data flow, gateways are broadly divided into two categories ***Unidirectional Gateways*** and ***Bi directional gateways.***

Features of Gateways :

1. Gateway is located at the boundary of a network and manages all data that inflows (or) outflows from that network.
2. It forms a passage between two different networks operating with different transmission protocols.
3. A gateway operates as a protocol converter, providing compatibility between the different protocols used in the two different networks.
4. The feature that differentiates a gateway from other network devices is that it can operate at any layer of the OSI model.
5. It also stores information about the routing paths of the communicating networks.

2.5 WIRELESS NETWORK ADAPTER

A wireless adapter is a hardware device that is attached to a computer (or) laptop and allows it to connect to a wireless

network. Typically, they come in the form of a USB dongle device that you input into your computer. There are two main types of wireless adapters, based on the network type they help you connect to :

1. **WiFi Adapters :** They help you connect to WiFi networks nearby.
2. **Cellular/Mobile Broadband Adapters :** They connect to 3G (or) 4G/LTE cellular networks.

2.6 FUNCTIONS OF LAN TOOLS

2.6.1 *Anti-Magnetic Mat*

Anti magnetic mat reduces the risk of electrostatic discharge while working with electrostatic sensitive equipment. This is one of the tool which is used while LAN connectivity is done (or) laptop repair is in progress.

2.6.2. *Anti-Magnetic Gloves*

Anti-Magnetic Gloves are wore to the hands in order to be safeguarded while LAN connectivity (or) when Motherboard repairs are in progress such that no component is attracted to the magnetic force.

2.6.3 *Crimping Tool*

Crimp tools are a varied collection of devices used to join materials (or) components by pressing them together and creating a seal (or) crimp. One of the most common uses of crimping tools is the attachment of connectors to the end of electrical cables.

2.6.4. *Cable Tester*

A cable tester is an electronic device used to verify the electrical connections in a signal cable (or) other wired assembly. Basic cable testers are continuity testers that verify the existence of

a conductive path between ends of the cable, and verify the correct wiring of connectors on the cable.

2.6.5 Cutter

Cutter is used to cut LAN cables when they fail (or) even to attach to the other cable.

2.6.6 Loop Backplug

A loopback plug is a device used to test ports (such as serial, parallel USB and network ports) to identify network and network interface card (NIC) issues. A loopback plug device is classified as male (or) female. A loopback plug is also known as a ***loopback adapter*** (or) ***loopback cable.***

2.6.7 Tonerprobe

A toner probe is used to trace network cables between two different locations. For example, if you have 50 cables going from an office to a wiring closet, you sometimes need to identify both ends of the same cable. You can connect the component that creates the tone to one end of the wire in the office.

2.6.8 Punch down Tool

It is used for inserting wire into insulation-displacement connectors on punch down blocks, patch panels, keystone modules and surface mount boxes.

2.6.9 Protocol Analyser

A Protocol Analyzer is a measurement tool (or) device used to capture and monitor the data over a communication channel. It captures the data on the communication channel and converts the data bits into a meaningful protocol sequence.

2.6.10. Multimeter

A digital multimeter is a test tool used to measure two (or) more electrical values principally voltage (volts), current (amps)

and resistance (ohms). It is a standard diagnostic tool for technicians in the electrical/electronic industries.

2.7 TOPOLOGIES WITH THEIR MERITS AND DE-MERITS

Network topology is the arrangement of the various elements (links, nodes, etc.) of a computer network. Essentially, it is the topological structure of a network and may be depicted physically (or) logically. Physical topology is the placement of the various components of a network, including device location and cable installation, while logical topology illustrates how data flows within a network, regardless of its physical design. Distances between nodes, physical interconnections, transmission rates (or) signal types may differ between two networks, yet their topologies may be identical.

2.7.1 *BUS Topology*

Bus topology is a network type in where every computer and network device is connected to single cable.

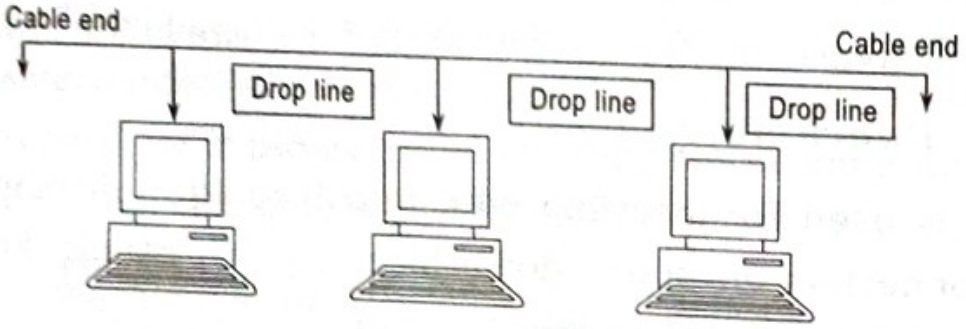


FIG 2.4 :

Features of Bus Topology :

1. It transmits data only in one direction.
2. Every device is connected to a single cable.

Advantages of Bus Topology :

1. It is cost effective.
2. Cable required is least compared to other network topology.

3. Used in small networks.
4. It is easy to understand.
5. Easy to expand joining two cables together.

Disadvantages of Bus Topology :

1. Cables fails then whole network fails.
2. If network traffic is heavy (or) nodes are more the performance of the network decreases.
3. Cable has a limited length.
4. It is slower than the ring topology.

2.7.2 *RING Topology*

It is called ***ring topology*** because it forms a ring as each computer is connected to another computer, with the last one connected to the first. Exactly two neighbours for each device.

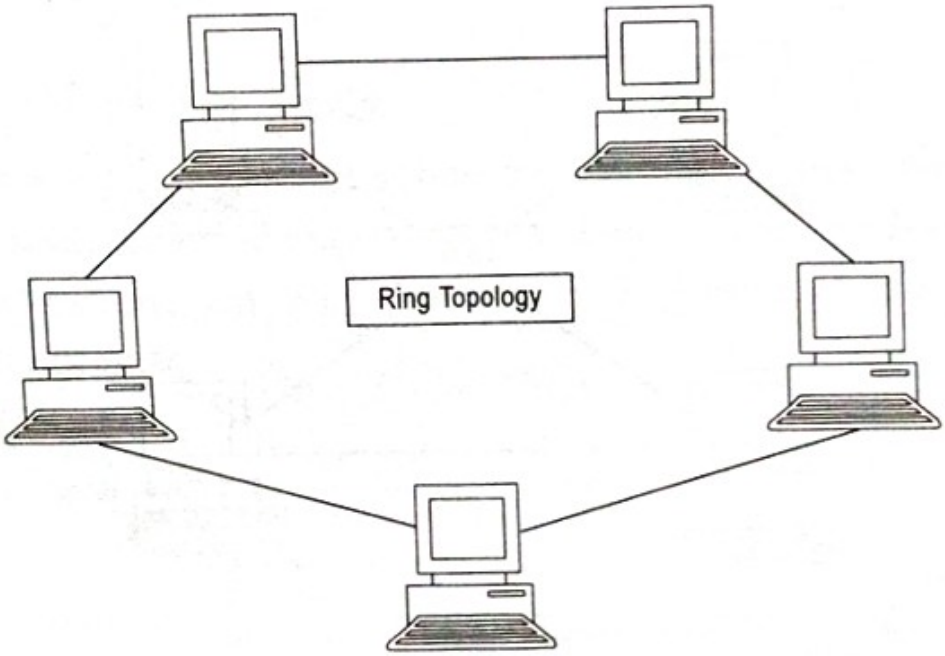


FIG 2.5 :

Features of Ring Topology :

1. A number of repeaters are used and the transmission is unidirectional.
2. Date is transferred in a sequential manner that is bit by bit.

Advantages of Ring Topology :

1. Transmitting network is not affected by high traffic (or) by adding more nodes, as only the nodes having tokens can transmit data.
2. Cheap to install and expand.

Disadvantages of Ring Topology :

1. Troubleshooting is difficult in ring topology.
2. Adding (or) deleting the computers disturbs the network activity.
3. Failure of one computer disturbs the whole network.

2.7.3 *Star Topology*

In this type of topology all the computers are connected to a single hub through a cable. This hub is the central node and all others nodes are connected to the central node.

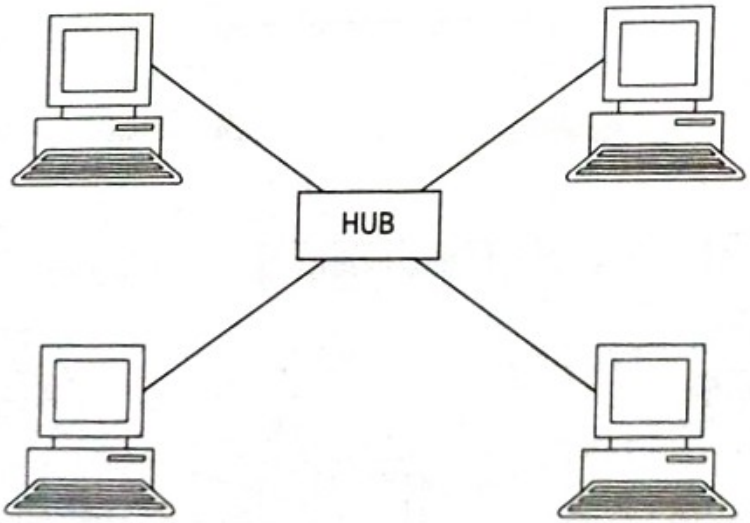


FIG 2.6 :

Features of Star Topology :

1. Every node has its own dedicated connection to the hub.
2. Acts as a repeater for data flow.
3. Can be used with twisted pair, Optical Fibre (or) coaxial cable.

Advantages of Star Topology :

1. Fast performance with few nodes and low network traffic.
2. Hub can be upgraded easily.
3. Easy to troubleshoot.
4. Easy to setup and modify.
5. Only that node is affected which has failed rest of the nodes can work smoothly.

Disadvantages of Star Topology :

1. Cost of installation is high.
2. Expensive to use.
3. If the hub is affected then the whole network is stopped because all the nodes depend on the hub.
4. Performance is based on the hub that is it depends on its capacity.

2.7.4 *Mesh Topology*

It is a point-to-point connection to other nodes (or) devices. Traffic is carried only between two devices (or) nodes to which it is connected. Mesh has n (n-2)/2 physical channels to link h_n devices.

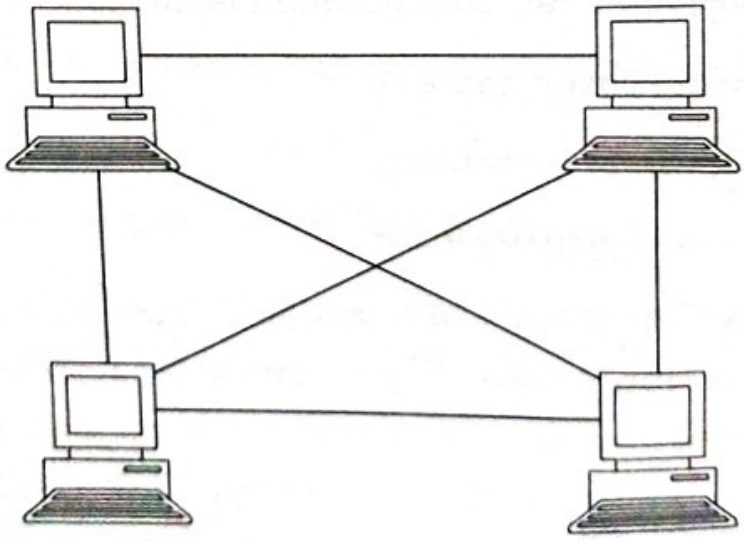


FIG 2.7 :

Types of Mesh Topology :

1. **Partial Mesh Topology :** In this topology some of the systems are connected in the same fashion as mesh topology but some devices are only connected to two (or) three devices.
2. **Full Mesh Topology :** Each and every nodes (or) devices are connected to each other.

Features of Mesh Topology :

1. Fully connected.
2. Robust.
3. Not flexible.

Advantages of Mesh Topology :

1. Each connection can carry its own data load.
2. It is robust.
3. Fault is diagnosed easily.
4. Provides security and privacy.

Disadvantages of Mesh Topology :

1. Installation and configuration is difficult.
2. Cabling cost is more.
3. Bulk wiring is required.

2.7.5 Hybrid Topology

It is two different types of topologies which is a mixture of two (or) more topologies. For example if in an office in one department ring topology is used and in another star topology is used, connecting these topologies will result in Hybrid Topology (ring topology and star topology).

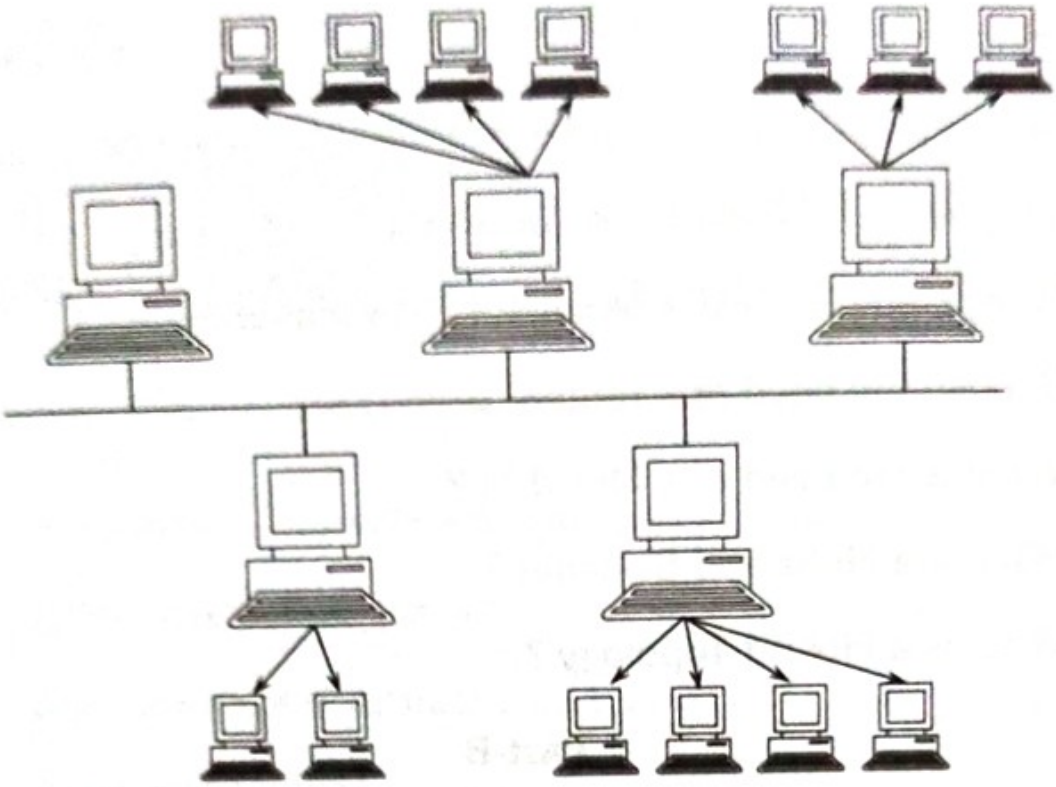


FIG 2.8 :

Features of Hybrid Topology :

1. It is a combination of two (or) topologies.
2. Inherits the advantages and disadvantages of the topologies included.

Advantages of Hybrid Topology :

1. Reliable as Error detecting and trouble shooting is easy.
2. Effective.
3. Scalable as size can be increased easily.
4. Flexible.

Disadvantages of Hybrid Topology :

1. Complex in design.
2. Costly.

Part-A

1. Why are LAN cables and connectors used ?
2. What is the need of a wireless network adapter ?
3. Explain the need of a router.
4. What is the need of a MODEM ?
5. What are Hubs and Switches ?
6. What is a Hybrid Topology ?

Part-B

1. Explain about different LAN cables with its diagrammatic representations.
2. What are the different LAN connectors used for LAN cable connection ?
4. What are the different LAN tools used while making a LAN connection ?

Part-C

1. Explain about different LAN devices such as Hubs, Repeaters, Switches,, Routers, Modems, Gateways and NICs.
2. Explain different network topologies along with their advantages and disadvantages.

Chapter-3

NETWORK ADDRESSING AND SUB-NETTING

CHAPTER OUTLINE

3.1 Introduction to Network Addressing 2

3.2 TCP/IP Addressing Scheme 2

3.3 Components of IP Address 3

3.4 IP Address Classes 3

3.5 Subnet and the Necessity of Sub-netting 5

3.6 Sub-Netting with a Simple Example 6

3.7 Advantages and Disadvantages of Subnetting 11

3.8 Internet Protocol Addressings 12

3.9 Need for IPv6 13

3.10 Classful Addressing and Classless Addressing in IPv4 13

3.11 Internet Protocol Version-6 (IPv6) Addressing 17

3.1 INTRODUCTION TO NETWORK ADDRESSING

A network address is an identifier for a node (or) network interface of a telecommunications network. The process (or) system of assigning network address is called as ***network addressing***. Network addresses are often designed to be unique across the network, although some networks allow for relative (or) local addresses that may not be unique. More than one type of network address may be used in any one network. In some cases terminal nodes may have more than one network address, for example, each link interface may be uniquely identified. In addition, non terminal nodes are often assigned network addresses.

1. **IP Address :** A logical numeric address that is assigned to every single computer, printer, switch, router (or) any other device that is part of a TCP/IP-based network.
2. **Subnet :** A separate and identifiable portion of an organization's network, typically arranged on one floor, building (or) geographical location.
3. **Subnet Mask :** A 32-bit number used to differentiate the network component of an IP address by dividing the IP address into a network address and host address.
4. **Network Interface Card (NIC) :** A computer hardware component that allows a computer to connect to a network.

3.2 TCP/IP ADDRESSING SCHEME

An IP address is an identifier for a computer (or) device on a TCP/IP network. Networks using the TCP/IP protocol route messages based on the IP address of the destination. TCP/IP Addressing Scheme is the means whereby an entity on a network can be addressed. It is made up solely of numbers, and these numbers are conventionally written in the particular

form of XXX.XXX.XXX.XXX, which is referred to as ***dotted decimal format.*** Any one of the numbers between the dots can be between 0 and 255, so example IP addresses include:

- 205.112.45.60
- 34.243.44.155

These numbers can also be written in binary form by taking each of the decimal values separated by dots and converting to binary. So a number like 205.112.45.60 could be written as :

11001101.01110000.00101101.00111100

3.3 COMPONENTS OF IP ADDRESS

The total IP address 32 bits are considered a single ***"entity"***; they have an internal structure containing two components :

1. **Network Identifier (Network ID) :** A certain number of bits, starting from the left-most bit, it is used to identify the network where the host (or) other network interface is located. This is also sometimes called the ***network prefix*** (or) even just the ***prefix.***
2. **Host Identifier (Host ID) :** The remainder of the bits is used to identify the host on the network.

3.4 IP ADDRESS CLASSES

The Class of the address determines which part belongs to the network address and which part belongs to the node address. All nodes on a given network share the same network prefix but must have a unique host number.

1. **Class A Network :** In a Class A Network binary address start with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network

and the remaining 24 bits indicate the host within the network. An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

2. **Class B Network :** In a Class B Network, binary addresses start with 10, therefore the decimal number can be anywhere from 128 to 191. The number 127 is reserved for loopback and is used for internal testing on the local machine. The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

3. **Class C Network :** Binary addresses start with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

4. **Class D Network :** In a Class D Network, binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multi casting.

5. **Class E Network :** In a Class E Network, binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented (or) utilized in a standard way.

First Octet Valve	Class	Example IP Address
0 - 126	Class A	34.126.35.125
128-191	Class B	134.23.45.123
192-233	Class C	212.11.123.3
224-239	Class D	225.2.3.40
240 - 255	Class E	245.192.1.123

Class	Address Components	Network/Host
Class A	Network Host.Host.Host	34.126.35.125
Class B	Network.Network.Host.Host	134.23.45.123
Class C	Network.NetworkNetwork.Host	212.11.123.3
Class D	Not defined	Not defined
Class E	Not defined	Not defined

3.5 SUBNET AND THE NECESSITY OF SUB-NETTING

To subnet a network is to create logical divisions of the network. Subnetting, therefore, involves dividing the network into smaller portions called ***subnets***. Subnetting applies to IP addresses because this is done by borrowing bits from the host portion of the IP address. In a sense, the IP address then has three components-the network part, the subnet part and finally, the host part.

We create a subnet by logically grabbing the last bit from the network component of the address and using it to determine the number of subnets required. We are going to borrow the left-most bit of the host address and declare it as identifying the subnet. If the bit is a 0, then that will be one subnet ; if the bit is a 1, that would be the second subnet. Of course, with only one borrowed bit we can only have two possible subnets. By the same token, that also reduces the number of hosts we can have on the network to 127 (but actually 125 useable

addresses given all zeros and all ones are not recommended addresses), down from 255. The reason a subnet mask has this name is that it literally masks out the host bits being borrowed from the host address portion of the IP address. Of course, more bits borrowed means fewer individually addressable hosts that can be on the network.

3.6 SUB-NETTING WITH A SIMPLE EXAMPLE

VLSM is a process of dividing an IP space into the subnets of different sizes without wasting IP addresses. When we perform sub-netting, all subnets have the same number of hosts, this is known as ***FLSM (Fixed Length Subnet Mask).*** In FLSM all subnets use same subnet mask, this lead to inefficiencies. In real life scenario, some subnets may require large number of host addresses while other may require only few addresses.

For example, assume that you are a network administrator at your college. Company have three departments connected with WAN links.

1. Development department have 74 computers.
2. Production department have 52 computers.
3. Administrative department have 28 computers.
4. All departments are connected with each other via wan link.
5. Each WAN link requires two IP addresses.

With FLSM, to accumulate this requirement you have two choices, either purchase a class B IP address space (or) purchase at least two class C IP address space.

First choice with a example class B address space.

172.168.1.0/23

Subnetting of this address space would give us 128 subnets and 510 hosts in each subnet. Our network requires only 6 subnets and 160 addresses. Every IP address adds more dollars in company bill. You would have to pay for 65356 addresses while you need only 160 addresses. Would you consider this address space for company ?

Second choice with two example class C address spaces.

192.168.1.0/25

192.168.2.0/26

Subnetting of first address 192.168.1.0/25 would give us 2 subnets and 126 hosts in each subnet.

Subnetting of second address 192.168.2.0/26 would give us 4 subnets and 62 hosts in each subnet.

Collectively we are getting 6 subnets and 500 hosts from these two address spaces. We are still wasting more than 300 IP address and we would have to purchase two address spaces.

Variable Length Subnet Mask : Variable Length Subnet Mask (VLSM) extends classic sub-netting. VLSM is a process of breaking down subnets into the smaller subnets, according to the need of individual networks. In above example company have requirement of 6 subnets and 160 host addresses. With VSLM you can fulfill this requirement with single class C address space. In VLSM Subnetting, we do subnetting of subnets according the network requirement.

Steps for VLSM Subnetting

1. Find the largest segment. Segment which need largest number of hosts address.
2. Do subnetting to fulfill the requirement of largest segment.
3. Assign the appropriate subnet mask for the largest segment.

4. For second largest segments, take one of these newly created subnets and apply a different, more appropriate, subnet mask to it.
5. Assign the appropriate subnet mask for the second largest segment.
6. Repeat this process until the last network.

VLSM Example : Now you know the steps of VLSM Subnetting. Let's understand it with above example. Our company requires 6 subnets and 160 hosts.

Step 1 : Order all segments according the hosts requirement (Largest to smallest).

Subnet	Segment	Hosts
1	Development	74
2	Production	52
3	Administrative	28
4	Wan link 1	2
5	Wan link 2	2
6	Wan link 3	2

Step 2 : Do sub-netting for largest segment. Our largest segment needs 74 host addresses. /25 provide us two subnets with 126 hosts in each subnet.

192.168.1.0/25

Subnet	Subnet 1	Subnet 2
Network ID	192.168.1.0	192.168.1.128
First host address	192.168.1.1	192.168.1.129
Last host address	192.168.1.126	192.168.1.254
Broad Cast ID	192.168.1.127	192.168.1.255

Step 3 : Assign subnet mask to the largest segment. As you can see in above table, subnet 1 fulfill our largest segment requirement. Assign it to our segment

Segment	Development
Requirement	74
CIDR	/25
Subnet mask	255.255.255.128
Network ID	192.168.1.0
First hosts	192.168.1.1
Last hosts	192.168.1.126
Broadcast ID	192.168.1.127

Step 4 : Do subnetting for second largest segment from next available subnet. Next segment requires 52 host addresses. Subnetting of /25 has given us two subnets with 126 hosts in each, from that we have assigned first subnet to development segment. Second segment is available, we would do subnetting of this.

/26 provide us 4 subnets with 62 hosts in each subnet.

192.168.1.0/26

Subnet	Subnet 1	Subnet 2	Subnet 3	Subnet 4
Network ID	0	64	128	192
First Address	1	65	129	193
Last Address	62	126	190	254
Broadcast ID	63	127	191	255

We cannot use subnet 1 and subnet 2 (address from 0 to 127) as they are already assigned to development department. We can assign subnet 3 to our production department.

Segment	Production
Requirement	52
CIDR	/26
Subnet mask	255.255.255.192
Network ID	192.168.1.128

First hosts	192.168.1.129
Last hosts	192.168.1.190
Broadcast ID	192.168.1.191

Step 5 : Our next segment requires 28 hosts. From above subnetting we have subnet 3 and subnet 4 available. Do subnetting for the requirement of 28 hosts.

192.168.1.0/27

Subnet	Sub 1	Sub 2	Sub 3	Sub 4	Sub 5	Sub 6	Sub 7	Sub 8
Net ID	0	32	64	96	128	160	192	224
First Host	1	33	65	95	129	161	193	225
Last Host	30	62	94	126	158	190	222	254
Broadcast ID	31	63	95	127	159	191	223	255

Subnets 1 to 6 [address from 0 to 191] are already occupied by previous segments. We can assign subnet 7 to this segment.

Segment	Administrative
Requirement	28
CIDR	/27
Subnet mask	255.255.255.224
Network ID	192.168.1.192
First Hosts	192.168.1.193
Last Hosts	192.168.1.222
Broad cast ID	192.168.1.223

Step 6 :- Our last three segments require 2 hosts per subnet. Do subnetting for these.

192.168.1.0/30

Valid subnets are :

0,4, 812, 16, 20, 24, 28, 32, 36, 40, 44, 48, 52, 56, 60, 64, 68, 72, 76, 80, 84, 88, 92, 96, 100, 104, 108, 112, 116, 120, 124, 128, 132, 136, 140, 144, 148, 152, 156, 160, 164, 168, 172, 176, 180, 184, 188, 192, 196, 200, 204, 208, 212, 216, 220, 224, 228, 232, 236, 240, 244, 248, 252, 256

From these subnets, subnet 1 to subnet 56 (Address from 0 - 220) are already assigned to previous segments. We can use 224,228, and 232 for wan links.

Subnet	Subnet 57	Subnet 58	Subnet 59
Network ID	224	228	232
First host	225	229	233
Last host	226	230	234
Broadcast ID	227	231	235

3.7 ADVANTAGES AND DISADVANTAGES OF SUBNETTING

Advantages of using Subnetting :

1. It is useful to control and to reduce the network traffic by limiting number of broadcasts.
2. It is allowed any organization to subnet its network without needed to have a new network IP through an internet service provider (ISP).
3. Subnetting was so helpful to solve the problem of lacking IP addresses on the Internet.
4. Allowing to use two (or) more LAN technologies together in the same network.
5. Subnets also helpful to minimize the size of the routing tables on the internet since additional network numbers will not being added to the table.

6 When you want to isolate segments for security reasons such as accounting and sales segment.

7. When you want to isolate bad segments such as domination hosts which use most of the LAN Bandwidth.

Disadvantages of using Subnetting :

1. Subnetting decreases the total number of IP addresses in the network but may need buying additional hardware such as a router. So, it may cost lots of money.
2. It cannot correct the lack of efficiency because companies still assign address block regarding to classes.

3.8 INTERNET PROTOCOL ADDRESSINGS

3.8.1 *IPv4*

IPv4 stands for Internet Protocol version 4. It is the underlying technology that makes it possible for us to connect our devices to the web. Whenever a device accesses the Internet, it is assigned a unique, numerical IP address such as 99.48.227.227. To send data from one computer to another through the web, a data packet must be transferred across the network containing the IP addresses of both devices.

3.8.2 *IPv6*

IPv6 is the next generation Internet Protocol (IP) address standard intended to supplement and eventually replace IPv4, the protocol many Internet services still use today. Every computer, mobile phone, home automation component, IoT sensor and any other device connected to the Internet needs a numerical IP address to communicate between other devices. The original IP address scheme, called **IPv4**, is running out of addresses due to its widespread usage from the proliferation of so many connected devices.

3.9 NEED FOR IPV6

IPv6 (Internet Protocol version 6) is the sixth revision to the Internet Protocol and the successor to IPv4. It functions similarly to IPv4 in that it provides the unique IP addresses necessary for Internet-enabled devices to communicate. However, it does have one significant difference : it utilizes a 128-bit IP address.

Need of IPv6 :

1. No more NAT (Network Address Translation).
2. Auto-configuration.
3. No more private address collisions.
4. Better multicast routing.
5. Simpler header format.
6. Simplified, more efficient routing.
7. True quality of service (QoS), also called ***"flow labeling"***.
8. Built-in authentication and privacy support.
9. Flexible options and extensions.
10. Easier administration (no more DHCP).

3.10 CLASSFUL ADDRESSING AND CLASSLESS ADDRESSING IN IPV4

The Class of the address determines which part belongs to the network address and which part belongs to the node address. All nodes on a given network share the same network prefix but must have a unique host number.

1. **Class A Network :** In a Class A Network binary address start with 0, therefore the decimal number can be anywhere from 1 to 126. The first 8 bits (the first octet) identify the network and the remaining 24 bits indicate the host within the network.

An example of a Class A IP address is 102.168.212.226, where "102" identifies the network and "168.212.226" identifies the host on that network.

2. **Class B Network :** In a Class B Network, binary addresses start with 10, therefore the decimal number can be anywhere from 128 to 191. The number 127 is reserved for loopback and is used for internal testing on the local machine. The first 16 bits (the first two octets) identify the network and the remaining 16 bits indicate the host within the network. An example of a Class B IP address is 168.212.226.204 where "168.212" identifies the network and "226.204" identifies the host on that network.

3. **Class C Network :** Binary addresses start with 110, therefore the decimal number can be anywhere from 192 to 223. The first 24 bits (the first three octets) identify the network and the remaining 8 bits indicate the host within the network. An example of a Class C IP address is 200.168.212.226 where "200.168.212" identifies the network and "226" identifies the host on that network.

4. **Class D Network :** In a Class D Network, binary addresses start with 1110, therefore the decimal number can be anywhere from 224 to 239. Class D networks are used to support multicasting.

5. **Class E Network :** In a Class E Network, binary addresses start with 1111, therefore the decimal number can be anywhere from 240 to 255. Class E networks are used for experimentation. They have never been documented (or) utilized in a standard way.

First Octet Valve	Class	Example IP Address
0 - 126	Class A	34.126.35.125
128-191	Class B	134.23.45.123
192-233	Class C	212.11.123.3
224-239	Class D	225.2.3.40
240 - 255	Class E	245.192.1.123

Class	Address Components	Network/Host
Class A	Network Host.Host.Host	34.126.35.125
Class B	Network.Network.Host.Host	134.23.45.123
Class C	Network.NetworkNetwork.Host	212.11.123.3
Class D	Not defined	Not defined
Class E	Not defined	Not defined

CIDR (Classless Inter-Domain Routing, sometimes called ***supernetting***) is a way to allow more flexible allocation of Internet Protocol (IP) addresses than was possible with the original system of IP address classes. As a result, the number of available Internet addresses was greatly increased, which along with widespread use of network address translation (NAT), has significantly extended the useful life of IPv4. Originally, IP addresses were assigned in four major address classes, A through D. Each of these classes allocates one portion of the 32-bit IP address format to identify a network gateway — the first 8 bits for class A, the first 16 for class B, and the first 24 for class C. The remainder identify hosts on that network — more than 16 million in class A, 65,535 in class B and 254 in class C. (Class D addresses identify multicast domains.)

To illustrate the problems with the class system, consider that one of the most commonly used classes was Class B. An organization that needed more than 254 host machines would

often get a Class B license, even though it would have far fewer than 65,534 hosts. This resulted in most of the block of addresses allocated going unused.

CIDR reduced the problem of wasted address space by providing a new and more flexible way to specify network addresses in routers. CIDR lets one routing table entry represent an aggregation of networks that exist in the forward path that don't need to be specified on that particular gateway. This is much like how the public telephone system uses area codes to channel calls toward a certain part of the network. This aggregation of networks in a single address is sometimes referred to as a supernet.Using CIDR, each IP address has a network prefix that identifies either one (or) several network gateways. The length of the network prefix in IPv4 CIDR is also specified as part of the IP address and varies depending on the number of bits needed, rather than any arbitrary class assignment structure. A destination IP address (or) route that describes many possible destinations has a shorter prefix and is said to be less specific. A longer prefix describes a destination gateway more specifically. Routers are required to use the most specific, (or) longest, network prefix in the routing table when forwarding packets. A CIDR network address looks like this under IPv4 :

192.30.250.00/18

The "192.30.250.0" is the network address itself and the "18" says that the first 18 bits are the network part of the address, leaving the last 14 bits for specific host addresses.

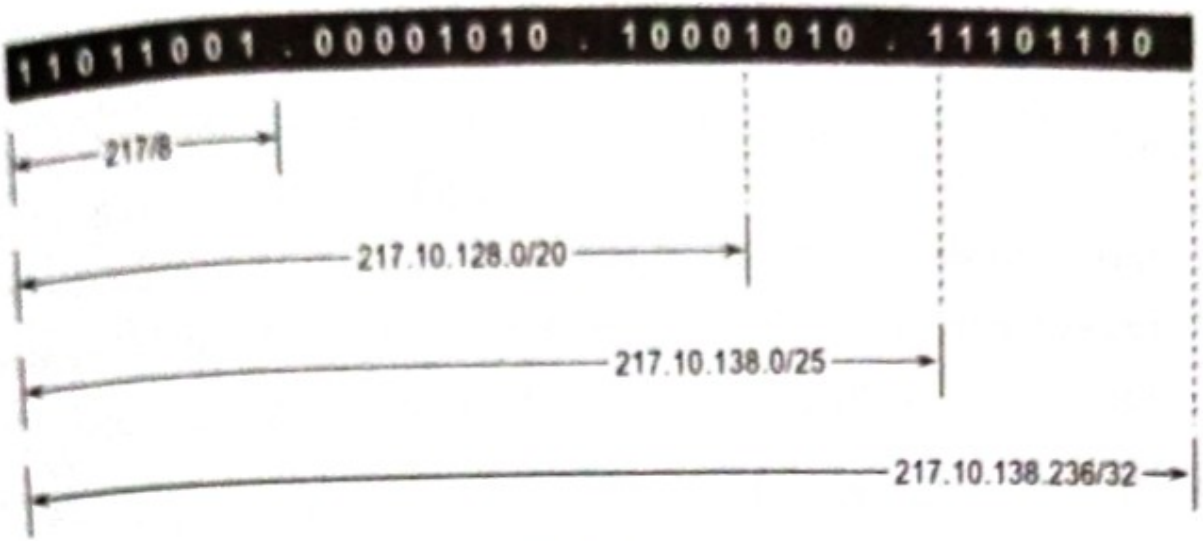


FIG 3.1 :

3.11 INTERNET PROTOCOL VERSION-6 (IPV6) ADDRESSING

Internet Protocol version 6 (IPv6) is the latest revision of the Internet Protocol (IP) and the first version of the protocol to be widely deployed. IPv6 was developed by the Internet Engineering Task Force (IETF) to deal with the long-anticipated problem of IPv4 address exhaustion. IPv6 is redesigned entirely. It offers the following features :

- **Larger Address Space**

  In contrast to IPv4, IPv6 uses 4 times more bits to address a device on the Internet. This much of extra bits can provide approximately 3.4 × 1038 different combinations of addresses. This address can accumulate the aggressive requirement of address allotment for almost everything in this world. According to an estimate, 1564 addresses can be allocated to every square meter of this earth.

- **Simplified Header**

  IPv6's header has been simplified by moving all unnecessary information and options (which are present in IPv4 header) to the end of the IPv6 header. IPv6 header is only twice as bigger than IPv4 provided the fact that IPv6 address is four times longer.

- **End-to-end Connectivity**

  Every system now has unique IP address and can traverse through the Internet without using NAT (or) other translating components. After IPv6 is fully implemented, every host can directly reach other hosts on the Internet, with some limitations involved like Firewall, organization policies, etc.,

- **Auto-configuration**

  IPv6 supports both stateful and stateless auto configuration mode of its host devices. This way, absence of a DHCP server does not put a halt on inter segment communication.

- **Faster Forwarding/Routing**

  Simplified header puts all unnecessary information at the end of the header. The information contained in the first part of the header is adequate for a Router to take routing decisions, thus making routing decision as quickly as looking at the mandatory header.

- **IPSec**

  Initially it was decided that IPv6 must have IPSec security, making it more secure than IPv4. This feature has now been made optional.

- **No Broadcast**

  Though Ethernet/Token Ring are considered as broadcast network because they support Broadcasting, IPv6 does not have any broadcast support any more. It uses multicast to communicate with multiple hosts.

- **Any cast Support**

  This is another characteristic of IPv6. IPv6 has introduced Anycast mode of packet routing. In this mode, multiple

interfaces over the Internet are assigned same Any cast IP address. Routers, while routing, send the packet to the nearest destination.

- **Mobility :**

  IPv6 was designed keeping mobility in mind. This feature enables hosts (such as mobile phone) to roam around in different geographical area and remain connected with the same IP address. The mobility feature of IPv6 takes advantage of auto IP configuration and Extension headers.

- **Enhanced Priority Support :**

  IPv4 used 6 bits DSCP (Differential Service Code Point) and 2 bits ECN (Explicit Congestion Notification) to provide Quality of Service but it could only be used if the end-to-end devices support it, that is, the source and destination device and underlying network must support it.

  In IPv6, Traffic class and Flow label are used to tell the underlying routers how to efficiently process the packet and route it.

- **Smooth Transition :**

  Large IP address scheme in IPv6 enables to allocate devices with globally unique IP addresses. This mechanism saves IP addresses and NAT is not required. So devices can send/receive data among each other, for example, VoIP and/or any streaming media can be used much efficiently.

  Other fact is, the header is less loaded, so routers can take forwarding decisions and forward them as quickly as they arrive.

- **Extensibility**

  One of the major advantages of IPv6 header is that it is extensible to add more information in the option part. IPv4 provides only 40-bytes for options, whereas options in IPv6 can be as much as the size of IPv6 packet itself.

An IPv6 address is 4 times larger than IPv4, but surprisingly, the header of an IPv6 address is only 2 times larger than that of IPv4. IPv6 headers have one Fixed Header and zero (or) more Optional (Extension) Headers. All the necessary information that is essential for a router is kept in the Fixed Header. The Extension Header contains optional information that helps routers to understand how to handle a packet/flow.

Fixed Header :

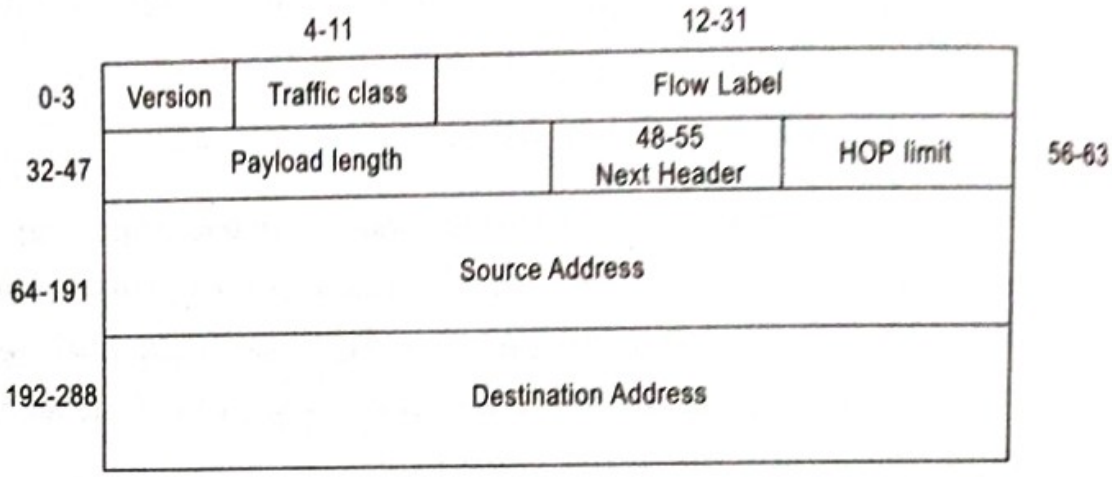


FIG 3.2 :

IPv6 fixed header is 40 bytes long and contains the following information.

1. **Version (4-bits) :** It represents the version of Internet Protocol, i.e., 0110.
2. **Traffic Class (8-bits) :** These 8 bits are divided into two parts. The most significant 6 bits are used for Type of Service to let the Router Known what services should be provided to this packet. The least significant 2 bits are used for Explicit Congestion Notification (ECN).
3. **Flow Label (20-bits) :** This label is used to maintain the sequential flow of the packets belonging to a communication. The source labels the sequence to help the router identify that a particular packet belongs to a specific flow of information. This field helps avoid re-ordering of data packets. It is designed for streaming/real-time media.

4. **Payload Length (16-bits) :** This field is used to tell the routers how much information a particular packet contains in its payload. Payload is composed of Extension Headers and Upper Layer data. With 16 bits, up to 65535 bytes can be indicated; but if the Extension Headers contain Hop-by-Hop Extension Header, then the payload may exceed 65535 bytes and this field is set to 0.

5. **Next Header (8-bits) :** This field is used to indicate either the type of Extension Header, (or) if the Extension Header is not present then it indicates the Upper Layer PDU. The values for the type of Upper Layer PDU are same as IPv4's.

6. **Hop Limit (8-bits) :** This field is used to stop packet to loop in the network infinitely. This is same as TTL in IPv4. The value of Hop Limit field is decremented by 1 as it passes a link (router/hop). When the field reaches 0 the packet is discarded.

7. **Source Address (128-bits) :** This field indicates the address of originator of the packet.

8. **Destination Address (128-bits) :** This field provides the address of intended recipient of the packet.

Extension Headers :

In IPv6, the Fixed Header contains only that much information which is necessary, avoiding those information which is either not required (or) is rarely used. All such information is put between the Fixed Header and the Upper layer header in the form of Extension Headers. Each Extension Header is identified by a distinct value.

When Extension Headers are used, IPv6 Fixed Header's Next Header field points to the first Extension Header. If there is one more Extension Header, then the first Extension Header's 'Next-Header' field points to the second one, and so on. The last Extension Header's 'Next-Header' field points to the Upper

Layer Header. Thus, all the headers points to the next one in a linked list manner. If the Next Header field contains the value 59, it indicates that there are no headers after this header, not even Upper Layer Header.

The following Extension Headers are supported.

Extension Header	Next Header value	Description
Hop-by-Hop options header	0	Read by all devices in transit network.
Routing header	43	Contains methods to support making routing decision.
Fragment header	44	contains parameters of datagram fragmentation.
Destination options header	60	read by destination devices.
Authentication header	51	Information regarding authenticity.
Encapsulating security	50	encryption information.

REVIEW QUESTIONS

Part-A

1. What is the need of Addressing ?
2. What is TCP/IP addressing ?
3. What is the need of IPV6 ?
4. What is IPV4 addressing ?
5. What is sub netting ?

Part-B

1. Explain in detail about IP address components.
2. What are the different classes of IP addresses.
3. Explain IPv4 addressing scheme.
4. Explain IPv6 addressing scheme.
5. What is the difference between classful addressing and class less addressing ?

Part-C

1. Explain IPv4 and IPv6 addressing.

Chapter-4

NETWORKS PROTOCOLS AND MANAGEMENT

CHAPTER OUTLINE

4.1 Need of Protocols in Computer Networks 2

4.2 Protocols 2

4.3 Simple Network Management Protocol (SNMP) 6

4.4 Working of SNMP 8

4.5 DHCP, DNS 10

4.6 Overview of Network Management 10

4.7 Network Monitoring and Troubleshooting 11

4.8 Remote Monitoring (RMON) 17

4.1 NEED OF PROTOCOLS IN COMPUTER NETWORKS

In the era of Computer and Mobile technologies, computer network technology is growing at a very fast speed and frequency. Billions of electronic devices and gadgets are operating to make this happen. These devices are designed and manufactured by different manufacturers. They may have been developed using different hardware and software resources. Due to this, they are unable to establish a connection and communicate with each other for sharing data and other information. Hence, to resolve this problem, we need protocols. Protocols provide us with a medium and set of rules to establish communication between different devices for the exchange of data and other services.

4.2 PROTOCOLS

4.2.1 *Hyper Text Transfer Protocol (HTTP)*

HTTP (Hyper Text Transfer Protocol) is the set of rules for transferring files (text, graphic images, sound, video, and other multimedia files) on the World Wide Web. As soon as a Web user opens their Web browser, the user is indirectly making use of HTTP. HTTP is an application protocol that runs on top of the TCP/IP suite of protocols (the foundation protocols for the Internet). HTTP concepts include (as the Hypertext part of the name implies) the idea that files can contain references to other files whose selection will elicit additional transfer requests. Any Web server machine contains, in addition to the Web page files it can serve, an HTTP daemon, a program that is designed to wait for HTTP requests and handle them when they arrive. Your Web browser is an HTTP client, sending requests to server machines. When the browser user enters file requests by either "opening" a Web file (typing in a Uniform Resource Locator or URL) (or) clicking on a hypertext link,

the browser builds an HTTP request and sends it to the Internet Protocol address (IP address) indicated by the URL. The HTTP daemon in the destination server machine receives the request and sends back the requested file (or) files associated with the request.

4.2.2 File TransferProtocol (FTP)

FTP is a client-server protocol that relies on two communications channels between client and server : a command channel for controlling the conversation and a data channel for transmitting file content. Clients initiate conversations with servers by requesting to download a file. Using FTP, a client can upload, download, delete, rename, move and copy files on a server. A user typically needs to log on to the FTP server, although some servers make some (or) all of their content available without login, also known as ***anonymous FTP.*** FTP sessions work in passive (or) active modes. In active mode, after a client initiates a session via a command channel request, the server initiates a data connection back to the client and begins transferring data. In passive mode, the server instead uses the command channel to send the client the information it needs to open a data channel. Because passive mode has the client initiating all connections, it works well across firewalls and Network Address Translation (NAT) gateways.

4.2.3 Simple Mail Transfer Protocol (SMTP)

SMTP (Simple Mail Transfer Protocol) is a TCP/IP protocol used in sending and receiving e-mail. However, since it is limited in its ability to queue messages at the receiving end, it is usually used with one of two other protocols, POP3 (or) IMAP that let the user save messages in a server mailbox and download them periodically from the server. In other words, users typically use a program that uses SMTP for sending

e-mail and either POP3 (or) IMAP for receiving e-mail. On Unix-based systems, send-mail is the most widely-used SMTP server for e-mail. A commercial package, Sendmail, includes a POP3 server. Microsoft Exchange includes an SMTP server and can also be set up to include POP3 support. SMTP usually is implemented to operate over Internet port 25.

4.2.4 *Address Resolution Protocol (ARP)*

Address Resolution Protocol (ARP) is a procedure for mapping a dynamic IP address to a permanent physical machine address in a local area network (LAN). The physical machine address is also known as a ***media access control (MAC)*** address.

The job of ARP is essentially to translate 32-bit addresses to 48-bit addresses and vice versa. This is necessary because IP addresses in IP version 4 (IPv4) are 32 bits, but MAC addresses are 48 bits.

ARP works between Layers 2 and 3 of the Open Systems Interconnection model (OSI model). The MAC address exists on Layer 2 of the OSI model, the data link layer. The IP address exists on Layer 3, the network layer.

ARP can also be used for IP over other LAN technologies, such as token ring, fiber distributed data interface (FDDI) and IP over ATM.

How ARP works

When a new computer joins a LAN, it is assigned a unique IP address to use for identification and communication. When an incoming packet destined for a host machine on a particular LAN arrives at a gateway, the gateway asks the ARP program to find a MAC address that matches the IP address. A table called the ***ARP*** cache maintains a record of each IP address and its corresponding MAC address.

4.2.5 Reverse Address Resolution Protocol (RARP)

RARP is abbreviation of Reverse Address Resolution Protocol which is a protocol based on computer networking which is employed by a client computer to request its IP address from a gateway servers Address Resolution Protocol table (or) cache. The network administrator creates a table in gateway-router, which is used to map the MAC address to corresponding IP address.

This protocol is used to communicate data between two points in a server. The client doesn't necessarily need prior knowledge the server identities capable of serving its request. Medium Access Control (MAC) addresses requires individual configuration on the servers done by an administrator. RARP limits to the serving of IP addresses only.

4.2.6 Telnet

Telnet is a user command and an underlying TCP/IP protocol for accessing remote computers. Through Telnet, an administrator (or) another user can access someone else's computer remotely. On the Web, HTTP and FTP protocols allow you to request specific files from remote computers, but not to actually be logged on as a user of that computer. With Telnet, you log on as a regular user with whatever privileges you may have been granted to the specific application and data on that computer.

A Telnet command request looks like this :

telnet the.libraryat.whatis.edu

The result of this request would be an invitation to log on with a user id and a prompt for a password. If accepted, you would be logged on like any user who used this computer every day. Telnet is most likely to be used by program developers and anyone who has a need to use specific applications (or) data located at a particular host computer.

4.3 SIMPLE NETWORK MANAGEMENT PROTOCOL (SNMP)

Simple Network Management Protocol (SNMP) is an application–layer protocol defined by the Internet Architecture Board (IAB) in RFC1157 for exchanging management information between network devices. It is a part of Transmission Control Protocol D Internet Protocol (TCPD IP) protocol suite.

SNMP is one of the widely accepted protocols to manage and monitor network elements. Most of the professional–grade network elements come with bundled SNMP agent. These agents have to be enabled and configured to communicate with the network management system (NMS).

SNMP consists of :

1 SNMP Manager.

2 Managed devices.

3 SNMP agent.

4 Management Information Database (or) Management Information Base (MIB).

1. **SNMP Manager :** A manager (or) management system is a separate entity that is responsible to communicate with the SNMP agent implemented network devices. This is typically a computer that is used to run one (or) more network management systems.

SNMP Manager's key Functions :

- Queries agents.
- Gets responses from agents.
- Sets variables in agents.
- Acknowledges asynchronous events from agents.

2. **Managed Devices** : A managed device (or) the network element is a part of the network that requires some form of monitoring and management e.g. routers, switches, servers, workstations, printers, UPSs, etc.,

3. **SNMP Agent** : The agent is a program that is packaged within the network element. Enabling the agent allows it to collect the management information database from the device locally and makes it available to the SNMP manager, when it is queried for. These agents could be standard (**Eg** : Net-SNMP) (or) specific to a vendor (**Eg** : HP insight agent)

SNMP Agent's key Functions :

- Collects management information about its local environment
- Stores and retrieves management information as defined in the MIB.
- Signals an event to the manager.
- Acts as a proxy for some non-SNMP manageable network node.

4. **Management Information Database (or) Management Information Base (MIB)** : Every SNMP agent maintains an information database describing the managed device parameters. The SNMP manager uses this database to request the agent for specific information and further translates the information as needed for the Network Management System (NMS). This commonly shared database between the Agent and the Manager is called ***Management Information Base (MIB).***

   Typically these MIB contains standard set of statistical and control values defined for hardware nodes on a network. SNMP also allows the extension of these standard values with values specific to a particular agent through the use of private MIBs.

In short, MIB files are the set of questions that a SNMP Manager can ask the agent. Agent collects these data locally and stores it, as defined in the MIB. So, the SNMP Manager should be aware of these standard and private questions for every type of agent.

4.4 WORKING OF SNMP

1. **Basic Commands of SNMP :** The simplicity in information exchange has made the SNMP as widely accepted protocol. The main reason being concise set of commands, here are they listed below :

   - **GET :** The GET operation is a request sent by the manager to the managed device. It is performed to retrieve one (or) more values from the managed device.
   - **GET NEXT :** This operation is similar to the GET. The significant difference is that the GET NEXT operation retrieves the value of the next OID in the MIB tree.
   - **GET BULK :** The GETBULK operation is used to retrieve voluminous data from large MIB table.
   - **SET :** This operation is used by the managers to modify (or) assign the value of the Managed device.
   - **TRAPS :** Unlike the above commands which are initiated from the SNMP Manager, TRAPS are initiated by the Agents. It is a signal to the SNMP Manager by the Agent on the occurrence of an event.
   - ***INFORM*** : This command is similar to the TRAP initiated by the Agent, additionally INFORM includes confirmation from the SNMP manager on receiving the message.
   - ***RESPONSE*** : It is the command used to carry back the value(s) (or) signal of actions directed by the SNMP Manager.

2. **Typical SNMP Communication :** Being the part of TCPD IP protocol suite, the SNMP messages are wrapped as User Datagram Protocol (UDP) and intern wrapped and transmitted in the Internet Protocol.

   The Fig. 4.1 will illustrate the four-layer model developed by Department of Defence (DoD).

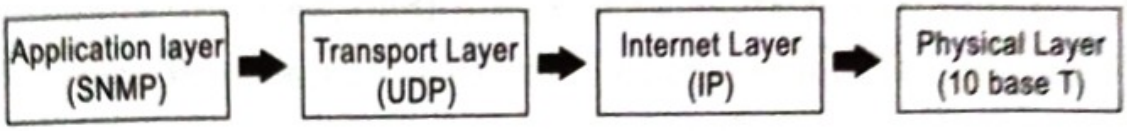


FIG 4.1 :

3. **SNMP Versions :** Since the inception SNMP, has gone through significant upgrades. However SNMP v1 and v2c are the most implemented versions of SNMP. Support to SNMP v3 has recently started catching up as it is more secured when compare to its older versions, but still it has not reached considerable market share.

4. **SNMPv1 :** This is the first version of the protocol, which is defined in RFCs 1155 and 1157.

5. **SNMPv2c :** This is the revised protocol, which includes enhancements of SNMPv1 in the areas of protocol packet types, transport mappings, MIB structure elements but using the existing SNMPv1 administration structure ("community based" and hence SNMPv2c). It is defined in RFC 1901, RFC 1905, RFC 1906, RFC 2578.

6. **SNMPv3 :** SNMPv3 defines the secure version of the SNMP. SNMPv3 also facilitates remote configuration of the SNMP entities. It is defined by RFC 1905, RFC 1906, RFC 3411, RFC 3412, RFC 3414, RFC 3415.

   Though each version had matured towards rich functionalities, additional emphasis was given to the security aspect on each upgrade. Here is a small clip on each editions security aspect.

4.5 DHCP, DNS

1. **DHCP :** Network administrators were assigning the IP address for every individual device. This was not as practical as such, and it took a lot of time. But to make this process easier, DHCP (Dynamic Host Configuration Protocol) was therefore invented. DHCP works in a centralized manner, using the server-client system. The DHCP server automatically and dynamically provides IP addresses to each new connected device.

2. **DNS :** Apart from DHCP, there what is known as the ***DNS (Domain Name System).*** DNS also works with the IP address for an individuals convenience, though in a different manner. Each device that is on the internet consists of a unique address. The same also applies to websites (or) domains. Human beings don't want to remember a different combination of numbers for every site that they like. People would want to put the most natural thing its name. However, its important to note that the name is not the address.

4.6 OVERVIEW OF NETWORK MANAGEMENT

Main Areas of Network Management are as Following :

1. **Network Administration :** This involves tracking and inventorying the many network resources such as monitoring transmission lines, hubs, switches, routers, and servers it also involves monitoring their performance and updating their associated software-especially network management software, network operating systems and distributed software applications used by network users.

2. **Network Operation :** This involves smooth network functioning as designed and intended, including close monitoring of activities to quickly and efficiently address and fix problems as they occur and preferably even before users are aware of the problem.

3. **Network Maintenance :** This involves timely repair and necessary upgrades to all network resources as well as preventive and corrective measures through close communication and collaboration with network administrators. Example work includes replacing (or) upgrading network equipment such as switches, routers and damaged transmission lines.

4. **Network Provisioning :** This involves configuring network resources to support the requirements of a particular service example services may be voice capabilities (or) increasing broadband requirements to facilitate more users.

4.7 NETWORK MONITORING AND TROUBLESHOOTING

Network monitoring refers to the practice of overseeing the operation of a computer net work using specialized management software tools. Network monitoring systems are used to ensure availability and overall performance of computers (hosts) and network services. These systems are typically employed on larger scale corporate and university IT networks. A network monitoring system is capable of detecting and reporting failures of devices (or) connections. It normally measures the processor (CPU) utilization of hosts, the network bandwidth utilization of links, and other aspects of operation. It will often send messages (sometimes called ***watchdog messages***) over the network to each host to verify it is responsive to requests. When failures, unacceptably slow response, (or) other unexpected behaviour is detected, these systems send additional messages called ***alerts to designated locations*** (such as a management server, an email address, (or) a phone number) to notify system administrators.

Network Monitoring Software Tools : The ping program is one example of a basic network monitoring program. Ping is a software tool available on most computers that sends Internet

Protocol (IP) test messages between two hosts. Anyone on the network can run these basic ping tests to verify the connection between two computers is working and also measure the current connection performance.

While ping is useful in some situations, more sophisticated network monitoring systems exist. These software programs are designed for use by professional administrators of larger computer networks. Examples of these software packages are HP Open view and LAN Desk.

One specific type of network monitoring system is designed to monitor the availability of Web servers. For larger enterprises that use a pool of Web servers distributed worldwide, these systems help to quickly detect problems at any location. Web site monitoring services available on the Internet include monitor.us.

Network troubleshooting is the collective measures and processes used to identify, diagnose and resolve problems and issues within a computer network. It is a systematic process that aims to resolve problems and restore normal network operations within the network.

Adapter Resources : Verify that the network adapter is properly installed and detected by the computer with no conflicts. In Microsoft Windows, open the Device Manager and verify there are no errors. **"Network adapters"** should be present for each network adapter installed in the computer. If conflicts exist (or) the network adapter is being detected as another device. The network card has not been properly installed in the computer. Try letting Windows re-detect and install the Network card by removing the network adapter and any other conflict devices from Device Manager and then rebooting the computer. If Windows re-detects the card but

does not find the drivers, download the network adapter drivers from the computer manufacturer (or) the network card manufacturer.

Verify Connections :

1. **Wired Network :** If this is a wired network, verify that the network cable is properly connected and make sure the LEDs next to the network jack are properly illuminated. For example, a network card with a solid green LED (or) light usually indicates that the card is either connected (or) receiving a signal. If the green light is flashing, this is an indication of data being sent (or) received. With RJ-45 port, one LED will light up if connected properly and the other will flash when transmitting data. If there are no lights (or) the lights are orange (or) red the card may be bad, not connected properly, (or) that the card is not receiving a signal from the network. If you are on a small (or) local network and have the capability of checking a hub, switch, (or) router verify that the cables are properly connected and that it has power. If after checking the connections the LED indicators appear bad, the network adapter, port, (or) cable may be defective.

2. **Wireless Network :** If you're using a laptop with a wireless network make sure if the laptop has a Wi-Fi button that it is turned on. Many laptops have a Wi-Fi button that allows the wireless network to be turned on and off. If the button is turned on, make sure you're using the correct Wi-Fi hotspot by right-clicking on the Network icon in the Windows Notification Area and clicking **"Connect to a network"**. Usually, the network with the strongest connection (the most bars) will be your wireless router. Finally, when connecting to most wireless networks you need to enter the proper SSID (password) to connect to the network. If the incorrect SSID has been entered you cannot access the network.

Adapter Functionality : Verify that the network card is capable of pinging itself by using the ping command. Windows users can ping the computer from a Windows command line. Unix and Linux users can ping from the shell.

To ping the card (or) the localhost, type either

ping 127.0.0.1 (or) ping localhost

Doing either of the above commands should get replies from the network card. If you receive an error (or) if the transmission fails the network card is not physically installed into the computer correctly, has the incorrect drivers, (or) that the card is bad.

Connect To The Router : If all of the above steps have been checked and your network has a router, make sure the computer can connect to the router by performing the below commands.

Determine the routers address : Using the ipconfig command (or ifconfig command for Linux) determine the router's address by looking at the Gateway address.

Below are the steps for Microsoft Windows users, Linux users can substitute ipconfig for ifconfig.

1. Open the Windows command line.
2. From the command prompt type **ipconfig** and press enter. This command should give you an output similar to the example below.

Ethernet adapter Local Area Connection :

Connection-specific DNS Suffix : computerhope.com.

IP Address. . . . . : 192.168.1.103

Subnet Mask . . . . . : 255.255.255.0

Default Gateway . . . . . : 192.168.1.1

The Default Gateway is the address of your router. Most home routers have a gateway address that starts with 192.168 like the address shown above. Assuming your gateway address is 192.168.1.1 attempt to ping the router to see if it can send and receive information by running the below command.

ping 192.168.1.1

If you get replies back from the router, the connection between your router and computer are good, and you can skip to the next step.

If you do not receive any replies back from the router either the router is not setup properly (or) your connection between the router and the computer are not correct.

Reset your router to make sure it is not a problem with your router by following the steps below.

1. Turn off the power to the computer and leave it off.
2. Unplug the power to your router and cable modem (or) DSL modem.
3. Leave the power cables disconnected for 10-15 seconds and then plug in your modem and then your router again.
4. Finally, turn on your computer again and repeat this step to see if you can ping your router.

If you have a wireless network and followed the above steps but cannot ping the router, turn the computer off again and connect the computer to the router using a cable instead of wireless.

Firewall : If your computer network utilizes a firewall, make sure all required ports required are open, especially port 80, which is the HTTP port. If possible, disable the firewall software program (or) disconnect the computer from the firewall to make sure it is not causing the network problems.

Internet is Not Working : If you're able to ping the router, but are still unable to connect to the Internet, either your router is improperly configured (or) the ISP is having issues.

If your Internet has been working but recently stopped working, give it a few minutes to make sure it is not a temporary outage. If after waiting a few minutes, you still have problems and you have not disconnected the power to your router and modem already follow the steps below.

1. Turn off the power to the computer and leave it off.
2. Unplug the power to your router and cable modem (or) DSL modem.
3. Leave the power cables disconnected for 10-15 seconds and then plug in your modem and then your router again.
4. Finally, turn on your computer again and repeat this step to see if you can ping your router.

If after following the above steps the Internet is still not working, open the Windows command line and run the below command.

ping google.com

Running the above command should get a reply from Google. If you get a reply, this is an indication that the Internet is working, but you may be encountering a problem with the Internet browser you are using to browse the Internet. Try an alternative browser such as Firefox (or) Chrome.

If you're getting no reply from Google, your router (or) modem is not reaching the Internet. If you have a router, make sure your router has DHCP enabled and that the WAN (or) Gateway address is the proper ISP address.

Finally, if trying the above steps has not helped contact the ISP to make sure there is no problem on their end and to assist you further with any special configurations.

4.8 REMOTE MONITORING (RMON)

RMON was initially developed to address the issue of remote site and local area network (LAN) segment management from a centralized location. The RMON standard specifies a group of functions and statistics that may be exchanged between RMON compatible network probes and console managers. RMON performs extensive network-fault detection and provides performance-tuning data to NAs. RMON collects nine information types, including bytes sent, packets sent, packets dropped and statistics by host. NAs use RMON to determine network user traffic (or) bandwidth levels and website access information. Additionally, issue alerts may be preconfigured. RMON uses certain network devices, such as servers, and contains network management applications that serve as clients. RMON controls the network by using its servers and applications simultaneously. When a network packet is transmitted, RMON facilitates packet status viewing and provides further information, in the event that a packet is blocked, terminated (or) lost.

Two RMON Versions are Available :

1. **RMON1 :** Outlines 10 management information base (MIB) groups for standard network monitoring. MIB groups are viewable in most advanced network hardware.
2. **RMON2 :** Focuses on higher traffic layers that exist above the medium access control (MAC) layer, Internet Protocol (IP) and application-level traffic. Facilitates network management applications to track all network layer packets.

REVIEW QUESTIONS

Part-A

1. What is the need of a protocol ?
2. What is HTTP.
3. What is the need of SMTP.
4. Explain what is FTP ?
5. What does ARP do ?
6. What is the difference between ARP and RARP ?

Part-B

1. Explain the working of SNMP.
2. What is Network Management?
3. What is Network monitoring and troubleshooting?

Part-C

1. Explain what are the protocols HTTP, FTP,SMTP, ARP, RARP SNMP meant for ?
2. What is RMON and its purpose ?
3. Explain in detail about Network Management and its purpose.

Chapter-5

BASIC NETWORK ADMINISTRATION

CHAPTER OUTLINE

5.1 Network Administration 2

5.2 Need of Network Administration 2

5.3 Responsibilities of Network Administrator 3

5.4 User and Group Managements 3

5.5 Working of Device Manager 4

5.6 Verification and Managing Ports 4

5.7 Procedure of Installing, Managing and Configuration of Printers 5

5.8 Disk Management Tools and Tasks 7

5.9 File Systems Management 10

5.10 NTFS (File and Folder) and Share Permissions 14

5.1 NETWORK ADMINISTRATION

Network administration involves a wide array of operational tasks that help a network to run smoothly and efficiently. Without network administration, it would be difficult for all but the smallest networks to maintain network operations.

The Main Tasks Associated with Network Administration Include :

1. Design, installation and evaluation of the network.
2. Execution and administration of regular backups.
3. Creation of precise technical documentation, such as network diagrams, network cabling documents, etc.,
4. Provision for precise authentication to access network resources.
5. Provision for troubleshooting assistance.
6. Administration of network security, including intrusion detection.

5.2 NEED OF NETWORK ADMINISTRATION

Since computer systems and networks have become critical attributes of modern organizations and institutions, continuous monitoring is necessary in order to ensure they run efficiently. This is the major reason why networks cannot function effectively without proper administration. The first importance of effective network administration revolves around installation. A network administrator is a professional who can identify and acquire the right systems that have the potential to support the business goals of the targeted company. With proper administration, the right networks and systems will be installed in an attempt to meet the intended objectives.

5.3 RESPONSIBILITIES OF NETWORK ADMINISTRATOR

1. Configure network hardware such as servers, routers and switches.
2. Upgrade, repair and maintain computer networks.
3. Troubleshoot various network issues.
4. Assist network architects with the design of network models whenever needed.
5. Deploy and update company-wide software.
6. Manage servers and operating systems.
7. Implement security measures.
8. Manage physical and cloud network storage.

5.4 USER AND GROUP MANAGEMENTS

User management describes the ability for administrators to manage user access to various IT resources like systems, devices, applications, storage systems, networks, SaaS services, and more. User management is a core part to any identity and access management (IAM) solution, in particular directory services tools. Controlling and managing user access to IT resources is a fundamental security essential for any organization. User management enables admins to control user access and on-board and off-board users to and from IT resources. Subsequently a directory service will then authenticate, authorize and audit user access to IT resources based on what the IT admin had dictated.

User management solves the problem of managing user access to various resources. For example, the marketing team generally requires access to different resources than the accounting team. Further, an employee on the marketing team likely doesn't need access to internal financial systems and

vice versa, a finance employee isn't requiring access to Salesforce (or) Marketo. User management enables IT administrators to manage resources and provision users based on need and role while keeping their digital assets secure. For end users, the tasks of user management are often invisible to them, but the results are not. End users want secure, frictionless access to their IT resources so that they can get their jobs done.

5.5 WORKING OF DEVICE MANAGER

Following are the responsibilities of Device Manager, It enables the user to find out all the devices and drivers in one glance.

1. View all the hardware components that make up your Windows computer (or) device.
2. View the properties of your devices.
3. Find missing drivers for your components.
4. Install drivers for your hardware components and peripherals.
5. View hidden devices in Device Manager.

5.6 VERIFICATION AND MANAGING PORTS

A firewall is an essential aspect of computing and no PC should ever be without one. Thats why Windows has one bundled and active as standard. Windows Firewall occasionally has to be told to let a program communicate with the network, which is where opening ports comes in.

Opening ports in Windows 10

You can manually permit a program to access the internet by opening a firewall port. You will need to know what port it uses and the protocol to make this work.

1. Navigate to Control Panel, System and Security and Windows Firewall.

2. Select Advanced settings and highlight Inbound Rules in the left pane.
3. Right click Inbound Rules and select New Rule.
4. Add the port you need to open and click Next.
5. Add the protocol (TCP or UDP) and the port number into the next window and click Next.
6. Select Allow the connection in the next window and hit Next.
7. Select the network type as you see fit and click Next.
8. Name the rule something meaningful and click Finish.

5.7 PROCEDURE OF INSTALLING, MANAGING AND CONFIGURATION OF PRINTERS

1. To Add a new Local Printer, open the Printers and Faxes folder from the start menu and click on Add a printer.
2. The Add Printer Wizard will appear. Click on Next.
3. Select Local Printer to install a new Local Printer.
4. Click on Next to continue.
5. The wizard will ask you which port the printer is connected to. You can also create a new port such as a TCP/IP port for network printers that are not connected to a print server. Click on Next to continue.
6. Choose the Manufacturer and Printer from the list shown. You may need a driver disk at this stage if your printer isn't supported.
7. Click on Next to continue.
8. The wizard will ask you to choose a name for the printer and whether you want it to be the default.
9. The wizard will ask you if you want to share the printer. Select Do not share this printer and click Next to continue.

10 You can test the printer by sending it a test page. Click on Next to continue.

11 A summary page will appear, verify all options are correct and click Finish.

12 The new local printer has now been installed and is marked as the default printer.

Connecting to a Network Printer :

1. Click on Add a printer.
2. Click on Next.
3. Select A network printer.
4. Click on Next to continue.
5. The wizard will ask you where the printer is, you can either browse for (or) specify a printer using a URL (or) an UNC path.
6. For example \\10.0.0.243\hplaserj.2 will connect to a printer shared on the machine 10.0.0.243. Click on Next to continue.
7. The computer will automatically download drivers from the Print Server. Click on Yes to accept the warning.
8. Choose whether you want the printer to be your default and click Next.
9. A summary page will appear, verify all options are correct and click Finish.

10 The new printer is displayed in the Printers and Faxes window and is marked as default.

Sharing a Print Device :

1. To share a print device, right-click on the print device from the Printers and Faxes Window.

2. Select Sharing.
3. Select the Share this printer option.
4. A share name is suggested for you although this can be easily changed. If the printer is to be shared on a mixed network (i.e. Older version of Windows) then select Additional Drivers.
5. Additional Drivers can be installed for the supported platforms by selecting the relevant check boxes.
6. To configure permissions click on the Security Tab.
7. The Security Tab is used to configure permissions for the printer.
8. The Manage Printers permission allows a user to pause and restart the printer, change its settings and manage its permissions.
9. The Print permission allows a user (or) group to print to a printer.
10. The Manage Documents permission allows a user to pause, restart and delete queued documents. This permission does not allow a user to change any of the printer settings.
11. For example the Everyone group has been given the Print permission by default so all users can print to the printer but not manage the printer (or) other peoples print jobs.
12. Click on OK to continue.
13. The printer has now been shared.

5.8 DISK MANAGEMENT TOOLS AND TASKS

Disk management tools are utility software that is used to manage data on disk by performing various functions on it. Moreover, they perform functions like partitioning devices,

manage drives, disk checking, disk formatting, etc., Furthermore, there are various types of disk management tools like disk checkers, disk cleaners, and disk analyzers.

Basic Functions of Tools : The disk utility basically takes care of the computer disk system. It performs all the tasks which are necessary to keep the functioning of the disk smooth. Some basic functions that Disk Management tools perform are as follows :

1. Partitioning of the disk.
2. Formatting the disk.
3. Changing disks name.
4. Shrinking a disk partition.
5. Extending a disk partition.
6. Deleting a disk partition.
7. Changing the file system of a driver.

Types of Disk Management Tools :

1. **Disk Cleanup Tools :** These tools clean up the unnecessary and unwanted files on the system. Furthermore, this deletion of files thus helps to clean up the disk space. Moreover, it prevents unnecessary clutter and protects privacy.

   Temporary files, web caches, old backups, etc., are the files that make up the unwanted clutter on the disk. Privacy risk happens due to files that have information about files opened by each computer program. For example log files, HTTP cookies, etc., Examples of disk cleanup tools are Razer Cortex, PiriformCCleaner, etc.,

2. **Disk Compression Tools :** The disk compression tools (or) disk compression utility increases the amount of space on a disk by decreasing the size of information. The utility

compresses the information while storing it on this disk. On the other hand, the information decompresses when we have to read it. ***Examples of Disk Compression Utility are as Follows :***

(i) ***Microsft Windows*** : Drive Space.

(ii) ***Macintosh*** : Disk Doubler.

3. **Disk Checkers :** These tools scan the hard disk and remove any such areas which are corrupted (or) not saved properly. Furthermore, they perform this process so that the hard disk can operate more efficiently. Some tools perform the full surface scan while some others check only logical structures of the files.

4. **Disk Formatters :** They prepare a data storage device for the initial use. For example devices like hard disk, floppy disk, USB flash drive, etc., Moreover, they can also permanently erase a drive.

The Formatting has Three Levels :

(i) Low-level formatting

(ii) Partitioning

(iii) High-level formatting

5. **Disk Partitioning Tools :** These tools divide the disk into more than one region. Furthermore, it does this so that each region can be managed separately and hence, more efficiently. These regions are the ***partitions***. A ***partition table*** is also maintained which contains information about the location and size of each partition. Examples are GParted, disk part, GNU Parted, etc.,

6. **Disk Space Analyzers :** These tools indicate the space usage on the disk. Furthermore, they perform this task by analyzing the size of each file and folders and also, the sub folders. Usually, this information is indicated through graphical charts according to the folders size (or) other criteria. We can also

call them as ***disk usage analysis software***. Examples are Disk Report, KDE File light, GNOME Disk Usage Analyzer, etc.,

7. **Disk Defragmenter :** This utility software helps to reduce the fragmentation and hence, reduces the access speed. Defragmenting refers to rearranging files and storing them in contiguous memory locations. This means that when the contents of some files are scattered here and there it rearranges them and stores them in a contiguous memory area. These scattered parts are ***fragments***. Moreover, saves time in reading from files and writing files to disk. Examples of disk defragmenters are Perfect disk, Deflaggler, etc.,

8. **Backup Software :** This keeps a copy of all the information on a disk. Whenever some disk failure occurs (or) files are deleted accidentally, it restores the files. Restoring the whole disk is called ***disk cloning***.

5.9 FILE SYSTEMS MANAGEMENT

Files are used to provide a uniform view of data storage by the operating system. All the files are mapped onto physical devices that are usually non volatile so data is safe in the case of system failure.

File Attributes

The attributes of a file may vary a little on different operating systems. However, the common file attributes are "

Name

This denotes the symbolic name of the file. The file name is the only attribute that is readable by humans easily.

Identifier

This denotes the file name for the system. It is usually a number and uniquely identifies a file in the file system.

Type

If there are different types of files in the system, then the type attribute denotes the type of file.

Location

This points to the device that a particular file is stored on and also the location of the file on the device.

Size

This attribute defines the size of the file in bytes, words (or) blocks. It may also specify the maximum allowed file size.

Protection

The protection attribute contains protection information for the file such as who can read (or) write on the file.

Operations on Files

The operations that can performed on a file are "

Creating a file

To create a file, there should be space in the file system. Then the entry for the new file must be made in the directory. This entry should contain information about the file such as its name, its location etc.,

Reading a file

To read from a file, the system call should specify the name and location of the file. There should be a read pointer at the location where the read should take place. After the read process is done, the read pointer should be updated.

Writing a file

To write into a file, the system call should specify the name of the file and the contents that need to be written. There should

be a write pointer at the location where the write should take place. After the write process is done, the write pointer should be updated.

Deleting a file

The file should be found in the directory to delete it. After that all the file space is deleted so it can be reused by other files.

Repositioning in a file

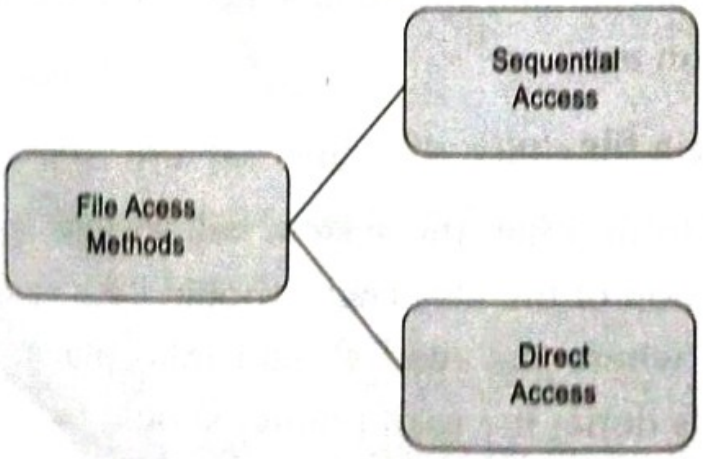
This is also known as ***file seek***. To reposition a file, the current file value is set to the appropriate entry. This does not require any actual I/O operations.

Truncating a file

This deletes the data from the file without destroying all its attributes. Only the file length is reset to zero and the file contents are erased. The rest of the attributes remain the same.

File Access Methods

The information in a file can be accessed in various ways. The most common among them are using sequential access (or) direct access. More details about these are –

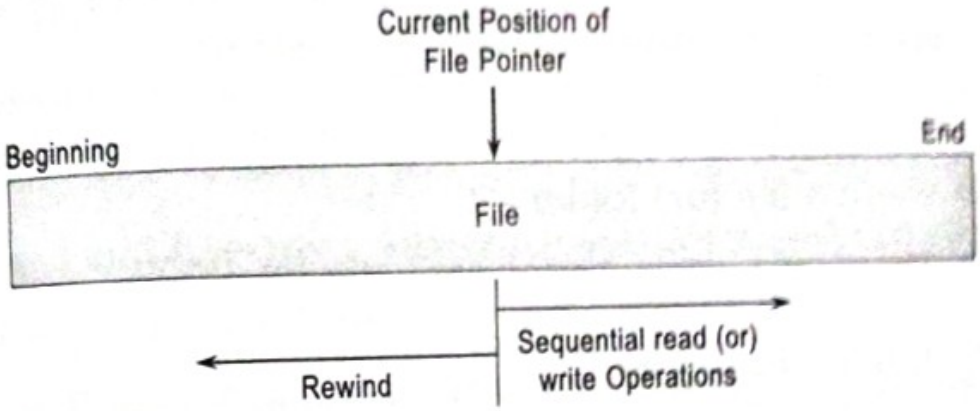


Sequential Access

The information in a file is processed in order using sequential access. The files records are accessed on after another. Most

of the file systems such as editors, compilers etc., use sequential access. It is based on the tape model of a file and so can be used with sequential access devices as well as random access devices.

A diagram to illustrate sequential access is as follows –



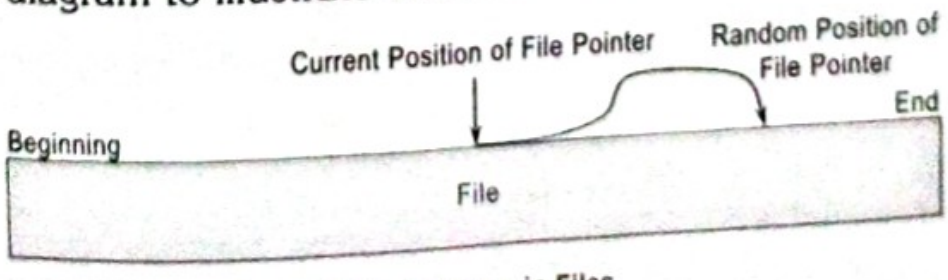
Squential Access in Files

As seen in the image, the read and write operations in the file can only be done in a sequential manner. However, the file can be reset to the beginning (or) rewinded as required.

Direct Access

In direct access (or) relative access files can be accessed in random for read and write operations. The direct access model is based on the disk model of a file, since it allows random accesses. In this method, the file is divided into numbered blocks. Any of these arbitrary blocks can be read (or) written. For example, we may read block 8, then write into block 10 and then read block 15. Direct access system is quite useful and mostly databases are of this type.

A diagram to illustrate direct access is as follows –



Direct Access in Files

As seen in the above image, the file pointer can be positioned randomly as required for read and write operations. This can be done without any particular order in positioning.

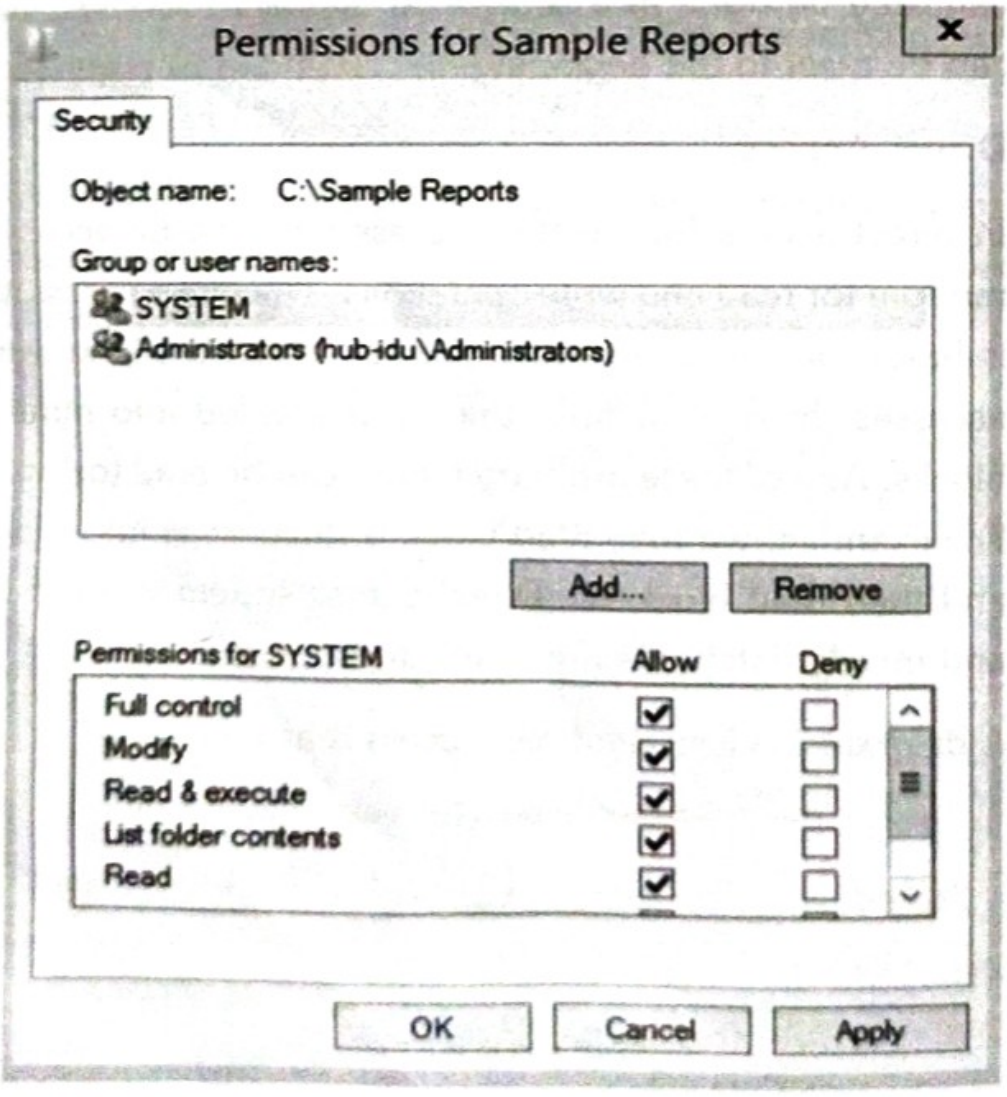
5.10 NTFS (FILE AND FOLDER) AND SHARE PERMISSIONS

NTFS permissions are used to manage access to the files and folders that are stored in NTFS file systems.

To see what kind of permissions you will be extending when you share a file (or) folder :

1. Right click on the file/folder.
2. Go to "Properties".
3. Click on the "Security" tab.

All then you'll navigate this window :



Besides Full Control, Change, and Read that can be set for groups (or) individually, NTFS offer a few more permission options :

1. **Full control :** Allows users to read, write, change and delete files and subfolders. In addition, users can change permissions settings for all files and sub directories.
2. **Modify :** Allows users to read and write of files and subfolders ; also allows deletion of the folder.
3. **Read and Execute :** Allows users to view and run executable files, including scripts.
4. **List Folder Contents :** Permits viewing and listing of files and subfolders as well as executing of files ; inherited by folders only.
5. **Read :** Allows users to view the folder and sub folder contents.
6. **Write :** Allows users to add files and subfolders, allows you to write to a file.

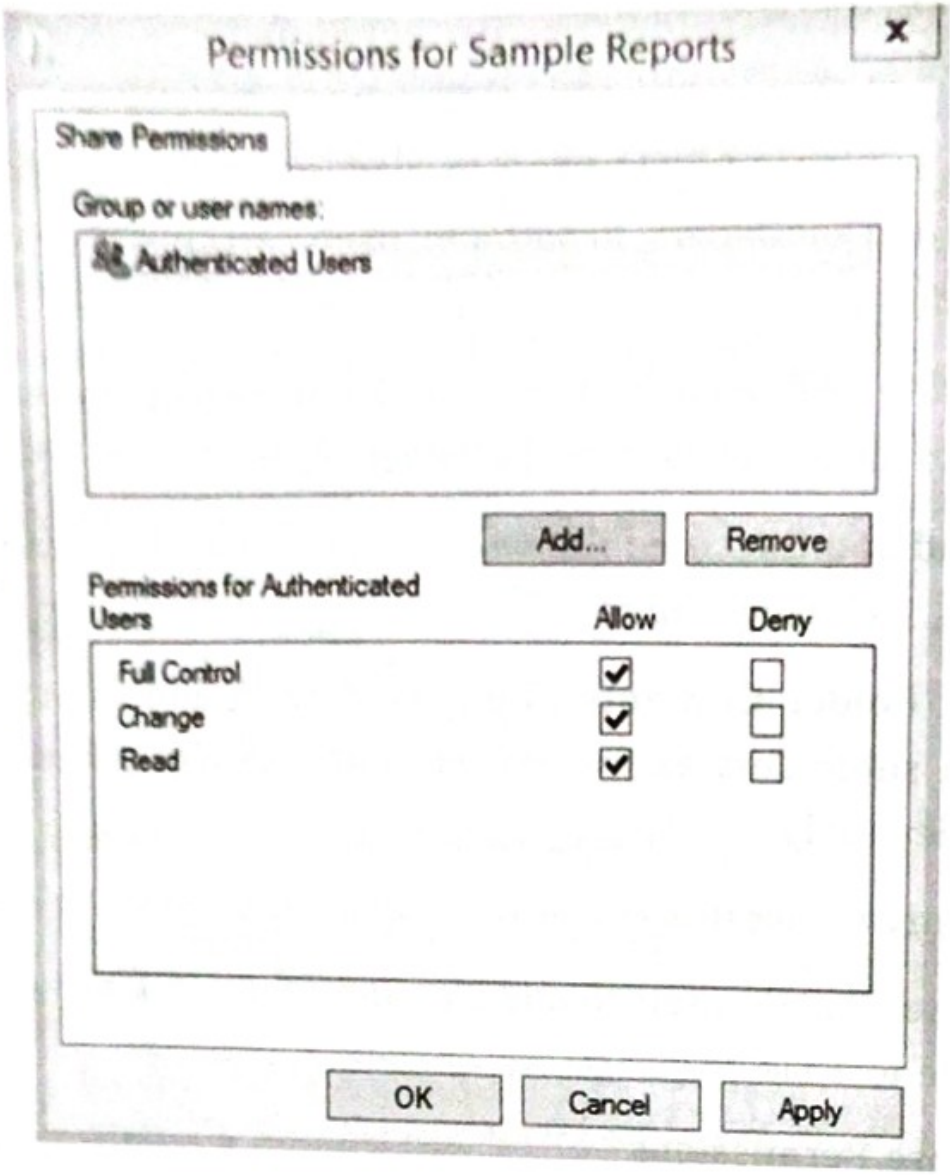
Share Permissions

When you *share* a folder and want to set the permissions for that folder thats a share. Essentially, share permissions determine the type of access others have to the shared folder across the network.

To see what kind of permissions you will be extending when you share a folder :

- Right click on the folder
- Go to "Properties"
- Click on the "Sharing" tab
- Click on "Advanced Sharing..."
- Click on "Permissions"

And you'll navigate to this window :



There are three types of share permissions : Full Control, Change and Read.

1. **Full Control:** Enables users to "read," "change," as well as edit permissions and take ownership of files.
2. **Change :** Change means that user can read/execute/write/ delete folders/files within share.
3. **Read :** Read allows users to view the folders contents.

Differences Bbetween NTFS and Share Permissions :

(i) Share permissions are easy to apply and manage, but NTFS permissions enable more granular control of a shared folder and its contents.

(ii) When share and NTFS permissions are used simultaneously, the most restrictive permission always wins. For example, when the shared folder permission is set to "Everyone Read Allow" and the NTFS permission is set to "Everyone Modify Allow", the share permission applies because it is most restrictive ; the user is not allowed to change the files on the shared drive.

(iii) Share permissions can be used when sharing folders in FAT and FAT32 file systems ; NTFS permissions cant.

(iv) NTFS permissions apply to users who are logged on to the server locally ; share permissions don't.

(v) Unlike NTFS permissions, share permissions allow you to restrict the number of concurrent connections to a shared folder.

(vi) Share permissions are configured in the "Advanced Sharing" properties in the "Permissions" settings. NTFS permissions are configured on the Security tab in the file (or) folder properties.

REVIEW QUESTIONS

Part-A

1. What is Network administration ?
2. What is a device manager ?
3. What is the need to manage a port ?
4. How to install a printer, describe in brief.
5. What are the different tools provided for disk management ?
6. What is the purpose of Disk Management ?
7. What is a file system ?

Part-B

1. Give the need of Network Administration.
2. What is the importance of Disk management and what are the tools for Disk management ?
3. What is User and group management in networking ?
4. How to open a port for connection ?
5. Describe in detail about File System Management.

Part-C

1. What are NTFS and Share permissions ?
2. What is File Systems Management ?
3. How to install and configure a printer ?

BOARD DIPLOMA EXAMINATION

MODEL PAPER (UNIT TEST-1)

COMPUTER NETWORKS

For IV Semester Examination

Time 90 Minutes — Max. Marks :40

PART – A — 16 Marks

Note : 1. *Answer **all** questions.*
2. *First question carries 4 marks, and remaining carries 3 marks each.*

1. (a) Transport layer is bottom layer of OSI reference model. (True/False) (CO2)

(b) MAN stands for _____ (CO3)

(c) _____ tool is used to affix a connector at the end of cable. (CO1)

(d) The class of private address range 172.16.0.0 to 172.31.255.255 is _____ (CO4)

(i) Class A (ii) Class B

(iii) Class C (iv) Class D

2. State the need of Networking. (CO1)
3. List any six LAN devices (CO3)
4. Give the functions of cable tester (CO3)
5. Describe IP address. (CO4)

PART - B — 3 X 8 = 24

Note : 1. *Answer any all questions and each question carries **8** marks.*
2. *Answer should be comprehensive and the criteria for valuation is the content but not the length of the answer.*

6. (a) Explain OSI reference model in detail. (CO2)

(or)

(b) Compare TCP/IP and OSI reference models (CO2)

7. (a) Explain coaxial and twisted pair cables. (CO1)

(or)

(b) Explain IP address classes in detail. (CO3)

3. (a) Explain Star and Mesh Topologies. (CO3)

(or)

(b) Explain Ring and Bus Topologies. (CO3)

BOARD DIPLOMA EXAMINATION

MODEL PAPER (END EXAMINATION)

COMPUTER NETWORKS

For IV Semester Examination

Time 3 Hours | Max. Marks : 80

PART - A — 10 × 3 = 30 MARKS

Note : *1. Answer **all** questions.*

1.	Write the importance of networking	CO1
2.	Write any three differences between LAN and WAN	CO1
3.	List any thee network cables	CO1
4.	Write about RJ-45 jack	CO1
5.	What are the components of IP address	CO4
6.	What is the importance of sub-netting.	CO4
7.	Differentiate between ARP and RARP	CO5
8.	Write the importance of protocols in networking	CO5
9.	List any three responsibilities of network administrator	CO6
10.	Write about disk management tools	CO6

PART - B — 5 X 8 = 40 MARKS

Note : *Answer all questions*

11. (a)	Explain about ISO reference model with neat diagram	CO2
	(or)	
11. (b)	Explain TCP/IP architecture with neat diagram	CO2
12. (a)	Explain any four LAN devices	CO3
	(or)	
12. (b)	Explain any four network topologies with neat diagrams	CO3
13. (a)	Explain subnetting with a suitable example	CO4
	(or)	

13. (b) Explain IPv4 address classes CO4

14. (a) Explain any four network protocols CO5

(or)

14. (b) Write different steps involved in monitoring and troubleshoot the network. CO6

15. (a) Write the steps to create and manage user groups using any network Operating system. CO6

(or)

15. (b) Write the steps to install and configure laser printer using any OS. CO6

PART - C 10 X 1 = 10 MARKS

16. Compare VLSM and CIDR. (CO5)

BOARD DIPLOMA EXAMINATION

JUNE/JULY-2022

COMPUTER NETWORKS

For IV Semester Examination

Time 3 Hours | Max. Marks : 80

PART - A — 10 × 3 = 30

Note : *Answer **all** questions. Each question carries 3 Marks*

1. What is the need for networking?
2. What is the importance of MAN?
3. What is the purpose of a router?
4. List the advantages of star topology.
5. What is the host identifier in a IP address?
6. Write about TCP/IP addressing scheme.
7. Write about SNMP.
8. Write the difference between ARP and RARP.
9. What is the need of Network Administration?
10. List the types of Disk management tools.

PART - B — 5 × 8 = 40

Note : *Answer all questions*

11. (a) Explain the OSI reference model with a neat diagram.

    (or)

11. (b) Explain various network communication standards.

12. (a) Explain different functions of following LAN Tools :

    (i) Anti-magnetic Mat

    (ii) Crimping Tool

    (iii) Loop Backplug

    (iv) Protocal Analyser

(or)

12. (b) Explain about the following topology :

(i) Ring topology (ii) Hybrid topology

13. (a) Explain the following IP address classes :

(i) Class A network (ii) Class B Network

(or)

13. (b) List the advantages and disadvantages of subnetting.

14. (a) Explain Network monitoring and Troubleshooting.

(or)

14. (b) Explain the following protocols :

(i) HTTP (ii) FTP

(iii) SMTP

15. (a) Explain user and group management.

(or)

15. (b) Explain file system management.

PART - C $10 \times 1 = 10$

Instructions : *Answer the following question. The question carries* ***ten*** *marks.*

16. A state is having a population of 8 crores. Out of this population 7 crores of the people are having their own individual computer system. All of these 7 crores people wants to connect to the network at the same time. All of these 7 crores computer systems wants to have an IP address at the same time. Whether IPv4 address or IPv6 address is sufficient or both of them are required for IP addresses. Justify your answer.