Jawaharlal Nehru Engineering College

Laboratory Manual

Computer Communication Network

For

Final Year Students

Lab Manual Made By

Ms. A. P.Phatale

Mr.A.V.Khake

MGM'S

Jawaharlal Nehru Engineering College
N-6, CIDCO, Aurangabad
Department of Electronics &Telecommunication

Vision of the Department:

To develop **GREAT** technocrats and to establish centre of excellence in the field of **Electronics and Telecommunications.**

- **G**lobal technocrats with human values
- **R**esearch and lifelong learning attitude,
- **E**xcellent ability to tackle challenges
- **A**wareness of the needs of society
- **T**echnical expertise

Mission of the Department:

1. To provide good technical education and enhance technical competency by providing good infrastructure, resources, effective teaching learning process and competent, caring and committed faculty.
2. To provide various platforms to students for cultivating professional attitude and ethical values.
3. Creating a strong foundation among students which will enable them to pursue their career choice.

Jawaharlal Nehru Engineering College

Technical Document

This technical document is a series of Laboratory manuals of Electronics and Telecommunication Department and is a certified document of Jawaharlal Nehru Engineering College. The care has been taken to make the document error-free. But still if any error is found. Kindly bring it to the notice of subject teacher and HOD.

Recommended by,

HOD

Approved by,

Principal

Copies:

1. Departmental Library
2. Laboratory
3. HOD

4. Principal

FOREWORD

It is my great pleasure to present this laboratory manual for Final year engineering students for the subject of Computer Communication Network keeping in view the vast coverage required for visualization of concepts of basic Computer Communication Network.

As a student, many of you may be wondering with some of the questions in your mind regarding the subject and exactly that has been tried to answer through this manual.

Faculty members are also advised that covering these aspects in initial stage it self, will greatly relieve them in future, as much of the load will be taken care by the enthusiastic energies of the students, once they are conceptually clear.

H.O.D.

LABORATORY MANUAL CONTENTS

This manual is intended for the Final year students of Electronics & telecommunication Branch in the subject of Computer Communication Network. This manual typically contains Practical/Lab Sessions related to Computer Communication Network covering various aspects related to the subject to enhance understanding of the subject.

Students are advised to thoroughly go through this manual rather than only topics mentioned in the syllabus, as practical aspects are the key to understanding conceptual visualization of theoretical aspects covered in the books.

Good Luck for your Enjoyable Laboratory Sessions

Ms. A. P.Phatale

Mr.A.V.Khake

Authors

SUBJECT INDEX

Dos and Don'ts in Laboratory:

1. Do not Power on any PC without instruction.

2. Strictly observe the instructions given by the teacher/Lab Instructor

Instruction for Laboratory Teachers:

1. Submission related to whatever lab work has been completed should be done during the next lab session.

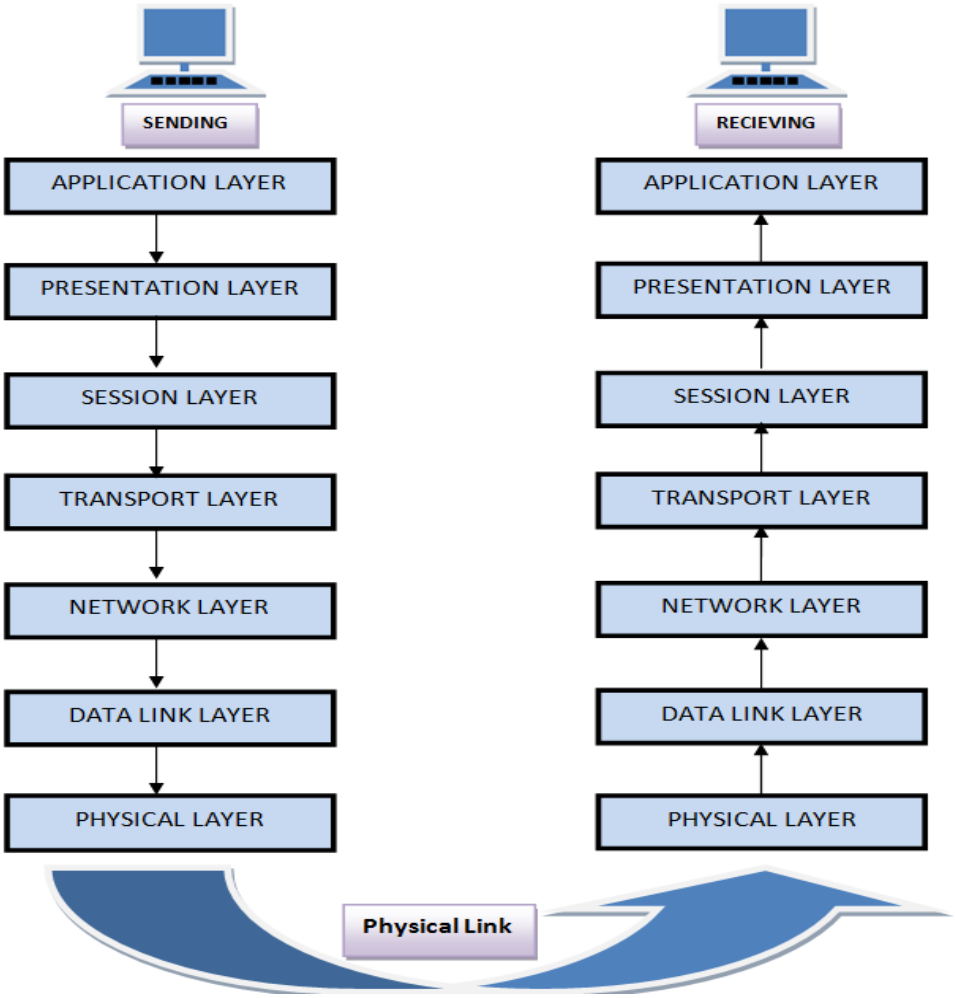
2. The promptness of submission should be encouraged by way of marking and evaluation patterns that will benefit the sincere students.

EXPERIMENT NO.1

Aim: Study of ISO-OSI reference model

Theory: There are n numbers of users who use computer network and are located over the world. So to ensure national and worldwide data communication systems can be developed and are compatible to each other. ISO has developed this. ISO stands for International organization of Standardization. This is called a model for open system interconnection (OSI) and is normally called as OSI model.

The ISO-OSI model consists of seven layer architecture. It defines seven layers or levels in a complete communication system.



Feature of OSI Model:

- Big picture of network is understandable through this OSI model.
- We see how hardware and software work together.
- We can understand new technologies as they are developed.
- Troubleshooting is easier by separate networks.
- Can be used to compare basic functional relationships on different networks.

Functions of Different Layers:

Layer 1: The Physical Layer: It activates, maintain and deactivate the physical connection. Voltages and data rates needed for transmission is defined in the physical layer. It converts the digital bits into electrical signal.

Layer 2: Data Link Layer: Data link layer synchronizes the information which is to be transmitted over the data. Error controlling is easily done. The encoded data are then passed to physical. Error detection bits are used by the data link on layer. It also corrects the errors. Outgoing messages are assembled into frames. Then the system waits for the acknowledgements to be received after the transmission. It is reliable to send message.

Layer 3: The Network Layer: It routes the signal through different channels to the other end. It acts as a network controller. It decides by which route data should take. It divides the outgoing messages into packets and to assemble incoming packets into messages for higher levels.

Layer 4: Transport Layer: It decides if data transmission should be on parallel path or single path. Functions such as multiplexing, segmenting or splitting on the data done by layer four that is transport layer. Transport layer breaks the message (data) into small units so that they are handled more efficiently by the network layer.

Layer 5: The Session Layer: Session layer manages and synchronize the conversation between two different applications. Transfer of data from one destination to another session layer streams of data are marked and are resynchronized properly, so that the ends of the messages are not cut prematurely and data loss is avoided.

Layer 6: The presentation Layer: Presentation layer takes care that the data is sent in such a way that the receiver will understand the information (data) and will be able to use the data. Languages (syntax) can be different of the two communicating systems. Under this condition presentation layer plays a role translator.

Layer 7: Application Layer: It is the top layer. Manipulation of data (information) in various ways is done in this layer. Transferring of files disturbing the results to the user is also done in this layer. Mail services, directory services, network resource etc are services provided by application layer.

Merits of OSI reference model:

- OSI model distinguish between the services, interfaces and protocols.
- Protocols of OSI model are very well hidden.
- They can be replaced by new protocols as technology changes.
- Supports connection oriented as well as connectionless service.

Demerits of OSI reference model:

- Model was devised before the invention of protocols.
- Fitting of protocols is tedious task.

Conclusion: - By using seven layered structure it is possible to have communication between two computers.

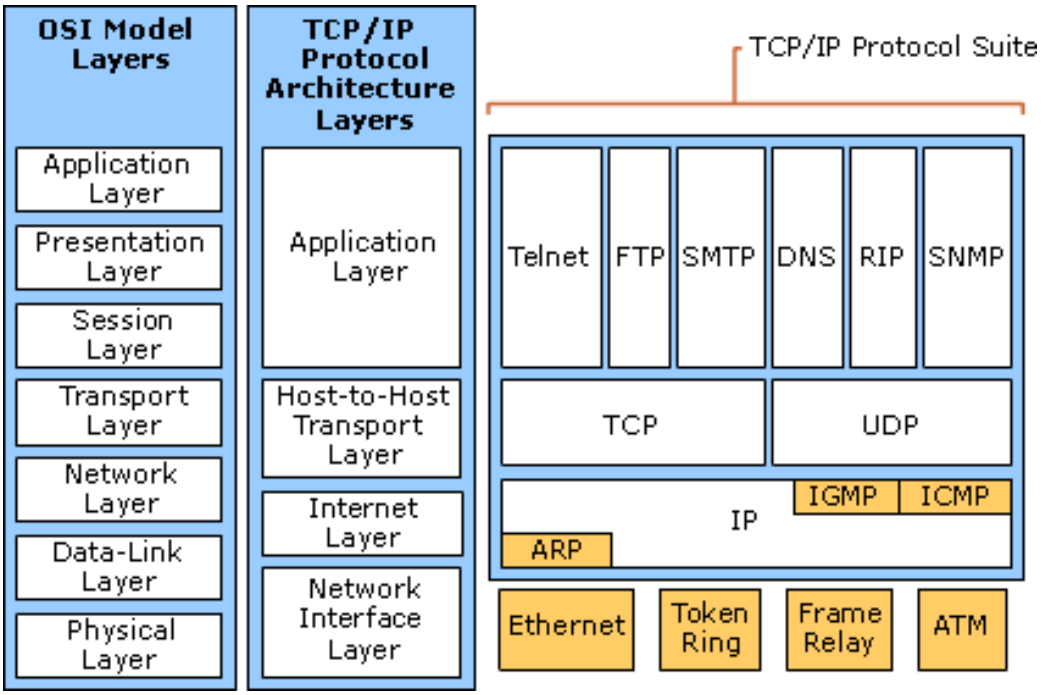
EXPERIMENT NO.2

Aim: Study of TCP / IP protocol and Internet

Theory: The Internet Protocol Suite (commonly known as TCP/IP) is the set of communications protocols used for the Internet and other similar networks. It is named from two of the most important protocols in it: the Transmission Control Protocol (TCP) and the Internet Protocol (IP), which were the first two networking protocols defined in this standard.

The TCP/IP model consists of four layers From lowest to highest, these are the Link Layer, the Internet Layer, the Transport Layer, and the Application Layer.

Block Diagram:



Conclusion: In this way we have studied different protocols of TCP/IP.

EXPERIMENT NO.3

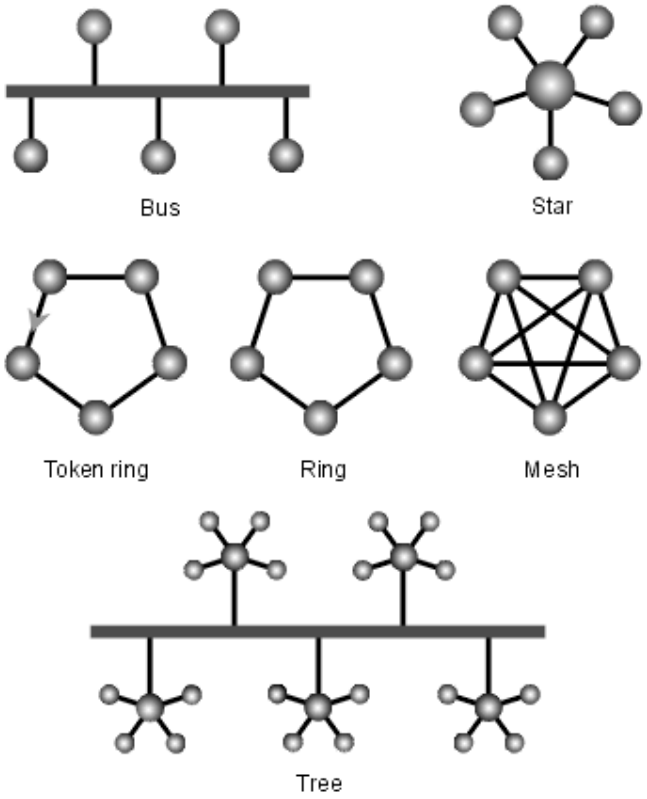
Aim: Study of topologies and interconnection devices.

Theory: A local area network (LAN) is a computer network covering a small physical area, like a home, office, or small group of buildings, such as a school, or an airport. The defining characteristics of LANs, in contrast to wide-area networks (WANs), include their usually higher data-transfer rates, smaller geographic place.

LAN transmission medias: The three main types of transmission medium used in LANs are twisted pair, coaxial cable and optic fiber and wireless LAN.

LAN Topologies:

Que. Explain the working of following LAN topologies.



LAN interconnection devices: All networks are made up of basic hardware building blocks to interconnect network nodes, such as Network Interface Cards (NICs), Bridges, Hubs, Switches, and Routers.

Network interface cards: A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network.

Repeaters: A repeater is an electronic device that receives a signal and retransmits it at a higher power level, or to the other side of an obstruction, so that the signal can cover longer distances without degradation. In most twisted pair Ethernet configurations, repeaters are required for cable which runs longer than 100 meters.

Hubs: A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission.

Bridges: A network bridge connects multiple network segments at the data link layer (layer 2) of the OSI model. Bridges do not promiscuously copy traffic to all ports, as hubs do, but learn which MAC addresses are reachable through specific ports.

Bridges come in three basic types:

1. Local bridges: Directly connect local area networks (LANs)
2. Remote bridges: Can be used to create a wide area network (WAN) link between LANs. Remote bridges, where the connecting link is slower than the end networks, largely have been replaced by routers.
3. Wireless bridges: Can be used to join LANs or connect remote stations to LANs.

Switches: A network switch is a device that forwards and filters OSI layer 2 datagram (chunk of data communication) between ports (connected cables) based on the MAC addresses in the packets.

Routers: A router is a networking device that forwards packets between networks using information in protocol headers and forwarding tables to determine the best next router for each packet. Routers work at the Network Layer of the OSI model and the Internet Layer of TCP/IP.

Conclusion: Thus we have studied LAN.

EXPERIMENT NO.4

Aim: Study of LAN, MAN & WAN

Theory: A computer network consists of two or more computers that are interconnected with each other and share resources such as printers, servers, and hardware and exchange the data in the form of files, facilitating electronic communication. Computers on a network can be connected through twisted pair cables, telephone lines, radio waves, satellites or optical fiber cables. The first computer network designed was the 'Advanced Research Projects Agency Network (ARPANET)' by the United States Department of Defense. Since then, myriads of new computer networking technologies have been designed. This tutorial only covers the first three network technologies i.e LAN, WAN and MAN. However, currently there are multiple networking technologies in use which have been enlisted below.

- Local Area Network (LAN)
- Wide Area Network (WAN)
- Metropolitan Area Network (MAN)
- Wireless Local Area Network (WLAN)

Local Area Network (LAN)

A Local Area Network (LAN) is a network that is restricted to smaller physical areas e.g. a local office, school, or house. Approximately all current LANs whether wired or wireless are based on Ethernet. On a 'Local Area Network' data transfer speeds are higher than WAN and MAN that can extend to a 10.0 Mbps (Ethernet network) and 1.0 Gbps (Gigabit Ethernet).

LAN networks can be implemented in multiple ways, for example twisted pair cables and a wireless Wi-Fi with the IEEE 802.11 standard can be used for this purpose. One end of the twisted pair cable is plugged into switches using 'RJ-45 connectors' whereas the other end is plugged to a computer or in another network. All new routers use the b/g/n IEEE 802.11 standards. The 'b' and 'g' operate in the 2.4 GHz spectrum, and 'n' operates in 2.4 and 5.0 GHz which allows better performance and less interference.

Computers and servers (provides services to other computers like printing, file storage and sharing) can connect to each other via cables or wirelessly in a same LAN. Wireless access in conjunction with wired network is made possible by Wireless Access Point (WAP). Devices with WAP functionality provide a bridge between computers and networks. A WAP is able to connect hundreds or even more of wireless users to a network. Servers in a LAN are mostly connected by a wire since it is still the fastest medium for network communication. But for workstations (Desktop, laptops, etc.) wireless medium is a more suitable choice, since at some point it is difficult and expensive to add new workstations into an existing system already having complex network wiring.

Token Ring and Fiber Distributed Data Interface (FDDI)

With Ethernet, 'Token Ring' and 'Fiber Distributed Data Interface (FDDI)' are also considered the major 'Local Area Network' technologies. In Token Ring network all computers are connected in a ring or star topology for prevention of data collision and with a data transfer rates of either 4 or 16 megabits per second by IEEE 802.5 standard version. In FDDI for data transmission optic fiber are used that extend the range of a LAN up to 200km and supports thousands of user.

Wide Area Network (WAN)

Wide Area Network is a computer network that covers relatively larger geographical area such as a state, province or country. It provides a solution to companies or organizations operating from distant geographical locations who want to communicate with each other for sharing and managing central data or for general communication.

WAN is made up of two or more Local Area Networks (LANs) or Metropolitan Area Networks (MANs) that are interconnected with each other, thus users and computers in one location can communicate with users and computers in other locations.

In 'Wide Area Network', Computers are connected through public networks, such as the telephone systems, fiber-optic cables, and satellite links or leased lines. The 'Internet' is the largest WAN in a world. WANs are mostly private and are building for a particular organization by 'Internet Service Providers (ISPs)' which connects the LAN of the organization to the internet. WANs are frequently built using expensive leased lines where with each end of the leased line a router is connected to extend the network capability across sites. For low cost solutions, WAP is also built using a 'circuit switching' or 'packet switching' methods.

Metropolitan Area Network (MAN)

A Metropolitan Area Network (MAN) is a network that connects two or more computers, communicating devices or networks in a single network that has geographic area larger than that covered by even a large 'Local Area Network' but smaller than the region covered by a 'Wide Area Network'. MANs are mostly built for cities or towns to provide a high data connection and usually owned by a single large organization.

A Metropolitan Area Networks bridges a number of 'Local Area Networks' with a fiber-optical links which act as a backbone, and provides services similar to what Internet Service Provider (ISP) provide to Wide Area Networks and the Internet.

Major technologies used in MAN networks are 'Asynchronous Transfer Mode (ATM)', 'Fiber Distributed Data Interface (FDDI)' and 'Switched Multi-megabit Data Service (SMDS, a connectionless service)'. In most of the areas, these technologies are used to replace the simple 'Ethernet' based connections. MANs can bridge Local Area Networks without any cables by using microwave, radio wireless communication or infra-red laser which transmits data wirelessly.

'Distributed Queue Dual Bus (DQDB)' is the Metropolitan Area Network (MAN) IEEE 802.6 standard for data communication. Using DQDB, networks can extend up to 100km-160km and operate at speeds of 44 to 155Mbps.

Conclusion: - Depending upon physical area covered networks can be categories.

EXPERIMENT NO.5

Aim: Study of errors & error correction Techniques.

Theory: Computers on a network must be able to detect when data packets have been damaged in transmission. In order to detect these errors, computers on an Ethernet network attach a special code to each of its packets. When the Ethernet packets are created, the sending computer runs the data through a special mathematic formula and attaches the result called a Cyclic Redundancy Code, or CRC to the packet. The receiving computer then opens the packet, performs the same calculations and compares its answer with the answer included with the packet. If the CRC codes do not match, then the receiving computer asks the sending machine to retransmit the packet again. By keeping the packets small, this reduces the time that is required to retransmit the data following an error.

Error detection is most commonly realized using a suitable hash function (or checksum algorithm). A hash function adds a fixed-length *tag* to a message, which enables receivers to verify the delivered message by recomputing the tag and comparing it with the one provided.

There exists a vast variety of different hash function designs. However, some are of particularly widespread use because of either their simplicity or their suitability for detecting certain kinds of errors (e.g., the cyclic redundancy check's performance in detecting burst errors).

A random-error-correcting code based on minimum distance coding can provide a strict guarantee on the number of detectable errors, but it may not protect against a pre image attack. A repetition code, described in the section below, is a special case of error-correcting codes: although rather inefficient, a repetition code is suitable in some applications of error correction and detection due to its simplicity.

Repetition codes

A *repetition code* is a coding scheme that repeats the bits across a channel to achieve error-free communication. Given a stream of data to be transmitted, the data are divided into blocks of bits. Each block is transmitted some predetermined number of times. For example, to send the bit pattern "1011", the four-bit block can be repeated three times, thus producing "1011 1011 1011". However, if this twelve-bit pattern was received as "1010 1011 1011" – where the first block is unlike the other two – it can be determined that an error has occurred.

A repetition code is very inefficient, and can be susceptible to problems if the error occurs in exactly the same place for each group (e.g., "1010 1010 1010" in the previous

example would be detected as correct). The advantage of repetition codes is that they are extremely simple, and are in fact used in some transmissions of numbers stations.[5][6]

Parity bits[

A parity bit is a bit that is added to a group of source bits to ensure that the number of set bits (i.e., bits with value 1) in the outcome is even or odd. It is a very simple scheme that can be used to detect single or any other odd number (i.e., three, five, etc.) of errors in the output. An even number of flipped bits will make the parity bit appear correct even though the data is erroneous.

Extensions and variations on the parity bit mechanism are horizontal redundancy checks, vertical redundancy checks, and "double," "dual," or "diagonal" parity (used in RAID-DP).

Checksums

A checksum of a message is a modular arithmetic sum of message code words of a fixed word length (e.g., byte values). The sum may be negated by means of a ones'-complement operation prior to transmission to detect errors resulting in all-zero messages.

Checksum schemes include parity bits, check digits, and longitudinal redundancy checks. Some checksum schemes, such as the Damm algorithm, the Luhn algorithm, and the Verhoeff algorithm, are specifically designed to detect errors commonly introduced by humans in writing down or remembering identification numbers.

Conclusion: Thus we have studied errors & error correction Techniques

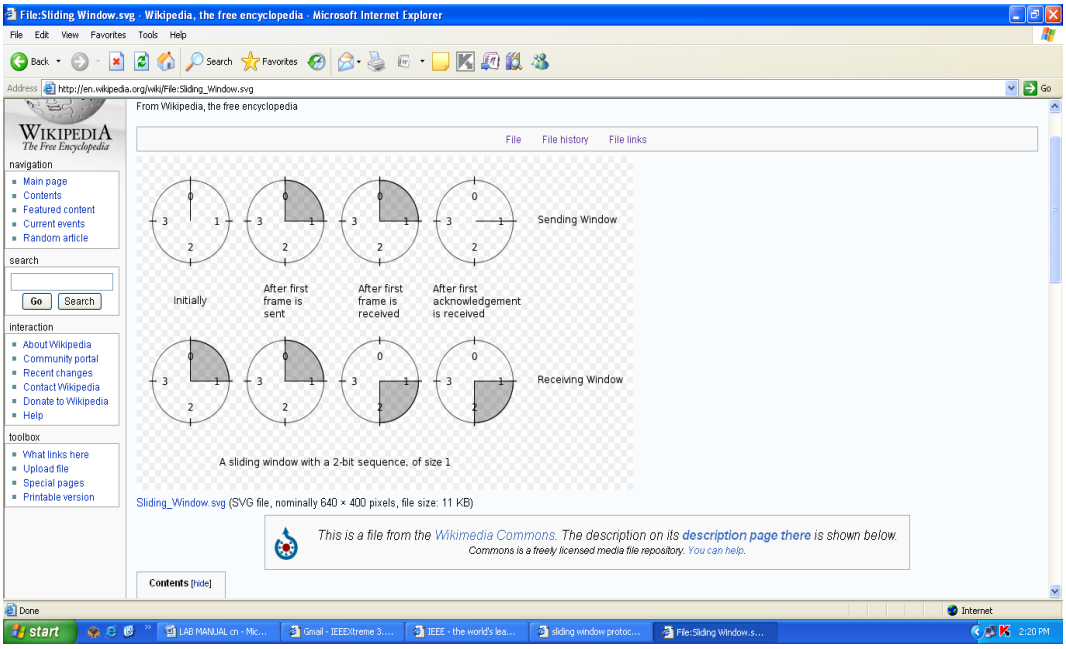
EXPERIMENT NO.6

Aim: Study of sliding window protocol.

Theory: At any instant of time, the sender maintains a set of sequence numbers which correspond to the frames it is permitted to send. Such frames are said to be a set of the *sending window*. Similarly, the receiver also maintains a *receiving window* which indicates the set of frames it is allowed to receive.

A window can be visualised as a circle divided into (2^n) – 1 part where n is the number of bits required to represent, in binary, the maximum sequence number in a given sequence of packets.

The upper and lower edges of a sending window indicate the set of packets which are allowed to be sent but have not been acknowledged. The upper and lower edges of a receiving window indicate the set of packets it may accept.



Conclusion : Thus we have studied working of Sliding window protocol.

EXPERIMENT NO.7

Aim: Study of windows socket programming (UDP&TCP).

Theory: The User Datagram Protocol (UDP) is one of the core members of the Internet Protocol Suite, the set of network protocols used for the Internet. With UDP, computer applications can send messages, in this case referred to as datagram's, to other hosts on an Internet Protocol (IP) network without requiring prior communications to set up special transmission channels or data paths. UDP is sometimes called the Universal Datagram Protocol. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet Protocol Suite. TCP is one of the two original components of the suite (the other being Internet Protocol, or IP), so the entire suite is commonly referred to as *TCP/IP*. Whereas IP handles lower-level transmissions from computer to computer as a message makes its way across the Internet, TCP operates at a higher level, concerned only with the two end systems, for example a Web browser and a Web server. In particular, TCP provides reliable, ordered delivery of a stream of bytes from a program on one computer to another program on another computer. Besides the Web, other common applications of TCP include e-mail and file transfer. Among its other management tasks, TCP controls segment size, flow control, the rate at which data is exchanged, and network traffic congestion.

Conclusion: Thus we have studied UDP & TCP.

EXPERIMENT NO.8

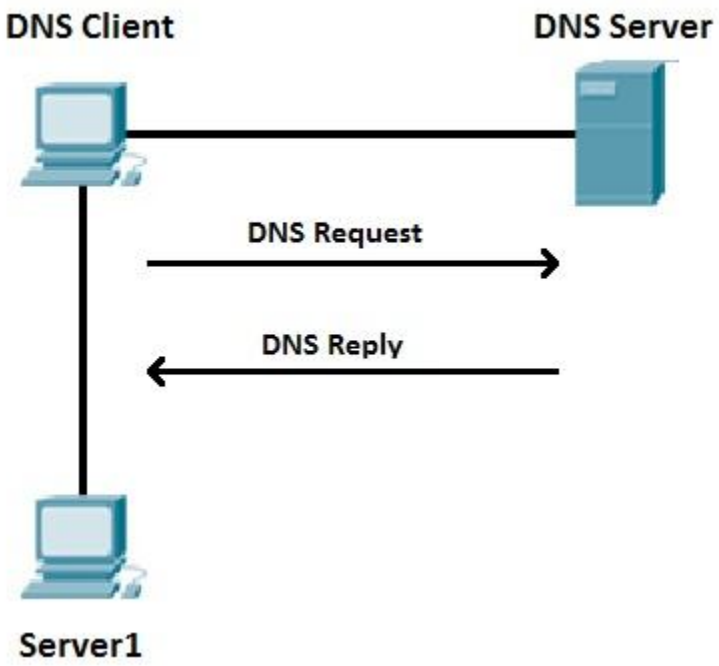
Aim: Study of DNS, WWW and Electronic mail

Theory: - DNS (Domain Name System)

DNS is a network protocol used to translate hostnames into IP addresses. DNS is not required to establish a network connection, but it is much more user friendly for human users than the numeric addressing scheme. Consider this example. You can access the Google homepage by typing 74.125.227.99, but it's much easier just to type www.google.com!

To use DNS, you must have a DNS server configured to handle the resolution process. A DNS server has a special-purpose application installed. The application maintains a table of dynamic or static hostname-to-IP address mappings. When a user request some network resource using a hostname, (for example by typing www.google.com in a browser), a DNS request is sent to the DNS server asking for the IP address of the hostname. The DNS server then replies with the IP address. The user's browser can now use that IP address to accesswww.google.com.

The figure below explains the concept:



Suppose that the DNS Client wants to communicate with the server named Server1. Since the DNC Client doesn't know the IP address of Server1, it sends a DNS Request to the DNS Server, asking for Server1's IP address. The DNS Server replies with the IP address of Server1 (DNS Reply).

The **World Wide Web** (**WWW**) is an open source information space where documents and other web resources are identified by URLs, interlinked by hyper text links, and can be accessed via the Internet.[1] It has become known simply as **the Web**. The World Wide Web was central to the development of the Age and is the primary tool billions of people use to interact on the Internet.

The World Wide Web was invented by English scientist Tim Berners-Lee in 1989. He wrote the first web browser in 1990 while employed at CERN in Switzerland.

Web pages are primarily text documents formatted and annotated with Hypertext Markup Language (HTML). In addition to formatted text, web pages may contain images, video, and software components that are rendered in the user's web browser as coherent pages of multimedia content. Embedded hyperlinks permit users to navigate between web pages. Multiple web pages with a common theme, a common domain name, or both, may be called a *website*. Website content can largely be provided by the publisher or interactive where users contribute content or the content depends upon the user or their actions. Websites may be mostly informative, primarily for entertainment, or largely for commercial purposes.

Electronic mail, most commonly called **email** or **e-mail** since around 1993, is a method of exchanging digital messages from an author to one or more recipients. Email operates across the Internet or other computer networks.

Some early email systems required the author and the recipient to both is online at the same time, in common with instant messaging. Today's email systems are based on a store-and-forward model. Email servers accept, forward, deliver, and store messages. Neither the users nor their computers are required to be online simultaneously; they need connect only briefly, typically to a mail server, for as long as it takes to send or receive messages.

Historically, the term electronic mail was used generically for any electronic document transmission. For example, several writers in the early 1970s used the term to describe fax document transmission. As a result, it is difficult to find the first citation for the use of the term with the more specific meaning it has today.

An Internet email message consists of three components, the message envelope, the message header, and the message body. The message header contains control information, including, minimally, an originator's email address and one or more recipient addresses.

Usually descriptive information is also added, such as a subject header field and a message submission date/time stamp.

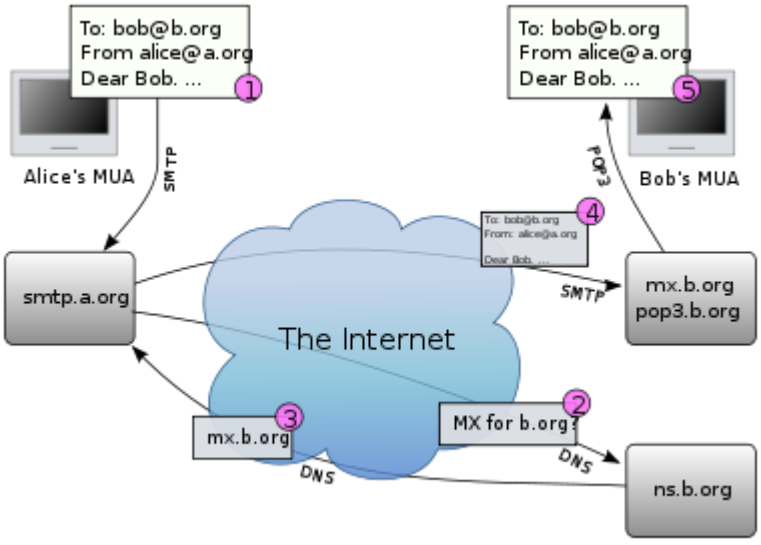
Originally an ASCII text-only communications medium, Internet email was extended by Multipurpose Internet Mail Extensions (MIME) to carry text in other character sets and multi-media content attachments. International email, with internationalized email addresses using UTF-8, has been standardized, but not yet widely adopted.

Electronic mail predates the inception of the Internet and was in fact a crucial tool in creating it, but the history of modern, global Internet email services reaches back to the early ARPANET. Standards for encoding email messages were proposed as early as 1973 (RFC 561). Conversion from ARPANET to the Internet in the early 1980s produced the core of the current services. An email message sent in the early 1970s looks quite similar to a basic text message sent on the Internet today.

Email is an information and communications technology. It uses technology to communicate a digital message over the Internet. Users use email differently, based on how they think about it. There are many software platforms available to send and receive. Popular email platforms include Gmail, Hotmail, Yahoo! Mail, Outlook, and many others.

Network-based email was initially exchanged on the ARPANET in extensions to the File Transfer Protocol (FTP), but is now carried by the Simple Mail Transfer Protocol (SMTP), first published as Internet standard 10 (RFC 821) in 1982. In the process of transporting email messages between systems, SMTP communicates delivery parameters using a message envelope separate from the message (header and body) itself.

The diagram to the right shows a typical sequence of events that takes place when sender Alice transmits a message using a mail user agent (MUA) addressed to the email



address of the recipient.

- The MUA formats the message in email format and uses the submission protocol, a profile of the Simple Mail Transfer Protocol (SMTP), to send the message to the local mail submission agent (MSA), in this case *smtp.a.org*.
- The MSA determines the destination address provided in the SMTP protocol (not from the message header), in this case *bob@b.org*. The part before the @ sign is the *local part* of the address, often the username of the recipient, and the part after the @ sign is a domain name. The MSA resolves a domain name to determine the fully qualified domain name of the mail server in the Domain Name System (DNS).
- The DNS server for the domain *b.org* (*ns.b.org*) responds with any MX records listing the mail exchange servers for that domain, in this case *mx.b.org*, a message transfer agent (MTA) server run by the recipient's ISP.
- smtp.a.org sends the message to mx.b.org using SMTP. This server may need to forward the message to other MTAs before the message reaches the final message delivery agent (MDA).
- The MDA delivers it to the mailbox of user *bob*.
- Bob's MUA picks up the message using either the Post Office Protocol (POP3) or the Internet Message Access Protocol (IMAP).

In addition to this example, alternatives and complications exist in the email system:

- Alice or Bob may use a client connected to a corporate email system, such as IBM Lotus Notes or Microsoft Exchange. These systems often have their own internal email format and their clients typically communicate with the email server using a vendor-specific, proprietary protocol. The server sends or receives email via the Internet through the product's Internet mail gateway which also does any necessary reformatting. If Alice and Bob work for the same company, the entire transaction may happen completely within a single corporate email system.
- Alice may not have a MUA on her computer but instead may connect to a webmail service.
- Alice's computer may run its own MTA, so avoiding the transfer at step 1.
- Bob may pick up his email in many ways, for example logging into mx.b.org and reading it directly, or by using a webmail service.
- Domains usually have several mail exchange servers so that they can continue to accept mail even if the primary is not available.

Many MTAs used to accept messages for any recipient on the Internet and do their best to deliver them. Such MTAs are called *open mail relays*. This was very important in the early days of the Internet when network connections were unreliable. However, this mechanism proved to be exploitable by originators of unsolicited bulk email and as a consequence open mail relays have become rare, and many MTAs do not accept messages from open mail relays.

Conclusion: - DNS, WWW and Electronic mail these are basics of computer communication network.

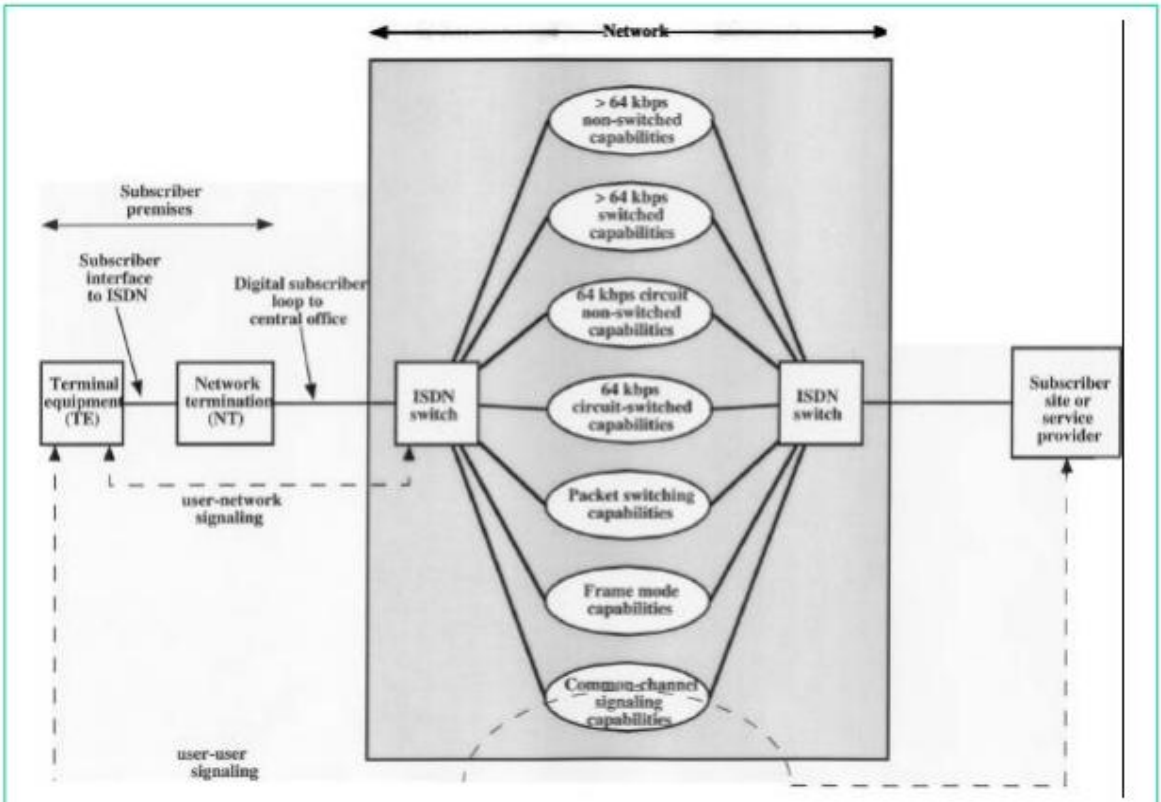
EXPERIMENT NO.9

Aim: Study of Integrated services Digital Network (ISDN)

Theory:-Integrated Services for Digital Network (ISDN) is a set of communication standards for simultaneous digital transmission of voice, video, data, and other network services over the traditional circuits of the public switched telephone network. It was first defined in 1988 in the CCITT red book. Prior to ISDN, the telephone system was viewed as a way to transport voice, with some special services available for data. The key feature of ISDN is that it integrates speech and data on the same lines, adding features that were not available in the classic telephone system. There are several kinds of access interfaces to ISDN defined as Basic Rate Interface (BRI), Primary Rate Interface (PRI),Narrowband ISDN(N-ISDN), and Broadband ISDN(B-ISDN).

ISDN is a circuit-switched telephone network system, which also provides access to packet switched networks, designed to allow digital transmission of voice and data over ordinary telephone copper wires, resulting in potentially better voice quality than analog phone can provide. It offers circuit-switched connections (for either voice or data), and packet-switched connections (for data), in increments of 64 kilobit/s. A major market application for ISDN in some countries is Internet access, where ISDN typically provides a maximum of 128 kbit/s in both upstream and downstream directions. Channel bonding can achieve a greater data rate; typically the ISDN B-channels of three or four BRIs (six to eight 64 k bit/s channels) are bonded.

ISDN supports a new physical connector for users, a digital subscriber line, and a variety of transmission services. Physical interface provides a standardized means of attaching to the network. The interface supports a basic service consisting of three time multiplexed channels, two at 64 kbps and one at 16 kbps. In addition, there is a primary service that provides multiple 64- kbps channels. For both basic and primary service, an interface is defined between the customer's equipment (TE) and a device on the customer's premises, known as a network termination (NT).



ISDN architecture

- The subscriber line is the physical path from the subscriber's NT to the ISDN central office. ISDN central office connects subscriber lines to the digital network, providing access to lower-layer transmission facilities: – Circuit-switched capabilities. same facility provided by other digital-switched Telecom. net's (64 kbps) – Non-switched capabilities. A 64 kbps dedicated link, higher rates in B-ISDN using PVC in ATM tx – Switched capabilities. high speed (>64 kbps) switched connections using ATM in B-ISDN – Packet-switched capabilities Resembles packet-switched service provided by other data networks – Frame-mode capabilities. A service that supports frame relay – Common-channel signalling capabilities used to control the network and provide call management

Conclusion: Thus we have studied ISDN.

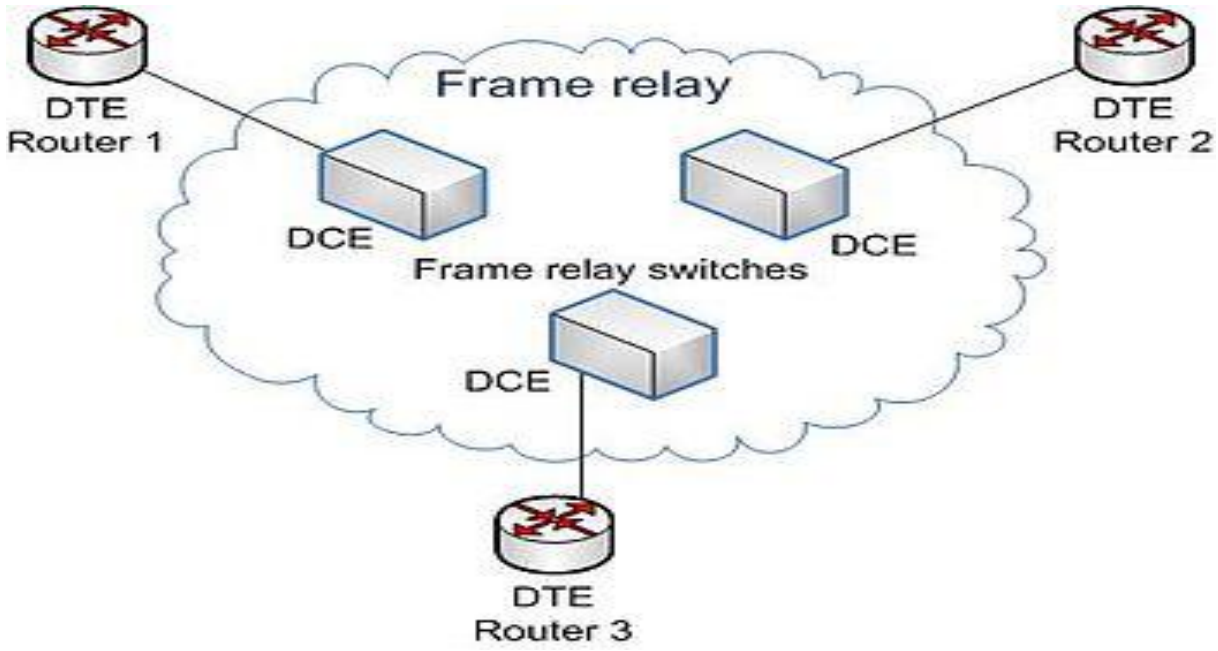
EXPERIMENT NO.10

Aim: Study of Frame relay

Theory: - Frame Relay is a standardized wide area network technology that specifies the physical and logical link layers of digital telecommunications channels using a packet switching methodology. Originally designed for transport across Integrated Services Digital Network (ISDN) infrastructure, it may be used today in the context of many other network interfaces.

Network providers commonly implement Frame Relay for voice (VoFR) and data as an encapsulation technique, used between local area networks (LANs) over a wide area network (WAN). Each end-user gets a private line (or leased line) to a Frame Relay node. The Frame Relay network handles the transmission over a frequently changing path transparent to all end-user extensively used WAN protocols. It is less expensive than leased lines and that is one reason for its popularity. The extreme simplicity of configuring user equipment in a Frame Relay network offers another reason for Frame Relay's popularity.

With the advent of Ethernet over fiber optics, MPLS, VPN and dedicated broadband services such ascable modem and DSL, the end may loom for the Frame Relay protocol and encapsulation. However many rural areas remain lacking DSL and cable modem services. In such cases, the least expensive type of non-dial-up connection remains a 64-kbit/s Frame Relay line. Thus a retail chain, for instance, may use Frame Relay for connecting rural stores into their corporate WAN.



The designers of Frame Relay aimed to provide a telecommunication service for cost-efficient data transmission for intermittent traffic between local area networks (LANs) and between end-points in a wide area network (WAN). Frame Relay puts data in variable-size units called "frames" and leaves any necessary error-correction (such as retransmission of data) up to the end-points. This speeds up overall data transmission. For most services, the network provides a permanent virtual circuit (PVC), which means that the customer sees a continuous, dedicated connection without having to pay for a full-time leased line, while the service-provider figures out the route each frame travels to its destination and can charge based on usage.

An enterprise can select a level of service quality, prioritizing some frames and making others less important. Frame Relay can run on fractional T-1 or full T-carrier system carriers (outside the Americas, E1 or full E-carrier). Frame Relay complements and provides a mid-range service between basic rate ISDN, which offers bandwidth at 128 kbit/s, and Asynchronous Transfer Mode (ATM), which operates in somewhat similar fashion to Frame Relay but at speeds from 155.520 Mbit/s to 622.080 Mbit/s.[1]

Frame Relay has its technical base in the older X.25 packet-switching technology, designed for transmitting data on analog voice lines. Unlike X.25, whose designers expected analog signals with a relatively high chance of transmission errors, Frame Relay is a fast packet switching technology operating over links with a low chance of transmission errors (usually practically lossless like PDH), which means that the protocol does not attempt to correct errors. When a Frame Relay network detects an error in a frame, it simply drops that frame. The end points have the responsibility for detecting and retransmitting dropped frames. (However digital networks offer an incidence of error extraordinarily small relative to that of analog networks.)

Frame Relay often serves to connect local area networks (LANs) with major backbones, as well as on public wide-area networks (WANs) and also in private network environments with leased lines over T-1 lines. It requires a dedicated connection during the transmission period. Frame Relay does not provide an ideal path for voice or video transmission, both of which require a steady flow of transmissions. However, under certain circumstances, voice and video transmission do use Frame Relay.

Frame Relay originated as an extension of integrated services digital network (ISDN). Its designers aimed to enable a packet-switched network to transport over circuit-switched technology. The technology has become a stand-alone and cost-effective means of creating a WAN.

Frame Relay switches create virtual circuits to connect remote LANs to a WAN. The Frame Relay network exists between LAN border devices, usually a router, and the carrier switch. The technology used by the carrier to transport data between the switches is variable and may differ among carriers (i.e., to function, a practical Frame Relay implementation need not rely solely on its own transportation mechanism).

The sophistication of the technology requires a thorough understanding of the terms used to describe how Frame Relay works. Without a firm understanding of Frame Relay, it is difficult to troubleshoot its performance.

Frame-relay frame structure essentially mirrors almost exactly that defined for LAP-D. Traffic analysis can distinguish Frame Relay format from LAP-D by its lack of a control field.

Conclusion: - Frame relay is one of standard used for wide area network but it is originally designed for Integrated Services Digital Network (ISDN) infrastructure.

EXPERIMENT NO.11

Aim: Study of Asynchronous Transfer Mode (ATM).

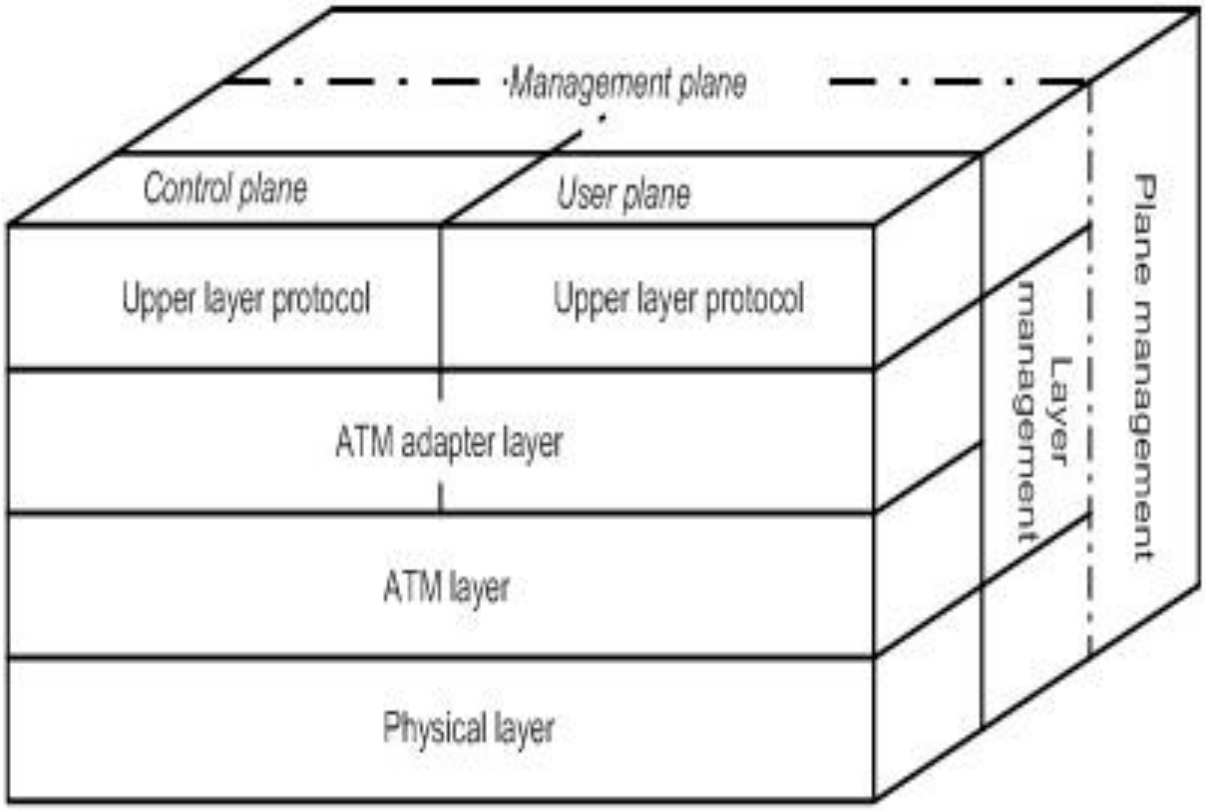
Theory: - ATM: Asynchronous Transfer Mode (ATM) is a standard switching technique designed to unify telecommunication and computer networks.

ATM uses a connection-oriented model in which a virtual circuit must be established between two endpoints before the actual data exchange begins.

ATM is a packet network. It supports multiplexing of various signals over the same physical channel. It has been design to deliver voice, data and video information. Medium: ATM network is capable of supporting high data rates up to 155 Mbps (approx) so Transmission medium used for ATM is optical Fibers instead of coaxial cables in order to support high data rates.

Limitations: ATM does not provide any error control or flow control at data link layer.

AS asynchronous TDM is used in it so the empty slot does not appears on the output line of multiplexer.



ATM provides Real time and Non real time services. Services provided as Service using the constant bit rate, compressed voice and video, IP based services available bit rate (ABR) and unspecified bit rate (UBR) services. Fixed packet size .By using small fixed length cells the ATM becomes so efficient that it can offer a constant data rate even though it is using packet switching techniques. ATM uses fixed length of packets that are known as cell.ATM cell packet size or cell size is 53 octets (bytes).In this Header is 5 bytes long and 48 bytes are reserved to carry the data. If the input is in the form of longs packets they are converted in small 53 bytes long ATM cells. One advantage of that is since all the packets are of same size, no packet has to wait, this avoids the introduction of delays.

Why cell size is 53 Bytes:

During the standardization process a conflict arose within the CCITT as to the payload size within an ATM cell. The US wanted 64 byte payloads because it was felt optimal for US networks. The Europeans and Japanese wanted 32 payloads because it was optimal for them. In the end 48 bytes was chosen as a compromise. So 48 bytes payload plus 5 bytes header is 53 bytes total.

ATM Protocol Architecture:

The physical layer of the protocol involves the specifications of a transmission medium and signal encoding scheme. The date rate specified at this layer is b/w 25.6 Mbps and 622.08 Mbps, but it can be higher and lower than these possibly

ATM Layer: This layer defines the transmission of data in fixed size cell and it also defines the logical connections.

ATM AAL Layer (ATM ADAPTIVE LAYER): This layer is service dependent layer nd used for supporting the information transfer protocol not based on ATM. THE AAl maps the higher layer information into the ATM cell and cell is transported over the ATM network

USER Plain: It is used for transferring user information along with associated control such as flow control, error control etc.

Control Plain: It is supported to perform the call control and connection control functions.

Management Plain: It includes the management .The management plain performs management functions related to a function related to a system they include.

- Provision of co-ordination b/w all plains.
- Layer Management.
- .Management functions relating to resources and parameter in its protocol entities.

Applications: TM is a core protocol used over the SONET/SDH, backbone of the public switched telephone network (PSTN) and Integrated Services Digital Network (ISDN), but its use is declining in favor of All IP.

It is also used in non-ISDN systems where the data rates are very high.

Conclusion: - Asynchronous transfer mode is used in both computer networks as well as in communication to establish connection between two endpoints before the actual data exchange begins.

EXPERIMENT NO.12

Aim: Write a program in C for PC to PC communication using RS232 port.

Components required: RS-232D connecter, Two computers.

Theory: What is NULL MODEM?

Null modem is used to connect two DTE's together. This is used to transfer files between the computers using protocols like Zmodem protocol, xmodem protocol, etc

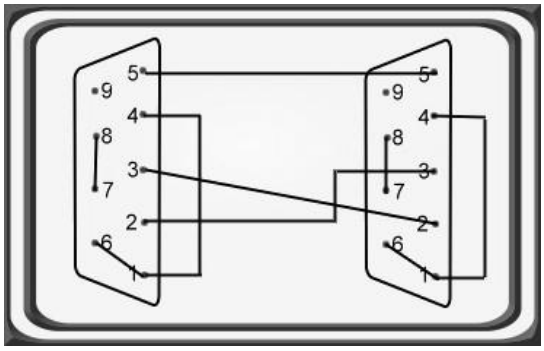


Figure: Connections of the Null modem using RS-232D connecter

Above-mentioned figure shows the wiring of the null modem. The main feature indicated here is that the to make the computer to chat with the modem rather than another computer. The guest & host computer connected through the TD, RD, and SG pins. Any data that is transmitted through TD line from the Host to Guest is received on RD line. The Guest computer must have the same setup as the Host. The signal ground (SG) line of the both must be shorted so that grounds are common to each computer.

The Data Terminal Ready (DTR) is looped back to Data Set Ready and Carrier Detect on both computers. When the Data Terminal Ready is asserted active, then the Data Set Ready and Carrier Detect immediately become active. At this point, the computer thinks the Virtual Modem to which it is connected is ready and has detected the carrier of the other modem.

The Ring indicator line is only used to tell the computer that there is a ringing signal on the phone line. As we do not have, a modem connected to the phone line this is left disconnected

Note: To know about the RS232 ports available in your computer, Right click on "My Computer", Goto 'Properties', Select tab 'Device Manager', go to Ports(COM & LPT), In that you will find 'Communication Port(Com1)' etc. If you right click on that and go to properties, you will get device status. Make sure that you have enabled the port (Use this port is selected).

D-Type-9 pin no.	D-Type-25 pin no.	Pin outs	Function
3	2	RD	Receive Data (Serial data input)
2	3	TD	Transmit Data (Serial data output)
7	4	RTS	Request to send (acknowledge to modem that UART is ready to exchange data
8	5	CTS	Clear to send (i.e.; modem is ready to exchange data)
6	6	DSR	Data ready state (UART establishes a link)
5	7	SG	Signal ground
1	8	DCD	Data Carrier detect (This line is active when modem detects a carrier
4	20	DTR	Data Terminal Ready.
9	22	RI	Ring Indicator (Becomes active when modem detects ringing signal from PSTN

Table: R S 232 D connector pin description

```
#include <bios.h>
#include <conio.h>
#define COM1       0
#define DATA_READY 0x100
#define SETTINGS ( 0x80 | 0x02 | 0x00 | 0x00)
int main(void)
{
  int in, out, status;
  bioscom(0, SETTINGS, COM1); /*initialize the port*/
  cprintf("Data sent to you:  ");
  while (1)
  {
    status = bioscom(3, 0, COM1); /*wait until get a data*/
    if (status & DATA_READY)
        if ((out = bioscom(2, 0, COM1) & 0x7F) != 0)  /*input a data*/
          putch(out);
        if (kbhit())
        {
          if ((in = getch()) == 27)   /* ASCII of Esc*/
            break;
          bioscom(1, in, COM1);   /*output a data*/
        }
  }
  return 0;
}
```

Result: Write the output of the program

Conclusion: In this way we have performed program in C for PC to PC communication using RS232 port

3. Quiz on the Subject

1. What are the different layers of TCP/IP protocol suite?
2. Compare between TCP/IP and OSI model?
3. Explain IGMP & ICMP.
4. Explain LAN standards IEEE802.x.
5. Explain different techniques of error correction Techniques CRC and ARQ
6. Explain the working of Sliding window protocol.
7. Explain UDP and TCP.
8. What is Proxy Server?
9. What are the perquisites to configure server?
10. What are the criteria necessary for an effective and efficient network?

4. Conduction of VIVA-VOCE Examinations: -

Teacher should conduct oral exams of the students with full preparation. Normally the objective questions with guess are to be avoided. To make it meaningful, the questions should be such that depth of the student in the subject is tested. Oral Exams are to be conducted in co-cordial situation. Teachers taking oral exams should not have ill thoughts about each other & courtesies should be offered to each other in case of opinion, which should be critically suppressed in front of the students.

5. Evaluation and marking system: -

Basic honesty in the evaluation and marking system is essential and in the process impartial nature of the evaluator is required in the exam system. It is a primary responsibility of the teacher to see that right students who really put their effort &intelligence are correctly awarded.

The marking pattern should be justifiable to the students without any ambiguity and teacher should see that students are faced with just circumstance.