LNCT SM
GROUP OF COLLEGES
"WORKING TOWARDS BEING THE BEST"

Name of Student: _____

Enrolment No.: _____

Class: _____

Section: _____

Session: _____

Data Communication Lab

[EC-605]Manual

Department of Electronics and Communication Engineering
LAKSHMI NARAIN COLLEGE OF TECHNOLOGY EXCELLENCE BHOPAL
Kalchuri Nagar, Raisen Road Bhopal (MP) 462023

Vision and Mission of the Department

Vision

To become reputed in providing technical education in the field of electronics and communication engineering and produce technocrats working as leaders.

Mission

- To provide congenial academic environment and adopting innovative learning process.
- To Keep valuing human values and transparency while nurturing the young engineers.
- To strengthen the department by collaborating with industry and research organization of repute.
- To facilitate the students to work in interdisciplinary environment and enhance their skills for employ ability and entrepreneurship.

Program Specific Outcomes (PSO's)

- PSO1: Analyze specific engineering problems relevant to Electronics & Communication Engineering by applying the knowledge of basic sciences, engineering mathematics and engineering fundamentals.
- PSO2: Apply and transfer interdisciplinary systems and engineering approaches to the various areas, like Communications, Signal processing, VLSI and Embedded system, PCB Designing.
- PSO3: Inculcate the knowledge of Engineering and Management principles to meet demands of industry and provide solutions to the current real time problems
- PSO4: Demonstrate the leadership qualities and strive for the betterment of organization, environment and society

Program Educational Objectives (PEO's)

Student will be able to

- Recognize and apply appropriate experimental and scientific skills to solve real world problems to create innovative products and systems in the field of electronics and communication engineering.
- To evolve graduates with ability to apply, analyze, design in electronics & Communication System.
- Motivate graduates to become responsible citizens with moral & ethical values for the welfare of Society.
- Inculcate the habit of team work with professional quality of leadership to become successful contributors in industry and/ or entrepreneurship in view of Global & National status of technology.

Course: DATA COMM. LAB (EC605)

Course Outcomes (CO's)

CO1. Connect computers in local area network

CO2. Encode given signal in various line encoding technique using MATLAB

CO3. Generate CRC code for the given data bit and the divisor using MATLAB

CO4. Plot Efficiency of Pure Aloha and slotted Aloha using MATLAB

CO5.Plot Channel Efficiency for Ethernet in MATLAB

Code of Conducts for the Laboratory

- All bags must be left at the indicated place.
- The lab timetable must be strictly followed.
- Be **PUNCTUAL** for your laboratory session.
- Noise must be kept to a minimum.
- Workspace must be kept clean and tidy at all time.
- Handle the experiment kit and interfacing its with care.
- All students are liable for any damage to the accessories due to their own negligence.
- Students are strictly **PROHIBITED** from taking out any items from the laboratory.
- Students are **NOT** allowed to work alone in the laboratory without the Lab Supervisor
- Report immediately to the Lab Supervisor if any malfunction of the accessories, is there.
- Before leaving the lab Place the stools properly.
- Please check the laboratory notice board regularly for updates.

INDEX

Name of Student:_____ Enrolment No.:_____

Sl. No.	Title of the Experiment	Date of Experiment	Date of Submission	Remark
1	To establish link between two PC and transfer packet.			
2	To establish link between two PC and transfer information using command prompt.			
3	To establish link between two ends of pc using hub and switch to transfer information.			
4	Implementation of LAN and Hybrid topology.			
5	To study about different physical equipment used for networking.			
6	To Study OSI reference model and TCP/IP reference model			
7	To Study parallel and Serial Transmission			
8	Study of digital interface rs-232			
9	To Study NIC Card			
10	To study of different switching technique.			

EXPERIMENT-01

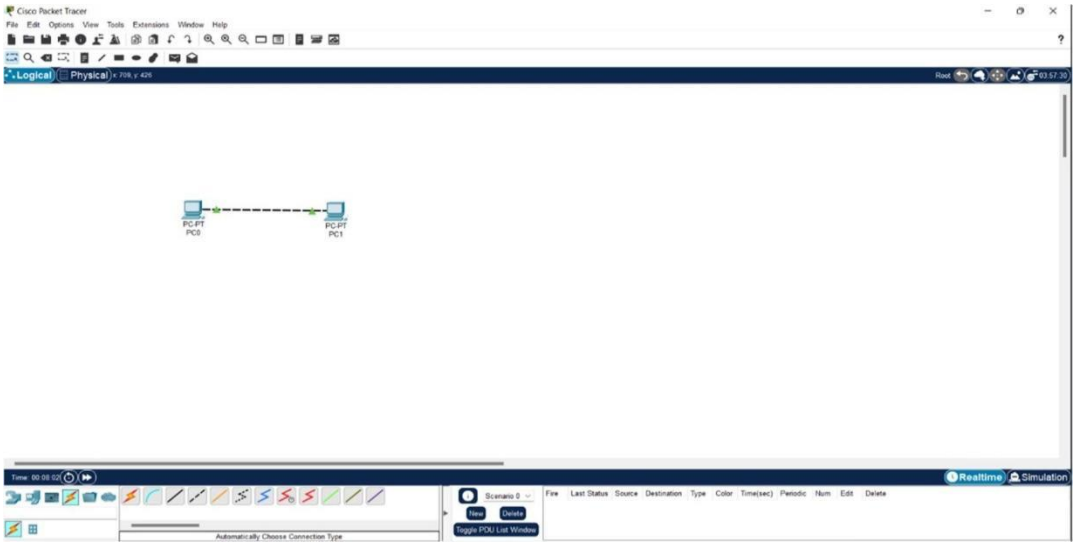
AIM: - To establish link between two PC and transfer packet.

APPARATUS: - Cisco Packet Tracer.

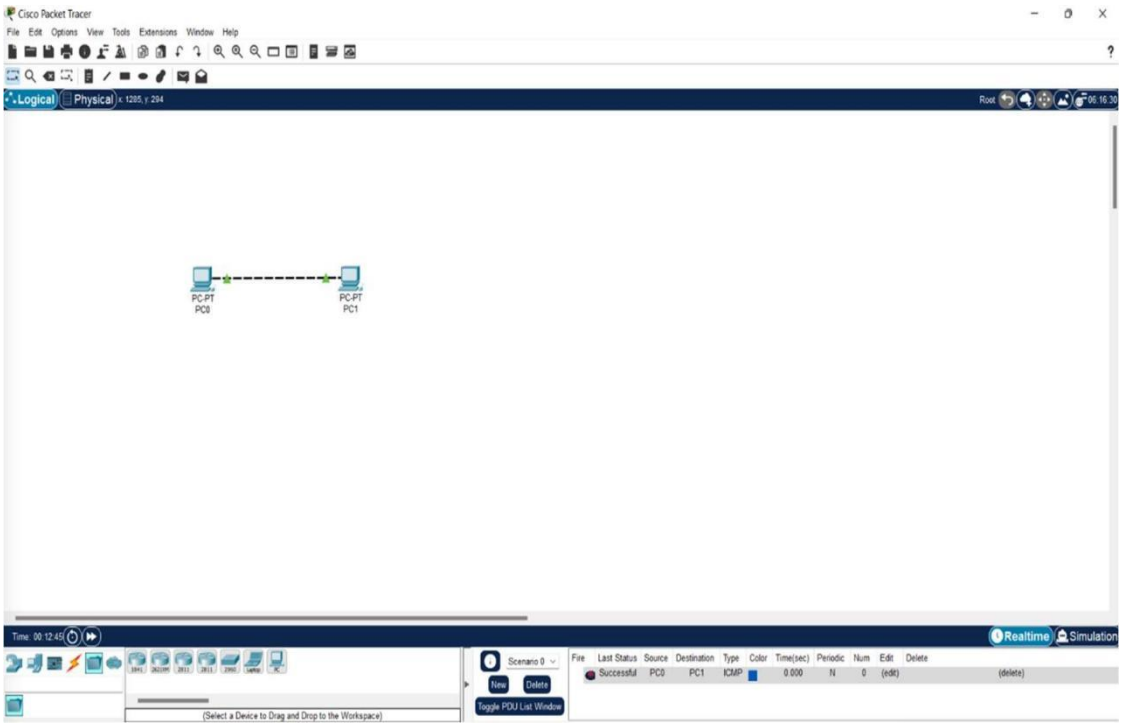
PROCEDURE: -

- Start the desktop or laptop.
- Click on the logo of Packet Tracer and blank screen with all specification will be displayed.
- Click on end devices displayed on the cisco packet tracer page.
- Select the generic option which will provide two pcs (PC0, PC1).
- Connect PC0, PC1 with connection lines provided in the system.
- Configure the IP address of both the pcs with IP address 10.0.0.1,10.0.0.2 and to send message click on the last second option on the right-side corner of the window.
- It will show Successful setup of pc (PC0, PC1) with ICMP protocol and take the screenshot of those pictures and paste it.
- This was the one method of connecting the link and there is another format for connection.
- After the deletion of first method click on the right-side corner where simulation option is available and select simulation option.
- Click on the edit filter and remove all selected filter and click on the ICMP protocol option.
- To send message on both the pc with the help of drag option and click on the auto capture option which will show all the result of message transferring and receiving with successful link connection.
- Take the screenshot of those pictures and paste it here.

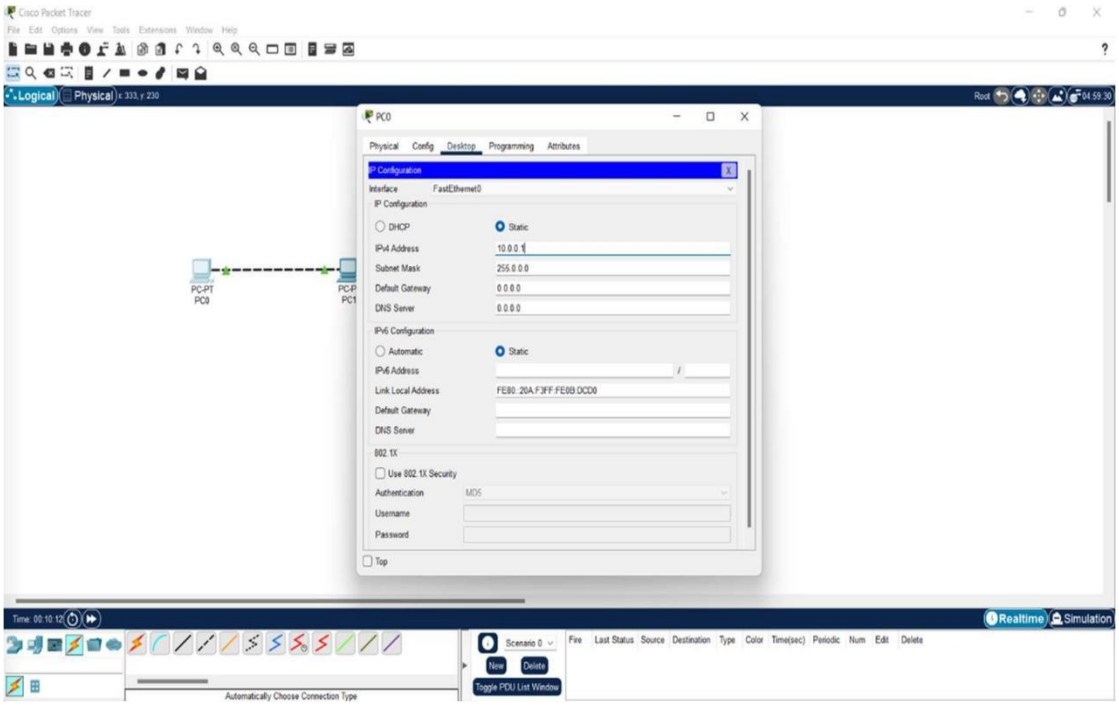
DIAGRAMS: -



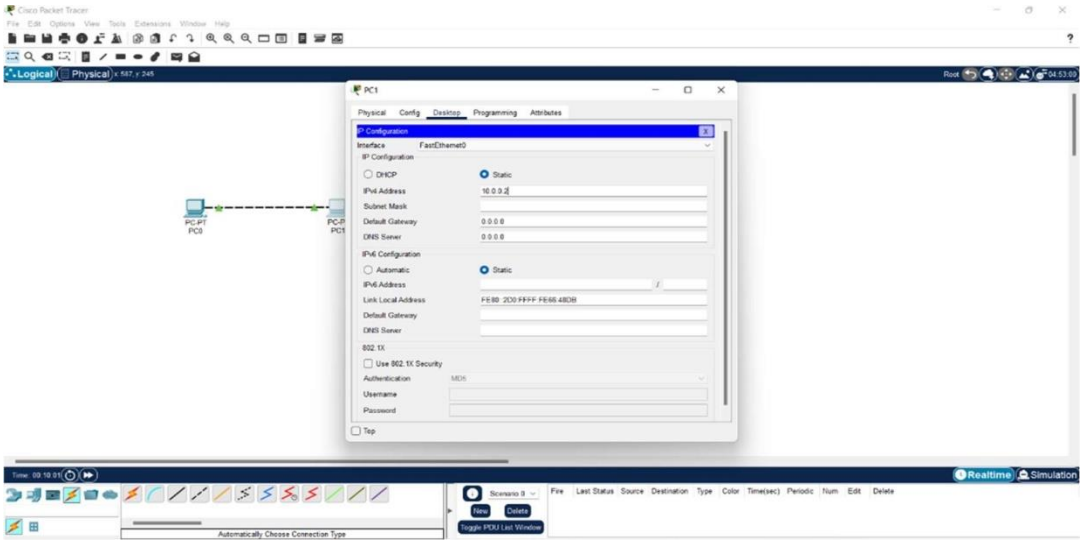
1.1)Connection two pcs together with connection lines.



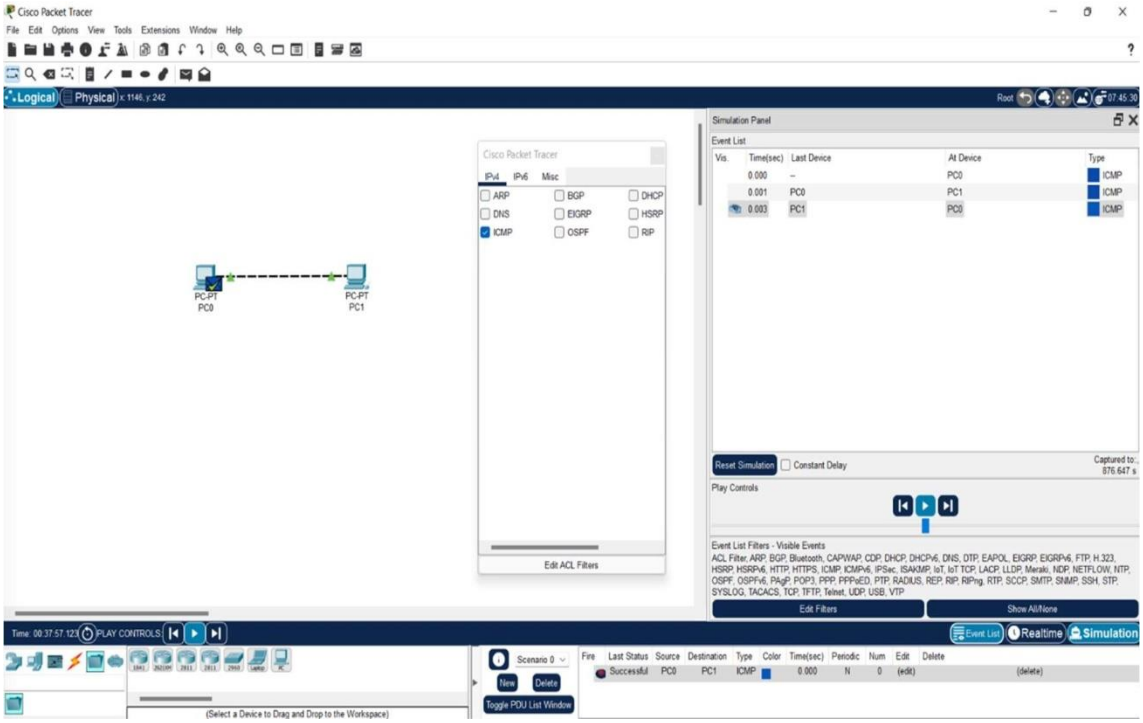
1.2)Successful setup of connection between two pcs.



1.3) Setting up the IP address of PC0



1.4)Setting up the IP address of PC1



1.5)Successful setup link connection by simulation method.

RESULT: -

CONCLUSION: -

EXPERIMENT-02

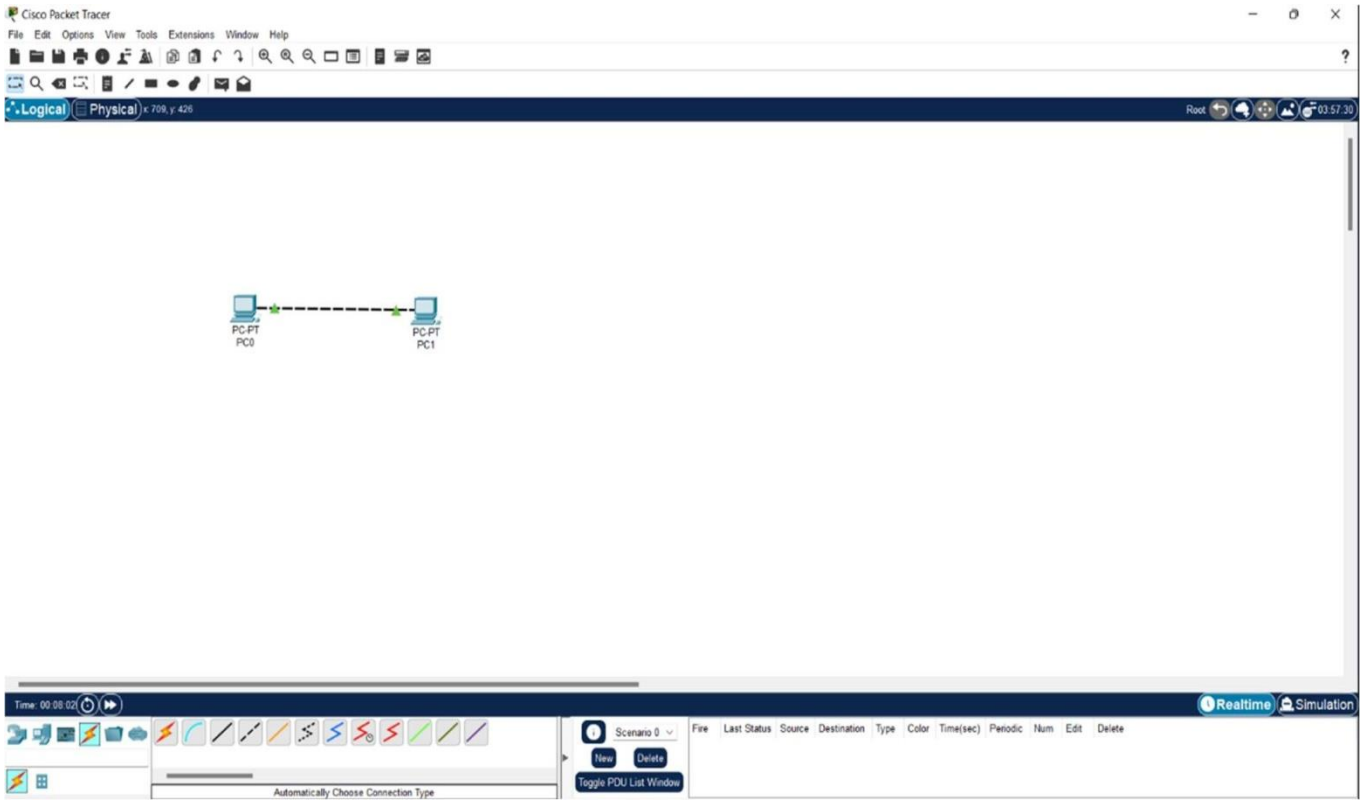
AIM: - To establish link between two PC and transfer information using command prompt.

APPARATUS: - Cisco Packet Tracer.

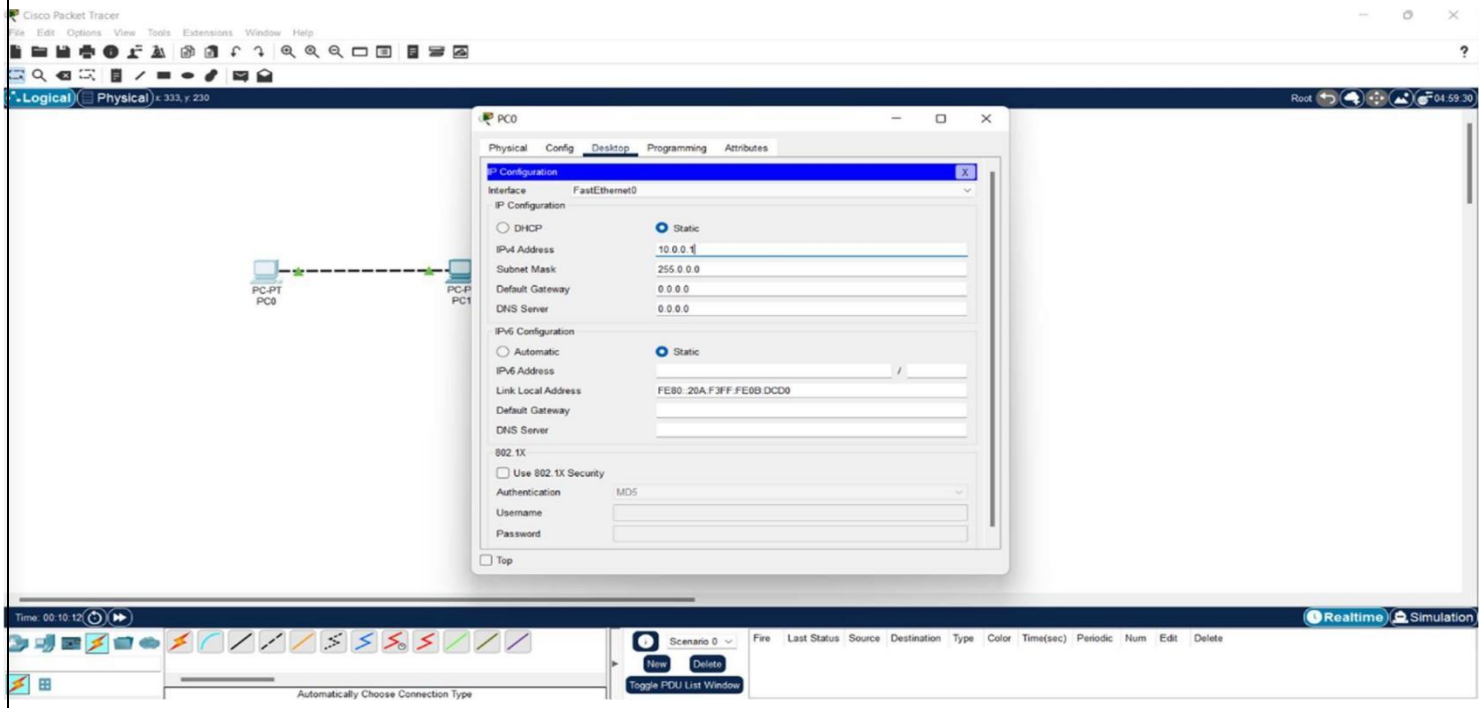
PROCEDURE: -

- Start the desktop or laptop.
- Click on the logo of Packet Tracer and blank screen with all specification will be displayed.
- Click on end devices displayed on the cisco packet tracer page.
- Select the generic option which will provide two pcs (PC0, PC1).
- Connect PC0, PC1 with connection lines provided in the system.
- Configure the IP address of both the pcs with IP address 10.0.0.1,10.0.0.2.
- Click command prompt and provide information.
- ipconfig
- ipconfig /all
- ping 10.0.0.2
- This was the one method of connecting the link and send information using command prompt.
- Take the screenshot of those pictures and paste it here.

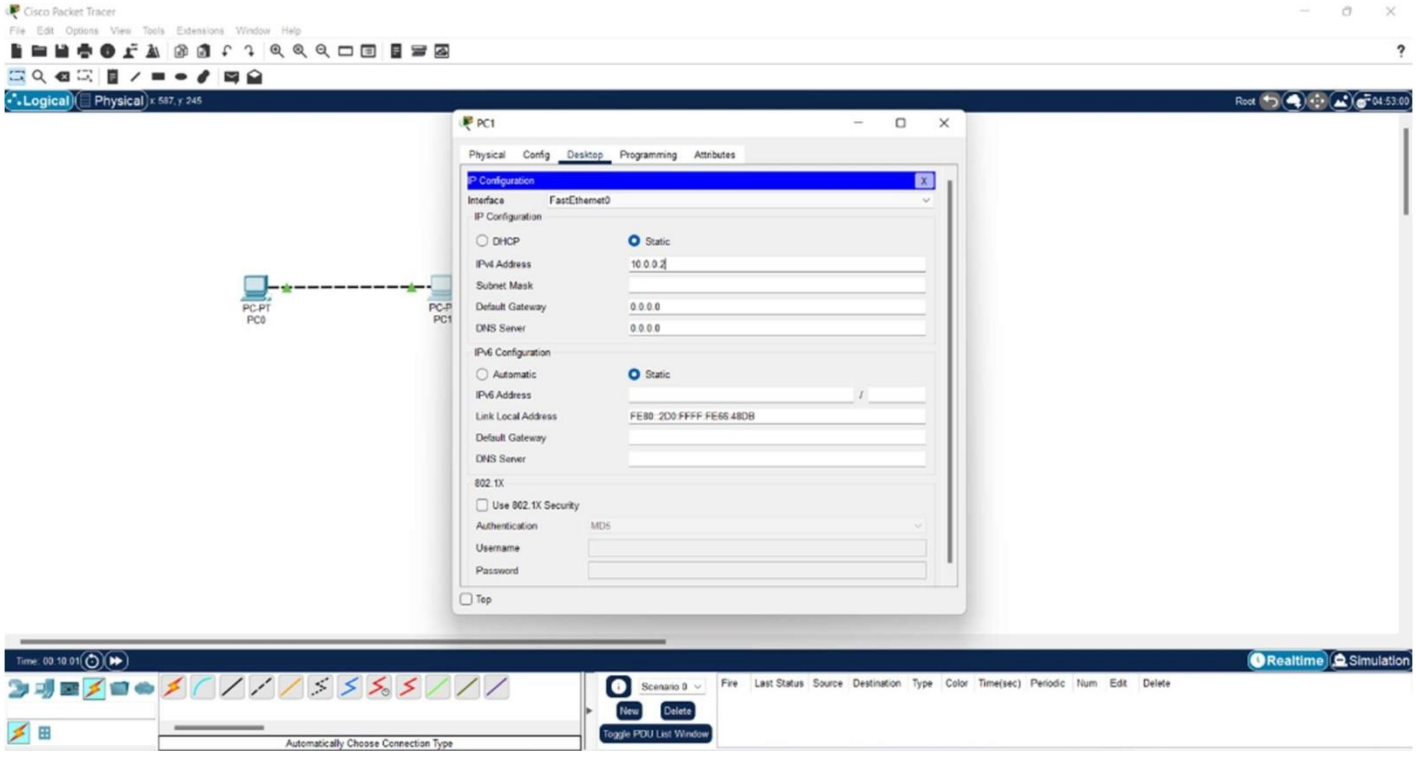
DIAGRAMS: -



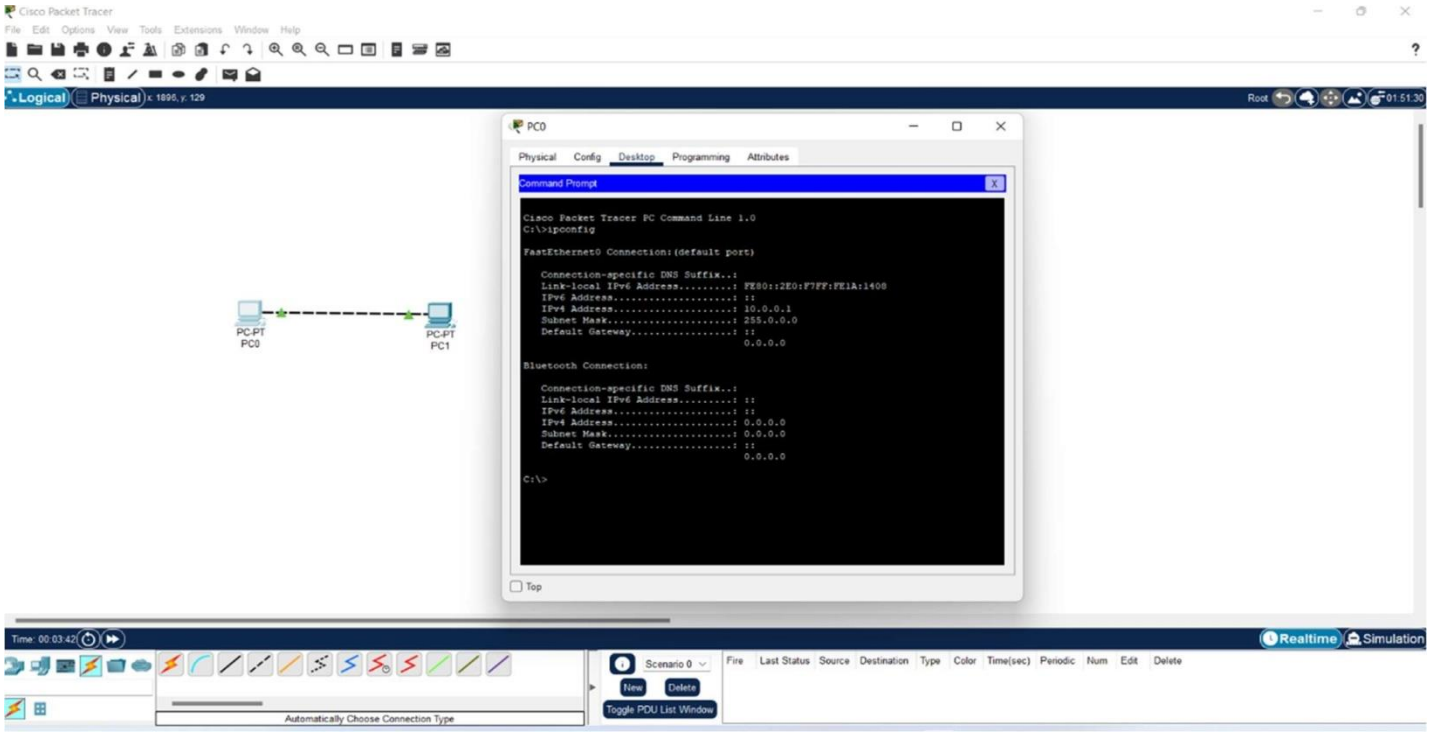
2.1)Connection two pcs together with connection lines.



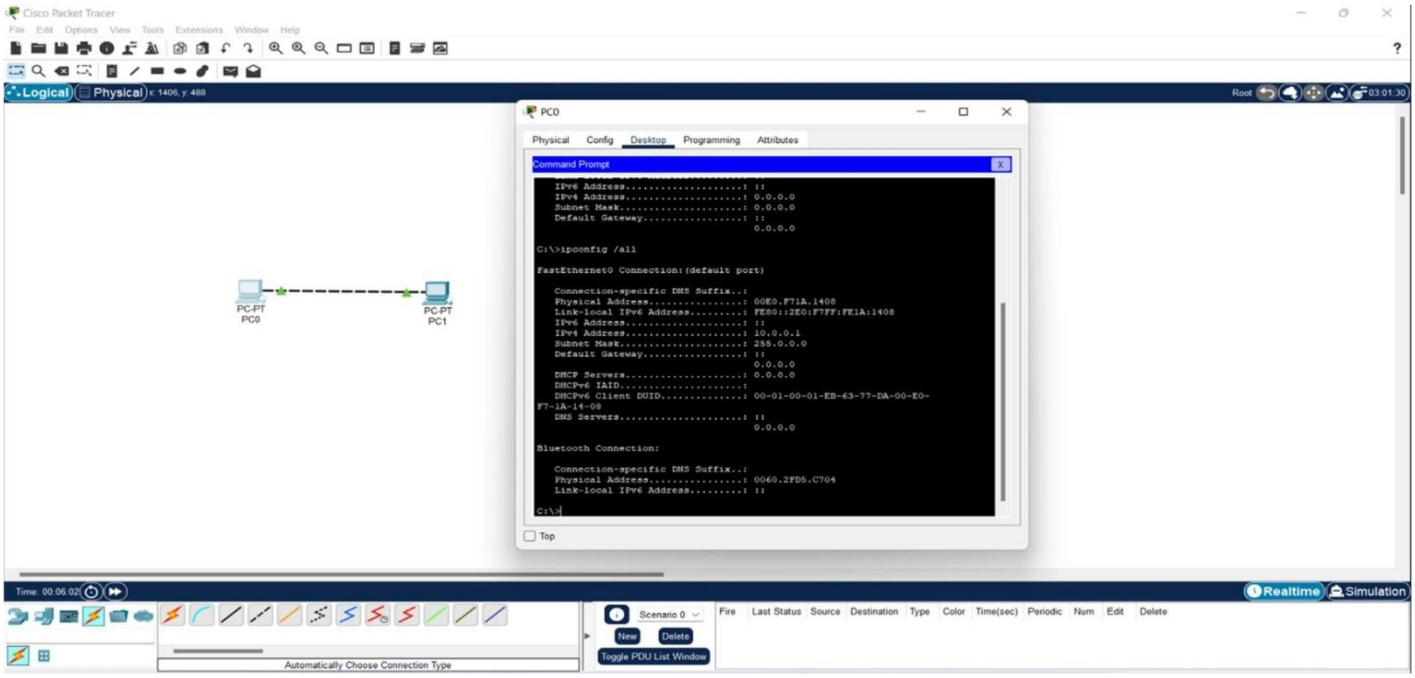
2.2)Setting up the IP address of PC0



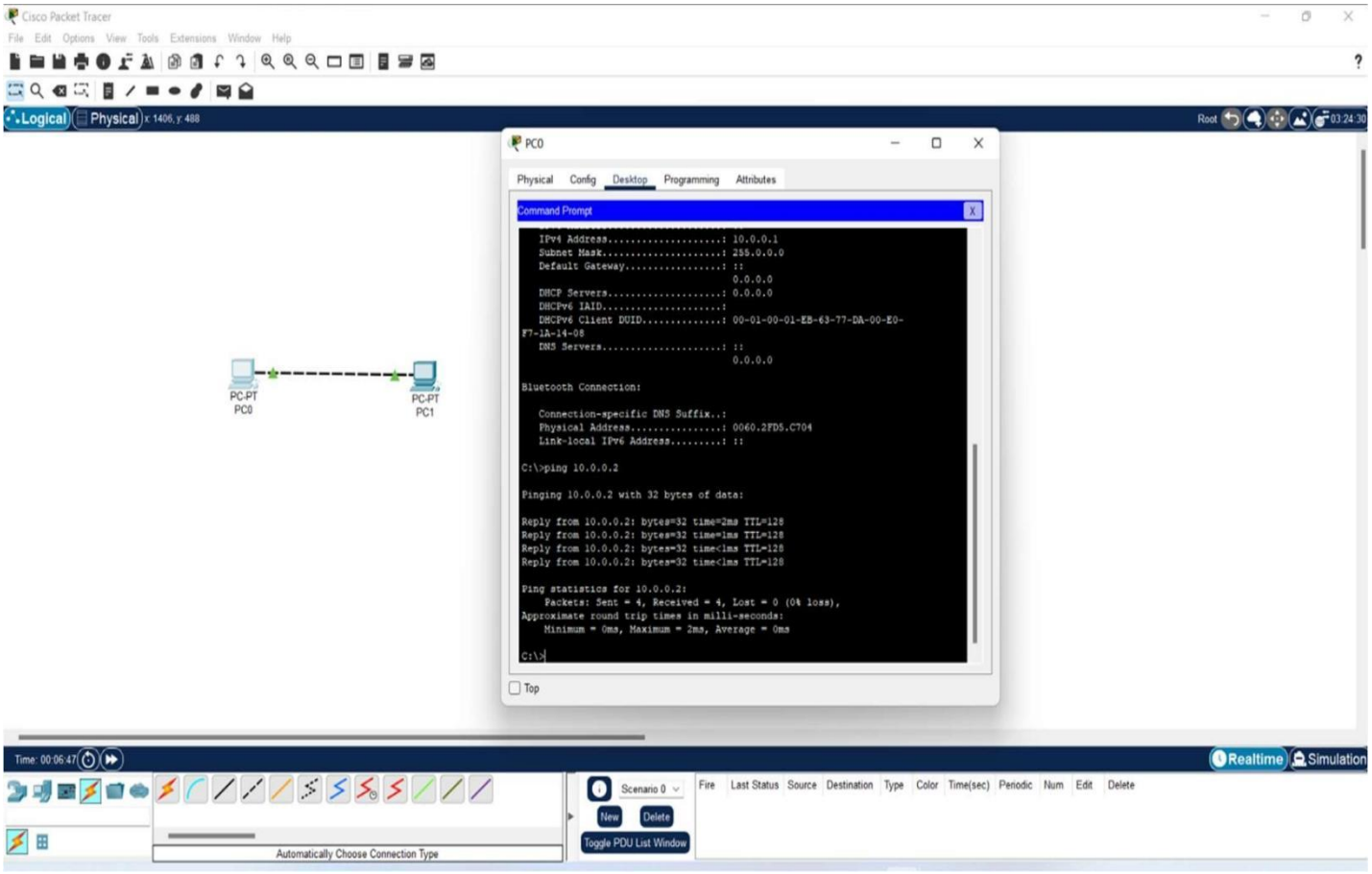
2.3)Setting up the IP address of PC1



2.4)Set the ip config in command prompt for pc setup.



2.5)Set the ip config / all in command prompt for physical address.



2.6) Connections establish between two pcs.

RESULT: -

CONCLUSION: -

EXPERIMENT-03

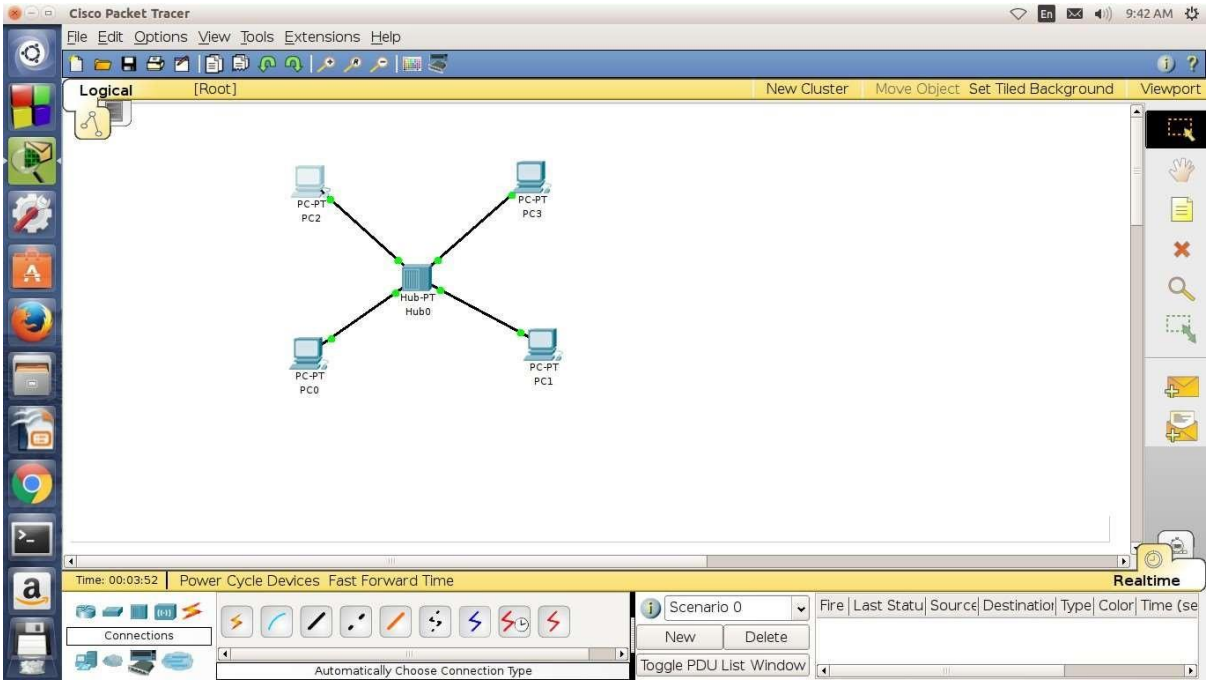
AIM: - To establish link between two ends of pc using hub and switch to transfer information.

APPARATUS: - Cisco Packet Tracer.

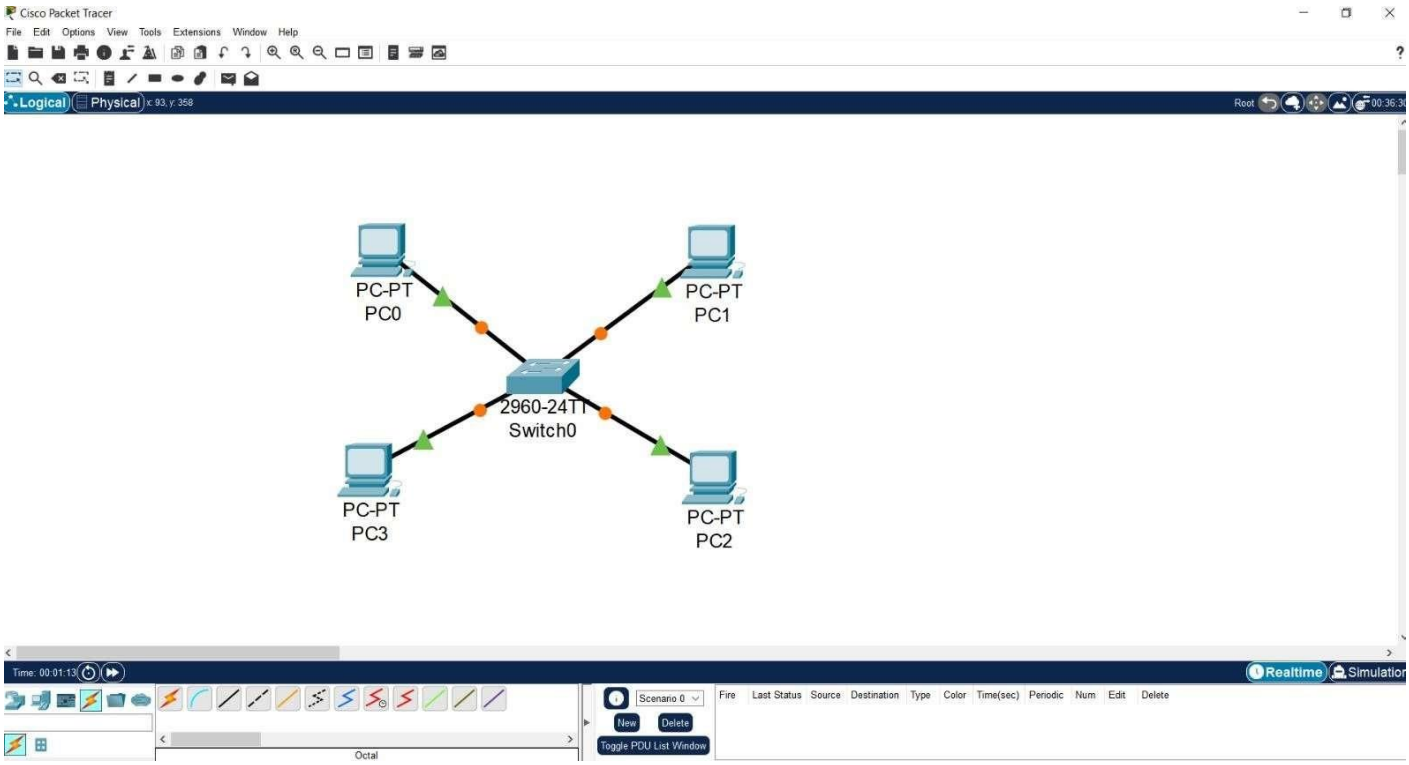
PROCEDURE:-

- Start the Desktop or Laptop.
- Click on the logo of Packet Tracer and blank screen with all specification will be displayed.
- Click on End Devices displayed on the Cisco Packet Tracer page.
- Select the Generic option which will provide 4 pc's (PC0, PC1, PC2, PC3).
- Connect all pcs with connection lines provided in the system.
- Select Hub now connect hub with all pcs
- Configure the I.P Address of all the pcs with I.P Address (10.0.0.1,10.0.02,10.0.0.3,10.0.0.4).
- Send message click on the last second option on the right-side corner of the window.
- Now click on simulation which shows the message transfer between two pcs.
- Now replace Hub by Switch. Click on simulation which shows the message transfer between two pcsdiagonally.

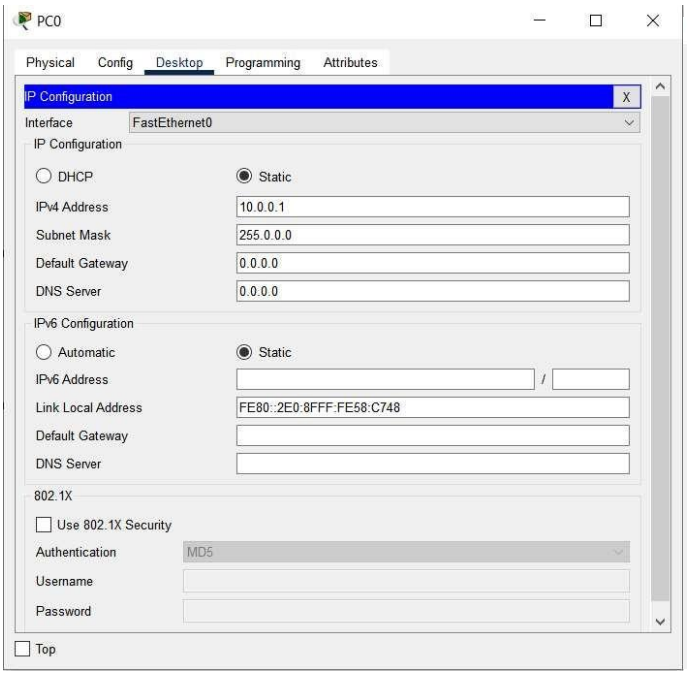
SCREENSHOT : -



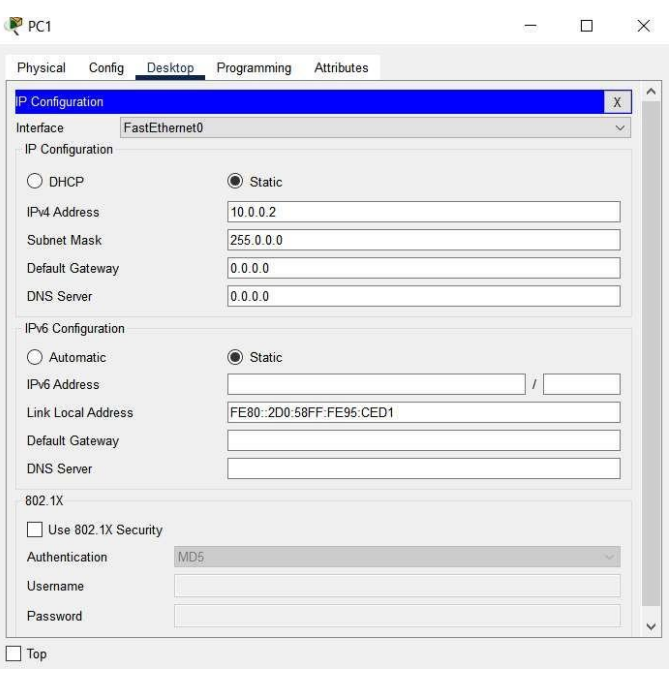
1) Connect four pcs together with a hub through connection lines.



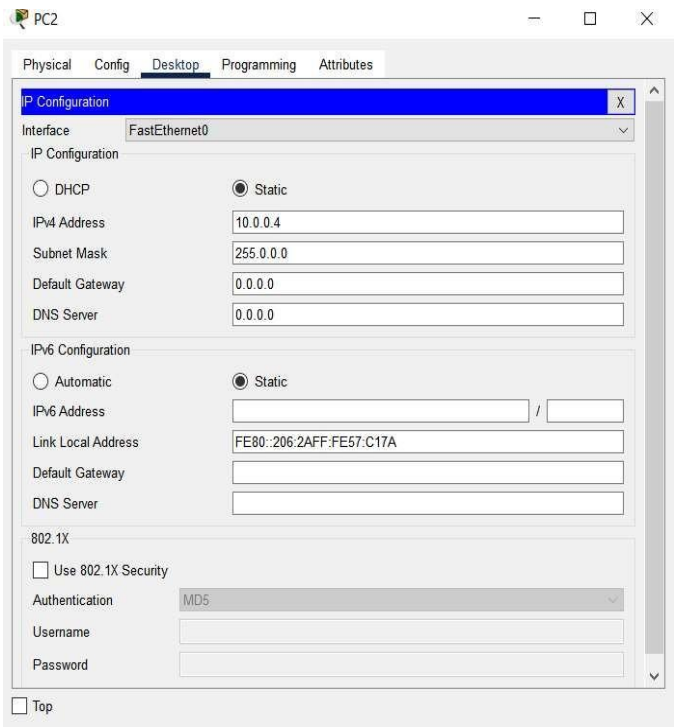
1.1) Connect four pcs together with a switch through connection lines.



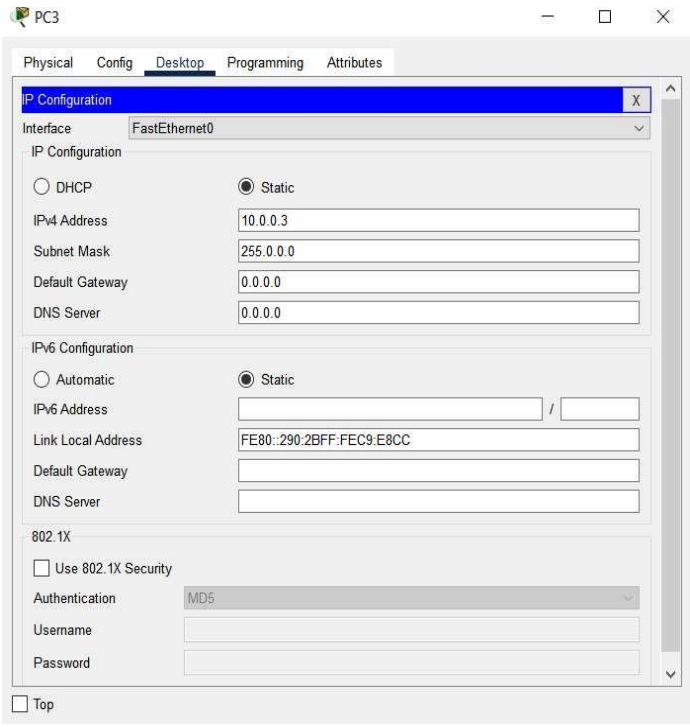
3.1.1) Setting up the IP address of PC0



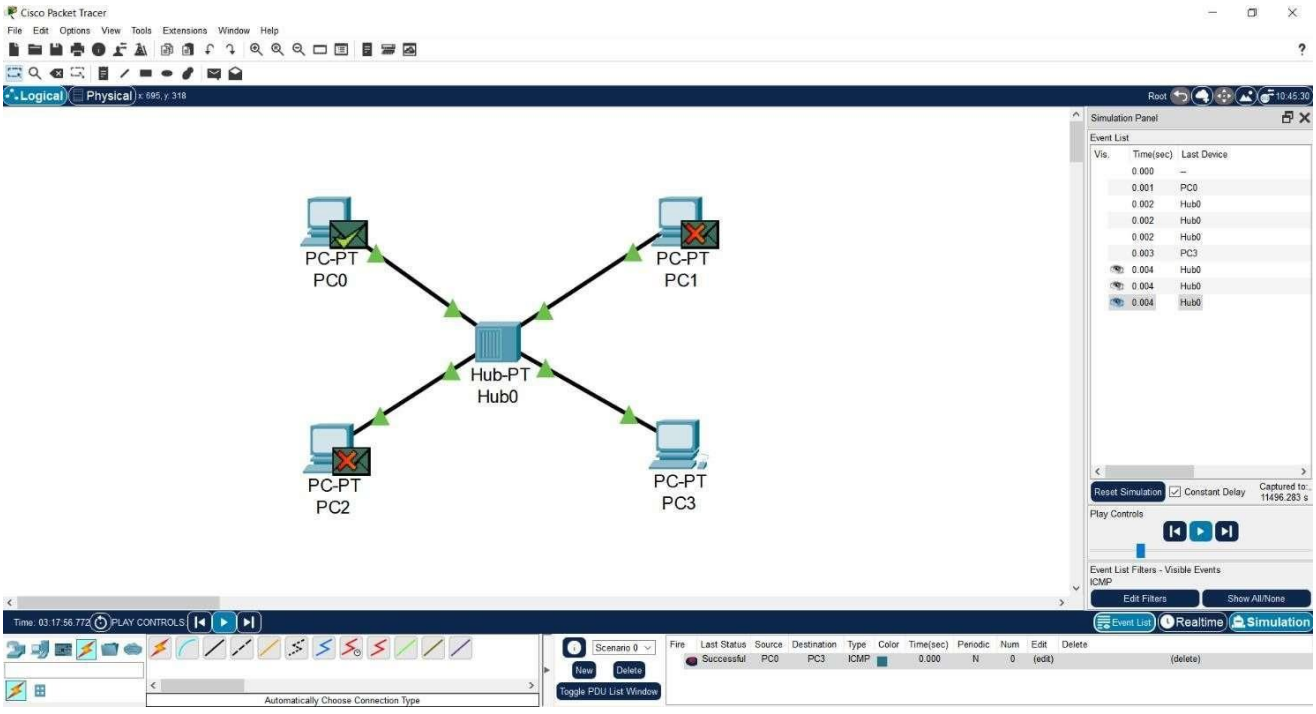
3.1.2) Setting up the IP address of PC0



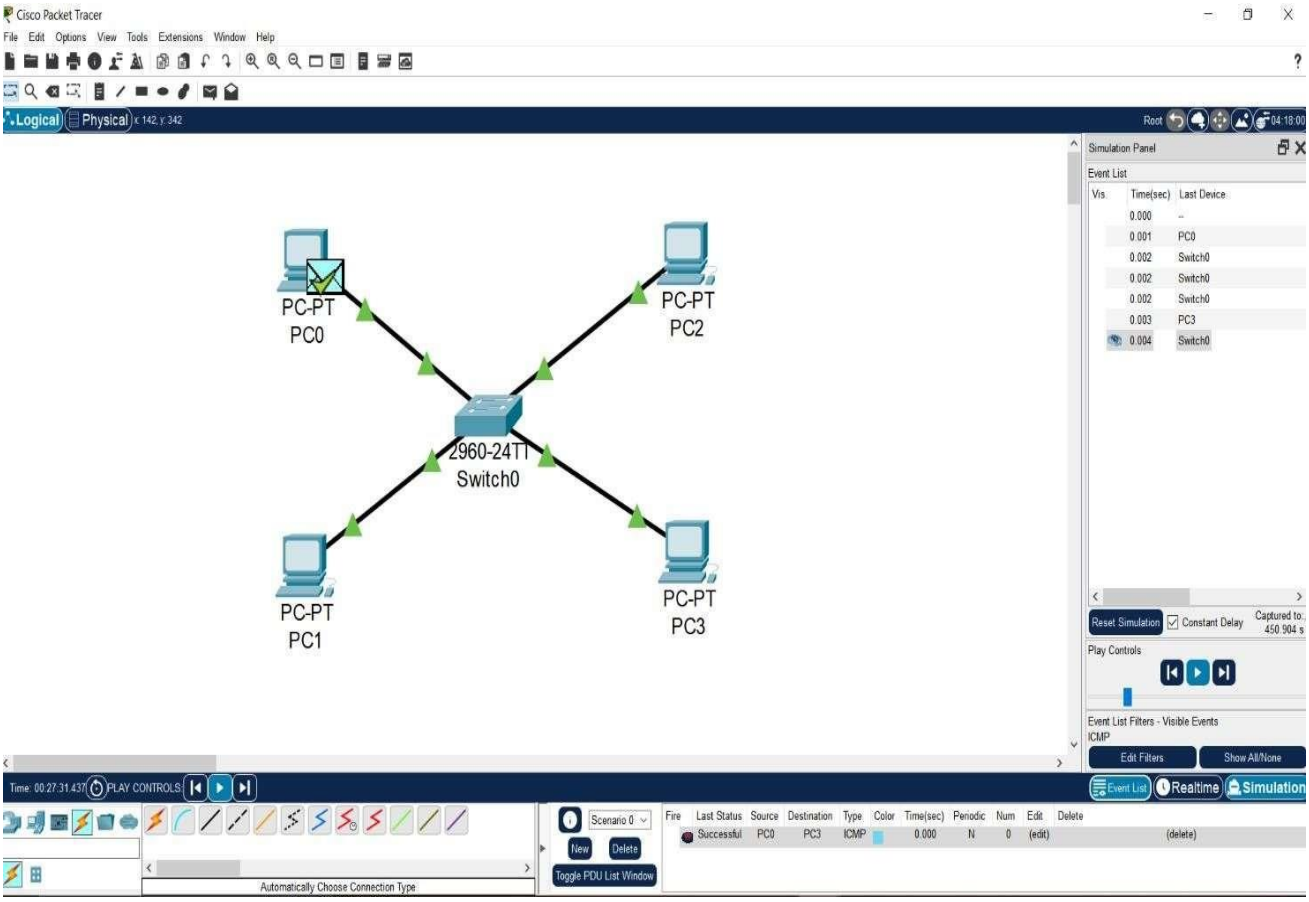
3.1.3) Setting up the IP address of PC0



3.1.4) Setting up the IP address of PC0



1.2) Connection between four computers through a hub is established and message is transferred.



1.3) Connection between four computers through a switch is established and message is transferred.

RESULT: - Hub broadcasts message to all systems and switch broadcasts message only to destination.

CONCLUSION: - With the help of cisco packet tracer, transmission of information and connection between two ends of pc using hub and switch can be established.

EXPERIMENT-04

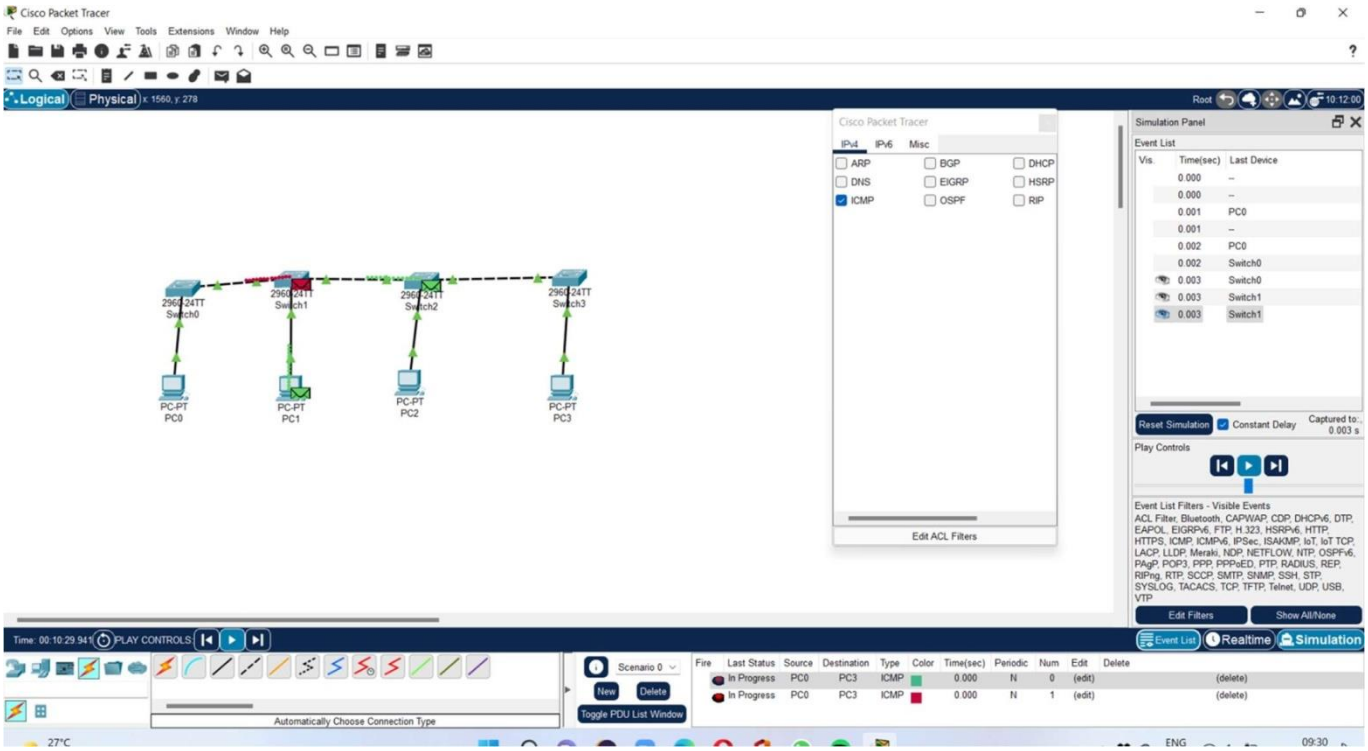
AIM: - Implementation of LAN and Hybrid topology.

APPARATUS: - Cisco Packet Tracer.

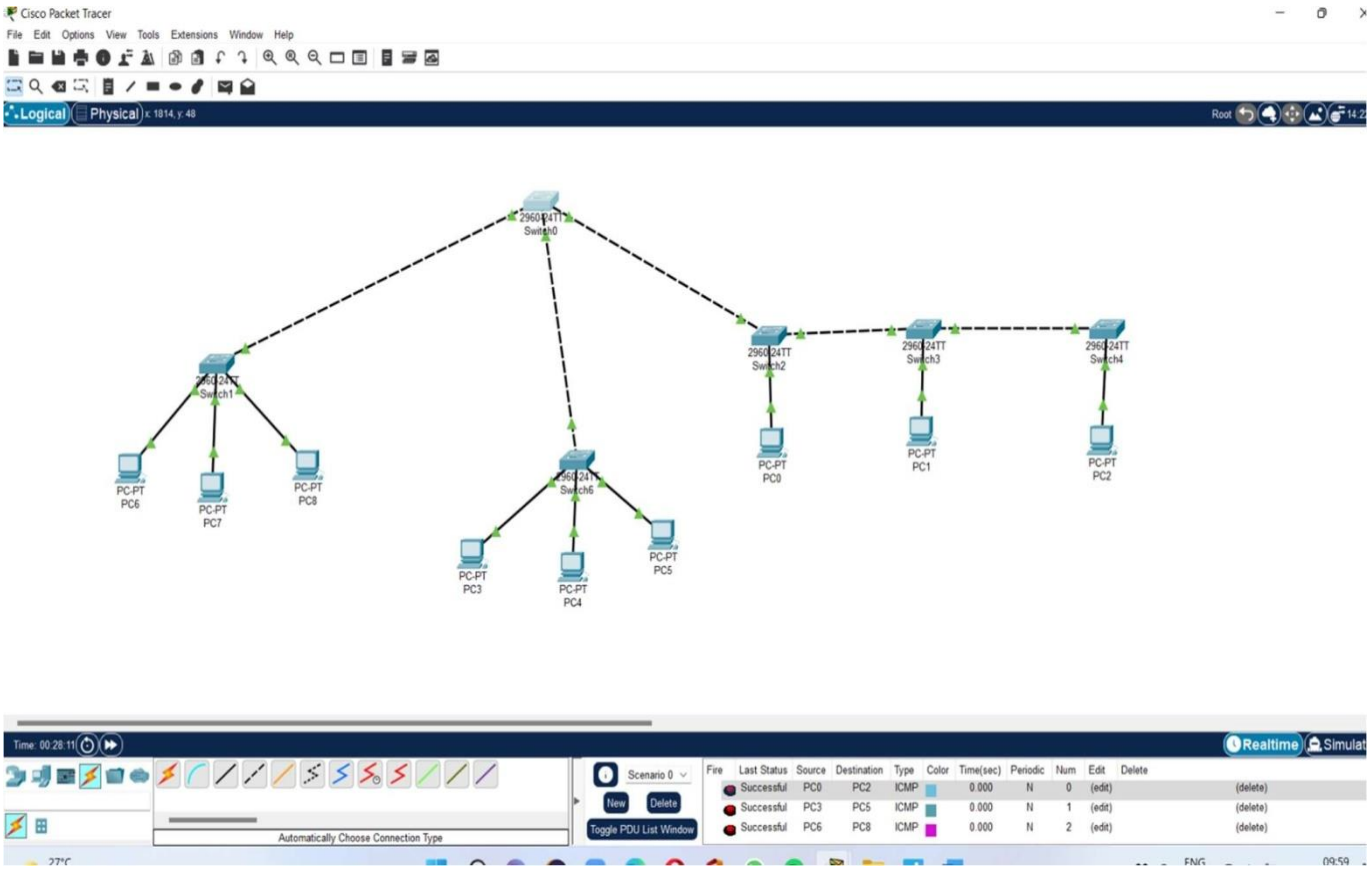
PROCEDURE:-

- Start the Desktop or Laptop.
- Click on the logo of Packet Tracer and blank screen with all specification will be displayed.
- Click on End Devices displayed on the Cisco Packet Tracer page.
- Select the Generic option which will provide 4 pc's (PC0, PC1, PC2, PC3).
- Select switches (2950-24) place it in series.
- Connect all PCs and switches with wire to form LAN network as shown in screenshot.
- Configure the I.P Address of all the pcs with I.P Address (10.0.0.1,10.0.02,10.0.0.3,10.0.0.4).
- Send message click on the last second option on the right-side corner of the window.
- Now click on simulation which shows the message transfer between two pcs.
- Now similarly make a hybrid topology and repeat the procedure.

SCREENSHOT : -



2) LAN Network



2.1) Hybrid Network

RESULT: - Packet transfer using LAN and Hybrid network is successfully done.

CONCLUSION: - With the help of cisco packet tracer using LAN and Hybrid network can be established.

EXPERIMENT-05

AIM: To study about different physical equipment used for networking.

What is Computer Network?

Computer network means an interconnected collection of autonomous computers. Two computes said to be connected if they are able to exchange information. The connection needs not to be via a copper wire, fiberoptics, microwares and communication satellite can also be used.

By requiring the computer to be autonomous, we wish to include from our definition system in which there is a clear master/slave relation. If one computer can forcibly start, stop or control another one, the computers are not autonomous. A system with one control unit and many slaves is not a network, nor is a large computer with remote printers.

Advantages of Computer network:

- Resource Sharing
- High Reliability
- Saving Money

SERVER

Concept of a server is based on one or more personal computers to perform specific tasks for a number ofother PCs. The most common function is disk, file and print servers.

A **Disk Server** provides low-level support and performs basic read/write operation to disk sectors.

A **File Sever** is a higher-level support mechanism, performing such function as lockout and dynamic allocationof space on disk.

In a star layout the server is the principal connection point. All nodes, including the server, are connected to a hub. This enables the server to house and administer software, fie sharing, file saving and to allocate printersor other peripherals.

In a bus layout, the server acts like arbitrator, each node talks to the server when requesting information. The server then locates the information on one of the connected clients and sends it to the requesting client.
Servers in any network can be an ordinary node but having more capabilities pf handling the data and having more speed. There are special servers also available in the market like HPLC2000, which can connect 18 * 3HDD and having 512 MB of RAM.

WORKSTATION

A node or stand-alone PC that is connected with network is called Workstation. A workstation is generallya Client.

NIC (Network Interface Card):

The network Interface Card (NIC) is the interface between the PC and physical network connection. In Ethernet systems, the NIC connection to a segment of coaxial or UTP cable (fiber NICs are available but not very common yet). As with any other type of adapter card NICs come in ISA, PCMCIA, and PCI bus varieties.

The NIC is responsible for the operation that tasks place in the physical layer of the OSI model. It is only concerned with sending and receiving) 0s and 1s, using the IEEE 802.3 Ethernet standard.

In windows, the NIC card is identified in the network property; to use protocol with NIC you must bind the protocol to the adapter car. This is typical done automatically when the protocol is added.

All the NICs are manufactured with a unique 4-bit Mac address using the WINIPCFG utility (from the run menu). IT is also called as Network Adapter Card.

Function of NIC:

- Data Transfer
- Data Buffering
- Frame Construction
- Media Access Control
- Parallel/Serial Conversion
- Data Encoding/Decoding
- Data Transmission/Reception

CABLES

To transmit the data the medium must exist, usually in the form of cables or wireless media. Here are somemost commonly used cable types.

1.) Thick Coaxial Cables (thick net) (RG-11)

Thick coaxial cables or thick wire is known as the Ethernet standard RG-11. This cable is mostly used as backbone cable, distributing Ethernet signal throughout a building, an office complex or other large installation. It is used in 10base5 Ethernet standard. RG-11 is thicker and more study than RG-58 coax.

The length may be up to 500 meters with a max of five segments connected by repeaters. This gives a total distance of 2500 meters. This is called a network diameter. RG-11 cable is typically orange; withblack rings around the cable every 2.5-meter to allow taps into the cable.

2.) Thin coaxial cables (thin net) (RG-58)

RG-58 is typically used for wiring laboratories and offices, or another small group of computers. The maximum length of thin wire Ethernet segment is 185 meters, Which is due to the nature of the CSMA/CD method of operation, the cable attenuation, and the speed at which signals propagate inside the coax. The length is limited to guarantee that collision is detected when machines that are apart transmit at the same time. BNC connectors are used to terminate each end of the cable.

When many machines are connected to the same Ethernet segment, a daisy chain approach is used.

The BNC connectors allow the network interface card to the next machine. The machine each end of the cable must use a terminating resistor to eliminate collision-causing reflection in the cable.

3.) Twisted pair cables

Twisted pair is probably the most widely used cabling system in Ethernet in networks. Two copper wires twist around each other to form the twisted pair cable. Depending on category several insulatedwire strands can reside in the cable.

Twisted pair is available in two basic types:-

- Unshielded Twisted Pair (UTP)
- Shielded Twisted Pair (STP)

Unshielded Twisted Pair

Mostly the UTP is used. A twisted pair segment can't exceed 100 meters. This limitation is the only drawbackto twisted pair. Twisted pair is used for 10/100 based Ethernet networks.

UTP cables are wired as straight through or crossover cables. Straight through cables typically connect the computer's networks interface can't to be a port on the hub. Crossover cables are used for NIC to communication and for hub-to-hub connections when no crossover port is available.

UTP categories

Category	Descriptor
1	Used for voice for data.
2	Contains four twisted pair and a data transmission up to 4 Mbps. Used for some token ring network.
3	Contains four twisted pair and a data transmission up to 10 Mbps. Used for some token ring network.

4	Contains four twisted pair and a data transmission up to 16 Mbps. Used for some token ring network.
5	Contains four twisted pair and a data transmission up to 100 Mbps. Used for some token ring network.

Category-5 cables can be purchased or crimped as either straight through or crossed. A category-5 cable has 8 thin. Colors coded wires inside that run from one end of the cable to the other. Ethernet networks for communication use only wires 1, 2, 3 and to be connected in both jacks.

Straight through cables are used for connecting to a hub. Crossed cables are used for connecting a hub to another hub (there is an exception: some hubs are a built in up link port that is crossed internally which, ,allows a you to uplink hubs with a straight cable instead.)

In a straight through cable wires 1,2,3 and 6 at the other end. In a crossed cable, one order of the wires changefrom one end to the other wire 1 becomes 3 and 2 becomes 6

For PC 2 PC Communication without HUB (Cross Cable Connection)

Sr. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Green	Transmit
03	Green White	Orange White	Receive
04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For PC 2 PC Communication with HUB (Simple Cable Connection

Sr. No.	One Site	Second Site	Pin Configuration
01	Orange White	Orange White	Transmit
02	Orange	Green	Transmit
03	Green White	Orange White	Receive
04	Blue	Blue	Not Use
05	Blue White	Blue White	Ground
06	Green	Green	Receive
07	Brown White	Brown White	DTR
08	Brown	Brown	DTS

For One Cable in Two PC Communication through HUB (Simple Cable Connection)

First Connection:

Sr. No.	One Site	Second Site	Pin Configuration
01	Orange White	Green White	Transmit
02	Orange	Orange	Transmit
03	Green White	Green White	Receive
04	Green	Green	Receive

Second Connection:

Sr. No.	One Site	Second Site	Pin Configuration
01	Blue	Green White	Transmit
02	Blue White	Orange	Transmit
03	Brown White e	Green White	Receive
04	Brown	Green	Receive

Shielded Twisted Pair

It is 150Ω cable containing additional shielding that protects signals against electromagnetic Interference (EMI) produced by electric motors power lines etc. It is primarily used in Token Ring Network & where UTP cable would provide insufficient protection against interface.

Wires within cables are encased in a metallic sheath that is conductive as copper in wires. This sheath when properly grounded converts it ambient noise into current, like antenna. This current is carried to wires within where it creates an equal and opposite current flowing in twisted pair thus getting cancelled and no noise signal is resulted.

1. Fiber Optic.

Fiber Optic relies on pulsed as light to carry information. Two types of plastic or glass with different physical propertied are used (the inner core and the outer cladding) to allow a beam of light to reflect off the boundary between the core and cladding. Some fiber optic cables allow many different paths other allow one single mode. They are called multimode and single mode fibers. A popular multimodefiber has core/cladding dimensions of 62.5/125 nanometers.

REPEATER

A Repeater is a purely electrical device that extends maximum distance a LAN cable can span by Amplifying signals passing through it. A Repeater connects two segments and broadcasts packets between them. Since signal loss is a factor in the maximum length of a segment, a Repeater is used to amplify the signal and extend the usable length. A common Ethernet rule is that no more than four repeaters may be used to join segments together. This is a physical limitation designed to keep collision

detection working properly. Repeaters operateat layer 1 (Physical layer) of the OSI model.

BRIDGES

This networks bridge provides an inexpensive and easy way to connect network segments. A bridge provides Amplification function of a repeater plus, ability to select filter packets based on their addresses. When network grows in size, it is often necessary to partition it in to smaller group of nodes to help isolate traffic and improve performance. One way t do this is to use bridge, the operation of it is to keep one segment traffic to that side and other to other side will cross the bridge, The bridge learns which packets should cross it as it is used.

ROUTERS

A router is a device that connects two LANs together to form an inter-network. A router is the basic building block of the Internet. Each router connects two or more networks together by providing an interface for an Ethernet network and ring network to which it is connected. The router examines each packet of information to detection weather the packet must be translated form on one network to another network performing a function similar to a bridge. Unlike a bridge, a router can connect network that use different technologies, addressing methods, media type, frame format and speeds.

A router is a special purpose device designed to interconnect networks. Such that three networks can beconnected using two routers.
Routers maintain routing tables in their memories to store information about the physical connection on he network; the router examines each packet of data, checks the routing table and then forwards the packet if necessary. Every other router in the path (between any state destinations) performs a similar procedure. Note that a router does not maintain any state information about the packets; it simply moves them along the network.Routers are operated at layer 3(network) of OSI model.

GATEWAYS

A node on a network that serves as an entrance to another network. In enterprises, the gateway node often acts as a proxy server and a firewall. The gateway is also associated with both a switch, which provides the actual path for the packet in and out of the gateway.
It is also known as a computer system located on earth that switches data signals and voice signals between satellites and terrestrial networks.
A gateway can operate at any layer of the OSI/RM. The hob of a gateway, also called a protocol converter, is much more complex than that of a router or switch. Typically a gateway must convert from one protocol stackto another. E.g. a gateway may connect a TCP/IP network to an IPX./SPX network.
A Circuit Level Gateway function provided by Application level gateway products enables trusted users on private network to access Internet services with all security of a proxy server.

An Application Level Gateway provide much stricter form of security that packet filters, but they are designedto regulate access only for a particular application.

TANSCEIVERS

A transceiver converts from one media type to another. For example, a 10base2 coaxial cable with a fiber optic cable. It is common to use more then one media type an installation, so many different kinds of

transceivers are available.

HUBS

Hubs are also called concentrators; expand one Ethernet connection into many. For example, a four-port hub connects up to four machines via UTP cables. The hub provides a star connection for the four ports. Many hubs contains a single BNC connectors as well to connect the hub to existing 10base2 network wiring, the hub can also be connected via one of its ports. One pot is desired to operate in either straight through or crossover mode, selected by a switch on the hub

Hubs that can connect in this fashion are called stackable hubs.
A hub is similar to a repeater, expect it broadcasts data received by any port to all other ports on the hub. Most hubs contain a small amount of intelligence as well. Examining received packets and checking them for integrity. If a bad packet arrives or the hub determines that a port is unreliable. It will shut down the line underthe error condition is appears.
The hub also acts like a repeater. Because of its slight delay when processing a packet, the numbers of hubsthat may be connected in a series are limited.

There are three types of HUB passive hub, active hub and intelligent hub.

The Passive hubs do not process data signals with only purpose to combine the signal form several networkscables segments. All devices attached to the passive hub receive another packets that pass through the hub
.Hub does not clear up or amplify the signals, on the contrary absorbs a small part of the signals that is why the distance between a hub and a computer should not be more than half of the permissible distance between two computers. Passive hubs have limited functionality so are inexpensive and easy to configure. It has four ports with four BNC (British Naval Connectors) female connectors to configure networks station or terminatedwith a 93 Ω BNC Terminator.
The active hubs incorporate electronic components that amplify and cleanup the signals, that flaw between devices on the network. The process of cleaning up signal is called “signal regeneration”. The benefits of signals regeneration are:

- A network is more robust i.e. less sensitive errors.
- Distance between devices can be increased.

Active hubs cost is considerable more than passive hub (active hub function impart as multi port repeaters). Intelligent hubs are enhanced active hubs the following functions add intelligence to a hub. Intelligent Hubsare units have form of integrated management capability.

Hub Management

A hub supports networks network management protocols that enable the hub to send packets to centralnetwork console. Theses protocols enable network console to manage or control hub.

Switching hubs

Switching hubs include circuitry that quickly routes signals between ports on the hub. Insured of repeating a packet to all ports on the hub, it repeats a packet only to the port that connects to the

destination computer forthe packet.

SWITCHES

It is similar to a bridge, with some important enhancement. First, as witch may have multiple ports, thus directing packets to several different segments further partitioning and isolating network traffic in as way similar to router. For ex., if 8-port n way switch is there it can route packets from any input to any output. Some or all of incoming packet is called store and forward, which stores the received packet before examiningit to for error before retransmitting. Bad packets are not forwarded.
A switch typically has auto-sensing 10/100 mbps ports and will just the speed of each port accordingly; furthermore, a managed switch supports SNMP for further control over network traffic. Switches operated atlayer 2 (Data Link) of OSI model.

EXPERIMENT No: 6

AIM: To Study OSI reference model and TCP/IP reference model

Introduction:

Here, we will discuss two important network architectures - the OSI reference model and the TCP/IP reference model. Although the protocols associated with the OSI model are rarely used any more, the model itself is actually quite general and still valid, and the features discussed at each layer are still very important. The TCP/IP model has the opposite properties: the model itself is not of much use but the protocols are widely used.

OSI reference model:

Virtually all networks in use today are based in some fashion 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.

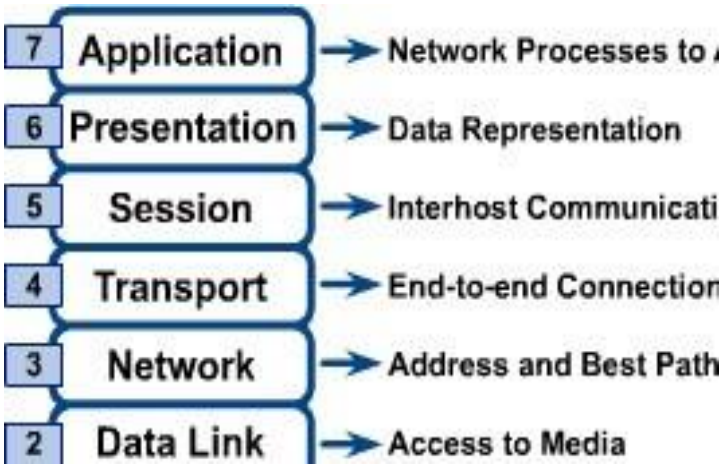


Fig.1

The principles that were applied to arrive at the seven layers can be briefly summarized as follows:

1. A layer should be created where a different abstraction is needed.
2. Each layer should perform a well-defined function.
3. The function of each layer should be chosen with an eye toward defining internationally standardized protocols.
4. The layer boundaries should be chosen to minimize the information flow across the interfaces.
5. The number of layers should be large enough that distinct functions need not be thrown together in the same layer out of necessity and small enough that the architecture does not become unwieldy.

The layers are as follows:

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.

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. The main task of the data link layer is to transform a raw transmission facility into a line that appears free of undetected transmission errors to the network layer. It accomplishes this task by having the sender break up the input data into data frames (typically a few hundred or a few thousand bytes) and transmits the frames sequentially. If the service is reliable, the receiver confirms correct receipt of each frame by sending back an acknowledgement frame.

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. The network layer controls the operation of the subnet. A key design issue is determining how packets are routed from source to destination. Routes can be based on static tables that are "wired into" the network and rarely changed. They can also be determined at the start of each conversation, for example, a terminal session (e.g., a login to a remote machine). Finally, they can be highly dynamic, being determined anew for each packet, to reflect the current network load.

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.

Layer 5: Session - Layer 5 establishes, maintains and ends communication with the receiving device. The session layer allows users on different machines to establish sessions between them. Sessions offer various services, including dialog control (keeping track of whose turn it is to transmit), token management (preventing two parties from attempting the same critical operation at the same time), and synchronization (check pointing long transmissions to allow them to continue from where they were after a crash).

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. Unlike lower layers, which are mostly concerned with moving bits around, the presentation layer is concerned with the syntax and semantics of the information transmitted. In order to make it possible for computers with different data representations to communicate, the data structures to be exchanged can be defined in an abstract way, along with a standard encoding to be used "on the wire." The presentation layer manages these abstract data structures and allows higher-level data structures (e.g., banking records), to be defined and exchanged.

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. The application layer contains a variety of protocols that are commonly needed by users. One widely-used application protocol is HTTP (Hypertext Transfer Protocol), which is the basis for the World Wide Web. When a browser wants a Web page, it sends the name of the page it wants to the server using HTTP. The server then sends the page back. Other application protocols are used for

file transfer, electronic mail, and network news

TCP/IP Reference Model:

The ARPANET was a research network sponsored by the DoD (U.S. Department of Defense). It connected hundreds of universities and government installations, using leased telephone lines. When satellite and radio networks were added later, the existing protocols had trouble interworking with them, so new reference architecture was needed. Thus, the ability to connect multiple networks in a seamless way was one of the major design goals from the very beginning. This architecture later became known as the TCP/IP Reference Model, after its two primary protocols.

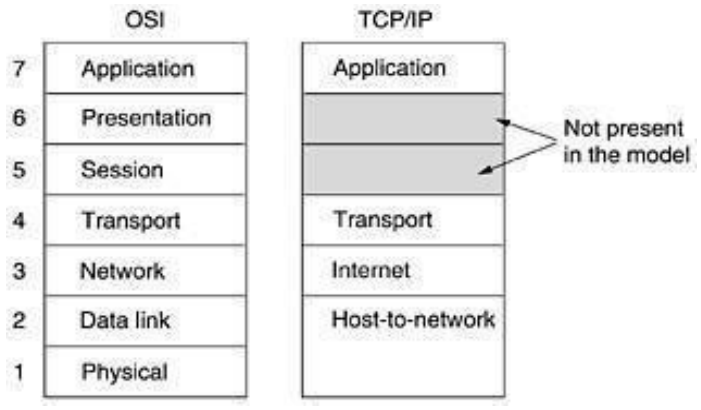


Fig.2

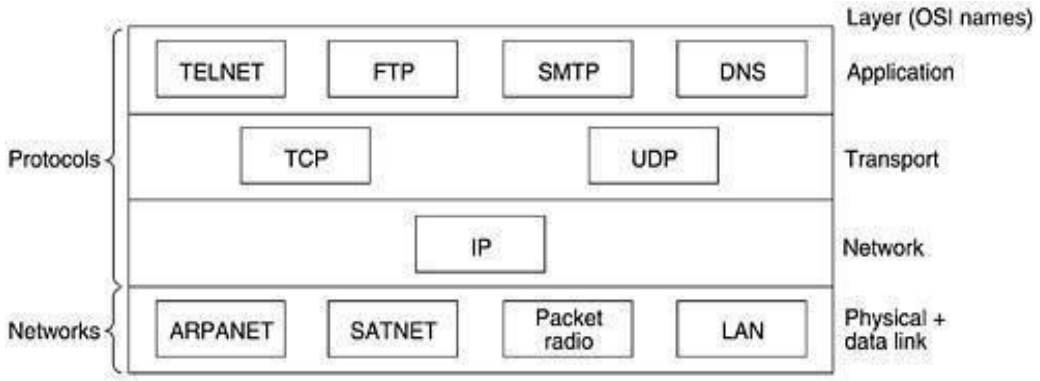
The Internet Layer: This layer is the linchpin that holds the whole architecture together. Its job is to permit hosts to inject packets into any network and have them travel independently to the destination (potentially on a different network). They may even arrive in a different order than they were sent, in which case it is the job of higher layers to rearrange them, if in-order delivery is desired.

The internet layer defines an official packet format and protocol called IP (Internet Protocol). The job of the internet layer is to deliver IP packets where they are supposed to go. Packet routing is clearly the major issue here, as is avoiding congestion. For these reasons, it is reasonable to say that the TCP/IP internet layer is similar in functionality to the OSI network layer. Figure 2 shows this correspondence.

The Transport Layer: The layer above the internet layer in the TCP/IP model is now usually called the transport layer. Two end-to-end transport protocols have been defined here. The first one, TCP (Transmission Control Protocol), is a reliable connection- oriented protocol that allows a byte stream originating on one machine to be delivered without error on any other machine in the internet. TCP also handles flow control to make sure a fast sender cannot swamp a slow receiver with more messages than it can handle.

The second protocol in this layer, UDP (User Datagram Protocol), is an unreliable, connectionless protocol for applications that do not want TCP's sequencing or flow control and wish to provide their own. It is also widely used for one-shot, client-server- type request-reply queries and applications in which prompt delivery is more important than accurate delivery, such as transmitting speech or video. The relation of IP, TCP, and UDP is shown in Fig.3. Since the model was developed, IP has been implemented on many other networks.

Figure 3. Protocols and networks in the TCP/IP model initially.



The Application Layer: On top of the transport layer is the application layer. It contains all the higher-level protocols. The early ones included virtual terminal (TELNET), file transfer (FTP), and electronic mail (SMTP), as shown in Fig 3

The file transfer protocol provides a way to move data efficiently from one machine to another. Electronic mail was originally just a kind of file transfer but later a specialized protocol (SMTP) but later a specialized protocol (SMTP) was developed for it. Many other protocols have been added to these over the years: the Domain Name System (DNS) for mapping host names onto their network addresses, NNTP, the protocol for moving USENET news articles around, and HTTP, the protocol for fetching pages on the World Wide Web, and many others.

The Host-to-Network Layer: Below the internet layer is a great void. The TCP/IP reference model does not really say much about what happens here, except to point out that the host has to connect to the network using some protocol so it can send IP packets to it. This protocol is not defined and varies from host to host and network to network. Books and papers about the TCP/IP model rarely discuss it.

A Comparison of the OSI and TCP/IP Reference Models

The OSI and TCP/IP reference models have much in common. Both are based on the concept of a stack of independent protocols. Also, the functionality of the layers is roughly similar. For example, in both models the layers up through and including the transport layer are there to provide an end-to-end, network-independent transport service to processes wishing to communicate. These layers form the transport provider. Again in both models, the layers above transport are application-oriented users of the transport service.

Three concepts are central to the OSI model:

1. Services.
2. Interfaces.
3. Protocols.

Probably the biggest contribution of the OSI model is to make the distinction between these three concepts explicit. Each layer performs some services for the layer above it. The service definition tells what the layer does, not how entities above it access it or how the layer works. It defines the layer's semantics.

A layer's interface tells the processes above it how to access it. It specifies what the parameters are and whatresults to expect. It, too, says nothing about how the layer works inside.

Finally, the peer protocols used in a layer are the layer's own business. It can use any protocols it wants to, as long as it gets the job done (i.e., provides the offered services). It can also change them at will without affectingsoftware in higher layers.

These ideas fit very nicely with modern ideas about object-oriented programming. An object, like a layer, has a set of methods (operations) that processes outside the object can invoke. The semantics of these methods define the set of services that the object offers. The methods' parameters and results form the object's interface. The code internal to the object is its protocol and is not visible or of any concern outside the object.

The TCP/IP model did not originally clearly distinguish between service, interface, and protocol, although people have tried to retrofit it after the fact to make it more OSI-like. For example, the only real services offered by the internet layer are SEND IP PACKET and RECEIVE IP PACKET.

As a consequence, the protocols in the OSI model are better hidden than in the TCP/IP model and can be replaced relatively easily as the technology changes. Being able to make such changes is one of the main purposes of having layered protocols in the first place.

The OSI reference model was devised before the corresponding protocols were invented. This ordering means that the model was not biased toward one particular set of protocols, a fact that made it quite general. The downside of this ordering is that the designers did not have much experience with the subject and did not have a good idea of which functionality to put in which layer.

For example, the data link layer originally dealt only with point-to-point networks. When broadcast networks came around, a new sub layer had to be hacked into the model. When people started to build real networks using the OSI model and existing protocols, it was discovered that these networks did not match the required service specifications (wonder of wonders), so convergence sub layers had to be grafted onto the model to provide a place for papering over the differences. Finally, the committee originally expected that each country would have one network, run by the government and using the OSI protocols, so no thought was given to internetworking. To make a long story short, things did not turn out that way.

With TCP/IP the reverse was true: the protocols came first, and the model was really just a description of the existing protocols. There was no problem with the protocols fitting the model. They fit perfectly. The only trouble was that the model did not fit any other protocol stacks. Consequently, it was not especially useful for describing other, non- TCP/IP networks.

Turning from philosophical matters to more specific ones, an obvious difference between the two models is the number of layers: the OSI model has seven layers and the TCP/IP has four layers.

EXPERIMENT-- 7

AIM: STUDY OF PARALLEL AND SERIAL TRANSMISSION.

Data transmission:

Data transmission, digital transmission or digital communications is the physical transfer of data (a digital bit stream) over a point-to-point or point-to-multipoint communication channel. Examples of such channels are copper wires, optical fibres, wireless communication channels, and storage media. The data is represented as an electro-magnetic signal, such as an electrical voltage, radiowave, microwave or infra-red signal. While analog communications is the transfer of continuously varying information signal, digital communications is the transfer of discrete messages. The messages are either represented by a sequence of pulses by means of a line code (baseband transmission), or by a limited set of continuously varying wave forms (passband transmission), using a digital modulation method. The passband modulation and corresponding demodulation (also known as detection) is carried out by modem equipment. According to the most common definition of digital signal, both baseband and passband signals representing bit-streams are considered as digital transmission, while an alternative definition only considers the baseband signal as digital, and passband transmission of digital data as a form of digital-to-analog conversion.

Data transmitted may be digital messages originating from a data source, for example a computer or a keyboard. It may also be an analog signal such as a phone call or a video signal, digitized into a bit-stream for example using pulse-code modulation (PCM) or more advanced source coding (analog-to-digital conversion and data compression) schemes. This source coding and decoding is carried out by codec equipment.

Baseband or passband transmission:

The physically transmitted signal may be one of the following:

1. A baseband signal

("digital-over-digital" transmission): A sequence of electrical pulses or light pulses produced by means of a line-coding scheme such as Manchester coding. This is typically used in serial cables, wired local area networks such as Ethernet, and in optical fiber communication. It results in a pulse amplitude modulated signal, also known as a pulse train.

2. A passband signal

("digital-over-analog" transmission): A modulated sine wave signal representing a digital bit-stream. Note that this is in some textbooks considered as analog transmission, but in most books as digital transmission. The signal is produced by means of a digital modulation method such as PSK, QAM or FSK. The modulation and demodulation is carried out by modem equipment. This is used in wireless communication, and over telephone network local-loop and cable-TV networks.

Serial and parallel transmission:

serial transmission is the sequential transmission of signal elements of a group representing a character or other entity of data. Digital serial transmissions are bits sent over a single wire, frequency or optical path sequentially. Because it requires less signal processing and less chances for error than parallel transmission, the transfer rate of each individual path may be faster. This

can be used over longer distances as a check digit or parity bit can be sent along it easily.

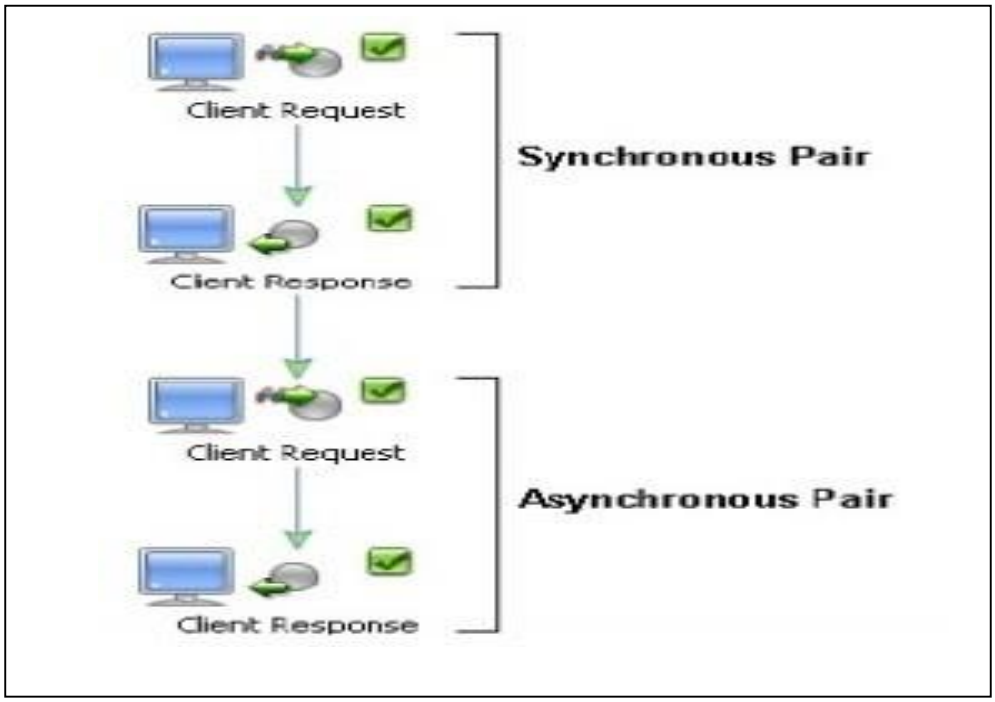
In telecommunications, parallel transmission is the simultaneous transmission of the signal elements of a character or other entity of data. In digital communications, parallel transmission is the simultaneous transmission of related signal elements over two or more separate paths. Multiple electrical wires are used which can transmit multiple bits simultaneously, which allows for higher data transfer rates than can be achieved with serial transmission. This method is used internally within the computer, for example the internal buses, and sometimes externally for such things as printers, The major issue with this is "skewing" because the wires in parallel data transmission have slightly different properties (not intentionally) so some bits may arrive before others, which may corrupt the message. A parity bit can help to reduce this. However, electrical wire parallel data transmission is therefore less reliable for long distances because corrupt transmissions are far more likely.

Asynchronous and synchronous data transmission:

Asynchronous transmission uses start and stop bits to signify the beginning bit character would actually be transmitted using 10 bits e.g.: A "0100 0001" would become "**1** 0100 0001 **0** ". The extra one at the start and end of the transmission tells the receiver first that a character is coming and secondly that the character has ended. This method of transmission is used when data is sent intermittently as opposed to in a solid stream. In the previous example the start and stop bits are in bold. The start and stop bits must be of opposite polarity. This allows the receiver to recognize when the second packet of information is being sent.

Synchronous transmission uses no start and stop bits but instead synchronizes transmission speeds at both the receiving and sending end of the transmission using clock signal(s) built into each component. A continual stream of data is then sent between the two nodes. Due to there being no start and stop bits the data transfer rate is quicker although more errors will occur, as the clocks will eventually get out of sync, and the receiving device would have the wrong time that had been agreed sending/receiving data, so some bytes could become corrupted. Ways to get around this problem include re-synchronization of the clocks and use of check digits to ensure the byte is correctly interpreted and received

Image of synchronous and asynchronous transmission



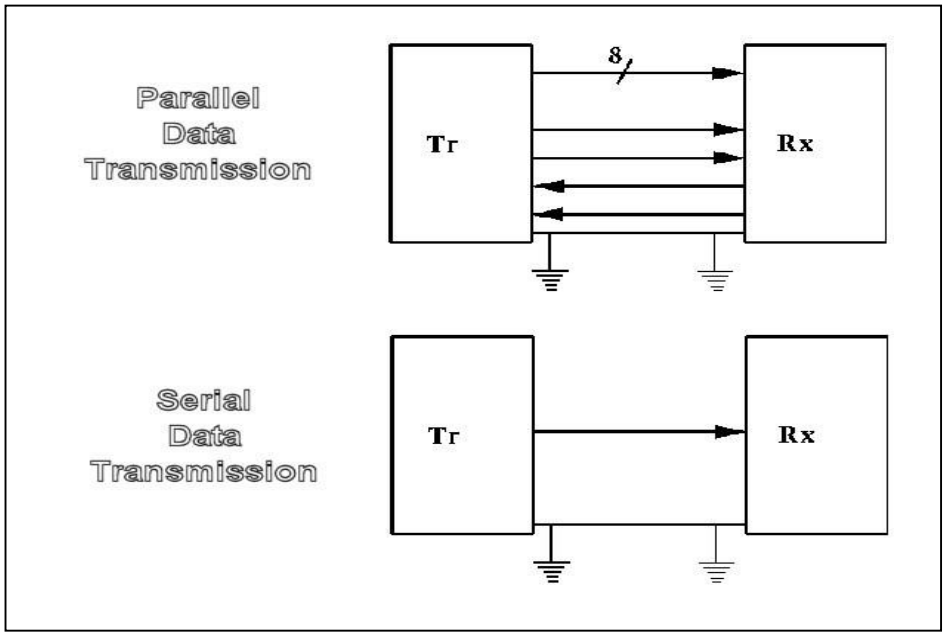
Serial data transmission: the process of transmitting binary words a bit at a time. Since the bits time-share the transmission medium, only one interconnecting lead is required. While serial data transmission is much simpler and less expensive because of the use of a single interconnecting line, it is a very slow method of data transmission. Serial data transmission is useful in systems where high speed is not a requirement. Serial data transmission techniques are widely used in transmitting data between a computer and its peripheral units. While the computer operates at very high speeds, most peripheral units are slow because of their electro mechanical nature. Slower serial data transmission is more compatible with such devices. Since the speed of serial transmission is more than adequate in such units, the advantages of low cost and simplicity of the signal interconnecting obtained.

Parallel data transmission: In a parallel data transmission system, each bit of the binary word to be transmitted must have its own data path. There are a variety of ways to implement this data path. The two basic classifications of transmission line circuits are single-ended and balanced. Single-ended transmission systems use a single-wire data path for each bit. When combined with a ground or return reference, the electrical circuit between the sending circuit and the receiving circuit is complete. In a balanced transmission line system, two conductor cables are used to send the data. The data on the dual-transmission line is complementary. The dual-transmission lines also use a ground return reference. While a single-ended transmission line is simpler and less expensive, it is subject to more noise problems than the balanced or dual-transmission line system

Parallel versus serial data transmission: there are two methods of transmitting digital data. These methods are parallel and serial transmissions. In parallel data transmission, all bits of the binary data are transmitted simultaneously. For example, to transmit an 8 bit binary number in parallel

from one unit to another, eight transmission lines are required. Each bit requires its own separate data path. All bits of a word are transmitted at the same time. This method of transmission can move a significant amount of data in a given period of time. Its disadvantage is the large number of interconnecting cables between the two units. For large binary words, cabling becomes complex and expensive. This is particularly true if the distance between the two units is great. Long multi wire cables are not only expensive, but also require special interfacing to minimize noise and distortion problems.

Images of the transmission:



Number of channels:

Serial Communications and Parallel communications both define a way of transportation of data over networks.

- In Serial devices: transmit data bit-after-bit, serially over time. When 8 bits are received, after 8 bit-times (plus a little extra for signal synchronization), they are assembled back into a byte and delivered to the software.
- In Parallel communication: a word of some data length, say like 8 bits, travels all at once, along multiple parallel channels (one channel per bit position). At the receiver, an 8-bit byte is received every "bit time". In effect, you have 8 serial channels transmitting and receiving data simultaneously, making it (by definition) at least 8 times faster than a single serial channel using the same transceiver technology.

Advantages:

Serial Transmission:

1. It is cheaper than Parallel transmission.
2. Need only one communication channel and reduces the cost of transmission by factor n.

Parallel transmission:

1. speed increases by the factor n.

Disadvantages of Parallel transmission:

1. It is costly.
2. Used for short distances only.

Disadvantages of serial transmission:

1. Causes slower transmission.

EXPERIMENT—8

AIM:- Study of digital interface RS-232

In telecommunications **RS-232** (Recommended Standard 232) is a standard for serial binary single-ended data and control signals connecting between a DTE (Data Terminal Equipment) and a DCE (Data Circuit-terminating Equipment). It is commonly used in computer serial ports. The standard defines the electrical characteristics and timing of signals, the meaning of signals, and the physical size and pin out of connectors.

Scope of the standard

The Electronics Industries Association (EIA) standard RS-232-C as of 1969 defines:

- Electrical signal characteristics such as voltage levels, signaling rate, timing and slew-rate of signals, voltage withstand level, short-circuit behavior, and maximum load capacitance.
- Interface mechanical characteristics, pluggable connectors and pin identification.
- Functions of each circuit in the interface connector.
- Standard subsets of interface circuits for selected telecom applications. The standard does not define such elements as character encoding (for example, ASCII, Baudot code or EBCDIC)
- the framing of characters in the data stream (bits per character, start/stop bits, parity
- protocols for error detection or algorithms for data compression
- bit rates for transmission, although the standard says it is intended for bit rate slower than 20,000 bits per second. Many modern devices support speeds of 115,200 bit/s and above
- power supply to external devices.

History

RS-232 was first introduced in 1962. The original DTEs were electro mechanical tele typewriters and the original DCEs were (usually) modems. When electronic terminals (smart and dumb) began to be used, they were often designed to be interchangeable with teletypes, and so supported RS-232. The C revision of the standard was issued in 1969 in part to accommodate the electrical characteristics of these devices. The standard has been renamed several times during its history as the sponsoring organization changed its name, and has been variously known as EIA RS-232, EIA 232, and most recently as TIA 232. The standard continued to be revised and updated by the Electronic Industries Alliance and since 1988 by the Telecommunications Industry Association (TIA). Revision C was issued in a document dated August 1969. Revision D was issued in 1986).

Limitations of the standard

- The large voltage swings and requirement for positive and negative supplies increases power consumption of the interface and complicates power supply design. The voltage swing requirement also limits the upper speed of a compatible interface.
- Single-ended signaling referred to a common signal ground limits the noise immunity and transmission distance.
- Multi-drop connection among more than two devices is not defined. While multi-drop "work-around" has been devised, they have limitations in speed and compatibility.

- Asymmetrical definitions of the two ends of the link make the assignment of the role of a newly developed device problematic; the designer must decide on either a DTE-like or DCE-like interface and which connector pin assignments to use.
- The handshaking and control lines of the interface are intended for the setup and take down of a dial-up communication circuit; in particular, the use of handshake lines for flow control is not reliably implemented in many devices. .
- The 25-way connector recommended in the standard is large compared to current practice.

Role in modern personal computers

PCI Express x1 card with one RS-232 port In the book PC 97 Hardware Design Guide, Microsoft deprecated support for the RS-232 compatible serial port of the original IBM PC design. Today, RS-232 has mostly been replaced in personal computers by USB for local communications. Compared with RS-232, USB is faster, uses lower voltages, and has connectors that are simpler to connect and use. Both standards have software support in popular operating systems. USB is designed to make it easy for device drivers to communicate with hardware. However, there is no direct analog to the terminal programs used to let users communicate directly with serial ports

Standard details

In RS-232, user data is sent as a time-series of bits. Both synchronous and asynchronous transmissions are supported by the standard. In addition to the data circuits, the standard defines a number of control circuits used to manage the connection between the DTE and DCE. Each data or control circuit only operates in one direction, that is, signaling from a DTE to the attached DCE or the reverse. Since transmit data and receive data are separate circuits, the interface can operate in a full duplex manner, supporting concurrent data flow in both directions. The standard does not define character framing within the data stream, or character encoding.

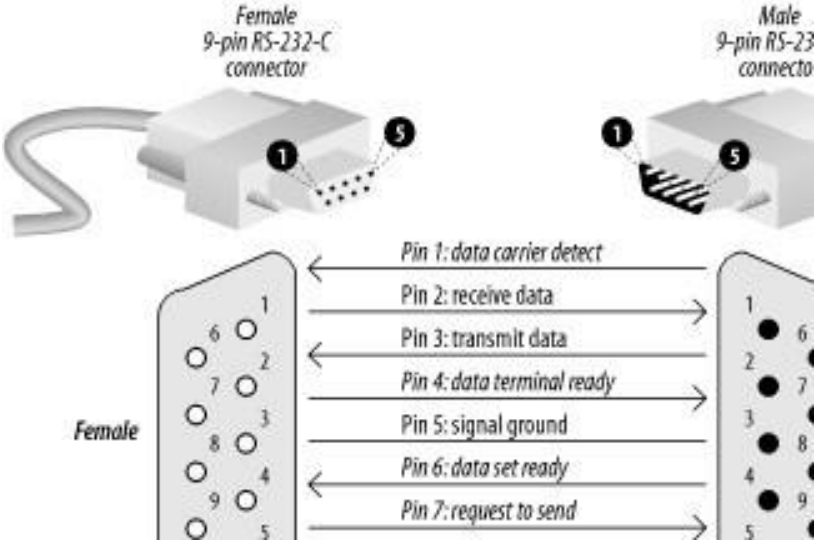
Voltage levels

is grammatic oscilloscope trace of voltage levels for an uppercase ASCII "K" character (0x4b) with 1 start bit, 8 data bits, 1 stop bit. The RS-232 standard defines the voltage levels that correspond to logical one and logical zero levels for the data transmission and the control signal lines. Valid signals are plus or minus 3 to15 volts; the ±3 V range near zero volts is not a valid RS-232 level. The standard specifies a maximum open-circuit voltage of 25 volts: signal levels of ±5 V, ±10 V, ±12 V, and ±15 V are all commonly seen depending on the power supplies available within a device. RS-232 drivers and receivers must be able to withstand indefinite short circuit to ground or to any voltage level up to ±25 volts. The slow or how fast the signal changes between levels, is also controlled.

Connectors

RS-232 devices may be classified as Data Terminal Equipment (DTE) or Data Communication Equipment (DCE); this defines at each device which wires will be sending and receiving each signal. The standard recommended but did not make mandatory the D-subminiature 25 pin connector. In general and according to the standard, terminals and computers have male connectors with DTE pin functions, and modems have female connectors with DCE pin functions. Other devices may have any combination of connector gender and pin definitions.

Many terminals were manufactured with female terminals but were sold with a cable with male connectors at each end; the terminal with its cable satisfied the recommendations in the standard.



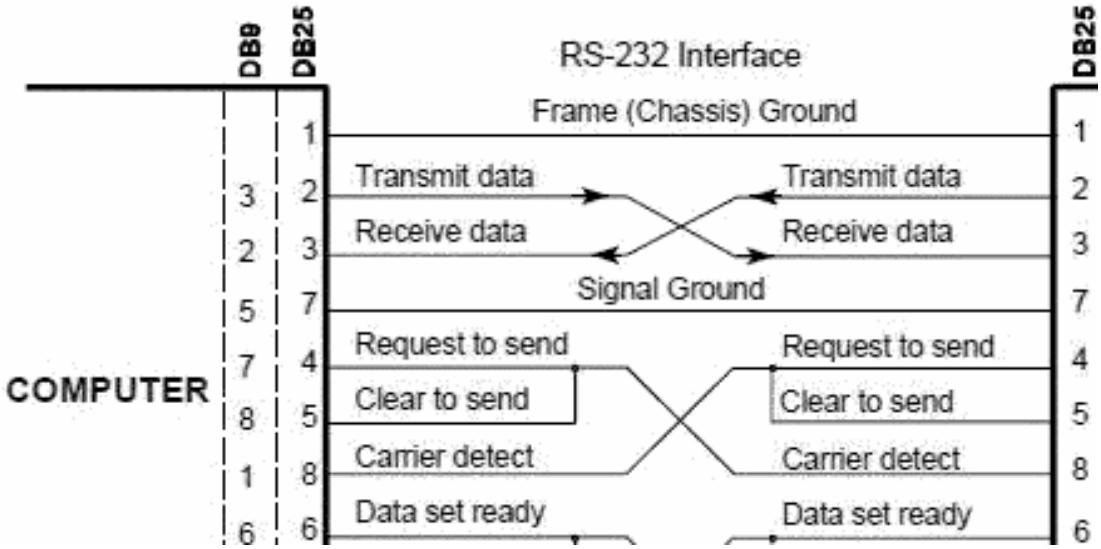
Conventions

For functional communication through a serial port interface, conventions of bit rate, character framing, communications protocol, character encoding, data compression, and error detection, not defined in RS 232, must be agreed to by both sending and receiving equipment. For example, consider the serial ports of the original IBM PC. This implementation used an 8250 UART using asynchronous start-stop character formatting with 7 or 8 data bits per frame, usually ASCII character coding, and data rates programmable between 75 bits per second and 115,200 bits per second. Data rates above 20,000 bits per second are out of the scope of the standard, although higher data rates are sometimes used by commercially manufactured equipment. In the particular case of the IBM PC, baud rates were programmable with arbitrary values, so that a PC could be connected to, for example, MIDI music controllers (31,250 bits per second) or other devices not using the rates typically used with modems. Since most devices do not have automatic baud rate detection, users must manually set the baud rate (and all other parameters) at both ends of theRS-232 connection.

RTS/CTS handshaking

Further information: Hardware flow control

In older versions of the specification, RS-232's use of the RTS and CTS lines is asymmetric: The DTE asserts RTS to indicate a desire to transmit to the DCE, and the DCE asserts CTS in response to grant permission. This allows for half-duplex modems that disable their transmitters when not required, and must transmit a synchronization preamble to the receiver when they are re-enabled. This scheme is also employed on present-day RS-232 to RS-485 converters, where the RS-232's RTS signal is used to ask the converter to take control of the RS-485 bus – a concept that doesn't otherwise exist in RS-232. There is no way for the DTE to indicate that it is unable to accept data from the DCE.



3-wire and 5-wire RS-232

A minimal "3-wire" RS-232 connection consisting only of transmits data, receive data, and ground, is commonly used when the full facilities of RS-232 are not required. Even a two-wire connection (data and ground) can be used if the data flow is one way (for example, a digital postal scale that periodically sends a weight reading, or a GPS receiver that periodically sends position, if no configuration via RS-232 is necessary). When only hardware flow control is required in addition to two-way data, the RTS and CTS lines are added in a 5-wire version.

Seldom used features

The EIA-232 standard specifies connections for several features that are not used in most implementations. Their use requires the 25-pin connectors and cables, and of course both the DTE and DCE must support them.

Signal rate selection

The DTE or DCE can specify use of a "high" or "low" signaling rate. The rates as well as which device will select the rate must be configured in both the DTE and DCE. The prearranged device selects the high rate by setting pin 23 to ON.

Loopback testing

Many DCE devices have a loopback capability used for testing. When enabled, signals are echoed back to the sender rather than being sent on to the receiver. If supported, the DTE can signal the local DCE (the one it is connected to) to enter loopback mode by setting pin 18 to ON, or the remote DCE (the one the local DCE is connected to) to enter loopback mode by setting pin21 to ON. The latter tests the communications link as well as both DCE's. When the DCE is in test mode it signals the DTE by setting pin 25 to ON.A commonly used version of loopback testing doesn't involve any special capability of either end. A hardware loopback is simply a wire connecting complementary pins together in the same connector. Loopback testing is often performed with a specialized DTE called a Bit Error Rate Tester.

Timing signals

Some synchronous devices provide a clock signal to synchronize data transmission, especially at higher data rates. Two timing signals are provided by the DCE on pins 15 and 17. Pin 15 is the transmitter clock, or send timing (ST); the DTE puts the next bit on the data line (pin 2) when this clock transitions from OFF to ON (so it is stable during the ON to OFF transition when the DCE registers the bit). Pin 17 is the receiver clock, or receive timing (RT); the DTE reads the next bit from the data line (pin 3) when this clock transitions from ON to OFF.

Related standards

Other serial signaling standards may not interoperate with standard-compliant RS-232 ports. For example, using the TTL levels of near +5 and 0 V puts the mark level in the undefined area of the standard. Such levels are sometimes used with NMEA 0183-compliant GPS receivers and depth finders. Other serial interfaces similar to RS-232:

- RS-422 (a high-speed system similar to RS-232 but with differential signaling)
- RS-423 (a high-speed system similar to RS-422 but with unbalanced signaling)
- RS-449 (a functional and mechanical interface that used RS-422 and RS-423 signals – itnever caught on like RS-232 and was withdrawn by the EIA)
- RS-485 (a descendant of RS-422 that can be used as a bus in multi drop configurations)
- MIL-STD-188 (a system like RS-232 but with better impedance and rise time control)
- EIA-530 (a high-speed system using RS-422 or RS-423 electrical properties in an EIA-232pin out configuration, thus combining the best of both; supersedes RS-449)

EXPERIMENT—9

AIM: - Study of network interface card (NIC)

Definition:-

A network interface card, more commonly referred to as a NIC, is a device that allows computers to be joined together in a LAN, or local area network. Networked computers communicate with each other using a given protocol or agreed-upon language for transmitting data packets between the different machines, known as nodes. The network interface card acts as the liaison for the machine to both send and receive data on the LAN.

Types of NIC:-

Network interface cards, referred to as NICs, are PC integrate cards that give inter-networking capabilities for a particular computing solution. There are many types of NICs that are utilized in changeable situations. The biggest variation between cards is depending upon their connective medium and speed capabilities. To a lesser extent, NICs can be distinguished by their type of connectivity to PC.

1. 10/100 Ethernet

These are networking cards that are utilized often in home or small office setting. As name implies, they are able of speeds up to 10 or 100 megabits per second, not to be confused with megabytes per second. These cards generally attach to PC using a PCI, PCIe or ISA motherboard interface slot. These cards are setup to utilize category 5 or 6 networking cables. The variation between category 5 and 6 networking cables is addition of more shielding in category 6 cable to decrease "cross-talk" that slows network transfer speeds.

2. Gigabit Ethernet

Gigabit Ethernet NICs give network transfer speeds of up to one Gigabit per second. These cards attach to PC using same means as before mentioned, though, they are much more likely to be formed for PCIe slots. These NICs can use Category 5, 5e, 6, and 7 cabling, with a preference for latter. Though, these NICs are more frequently created to use fiber optic cables for utilize in enterprise solutions like web servers or data storage centers.

EXPERIMENT—10

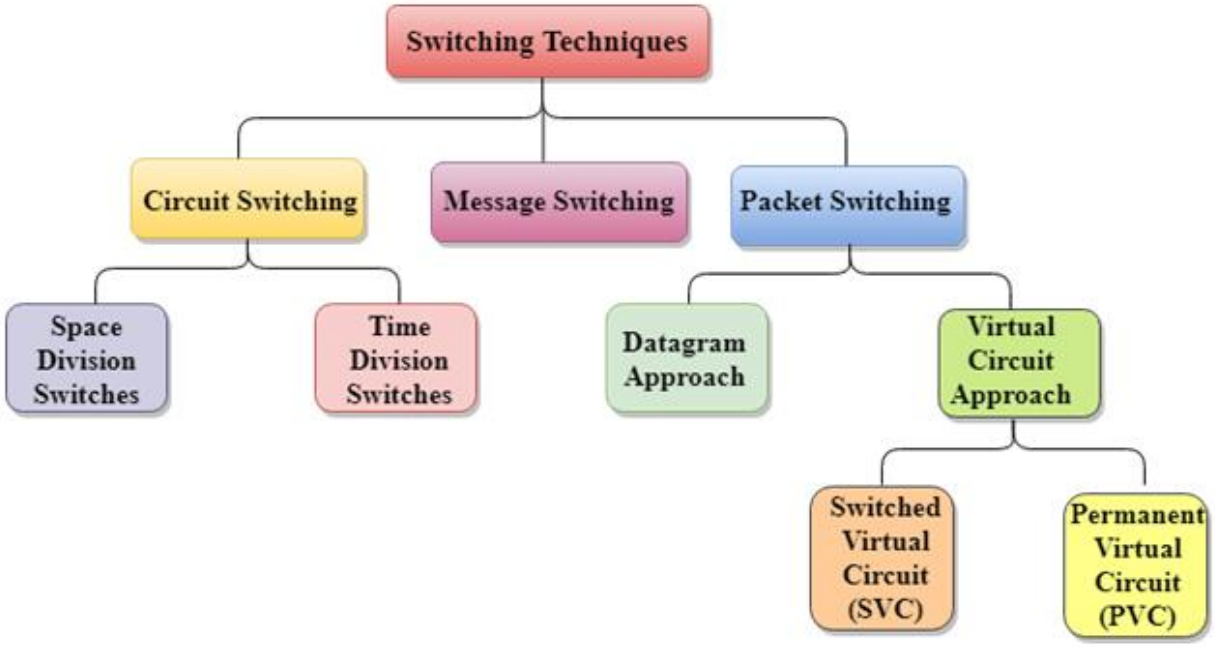
AIM: - Study of different switching technique.

Switching techniques-

In large networks, there can be multiple paths from sender to receiver. The switching technique will decide the best route for data transmission.

Switching technique is used to connect the systems for making one-to-one communication.

Classification Of Switching Techniques



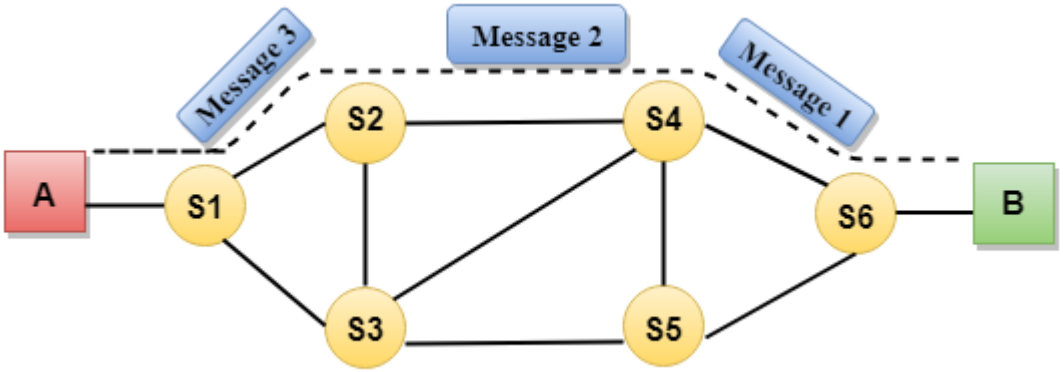
1) Circuit Switching-

- Circuit switching is a switching technique that establishes a dedicated path between sender and receiver.
- In the Circuit Switching Technique, once the connection is established then the dedicated path will remain to exist until the connection is terminated.
- Circuit switching in a network operates in a similar way as the telephone works.
- A complete end-to-end path must exist before the communication takes place.

- In case of circuit switching technique, when any user wants to send the data, voice, video, a request signal is sent to the receiver then the receiver sends back the acknowledgment to ensure the availability of the dedicated path. After receiving the acknowledgment, dedicated path transfers the data.
- Circuit switching is used in public telephone network. It is used for voice transmission.
- Fixed data can be transferred at a time in circuit switching technology

Communication through circuit switching has 3 phases:

- Circuit establishment
- Data transfer
- Circuit Disconnect



Circuit Switching can use either of the two technologies:

Space Division Switches:

- Space Division Switching is a circuit switching technology in which a single transmission path is accomplished in a switch by using a physically separate set of crosspoints.
- Space Division Switching can be achieved by using crossbar switch. A crossbar switch is a metallic crosspoint or semiconductor gate that can be enabled or disabled by a control unit.
- The Crossbar switch is made by using the semiconductor. For example, Xilinx crossbar switch using FPGAs.
- Space Division Switching has high speed, high capacity, and nonblocking switches.

Space Division Switches can be categorized in two ways:

- **Crossbar Switch**

- **Multistage Switch**

Crossbar Switch

The Crossbar switch is a switch that has n input lines and n output lines. The crossbar switch has n^2 intersection points known as **crosspoints.**

Disadvantage of Crossbar switch:

The number of crosspoints increases as the number of stations is increased. Therefore, it becomes very expensive for a large switch. The solution to this is to use a multistage switch.

Multistage Switch

- Multistage Switch is made by splitting the crossbar switch into the smaller units and then interconnecting them.
- It reduces the number of crosspoints.
- If one path fails, then there will be an availability of another path.

Advantages Of Circuit Switching:

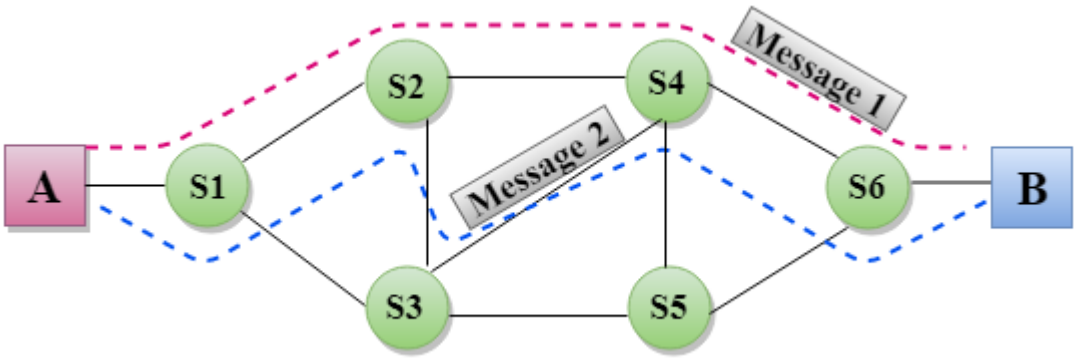
- In the case of Circuit Switching technique, the communication channel is dedicated.
- It has fixed bandwidth.

Disadvantages Of Circuit Switching:

- Once the dedicated path is established, the only delay occurs in the speed of data transmission.
- It takes a long time to establish a connection approx 10 seconds during which no data can be transmitted.
- It is more expensive than other switching techniques as a dedicated path is required for each connection.
- It is inefficient to use because once the path is established and no data is transferred, then the capacity of the path is wasted.
- In this case, the connection is dedicated therefore no other data can be transferred even if the channel is free.

Message Switching

- Message Switching is a switching technique in which a message is transferred as a complete unit and routed through intermediate nodes at which it is stored and forwarded.
- In Message Switching technique, there is no establishment of a dedicated path between the sender and receiver.
- The destination address is appended to the message. Message Switching provides a dynamic routing as the message is routed through the intermediate nodes based on the information available in the message.
- Message switches are programmed in such a way so that they can provide the most efficient routes.
- Each and every node stores the entire message and then forward it to the next node. This type of network is known as **store and forward network.**
- Message switching treats each message as an independent entity.



Advantages Of Message Switching

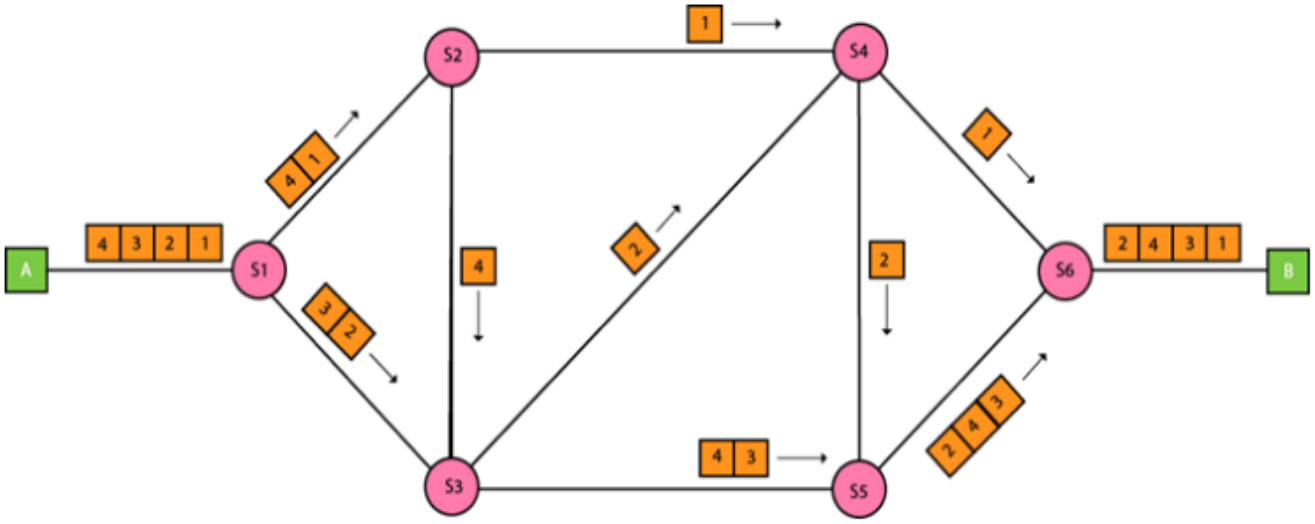
- Data channels are shared among the communicating devices that improve the efficiency of using available bandwidth.
- Traffic congestion can be reduced because the message is temporarily stored in the nodes.
- Message priority can be used to manage the network.
- The size of the message which is sent over the network can be varied. Therefore, it supports the data of unlimited size.

Disadvantages Of Message Switching

- The message switches must be equipped with sufficient storage to enable them to store the messages until the message is forwarded.
- The Long delay can occur due to the storing and forwarding facility provided by the message switching technique.

Packet Switching

- The packet switching is a switching technique in which the message is sent in one go, but it is divided into smaller pieces, and they are sent individually.
- The message splits into smaller pieces known as packets and packets are given a unique number to identify their order at the receiving end.
- Every packet contains some information in its headers such as source address, destination address and sequence number.
- Packets will travel across the network, taking the shortest path as possible.
- All the packets are reassembled at the receiving end in correct order.
- If any packet is missing or corrupted, then the message will be sent to resend the message.
- If the correct order of the packets is reached, then the acknowledgment message will be sent.



Approaches Of Packet Switching:

There are two approaches to Packet Switching:

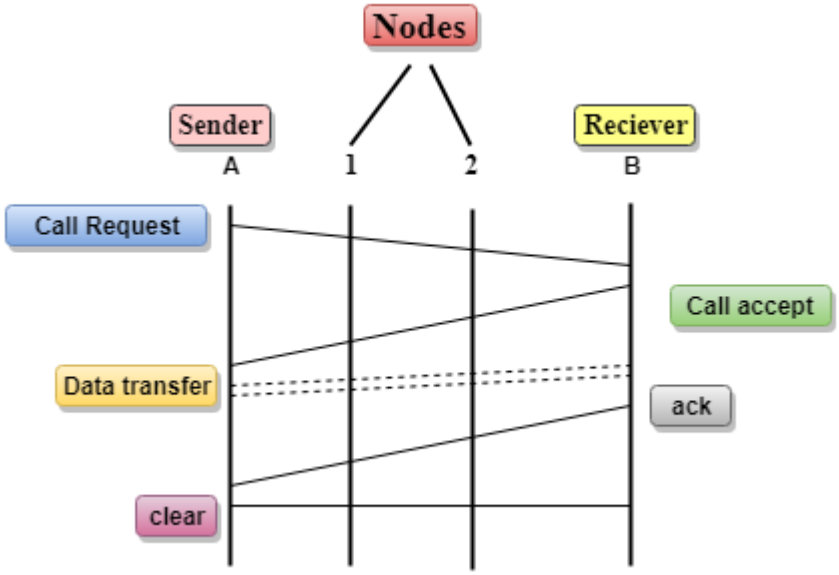
Datagram Packet switching:

- It is a packet switching technology in which packet is known as a datagram, is considered as an independent entity. Each packet contains the information about the destination and switch uses this information to forward the packet to the correct destination.
- The packets are reassembled at the receiving end in correct order.
- In Datagram Packet Switching technique, the path is not fixed.
- Intermediate nodes take the routing decisions to forward the packets.
- Datagram Packet Switching is also known as connectionless switching.

Virtual Circuit Switching

- Virtual Circuit Switching is also known as connection-oriented switching.
- In the case of Virtual circuit switching, a preplanned route is established before the messages are sent.
- Call request and call accept packets are used to establish the connection between sender and receiver.
- In this case, the path is fixed for the duration of a logical connection.

Let's understand the concept of virtual circuit switching through a diagram:



- In the above diagram, A and B are the sender and receiver respectively. 1 and 2 are the nodes.
- Call request and call accept packets are used to establish a connection between the sender and receiver.

- When a route is established, data will be transferred.
- After transmission of data, an acknowledgment signal is sent by the receiver that the message has been received.
- If the user wants to terminate the connection, a clear signal is sent for the termination.

Differences b/w Datagram approach and Virtual Circuit approach

Datagram approach	Virtual Circuit approach
Node takes routing decisions to forward the packets.	Node does not take any routing decision.
Congestion cannot occur as all the packets travel in different directions.	Congestion can occur when the node is busy, and it does not allow other packets to pass through.
It is more flexible as all the packets are treated as an independent entity.	It is not very flexible.

Advantages Of Packet Switching:

- **Cost-effective:** In packet switching technique, switching devices do not require massive secondary storage to store the packets, so cost is minimized to some extent. Therefore, we can say that the packet switching technique is a cost-effective technique.
- **Reliable:** If any node is busy, then the packets can be rerouted. This ensures that the Packet Switching technique provides reliable communication.
- **Efficient:** Packet Switching is an efficient technique. It does not require any established path prior to the transmission, and many users can use the same communication channel simultaneously, hence makes use of available bandwidth very efficiently.

Disadvantages Of Packet Switching:

- Packet Switching technique cannot be implemented in those applications that require low delay and high-quality services.

- The protocols used in a packet switching technique are very complex and requires high implementation cost.
- If the network is overloaded or corrupted, then it requires retransmission of lost packets. It can also lead to the loss of critical information if errors are nor recovered.