



Lab Code:20EC504/JO1B
Data Communication & Computer
Networks Lab Manual



Department of Electronics & Communication
Engineering

Bapatla Engineering College :: Bapatla
(Autonomous)

G.B.C. Road, Mahatmajipuram, Bapatla-522102, Guntur (Dist.)
Andhra Pradesh, India.

E-Mail:bec.principal@becbapatla.ac.in

Web:www.becbapatla.ac.in

Contents

S.No.	Title of the Experiment
1.	STUDY OF DIFFERENT TYPES OF NETWORK CABLES
2.	EXECUTE THE FOLLOWING COMMANDS
3.	STUDY OF DIFFERENT TYPES OF CABLES
4.	PRACTICALLY IMPLEMENT THE CROSS – WIRED CABLE AND STRAIGHT WIRED CABLE USING CRIMPING TOOL
5.	STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION OF ADDRESS, STATIC AND DYNAMIC ADDRESS)
6.	STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION IPV4 AND IPV6, SUBNET, SUPERNET)
7.	STUDY OF NETWORK DEVICES (SWITCH, ROUTER BRIDGE)
8.	Study of network IP
9.	Connect the computers in Local Area Network.
10.	CPU scheduling algorithms
11.	To perform the working of CSMA-CD protocol.
12.	CSMA-CA PROTOCOL

Bapatla Engineering College :: Bapatla (Autonomous)

Vision

- To build centers of excellence, impart high quality education and instill high standards of ethics and professionalism through strategic efforts of our dedicated staff, which allows the college to effectively adapt to the ever changing aspects of education.
- To empower the faculty and students with the knowledge, skills and innovative thinking to facilitate discovery in numerous existing and yet to be discovered fields of engineering, technology and interdisciplinary endeavors.

Mission

- Our Mission is to impart the quality education at par with global standards to the students from all over India and in particular those from the local and rural areas.
- We continuously try to maintain high standards so as to make them technologically competent and ethically strong individuals who shall be able to improve the quality of life and economy of our country.

Bapatla Engineering College :: Bapatla
(Autonomous)
Department of Electronics and Communication
Engineering

Vision

To produce globally competitive and socially responsible Electronics and Communication Engineering graduates to cater the ever changing needs of the society.

Mission

- To provide quality education in the domain of Electronics and Communication Engineering with advanced pedagogical methods.
- To provide self learning capabilities to enhance employability and entrepreneurial skills and to inculcate human values and ethics to make learners sensitive towards societal issues.
- To excel in the research and development activities related to Electronics and Communication Engineering.

Bapatla Engineering College :: Bapatla**(Autonomous)****Department of Electronics and Communication****Engineering**

Program Educational Objectives (PEO's)

PEO-I: Equip Graduates with a robust foundation in mathematics, science and Engineering Principles, enabling them to excel in research and higher education in Electronics and Communication Engineering and related fields.

PEO-II: Impart analytic and thinking skills in students to develop initiatives and innovative ideas for Start-ups, Industry and societal requirements.

PEO-III: Instill interpersonal skills, teamwork ability, communication skills, leadership, and a sense of social, ethical, and legal duties in order to promote lifelong learning and Professional growth of the students.

Program Outcomes (PO's)

Engineering Graduates will be able to:

PO1. Engineering knowledge: Apply the knowledge of mathematics, science, engineering fundamentals, and an engineering specialization to the solution of complex engineering problems.

PO2. Problem analysis: Identify, formulate, review research literature, and analyze complex engineering problems reaching substantiated conclusions using first principles of mathematics, natural sciences, and engineering sciences.

PO3. Design/development of solutions: Design solutions for complex engineering problems and design system components or processes that meet the specified needs with appropriate consideration for the public health and safety, and the cultural, societal, and environmental considerations.

PO4. Conduct investigations of complex problems: Use research-based knowledge and research methods including design of experiments, analysis and interpretation of data, and synthesis of the information to provide valid conclusions.

PO5. Modern tool usage: Create, select, and apply appropriate techniques, resources, and modern engineering and IT tools including prediction and modeling to complex engineering activities with an understanding of the limitations.

PO6. The engineer and society: Apply reasoning informed by the contextual knowledge to assess societal, health, safety, legal and cultural issues and the consequent responsibilities relevant to the professional engineering practice.

PO7.Environment and sustainability: Understand the impact of the professional engineering solutions in societal and environmental contexts, and demonstrate the knowledge of, and need for sustainable development.

PO8. Ethics: Apply ethical principles and commit to professional ethics and responsibilities and norms of the engineering practice.

PO9. Individual and Teamwork: Function effectively as an individual, and as a member or leader in diverse teams, and in multidisciplinary settings.

PO10. Communication: Communicate effectively on complex engineering activities with the engineering community and with society at large, such as, being able to comprehend and write effective reports and design documentation, make effective presentations, and give and receive clear instructions.

PO11. Project management and finance: Demonstrate knowledge and understanding of the engineering and management principles and apply

these to one's own work, as a member and leader in a team, to manage projects and in multidisciplinary environments.

PO12. Life-long learning: Recognize the need for and have the preparation and ability to engage in independent and life-long learning in the broadest context of technological change.

**Bapatla Engineering College :: Bapatla
(Autonomous)**

**Department of Electronics and Communication
Engineering**

Program Specific Outcomes (PSO's)

PSO1: Develop and implement modern Electronic Technologies using analytical methods to meet current as well as future industrial and societal needs.

PSO2: Analyze and develop VLSI, IoT and Embedded Systems for desired specifications to solve real world complex problems.

PSO3: Apply machine learning and deep learning techniques in communication and signal processing.

JOE-1 III B. Tech – V Semester (Code: 20EC504/1B)

DATA COMMUNICATION & COMPUTER NETWORKS

Lectures	2	Tutorial	0	Practical	2	Credits	3		
Continuous Internal Assessment			:	30	Semester End Examination (3 Hours)			:	70

Prerequisites: Basics of Computer hardware and software**Course Objectives:****CO1 (a):** To learn various protocols, Network hardware, and Network software.**CO1 (b):** To understand the working principle of various communication protocols.**CO2 (a):** To gain knowledge about functionality of each layer in OSI, TCP/IP protocols. CO2**(b):** To understand the working principle of data link layer**CO3 (a):** Understand basics and challenges of network communication.**CO3 (b):** To learn about the different types of LANS**CO4 (a):** Interpret the operation of the protocols that are used inside the Internet.**CO4 (b):** To understand the concepts of transport layer protocols**Course Outcomes: Students will be able to****CLO1 (a):** Independently understand basic computer network technology.**CLO1 (b):** Understand fundamental underlying principles of computer networking**CLO2 (a):** Understand and explain Data Communications System and its components.**CLO2 (b):** Understand details and functionality of layered network architecture.**CLO3 (a):** Identify the different types of network topologies and protocols.**CLO3 (b):** Compare routing algorithms**CLO4 (a):** Understand and building the skills of sub netting and routing mechanisms. CLO4 (b):

Analyze performance of various communication internet protocols.

SYLLABUS**UNIT – I**

Introduction to Data Communication and Networking: Uses of Computer Networks, Network Hardware, Network Software Internet Reference Models (OSI and TCP/IP).

Physical Layer: Basis for Data Communication, Guided Transmission Media, Wireless Transmission Medium, Circuit Switching and Telephone Network, High Speed Digital Access.

UNIT – II

Data Link Layer: Data Link Layer Design Issues, Error Detection and Correction, Data Link Control and Protocols, Example Data Link Protocol.

Medium Access Layer: Channel Allocation Problem, Multiple Access, CSMA, CSMA/CD, CSMA/CA.

UNIT – III

Local Area Network: Ethernet, Fast Ethernet, Gigabit Ethernet, Wireless LAN, Blue tooth, Connecting devices:-Repeaters, Hub, Bridges, Switch, Router, Gateways, Virtual LAN, Network Layer: Network Layer Design Issues, Routing Algorithms Congestion control Algorithms,

UNIT – IV

Transport layer: Transport Layer Service, Elements of Transport protocols, Internet protocols (UDP and TCP)

Application Layer: DNS- Domain Name System, Electronic Mail, World Wide Web, Multimedia (Audio Compression, Streaming Audio, Voice over IP, Video Compression, Video on Demand).

TEXT BOOKS:

1. Andrew S. Tanenbaum, David.J.Wetherall, “ComputerNetworks”, Prentice-Hall, 5th Edition, 2010.
2. Behrouz A. Foruzan, Data communication andNetworking, 4thEdition, TMH, 2004.

REFERENCE BOOKS:

1. W.Tomasi,”Introduction to Data Communications and Networking” Pearson education.
2. G.S.Hura and M.Singhal,”Data and Computer Communications”,CRCPress,Taylor and Francis Group.

LIST OF EXPERIMENTS

S.No.	Title of the Experiment
1.	STUDY OF DIFFERENT TYPES OF NETWORK CABLES
2.	EXECUTE THE FOLLOWING COMMANDS
3.	STUDY OF DIFFERENT TYPES OF CABLES
4.	PRACTICALLY IMPLEMENT THE CROSS – WIRED CABLE AND STRAIGHT WIRED CABLE USING CRIMPING TOOL
5.	STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION OF ADDRESS, STATIC AND DYNAMIC ADDRESS)
6.	STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION IPV4 AND IPV6, SUBNET, SUPERNET)
7.	STUDY OF NETWORK DEVICES (SWITCH, ROUTER BRIDGE)
8.	Study of network IP
9.	Connect the computers in Local Area Network.
10.	CPU scheduling algorithms
11.	To perform the working of CSMA-CD protocol.
12.	CSMA-CA PROTOCOL

NOTE: A minimum of 10 (Ten) experiments have to be Performed and recorded by the candidate to attain eligibility for Semester End Examination.

1.STUDY OF DIFFERENT TYPES OF NETWORK CABLES

Aim: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.

Apparatus (Components): RJ-45 connector, Clipping Tool, Twisted pair Cable

Procedure: To do these practical following steps should be done:

1. Start by stripping off about 2 inches of the plastic jacket off the end of the cable. Be very careful at this point, as to not nick or cut into the wires, which are inside. Doing so could alter the characteristics of your cable, or even worse render is useless. Check the wires, one more time for nicks or cuts. If there are any, just whack the whole end off, and start over.
2. Spread the wires apart, but be sure to hold onto the base of the jacket with your other hand. You do not want the wires to become untwisted down inside the jacket. Category 5 cable must only have 1/2 of an inch of 'untwisted' wire at the end; otherwise it will be 'out of spec'. At this point, you obviously have ALOT more than 1/2 of an inch of un-twisted wire.
3. You have 2 end jacks, which must be installed on your cable. If you are using a pre-made cable, with one of the ends whacked off, you only have one end to install - the crossed over end. Below are two diagrams, which show how you need to arrange the cables for each type of cable end. Decide at this point which end you are making and examine the associated picture below.

Table 1.1: Diagram shows you how to prepare Cross wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

Table 1.2 Diagram shows you how to prepare straight through wired connection

RJ45 Pin # (END 1)	Wire Color	Diagram End #1	RJ45 Pin # (END 2)	Wire Color	Diagram End #2
1	White/Orange		1	White/Green	
2	Orange		2	Green	
3	White/Green		3	White/Orange	
4	Blue		4	White/Brown	
5	White/Blue		5	Brown	
6	Green		6	Orange	
7	White/Brown		7	Blue	
8	Brown		8	White/Blue	

RESULT: Study of different types of network cables completed successfully.

2. EXECUTE THE FOLLOWING COMMANDS

AIM: To study the basic networking commands.

arp, ipconfig, hostname, netdiag, netstart, nslookup, pathping, ping, route, tracert

C:\>arp -a: ARP is short form of address resolution protocol, It will show the IP address of your computer along with the IP address and MAC address of your router.

C:\>hostname: This is the simplest of all TCP/IP commands. It simply displays the name of your computer.

C:\>ipconfig: The ipconfig command displays information about the host (the computer your sitting at) computer TCP/IP configuration.

C:\>ipconfig /all: This command displays detailed configuration information about your TCP/IP connection including Router, Gateway, DNS, DHCP, and type of Ethernet adapter in your system.

C:\>Ipconfig /renew: Using this command will renew all your IP addresses that you are currently (leasing) borrowing from the DHCP server. This command is a quick problem solver if you are having connection issues, but does not work if you have been configured with a static IP address.

C:\>Ipconfig/release: This command allows you to drop the IP lease from the DHCP server.

C:\>ipconfig /flushdns: This command is only needed if you're having trouble with your networks DNS configuration. The best time to use this command is after network configuration sets in, and you really need the computer to reply with flushed.

C:\>nbtstat -a: This command helps solve problems with NetBIOS name resolution. (Nbt stands for NetBIOS over TCP/IP)

C:\>net diag: Netdiag is a network testing utility that performs a variety of network diagnostic tests, allowing you to pinpoint problems in your network. Netdiag isn't installed by default, but can be installed from the Windows XP CD after saying no to the install. Navigate to the CD ROM drive letter and open the support\tools folder on the XP CD and click the setup.exe icon in the support\tools folder.

C:\>netstat: Netstat displays a variety of statistics about a computers active TCP/IP connections. This tool is most useful when you're having trouble with TCP/IP applications such as HTTP, and FTP.

C:\>nslookup: Nslookup is used for diagnosing DNS problems. If you can access a resource by specifying an IP address but not it's DNS you have a DNS problem.

C:\>pathping: Pathping is unique to Window's, and is basically a combination of the Ping and Tracert commands. Pathping traces the route to the destination address then launches a 25 second test of each router along the way, gathering statistics on the rate of data loss along each hop.

C:\>ping: Ping is the most basic TCP/IP command, and it's the same as placing a phone call to your best friend. You pick up your telephone and dial a number, expecting your best friend to reply with "Hello" on the other end. Computers make phone calls to each other over a network by using a Ping command. The Ping commands main purpose is to place a phone call to another computer on the network, and request an answer. Ping has 2 options it can use to place a phone call to another computer on the network. It can use the computers name or IP address.

C:\>route: The route command displays the computers routing table. A typical computer, with a single network interface, connected to a LAN, with a router is fairly simple and generally doesn't pose any network problems. But if you're having trouble accessing other computers on your network, you can use the route command to make sure the entries in the routing table are correct.

C:\>tracert: The tracert command displays a list of all the routers that a packet has to go through to get from the computer where tracert is run to any other computer on the internet.

RESULT: Study of different types of network commands completed successfully.

3. STUDY OF DIFFERENT TYPES OF CABLES

AIM: Study of different types of cables used in communication channel

Transmission Medium:

A communication channel that is used to carry the data from one transmitter to the receiver through the electromagnetic signals. The main function of this is to carry the data in the bits form through the Local Area Network(LAN). In data communication, it works like a physical path between the sender & receiver. For instance, in a copper cable network the bits in the form of electrical signals whereas in a fiber network ,the bits are available in the form of light pulses. The quality as well as characteristics of data transmission, can be determined from the characteristics of medium & signal. The properties of different transmission media are delay, bandwidth, maintenance, cost and easy installation.

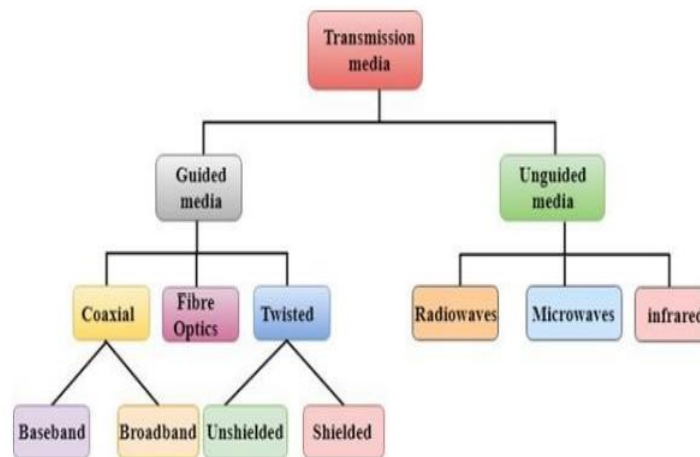


Fig 3.1 Classification of Transmission media

Bounded/Guided Transmission Media:

This kind of transmission media is also known as wired otherwise bounded media. In this type, the signals can be transmitted directly & restricted in a thin path through physical links. The types of Bounded /Guided transmission are discussed below.

Coaxial Cable:

Coaxial cable (or coax) carries signals of higher frequency ranges than those in twisted pair cable. It has a central core conductor of solid or stranded wire (usually copper) enclosed in an insulating sheath, which is, in turn, encased in an outer conductor of metal foil, braid, or a combination of the two. The outer conductor is also enclosed in an insulating sheath, and the whole cable is protected by a plastic cover.

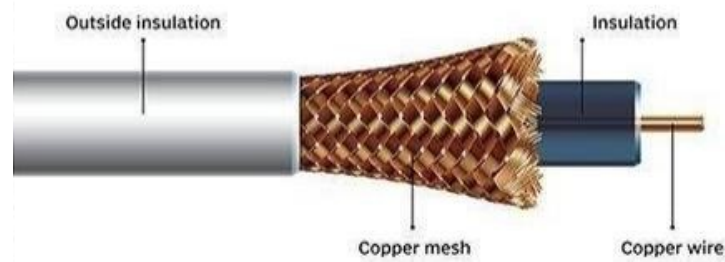


Fig 3.2 Coaxial cable

Applications:

1. Coaxial cable was widely used for both analog and digital data transmissions.
2. It has higher bandwidth.
3. Inexpensive when compared to fiber optical cables.
4. It uses for longer distances at higher data rates.
5. Excellent noise immunity.
6. Used in LAN and Television distribution.

Disadvantage :

1. Single cable failure can fail the entire network.
2. Difficult to install and expensive when compared with twisted pairs.
3. If the shield is imperfect, it can lead to grounded loop.

Fibre Optic Cable:

A fiber optic cable is a network cable that contains strands of glass fibers inside an insulated casing. They're designed for long-distance, high-performance data networking, and telecommunications. Compared to wired cables, fiber optic cables provide higher bandwidth and transmit data over longer distances. Fiber optic cables support much of the world's internet, cable television, and telephone systems.

Advantages of Fiber Optic Cables:

1. The loss of signal in optical fiber is less than that in copper wire.
2. Optical fibers usually have a longer life cycle for over 100 years.

Disadvantage:

1. It is expensive.
2. Difficult to install.

Fiber Optic Cable

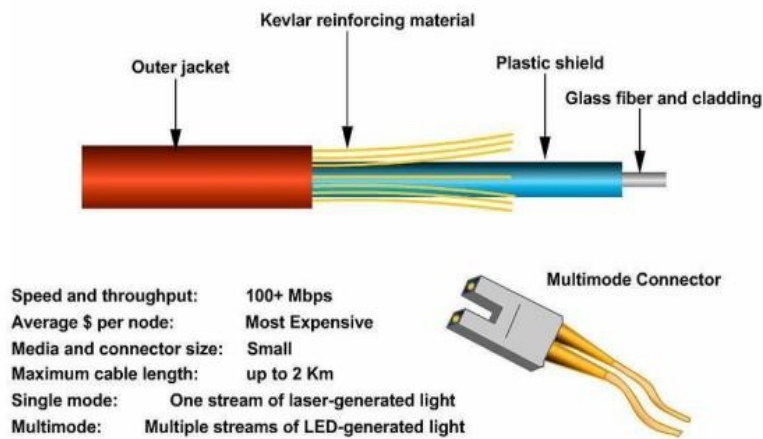


Fig 3.3 Fiber Optic Cable

Twisted pair cable:

A twisted pair cable is a type of cable made by putting two separate insulated wires together in a twisted pattern and running them parallel to each other. This type of cable is widely used in different kinds of data and voice infrastructures

Twisted pair is of two types:

1. Shielded Twisted Pair(STP)
2. Unshielded Twisted Pair(UTP)

Shielded Twisted Pair:

Shielded Twisted Pair (STP) cables additionally have an overall conducting metallic shields covering four twisted pair wires. There may be another conducting metallic shields covering individual twisted pairs also. These metallic shields blocks out electromagnetic interference to prevent unwanted noise from the communication circuit

Advantage of Shielded Twisted Pair:

1. The cost of the shielded twisted pair cable is not very high and not very low.
2. An installation of STP is easy.
3. It has higher capacity as compared to unshielded twisted pair cable.
4. It has a higher attenuation.
5. It is shielded that provides the higher data transmission rate

Disadvantages:

1. It is more expensive as compared to UTP and coaxial cable.
2. It has a higher attenuation rate.

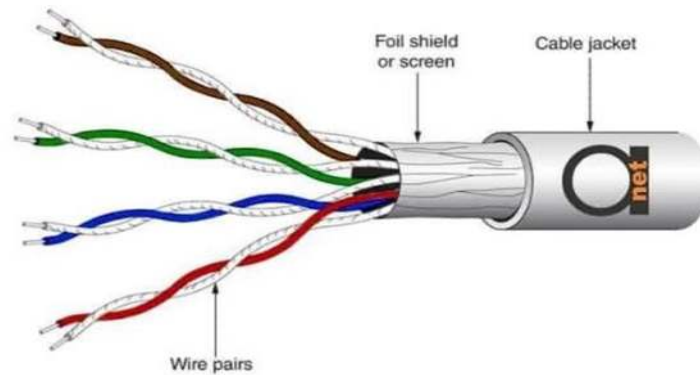


Fig 3.4 Unshielded Twisted Pair (UTP)

Unshielded Twisted Pair(UTP):

An unshielded twisted pair is widely used in telecommunication. It is most common type when compared with shielded twisted pair cable which consists of two conductors usually copper, each with its own colour plastic insulator

Advantages Of Unshielded Twisted Pair:

1. It is cheap.
2. Installation of the unshielded twisted pair is easy.
3. It can be used for high-speed LAN.

Disadvantage:

1. This cable can only be used for shorter distances because of attenuation.

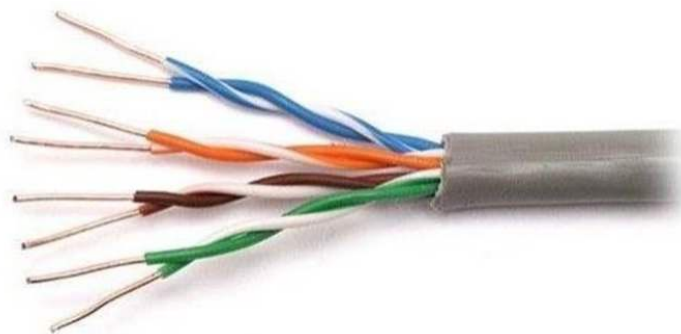


Fig 3.5 Unbounded/Unguided Transmission Media

Unguided medium transport electromagnetic waves without using a physical conductor. This type of communication is often referred to as wireless communication. Signals are normally broadcast through free space and thus are available to anyone who has a device capable of receiving them

Type of unguided Transmission media:

Radio Transmission:

Its frequency is between 10Khz to 1Ghz. It is simple to install and has high attenuation. These waves are used for multicast communication.

Types of propagation:

1. Troposphere
2. Ionosphere

Microwaves:

It is a line of sight transmission i.e. the sending and receiving antennas need to be properly aligned with each other. The distance covered by the signal is directly proportional to the height of the antenna. Frequency Range:1GHz – 300GHz. These are majorly used for mobile phone communication and television distribution.

Infrared:

Infrared waves are used for very short distance communication. They cannot penetrate through obstacles. This prevents interference between systems. Frequency Range:300GHz – 400THz. It is used in TV remotes, wireless mouse, keyboard, printer, etc.

RESULT: Study of different types of cables in communication channel completed successfully.

4.PRACTICALLY IMPLEMENT THE CROSS – WIRED CABLE AND STRAIGHT WIRED CABLE USING CRIMPING TOOL

Aim: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using crimping tool.

Requirements: Crimping tools, UTP Cable, RJ-45 connector, Cable tester.

Procedure:

Crimping Tools:

A crimping tool is a device used to conjoin two pieces of metal by deforming one or both of them to hold each other. The result of the tool's work is called a crimp. An example of crimping is affixing a connector to the end of a cable. For instance, network cables and phone cables are created using a crimping tool (shown below) to join RJ-45 and RJ-11 connectors to both ends of phone or Cat 5 cable



Fig 4.1 R3-11 and RJ-45 Crimping Tool

UTP Cables:

UTP stands for Unshielded Twisted Pair cable. UTP cable is a 100 ohm copper cable that consists of 2 to 1800 unshielded twisted pairs surrounded by an outer jacket. They have no metallic shield. This makes the cable small in diameter but unprotected against electrical interference. The twist helps to improve its immunity to electrical noise and EMI.

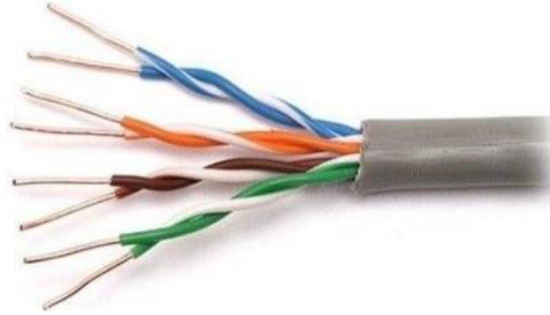


Fig 4.2 UTP Cable

RJ-45 Connector:

RJ-45 connector is a tool that we put on the end of the UTP cable. With this we can plug the cable in the LAN port.



Fig 4.3 RJ-45 Connector

Cable test:

A cable tester is an electronic device used to verify the electrical connections in a signal cable or other wired assembly. Basic cable testers are continuity testers that verify the existence of a conductive path between ends of the cable, and verify the correct wiring of connectors on the cable.



Fig 4.4 Cable Test

Straight cable:

A straight-through cable is a type of twisted pair cable that is used in

local area networks to connect a computer to a network hub such as a router. This type of cable is also sometimes called a patch cable and is an alternative to wireless connections where one or more computers access a router through a wireless signal. On a straight-through cable, the wired pins match. Straightthrough cable use one wiring standard: both ends use T568A wiring standard or both ends use T568B wiring standard. The following figure shows a straight-through cable of which both ends are wired as the T568B standard.

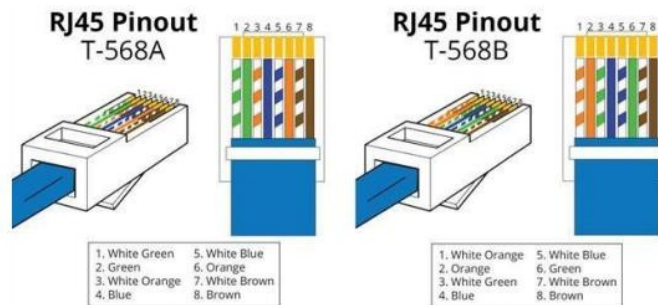


Fig 4.5 Straight Cable

Cross cable:

An Ethernet crossover cable is a type of Ethernet cable used to connect computing devices together directly. Unlike straight-through cable, crossover cables use two different wiring standards: one end uses the T568A wiring standard, and the other end uses the T568B wiring standard. The internal wiring of Ethernet crossover cables reverses the transmit and receive signals. It is most often used to connect two devices of the same type: e.g. two computers (via network interface controller) or two switches to each other.

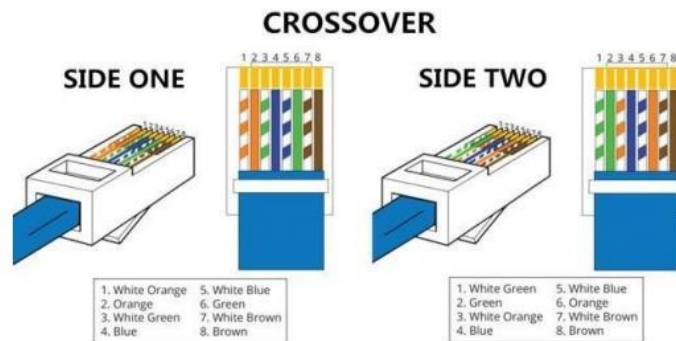


Fig 4.6 Cross Cable

Making Straight UTP Cable:

- Peel the end of the UTP cable , approximately 2 cm.
- Open the cable strands , align and follow the arrangement as standard cable image shown below .
- Once the order is according to the standard , cut and flatten the ends of the cable,

Put the cable is straight and aligned into the RJ - 45 connector , and make sure all cables are in correct position as follows:

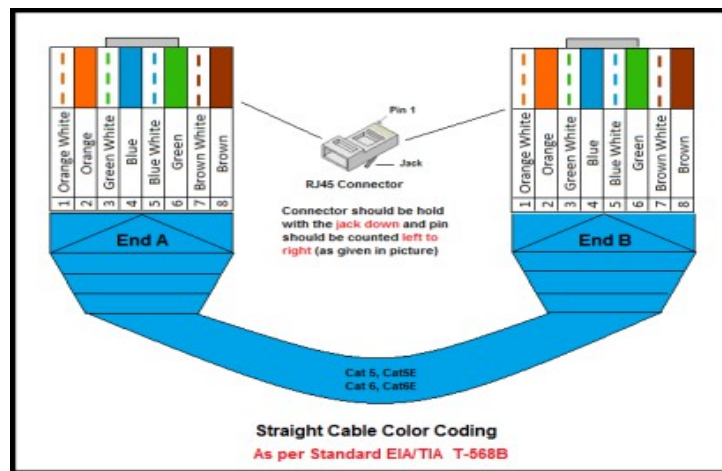


Fig 4.7 Straight Cable Color Coding

Orange White on no 1
 Orange on no 2 Green White on no 3
 Blue on no 4
 Blue White on no 5 Green on no 6
 White Brown on no 7 Brown on no 8

Make crimping using crimp tools , press crimping tool and make sure all the pins (brass) on the RJ - 45 connector has " bite " of each cable . usually when done will sound "click " . Once finished at the end of this one , do it again at the other end cable. The final step is to check the cable that you created earlier using the LAN tester , enter each end of the cable (RJ- 45) to each LAN port available on the tester , turn and make sure all of the LEDs light up according to the order of the wires we created

Creating Cross UTP Cable:-

Creating a cross cable has almost the same steps with straight cable , the difference lies only in the colour sequence from both ends of the cable . Unlike the straight cable that has the same colour sequence at both ends of the cable , the cross cable has a different colour sequences atboth ends of the cable.

The first ends is same with straight cable :

Orange White on no. 1 Orange on no. 2 Green White on no. 3 Blue on no. 4 Blue White on no. 5 Green on no. 6 .
 White chocolate on no. 7 Brown on no. 8

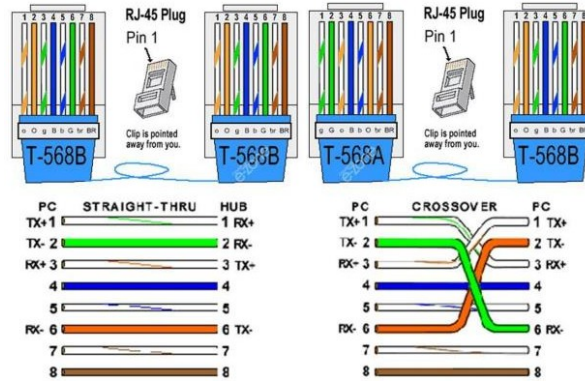


Fig 4.8 Ethernet Cable Wiring

For the second end of the cable, the colour composition is different from the first . The colour arrangement is as follows

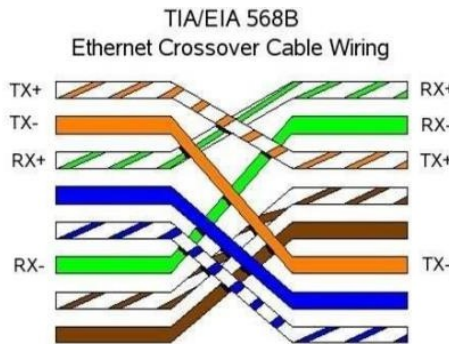


Fig 4.9 Ethernet Crossover Cable Wiring

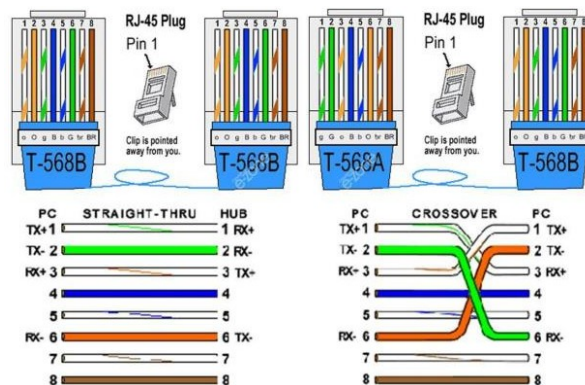


Fig 4.10 Ethernet Cable Wiring

Green White on no. 1 Green on no. 2 Orange White on no. 3 Blue on no. 4 Blue White on no. 5 Orange on no. 6 White chocolate no.7 Brown on no.8

RESULT: Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using crimping tool completed successfully.

5.STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION OF ADDRESS, STATIC AND DYNAMIC ADDRESS)

Aim: study the network IP address configuration

Procedure:

The IP address stands for Internet Protocol address is also called IP number or internet address. It helps us to specify the technical format of the addressing and packets scheme.

An IP address is a numerical label assigned to the devices connected to a computer network that uses the IP for communication. IP address act as an identifier for a specific machine on a particular network. It also helps us to develop a virtual connection between a source and a destination.

Types of IP address

There are mainly four types of IP addresses:

- Public
- Private
- Static
- Dynamic.

Public IP Addresses

A public IP address is an address where one primary address is associated with the whole network. In this type of IP address, each of the connected devices has the same IP address. This type of public IP address is provided by Internet Service Provider (ISP).

Private IP Addresses

A private IP address is a unique IP number assigned to every device that connects to internet network, which includes devices like computers, tablets, smartphones etc.,

Static IP addresses

A static IP address is an IP address that cannot be changed. These are fixed that are manually assigned to a system device. On the network configuration page, the network administrator manually inputs the IP address for every system. Moreover, the static address is not changed until it is directly updated by the network administrator or the Internet Service Provider. Furthermore, this address does not change with each network connection. In other words, the device always connects to the internet through the same IP address.

Dynamic IP addresses

The dynamic IP address is typically configured on devices via the DHCP protocol and regularly updates. The dynamic IP address constantly changes whenever the user links to a network. The Dynamic Host Configuration Protocol(DHCP) server employs a method for tracking and retrieving IP address information associated with active network components. The mechanism utilized for translation in dynamic address is known as Domain Name Server (DNS).

The DHCP and DNS are two protocols that are widely used while accessing the internet. When a user connects to the network, DHCP assigns a temporary dynamic IP address.

The main differences between Static and Dynamic IP addresses are as follows:

Table 5.1: Difference Between Static and Dynamic IP addresses

Features	Static IP address	Dynamic IP address
Definition	It is a permanent numeric address that is manually issued to a network device.	It is a temporary IP address allocated to a system when it connects to a network.
Provider	It is provided by Internet Service Provider (ISP).	It is provided by DHCP (Dynamic Host Configuration Protocol).
Changes	It doesn't change with time.	It may be changed at any time.
Device tracking	Devices may be traced easily.	Devices may be difficult to trace.
Cost	It is expensive to utilize and maintain.	It is less expensive to utilize and maintain.
Security	It is less secure than the dynamic IP address.	It offers high security.
Designation	It is complex to assign and reassign.	It is much easy to assign and reassign.
Stability	It is highly stable.	It is less stable.
Usage	These are appropriate for dedicated services like FTP, mail, and VPN servers.	Dynamic IP addresses are appropriate for a large network that needs an internet connection for all devices.

Image for Configuring Static IP Address

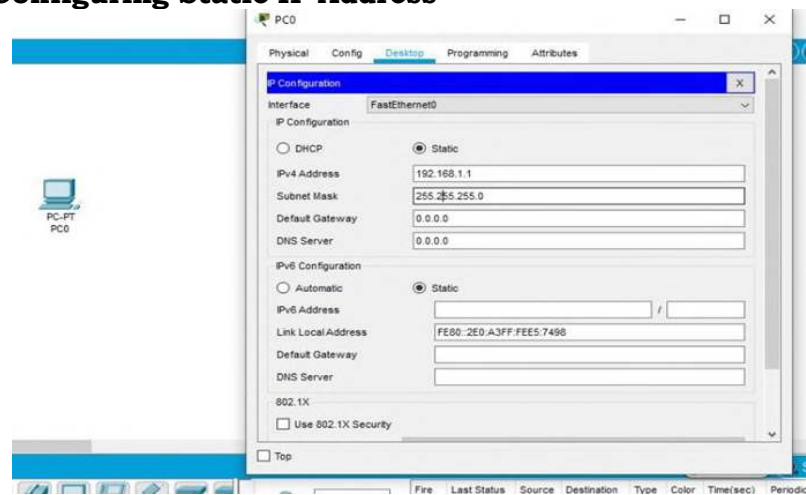


Fig5.1 Image for Configuring Static IP Address

Image for Configuring Dynamic IP Address

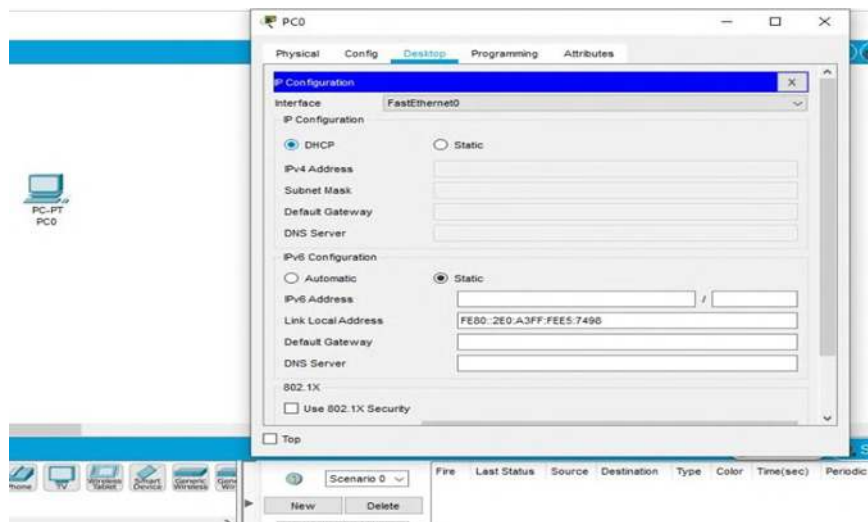


Fig5.2 Image for Configuring Dynamic IP Address

RESULT: study of Network IP address configuration completed successfully

6. STUDY THE NETWORK IP ADDRESS CONFIGURATION (CLASSIFICATION IPV4 AND IPV6, SUBNET, SUPERNET)

Aim: Study the classification IPV4, IPV6, SUBNET & SUPERNET

The Internet Protocol version 4 (IPv4) is a protocol for use on packet-switched Link Layer networks (e.g. Ethernet). IPv4 provides an addressing capability of approximately 4.3 billion addresses. The Internet Protocol version 6 (IPv6) is more advanced and has better features compared to IPv4.

Table 6.1: differences between IPv4 and IPv6

Features	IPv4	IPv6
Address length	IPv4 is a 32-bit address.	IPv6 is a 128-bit address.
Fields	IPv4 is a numeric address that consists of 4 fields which are separated by dot (.).	IPv6 is an alphanumeric address that consists of 8 fields, which are separated by colon.
Classes	IPv4 has 5 different classes of IP address that includes Class A, Class B, Class C, Class D, and Class E.	IPv6 does not contain classes of IP addresses.
Number of IP address	IPv4 has a limited number of IP addresses.	IPv6 has a large number of IP addresses.
Address configuration	It supports manual and DHCP configuration.	It supports manual, DHCP, auto-configuration, and renumbering.
Address space	It generates 4 billion unique addresses	It generates 340 undecillion unique addresses.
End-to-end connection integrity	In IPv4, end-to-end connection integrity is unachievable.	In the case of IPv6, end-to-end connection integrity is achievable.
Security features	In IPv4, security depends on the application. This IP address is not developed in keeping the security feature in mind.	In IPv6, IPSEC is developed for security purposes.
Address representation	In IPv4, the IP address is represented in decimal.	In IPv6, the representation of the IP address in hexadecimal.
Fragmentation	Fragmentation is done by the senders and the forwarding routers.	Fragmentation is done by the senders only.
Packet flow identification	It does not provide any mechanism for packet flow identification.	It uses flow label field in the header for the packet flow identification.
Checksum field	The checksum field is available in IPv4.	The checksum field is not available in IPv6.
Transmission scheme	IPv4 is broadcasting.	On the other hand, IPv6 is multicasting, which provides efficient network operations.
Encryption and	It does not provide encryption	It provides encryption


Authentication	and authentication.	and authentication.
Number of octets	It consists of 4 octets.	It consists of 8 fields, and each field contains 2 octets. Therefore, the total number of octets in IPv6 is 16.

Subnetting is a technique of partitioning an individual physical network into several small-sized logical sub-networks. These subnetworks are known as **subnets**. An IP address is made up of the combination of the network segment and a host segment. A subnet is constructed by accepting the bits from the IP address host portion which are then used to assign a number of small-sized sub-networks in the original network.

The Subnetting basically convert the host bits into the network bits. As mentioned above the subnetting strategy was initially devised for slowing down the depletion of the IP addresses.

The subnetting permits the administrator to partition a single class A, class B, class C network into smaller parts. **VLSM (Variable Length Subnet Mask)** is a technique which partitions IP address space into subnets of different sizes and prevent memory wastage. Furthermore, when the number of hosts is same in subnets, that is known as **FLSM (Fixed Length Subnet Mask)**.

The Subnetted address are listed below

Subnetted Address : 172.16.32.0/20					
In binary : 10101100.00010000.00100000.00000000					
1st Subnet	172 . 16 . 0010	0000 . 00	000000	= 172.16.32.0/26	
2nd Subnet	172 . 16 . 0010	0000 . 01	000000	= 172.16.32.64/26	
3rd Subnet	172 . 16 . 0010	0000 . 10	000000	= 172.16.32.128/26	
4th Subnet	172 . 16 . 0010	0000 . 11	000000	= 172.16.32.192/26	
5th Subnet	172 . 16 . 0010	0001 . 00	000000	= 172.16.33.0/26	
					

Supernetting is inverse process of subnetting, in which several networks are merged into a single network. While performing supernetting, the mask bits are moved toward the left of the default mask. The supernetting is also known as **router summarization** and **aggregation**. It results in the creation of more host addresses at the expense of network addresses, where basically the network bits are converted into host bits.

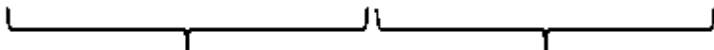
The supernetting is performed by internet service provider rather than the normal users, to achieve the most efficient IP address allocation. **CIDR (Classless Inter-Domain Routing)** is scheme used to route the network traffic across the internet. CIDR is a supernetting technique

where the several subnets are combined together for the network routing. In simpler words, CIDR allows the IP addresses to be organized in the subnetworks independent of the value of the addresses.

The Supernetting address are listed below

Supernetting Address : 172.16.168.0/24
In binary : 10101100.00010000.10101000.00000000

172.16.168.0/24	172 . 16 . 10101	000	00000000
172.16.169.0/24	172 . 16 . 10101	001	00000000
172.16.170.0/24	172 . 16 . 10101	010	00000000
172.16.171.0/24	172 . 16 . 10101	011	00000000
172.16.172.0/24	172 . 16 . 10101	100	00000000



 Number of common bits = 21 Non-common bits = 11

RESULT: Study the classification IPV4,IPV6,SUBNET &SUPERNET Completed Successfully.

7. STUDY OF NETWORK DEVICES

(SWITCH, ROUTER BRIDGE)

Aim: Study of following Network Devices in Detail

- Switch
- Bridge
- Router

Apparatus (Software): No software or hardware needed. Procedure: Following should be done to understand this practical.

1. **Switch:** A network switch or switching hub is a computer networking device that connects network segments. The term commonly refers to a network bridge that processes and routes data at the data link layer (layer 2) of the OSI model. Switches that additionally process data at the network layer (layer 3 and above) are often referred to as Layer 3 switches or multilayer switches.

Switch:- A switch is a Networking device in a computer network that connects other devices together. Multiple data cables are plugged into a switch to enable communication between different networked devices. Switches manage the flow of data across a network by transmitting a received network packet only to the one or more devices for which the packet is intended



Fig 7.1 Network Switch

Working of Switch:-Whenever a host sends a frame to any other host, then the source host is stored with the port in the address table of the MAC address switch. A switch always stores the address of the source in the table. Unless a host does send some data, its MAC address and port number will not be stored in the table of the switch. When you initialize the switch, the switch does not contain any information about any host and its address. In such a situation, when a host frame sends, its MAC address is stored in the table but due to no destination information, the switch sends the frame to all the hosts. When you initialize the switch, the switch does not contain any information about any host and its address. As soon as the second host sends some data, its address also gets stored in the table. Whenever a host sends the frames, the switch stores it if its address is not already present in the table. Thus a switch

creates its table. When all the hosts' addresses and port numbers come in the switch, the switch delivers the frame to all hosts only, delivering the same host to the host for which the data has been sent.

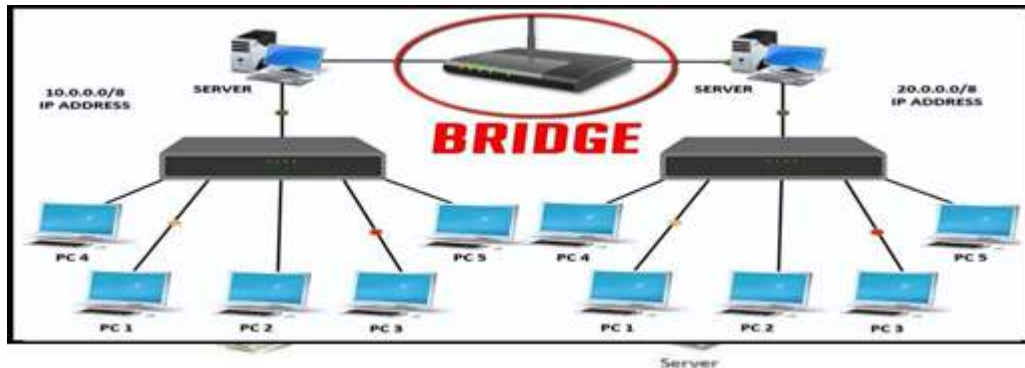


Fig 7.2 Bridge

Bridge: A network bridge connects multiple network segments at the data link layer (Layer 2) of the OSI model. In Ethernet networks, the term bridge formally means a device that behaves according to the IEEE 802.1D standard. A bridge and switch are very much alike; a switch being a bridge with numerous ports. Switch or Layer 2 switch is often used interchangeably with bridge. Bridges can analyze incoming data packets to determine if the bridge is able to send the given packet to another segment of the network.

Bridge:-

Bridge is termed as a network device which is helpful in filtering the data load of the traffic by dividing it into segments or packets. They are used to lower the load of traffic on the LAN and other networks. Bridges are passive devices, because there is no interaction between bridged and the paths of bridging. Bridges operate on the second layer of the OSI model that is the data link layer.



Fig 7.3 Bridge

Working of Bridge:-

When various network segments are established at the data link layer of the OSI model, we refer to it as bridge. However when the packets of data are transferred along a network, without locating the network addresses this process is termed as bridging. The process of bridging is helpful in

locating the addresses of unknown addresses to which it is viable to send data. In bridging the data packets contain a header or a packet header which holds the address to the intended device. Bridge can remember and recall the address of the devices for further transmission. There are two kinds of bridging modes, the transparent bridging and the source routing bridging. When the process of bridging occurs, it makes a bridging table along side where it stores the MAC addresses of the various terminals. This table helps the bridges to send the data packet to the exact location next time. However when a specific address does not meet the contents of the bridging table, the data packet is forwarded further ahead to every attached terminal in LAN except from the computer it is connected to. This type of bridging is called transparent bridging. When the source computer presents pathway information within the packet, this type of bridging is known as source route bridging. It is most commonly used in used on Token Ring networks.

Router: A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the data packet must be transferred from one network to another. Where multiple routers are used in a large collection of interconnected networks, the routers exchange information about target system addresses, so that each router can build up a table showing the preferred paths between any two systems on the interconnected networks.

Router:-



Fig 7.4 Router

Routers are networking devices operating at layer 3 or a network layer of the OSI model. They are responsible for receiving, analyzing, and forwarding data packets among the connected computer networks. When a data packet arrives, the router inspects the destination address, consults its routing tables to decide the optimal route and then transfers the packet along this route.

How a router works:-

A router examines a packet header's destination IP address and compares it against a routing table to determine the packet's best next hop. Routing tables list directions for forwarding data to particular network

destinations, sometimes in the context of other variables, like cost. They amount to an algorithmic set of rules that calculate the best way to transmit traffic toward any given IP address. A routing table often specifies a default route, which the router uses whenever it fails to find a better forwarding option for a given packet. For example, the typical home office router directs all outbound traffic along a single default route to its internet service provider (ISP). Routing tables can be static -- i.e., manually configured -- or dynamic. Dynamic routers automatically updated their routing tables based on network activity, exchanging information with other devices via routing protocols.

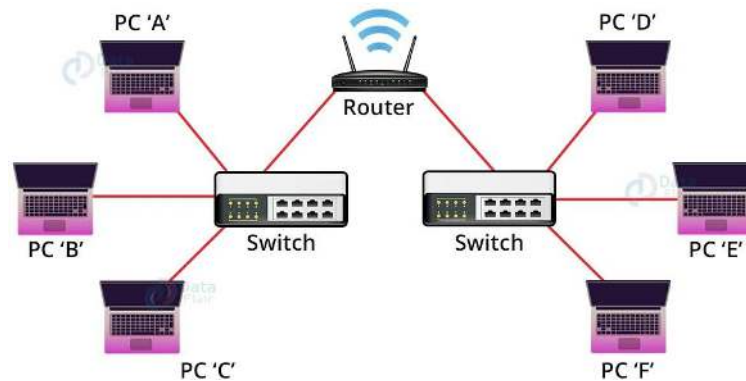


Fig 7.5: Router-Switch connection

RESULT: Study of network devices completed successfully.

8. Study of network IP

Aim: Study of network IP configuration

- Classification of IP address
- Sub netting
- Super netting

Apparatus (Software): NA

Procedure: Following is required to be study under this practical.

Classification of IP address: It is shown in the following table and how the ip addresses are classified and when they are used.

Table 8.1: Classification of IP address

Class	Address Range	Supports
Class A	1.0.0.1 to 126.255.255.254	Supports 16 million hosts on each of 127 networks.
Class B	128.1.0.1 to 191.255.255.254	Supports 65,000 hosts on each of 16,000 networks.
Class C	192.0.1.1 to 223.255.254.254	Supports 254 hosts on each of 2 million networks.
Class D	224.0.0.0 to 239.255.255.255	Reserved for multicast groups.
Class E	240.0.0.0 to 254.255.255.254	Reserved.

Sub netting: Why we Develop sub netting and How to calculate subnet mask and how to identify subnet address.

Super netting: Why we develop super netting and How to calculate supernet mask and how to identify supernetaddress.

RESULT: study of network IP completed successfully

9. Connect the computers in Local Area Network.

Aim: Connect the computers in Local Area Network.

Procedure: On the host computer

On the host computer, follow these steps to share the Internet connection:

1. Log on to the host computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click Network and Internet Connections.
4. Click **Network Connections**.
5. Right-click the connection that you use to connect to the Internet. For example, if you connect to the Internet by using a modem, right-click the connection that you want under Dial-up / other network available.
6. Click **Properties**.
7. Click the **Advanced** tab.
8. Under **Internet Connection Sharing**, select the **Allow other network users to connect through this computer's Internet connection** check box.
9. If you are sharing a dial-up Internet connection, select the **Establish a dial-up connection whenever a computer on my network attempts to access the Internet** check box if you want to permit your computer to automatically connect to the Internet.
10. Click **OK**.

You receive the following message: When Internet Connection Sharing is enabled, your LAN adapter will be set to use IP address 192.168.0. 1. Your computer may lose connectivity with other computers on your network. If these other computers have static IP addresses, it is a good idea to set them to obtain their IP addresses automatically. Are you sure you want to enable Internet Connection Sharing?

11. Click **Yes**.

The connection to the Internet is shared to other computers on the local area network (LAN).

The network adapter that is connected to the LAN is configured with a static IP address of 192.168.0. 1 and a subnet mask of 255.255.255.0 on the client computer.

To connect to the Internet by using the shared connection, you must confirm the LAN adapter IP configuration, and then configure the client

computer. To confirm the LAN adapter IP configuration, follow these steps:

1. Log on to the client computer as Administrator or as Owner.
2. Click **Start**, and then click **Control Panel**.
3. Click Network and Internet Connections.
4. Click **Network Connections**.
5. Right-click **Local Area Connection** and then click **Properties**.
6. Click the **General** tab, click **Internet Protocol (TCP/IP)** in the **connection uses the following items** list, and then click **Properties**.
7. In the **Internet Protocol (TCP/IP) Properties** dialog box, click **Obtain an IP address automatically** (if it is not already selected), and then click **OK**.

Note: You can also assign a unique static IP address in the range of 192.168.0.2 to 254. For example, you can assign the following static IP address, subnet mask, and default gateway:

8. IP Address 192.168.31.202
9. Subnet mask 255.255.255.0
10. Default gateway 192.168.31.1
11. In the **Local Area Connection Properties** dialog box, click **OK**.
12. Quit Control Panel.

RESULT: The computers are connected to LAN practically

10. CPU scheduling algorithms

AIM : To write a C program to simulate the following non-preemptive CPU scheduling algorithms to find turnaround time and waiting time for the following.

a)FCFS b) SJF

PROGRAM

```
#include<stdio.h>

#include<conio.h>
Main()
{
Int bt[20], wt[20],tat[20],i,n,float wtavg,tatavg;
Clrscr();
Print("\nEnter the number of processes --");
scanf("%d",&n);
for(I=0;I<n;I--)
{
Printf("\nEnter burst time for process%d--",I);
Scanf("%d",&bt[I]);
}
wt[0] = wtavg = 0;
tat[0] = tatavg = bt[0];
for(i=1;i<n;i++)
{
wt[i] = wt[i-1] +bt[i-1];
tat[i] = tat[i-1] +bt[i];
wtavg = wtavg + wt[i];
tatavg = tatavg + tat[i];
}
printf("\t PROCESS \tBURST TIME \t WAITING TIME\t
TURNAROUND TIME\n");
for(i=0;i<n;i++)
printf("\n\t P%d \t\t %d \t\t %d \t\t %d", i, bt[i], wt[i], tat[i]);
printf("\nAverage Waiting Time -- %f", wtavg/n); printf("\nAverage
Turnaround Time -- %f", tatavg/n); getch();
}
```

INPUT

```
Enter the number of processes --      3
Enter Burst Time for Process 0 --    24
Enter Burst Time for Process 1 --    3
Enter Burst Time for Process 2 --    3
```

OUTPUT

PROCESS	BURST TIME	WAITING TIME	TURNAROUND TIME
P0	24	0	24
P1	3	24	27
P2	3	27	30

Average Waiting Time-- 17.000000

Average Turnaround Time -- 27.000000

a) **SJF CPU SCHEDULING ALGORITHM**

```
#include<stdio.h>
#include<conio.h> main()
{
int p[20], bt[20], wt[20], tat[20], i, k, n, temp;
float wtavg, tatavg;
clrscr();
printf("\nEnter the number of processes -- ");
scanf("%d", &n);
for(i=0;i<n;i++)
{
p[i]=i;
printf("Enter Burst Time for Process %d -- ", i);
scanf("%d", &bt[i]);
}
for(i=0;i<n;i++) for(k=i+1;k<n;k++) if(bt[i]>bt[k])
{
temp=bt[i];
bt[i]=bt[k];
bt[k]=temp;
}
Wt[0]=wtavg=0;
}
tat[0]=tatavg=bt[0];
for(I=1;I<n;I++)
{
Wt[I]=wt[I-1]+bt[I-1];
Tat[I]=tat[I-1]+bt[I];
Wtavg=wtavg+wt[I];
Tatavg=tatavg+tat[I];
}
Printf("\n\tPROCESS\tBURST TIME\tWAITING TIME\tTURNAROUND
```



```

TIME\n");
For(I=0;I<n;I++)
    Printf("\n\t%d\t\t%d\t\t%d\t\t%d",p[I],w[I],tat[I]);
    Printf("\nAverage Waiting Time %f",wtavg/n);
Print("\nAverage Turnaround Time --%f",tatavg/n);
Getch();
}

```

INPUT

Enter the number of processes --
Enter Burst Time for Processes 0 --
Enter Burst Time for Processes 1 --
Enter Burst Time for Processes 2 --
Enter Burst Time for Processes 3 --

OUTPUT

PROCEDURE	BURST TIME	WAITING TIME	TURNAROUND TIME
P3	3	0	3
P0	6	3	9
P2	7	9	16
P1	8	16	24

Average Waiting Time -- 7,000000
Average Turnaround Time -- 13,000000

RESULT: CPU scheduling algorithms executed practically

11. Perform the working of CSMA-CD protocol.

Aim: To perform the working of CSMA-CD protocol.

EQUIPMENTS:

- LTS-01 trainer kit
- 4 or more Computers with win-2K / XP and Ethernet port available on them
- RJ-45 to RJ-45 LAN connecting cables
- L-SIM LAN protocol analyzer and simulator software

PROCEDURE:

1. Connect 3 or more computer LAN ports using RJ-45 to RJ-45 LAN connecting cables provided with the system to LTS-01 star topology ports.
2. Switch on the LTS-01 & Computers.
3. Run L-SIM software on all the computers, one should be server and others should be clients.
4. On the server computer select type of network as LAN.
5. On the server computer select the topology as STAR, select protocol as CSMA-CD click on create network button.
6. Remote computer details will appear on the computers connected in network, server will be able to see all clients and all clients will be able to see onlyserver.
7. Select the server computer to whom data file is to be transferred from one of the client computer; from the load button, previously stored/selected file information can be loaded or you can select any file, which is to be transmitted.
8. File size will appear in the software window, select the packet size, inter packet delay and click OK.
9. Total packets formed for that file will be indicated on computers, same details of file will appear on remote computer to which file is to be transmitted.
10. Click on file transfer button to transfer file.
11. During file transfer process try to send file to server from another client computer, file transfer from second transmitter will also gets initiated.
12. When packet from second sender collides with first sender it will be indicated as collision packet on server & Client-1.

13. File from first sender will resume after some time and second sender file will be kept on hold till first file transfer gets completed.
14. Once the first sender file reached to server its display is refreshed and server will show packet status for second sender.
15. Second sender file transfer will also get completed and thus collision of two packets transmitted simultaneously from two senders is detected and cleared.

PRACTICAL RESULT:

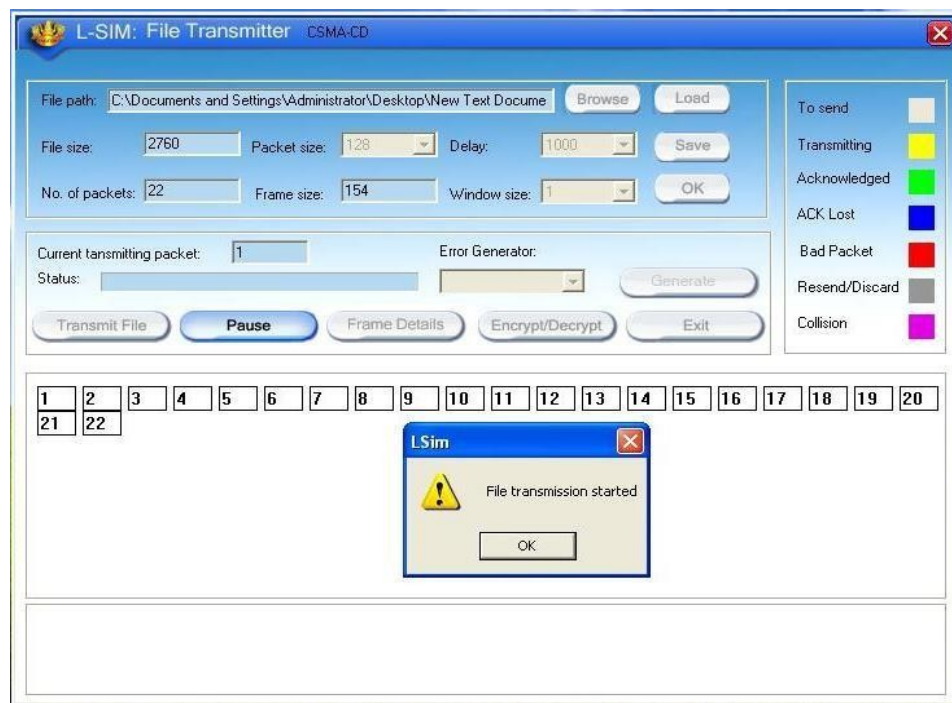


Fig 11.1: Starting of File transmission

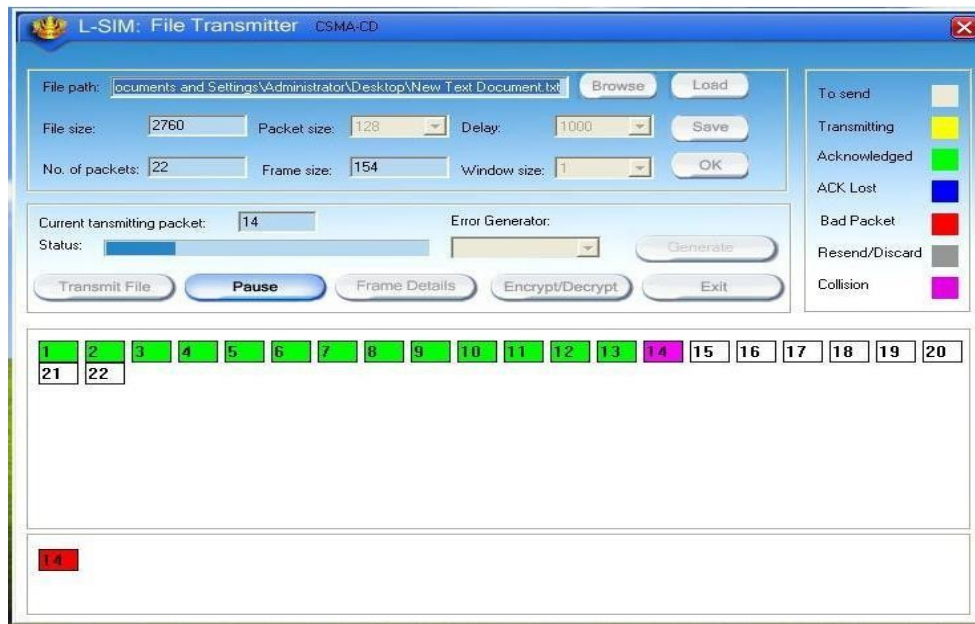


Fig11.2 Identification of Collision of packet

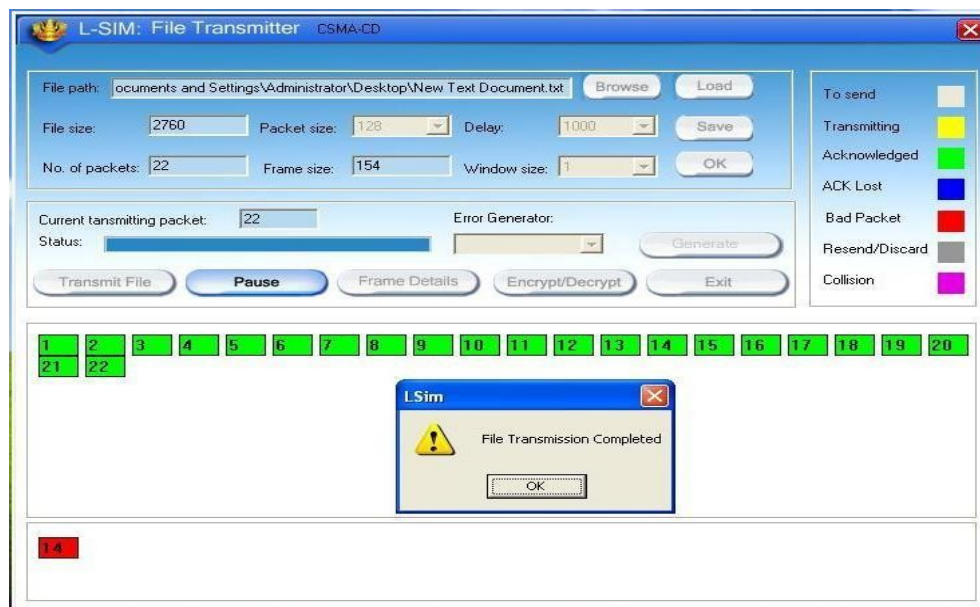


Fig 11.3 File transmission completion.

RESULT: The working of CSMA-CD protocol executed successfully

12. CSMA-CA PROTOCOL

Aim:To perform the working of CSMA-CA protocol.

EQUIPMENTS:

- LTS-01 trainer kit
- 4 or more Computers with win-2K / XP and Ethernet port available on them
- RJ-45 to RJ-45 LAN connecting cables
- L-SIM LAN protocol analyzer and simulator software

PROCEDURE:

1. Connect 3 or more computer LAN ports using RJ-45 to RJ-45 LAN connecting cables provided with the system to LTS-01 star topology ports. Switch on the LTS-01 & Computers.
2. Switch on the LTS-01 & Computers.
3. Run L-SIM software on all the computers, one should be server and others should be clients.
4. On the server computer select type of network as LAN.
5. On the server computer select the topology as STAR, select protocol as CSMA-CA click on create network button.
6. Remote computer details will appear on the computers connected in network, server will be able to see all clients and all clients will be able to see onlyserver.
7. Click on the Send RTS button to get the computer into transmitter mode.
8. Select the computer to whom data file is to be transferred, from the load button, previously stored/selected file information can be loaded or you can select any file, which is to be transmitted.
9. File size will appear in the software window, select the packet size, inter packet delay and click OK.
10. Total packets formed for that file will be indicated on computers, same details of file will appear on remote computer to which file is to be transmitted.
11. Click on file transfer button to transfer file.
12. During file transfer process try to get access to transmit file by clicking on Send RTS button on other computers, you will be prompted with channel is busy message.
13. Thus collision of two packets transmitted simultaneously from two senders is avoided.

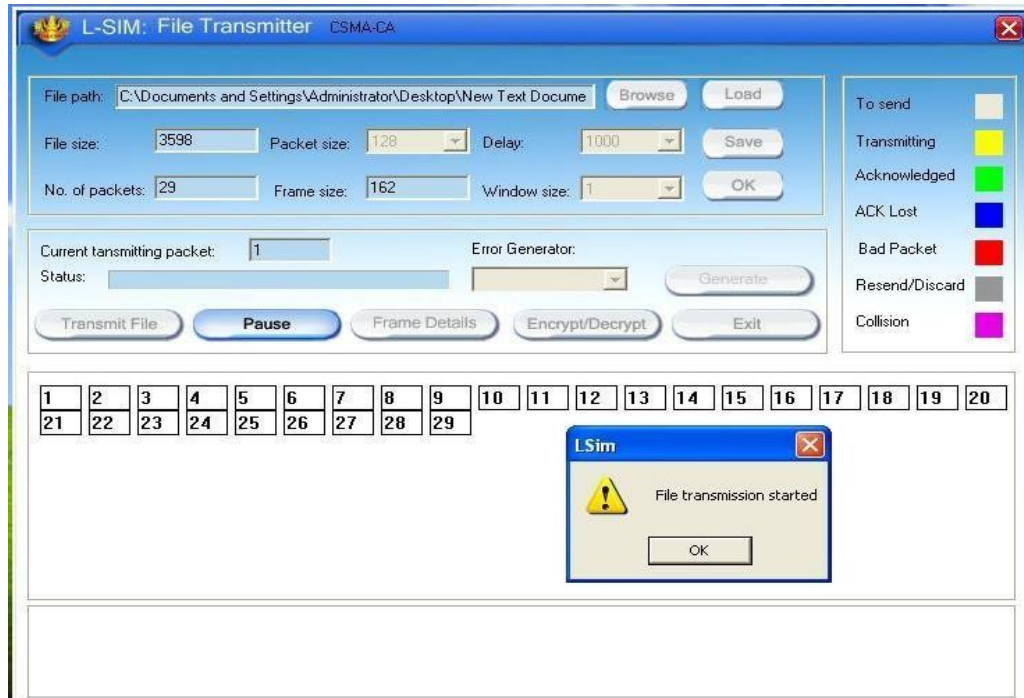
PRACTICAL RESULT:

Fig12.1 File Transmission Starting

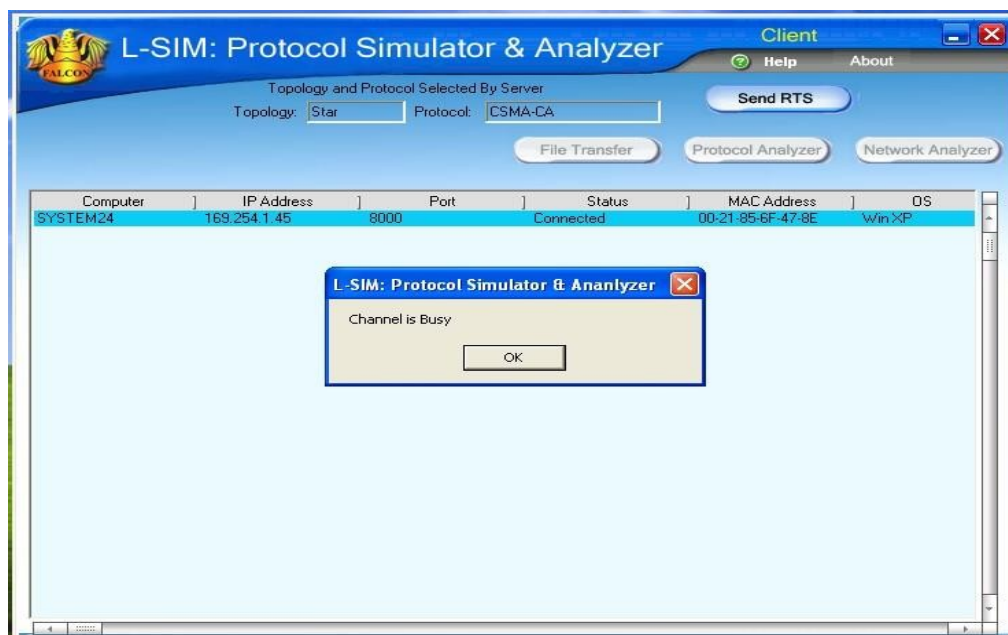


Fig 12.2 Indication of Channel Status

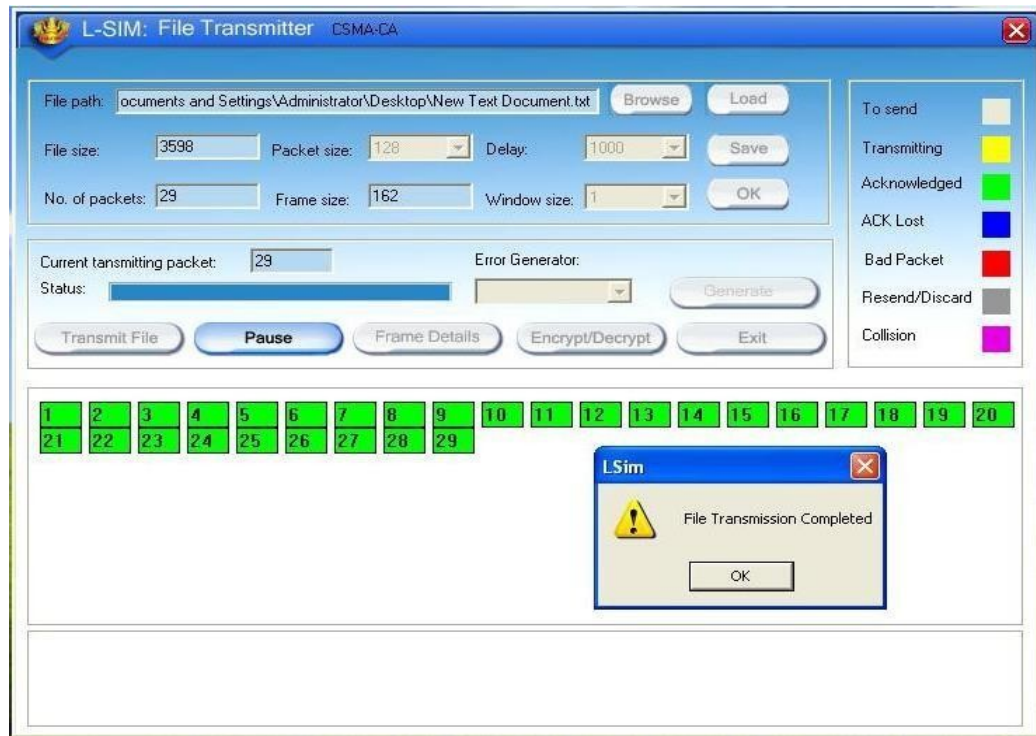


Fig 12.3 File Transmission completion

RESULT: The working of CSMA-CA protocol executed successfully.

REFERENCES

S.NO	REFERENCE
1.	B.A. Forouzan, Data Communications and Networking, 4rd Edition, McGraw Hill, 2007.
2.	A.S. Tanenbaum, Computer Networks, 4th Edition, Prentice Hall, 2003
3.	W. Stallings, Data and Computer Communications, 8th Edition, Prentice Hall, 2007.
4.	D.E. Comer and R. E. Droms, Computer Networks and Internets (Bk/CD-ROM), 2/e, Prentice Hall, 1999
5.	William Stallings, Data and Computer Communications, 6/e, Prentice Hall, 1999; 7/e, Pearson Prentice Hall, 2004
6.	R.O. Onvural and R. Cherukuri, Signaling in ATM Networks, Artech House, 1997.
7.	M. Sexton and A. Reid, Broadband Networking, Artech House, 1997.
8.	U. Black, ATM: Foundation for Broadband Networks, Prentice Hall, 1995.
9.	L.L. Peterson and B.S. Davie, Computer Networks, Morgan Kaufmann, 1996.
10.	D. Bertsekas and R. Gallager, Data Networks, 2nd Edition, Prentice Hall, 1992.
11.	T.N. Saadawi, M.H. Ammar and A.E. Hakeem, Fundamentals of Telecommunication Networks, Wiley, 1994.
12.	J.Y. Hui, Switching and Traffic Theory for Integrated Broadband Networks, Kluwer Academic Publishers, 1990.
13.	M. Schwartz, Broadband Integrated Networks, Prentice Hall, 1996.
14.	H.J.R. Dutton and P. Lenhard, Asynchronous Transfer Mode, 2nd Edition, Prentice Hall, 1995.
15.	B. Dorling, D. Freedman, C. Metz and J. Burger, Internetworking over ATM, Prentice Hall, 1996.