Sandip Foundation's

SANDIP INSTITUTE OFTECHNOLOGY & RESEARCH CENTRE, NASHIK

DEPARTMENT OF COMPUTER ENGINEERING

Savitribai Phule Pune University

Third Year of Computer Engineering (2015 Course)

310248: Computer Network Laboratory.

Teaching Scheme:	**Credit (01)**	**Examination Scheme:**
PR: 02 Hours/Week		**PR:50Marks**
		TW: 25Marks

_____ _____

Name & Sign of Faculty Head of the Department

Course Objectives:

1. To establish communication among the computing nodes in P2P and Client-Server architecture
2. Configure the computing nodes with understanding of protocols and technologies.
3. Use different communicating modes and standards for communication
4. Use modern tools for network traffic analysis
5. To learn network programming.

Course Outcomes:

On completion of the course, student will be able to–

1. Demonstrate LAN and WAN protocol behavior using Modern Tools.
2. Analyze data flow between peer to peer in an IP network using Application, Transport and Network Layer Protocols.
3. Demonstrate basic configuration of switches and routers.
4. Develop Client-Server architectures and prototypes by the means of correct standards and technology.

List of Assignments with Practical plan

Sr. No	Assignment Name	Date of Conduction	Reference
1	**Lab Assignment on Unit I: (MandatoryAssignment)** **Part A:** Setup a wired LAN using Layer 2 Switch and then IP switch of minimum four computers. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrate the PING packets captured traces using Wireshark Packet Analyzer Tool.		
1B	**Part B:** Extend the same Assignment for Wireless using Access Point		
2	**Lab Assignment on Unit II: (Use C/C++)** Write a program for error detection and correction for 7/8 bits ASCII codes using Hamming Codes or CRC. Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode. (50% students will perform Hamming Code and others will perform CRC)		
3	**Lab Assignment on Unit IV: (Use JAVA/PYTHON)** Write a program to demonstrate subletting and find the subnet masks.		
4	**Lab Assignment on Unit VI: (Use JAVA/PYTHON)** Write a program for DNS lookup. Given an IP address input, it should return URL and vice-versa.		
5	**Lab Assignment on Unit V: (Mandatory Assignment) (Use C/C++)** Write a program using TCP socket for wired network for following		

	a. Say Hello to Each other (For all students) b. File transfer (For all students) c. Calculator (Arithmetic) (50% students) d. Calculator (Trigonometry) (50% students) Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode		
6	**Lab Assignment on Unit V: (Mandatory Assignment) (Use C/C++)** Write a program using UDP Sockets to enable file transfer (Script, Text, Audio and Video one file each) between two machines. Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.		
7	**Lab Assignment on Unit V: (Mandatory Assignment) (Use C/C++)** Write a program to analyze following packet formats captured through Wireshark for wired network. 1. Ethernet 2. IP 3.TCP 4. UDP		
8	Installing and configure DHCP server and write a program to install the software on remote machine		
9	**Lab Assignment on Unit IV and Unit V: (Mandatory Assignment)** Use network simulator NS2 to implement: a. Monitoring traffic for the given topology b. Analysis of CSMA and Ethernet protocols c. Network Routing: Shortest path routing, AODV. d. Analysis of congestion control (TCP and UDP).		
10	**Lab Assignment on Unit IV: (Mandatory Assignment)** Configure RIP/OSPF/BGP using packet Tracer		

11	**Lab Assignment on Unit V: (Use JAVA/PYTHON)** Write a program using TCP sockets for wired network to implement a. Peer to Peer Chat b. Multiuser Chat		
12	**Lab Assignment on Unit V: (Use JAVA/PYTHON)** Write a program using UDP sockets for wired network to implement a. Peer to Peer Chat b. Multiuser Chat Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.		

Guidelines for Student Journal :

The laboratory assignments are to be submitted by student in the form of journal. Journal consists of prologue, Certificate, table of contents, and **handwritten write-up** of each assignment (Title, Objectives, Problem Statement, Outcomes, software & Hardware requirements, Date of Completion, Assessment grade/marks and assessor's sign, Theory- Concept in brief, algorithm, flowchart, test cases, conclusion/analysis. **Program codes with sample output of all performed assignments are to be submitted as softcopy.**

As a conscious effort and little contribution towards Green IT and environment awareness, attaching printed papers as part of write-ups and program listing to journal may be avoided. Use of DVD containing students programs maintained by lab In-charge is highly encouraged. For reference one or two journals may be maintained with program prints at Laboratory.

Guidelines for Practical Examination

Both internal and external examiners should jointly set problem statements. During practical assessment, the expert evaluator should give the maximum weightage to the satisfactory implementation of the problem statement. The supplementary and relevant questions may be asked at the time of evaluation to test the student's for advanced learning, understanding of the fundamentals, effective and efficient implementation. So encouraging efforts, transparent evaluation and fair approach of the evaluator will not create any uncertainty or doubt in the minds of the students. So adhering to these principles will consummate our team efforts to the promising start of the student's academics.

Guidelines for Laboratory Conduction

The instructor is expected to frame the assignments by understanding the prerequisites, technological aspects, utility and recent trends related to the topic. The assignment framing policy need to address the average students and inclusive of an element to attract and promote the intelligent students. The instructor may set multiple sets of assignments and distribute among batches of students. It is appreciated if the assignments are based on real world problems/applications. Encourage students for appropriate use of Hungarian notation, proper indentation and comments. Use of open source software is to be encouraged.

In addition to these, instructor may assign one real life application in the form of a mini-project based on the concepts learned. Instructor may also set one assignment or mini-project that is suitable to respective branch beyond the scope of syllabus.

Operating System recommended :- 64-bit Open source Linux or its derivative

Programming tools recommended: - Open Source C,C++, JAVA, PYTHON, Programming tool like G++/GCC, Wireshark, Etheral and Packet Tracer

Assignment No. A1

Title: Setup a wired LAN using switch

Objectives: To establish a wired LAN for four computers.

Problem Statement:

Setup a wired LAN using Layer 2 Switch and then IP switch of minimum four computers. It includes preparation of cable, testing of cable using line tester, configuration machine using IP addresses, testing using PING utility and demonstrate the PING packets captured traces using Wireshark Packet Analyzer Tool.

Outcomes:

Develop and demonstrate a wired LAN for four computers.

Tools Required:

Hardware: Computer, LAN Cards, RJ-45 Connectors, Switch, CAT-5 Cable, Cable tester, Crimping tool, etc.

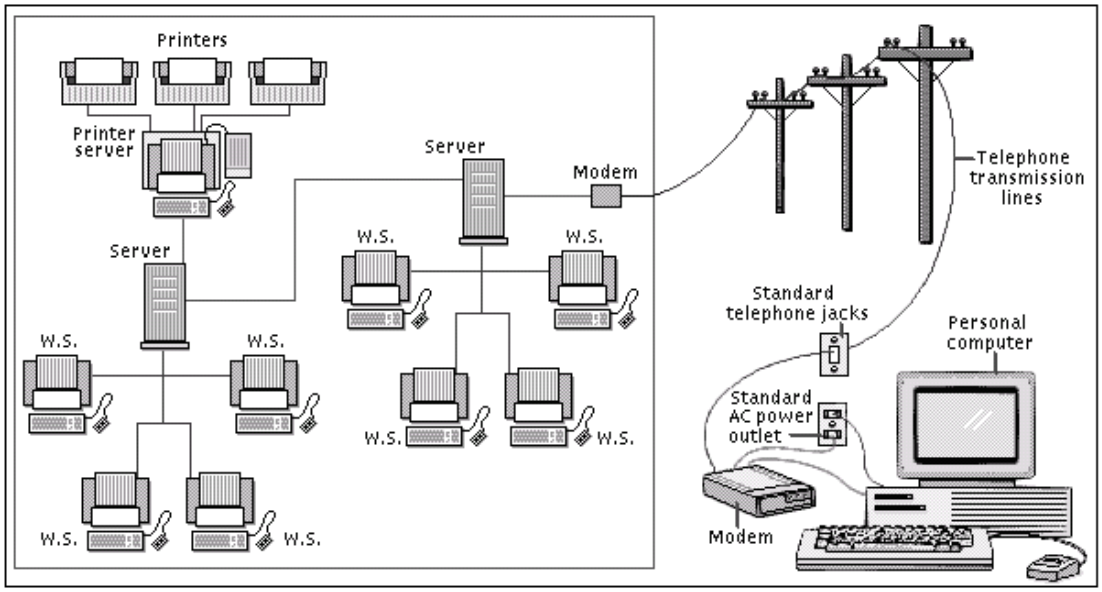
Software: Open source O.S.and wireshark

Theory:

Introduction:-

Computer Networks, the widespread sharing of information among groups of computers and their users, a central part of the information age. The popular adoption of the personal computer (PC) and the local area network (LAN) during the 1980s has led to the capacity to access information on a distant database; download an application from overseas; send a message to a friend in a different country; and share files with a colleague—all from a personal computer.

The networks that allow all this to be done so easily are sophisticated and complex entities. They rely for their effectiveness on many cooperating components. The design and deployment of the worldwide computer network can be viewed as one of the great technological wonders of recent decades.



Computer Network

Networks are connections between groups of computers and associated devices that allow users to transfer information electronically. The local area network shown on the left is representative of the setup used in many offices and companies. Individual computers, called work stations (WS), communicate to each other via cable or telephone line linking to servers. Servers are computers exactly like the WS, except that they have an administrative function and are devoted entirely to monitoring and controlling WS access to part or all of the network and to any shared resources (such as printers). The red line represents the larger network connection between servers, called the backbone; the blue line shows local connections. A modem (modulator/demodulator) allows computers to transfer information across standard telephone lines. Modems convert digital signals into analogue signals and back again, making it possible for computers to communicate, or network, across thousands of miles.

Study of Network Devices:-

NIC (Network Interface Card):-

Each computer includes the File server or a Network will have a card plugged in the PCI Expunction slot or will have on-board NIC (Network Interface Card), which will provide connectivity among the workstation in the network through cables.

Type's of Card:-

1. Arc net card (2.5 mbits/sec)
2. Ethernet card (10/100 mbps)
3. Token Ring card (4-16 mbits/sec)

Hub/Switch:-

These devices are used for Re-directing traffic, i.e. in a **Star** Topology the central device is used to ECHO/Re-Direct the packets coming from one workstation/node to the Destination workstation/node.

This is done by using the devices like Hub/Switch, during the present situation **Hub's are absolute due to their disadvantages of Echoing a packet from one node to all, which leads to increasing N/W traffic and packet Collision.**

Type of Hub:-

1. **Passive Hub:-**

   It is a device which do not require any type of power supply and does not boost incoming signal, it just echo the incoming signal to all nodes.

2. **Active Hub :-**

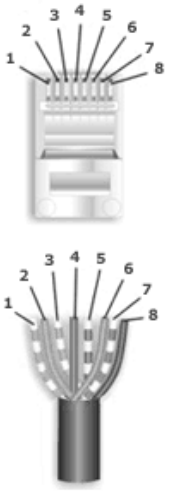
It is a device which requires power supply and boosts the incoming signal and echoes the signal to all nodes.

Hub where absolute due to use of an intelligent device called **Switch** which reads the destination adders and sends the incoming packet to it.

paring Rules and Color Code:-

The CAT 5 Cable consist of 8 wires which comes pares of White/Blue, Blue, White/Orange, Orange, White/Green, Green, White/Brown, Brown and they are coded for **Straight** and **Cross** combinations respectively.

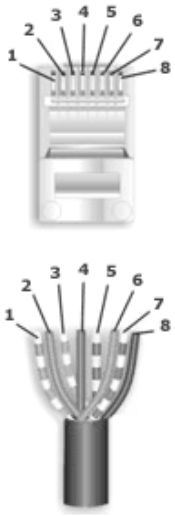
Straight:-



Pair #	Wire	Pin #
1-White/Blue	White/Blue	5
	Blue	4
2-Wht./Orange	White/Orange	1
	Orange	2
3-White/Green	White/Green	3
	Green	6
4-White/Brown	White/Brown	7
	Brown	8

Pair #	Wire	Pin #
1-White/Blue	White/Blue	5

Cross:-



	Blue	4
2-White/Green	White/Green	1
	Green	2
3-White/Orange	White/Orange	3
	Orange	6
4-White/Brown	White/Brown	7
	Brown	8

Connections among devices:-

Node to Node - Straight – Cross,

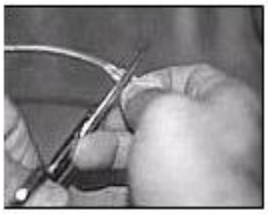
Switch to Node - Straight – Straight,

Switch to Switch - Straight – Cross.

How to Crimp a Cat 5 cable with RJ 45 Connector:-

1. Skin off the cable jacket approximately 1" or slightly more.

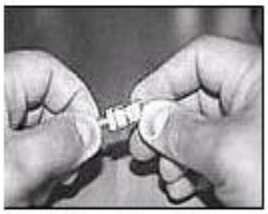
2. Un-twist each pair, and straighten each wire between the fingers.
3. Place the wires in the order of one of the two diagrams shown above .Bring all of the wires together, until they touch.



4. At this point, recheck the wiring sequence with the diagram.
5. Optional: Make a mark on the wires at 1/2" from the end of the cable jacket.

6. Hold the grouped (and sorted) wires together tightly, between the thumb, and the forefinger.
7. Cut all of the wires at a perfect 90 degree angle from the cable at 1/2" from the end of the cable jacket. This is a very critical step. If the wires are not cut straight, they may not all make contact. We suggest using a pair of scissors for this purpose.

8. Conductors should be at a straight 90 degree angle, and be 1/2" long, prior to insertion into the connector.
9. Insert the wires into the connector (pins facing up).



10. Push moderately hard to assure that all of the wires have reached the end of the connector. Be sure that the cable jacket goes into the back of the connector by about 3/16".
11. Place the connector into a crimp tool, and squeeze hard so that the handle reaches its full swing.

12. Repeat the process on the other end. For a straight through cable, use the same wiring.
13. Use a cable tester to test for proper continuity.

Cable Testing Tool:-

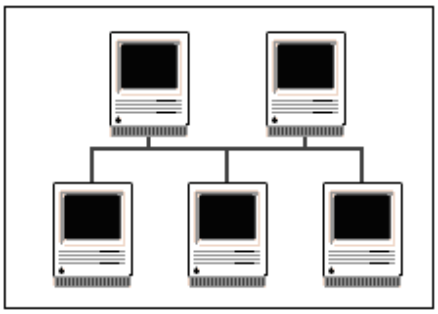
It is a tool used for testing weather there is no cut in between two terminals and to identify the type of pair crimp with.

Study of Topologies:-

What is a Topology?

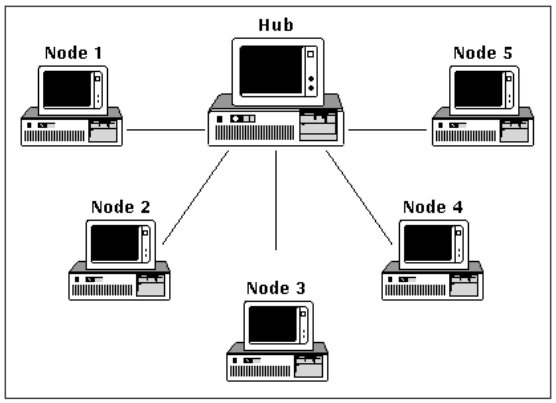
The physical topology of a network refers to the configuration of cables, computers, and other peripherals. Physical topology should not be confused with logical topology which is the method used to pass information between workstations.

1. Bus Topologies:-



In a bus network configuration, each node is connected to one main communications line. With this arrangement, even if one of the nodes goes down, the rest of the network can continue to function normally.

2. Star Topologies:-

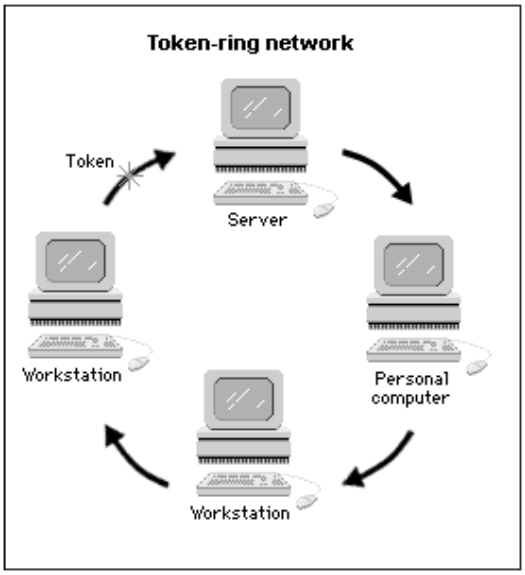


A star network consists of several nodes connected to a central hub/switch in a star-shaped configuration. Messages from individual nodes pass

directly to the hub/switch, which determines any further routing.

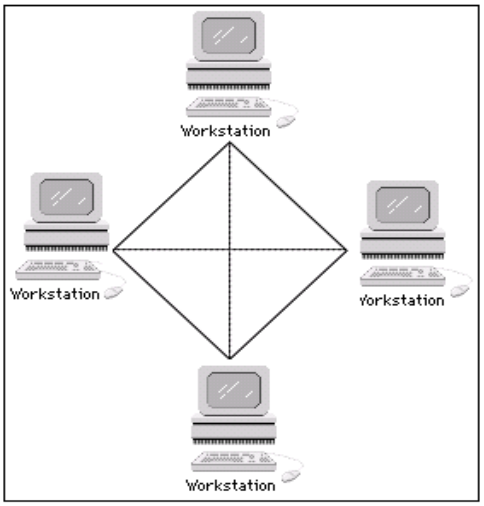
.

3. Ring Topology:-



Token Ring Network, in computer science, a LAN formed in a ring (closed loop) topology that uses token passing as a means of regulating traffic. On a token ring network, a token governing the right to transmit is passed from one station to the next in a physical circle. If a station has information to transmit, it "seizes" the token, marks it as being in use, and inserts the information. The "busy" token, plus message, is then passed around the circle, copied when it arrives at its destination, and eventually returned to the sender. The sender removes the attached message and then passes the freed token to the next station in line. Token ring networks are defined in the IEEE 802.5 standards.

4. Mesh Topology:-

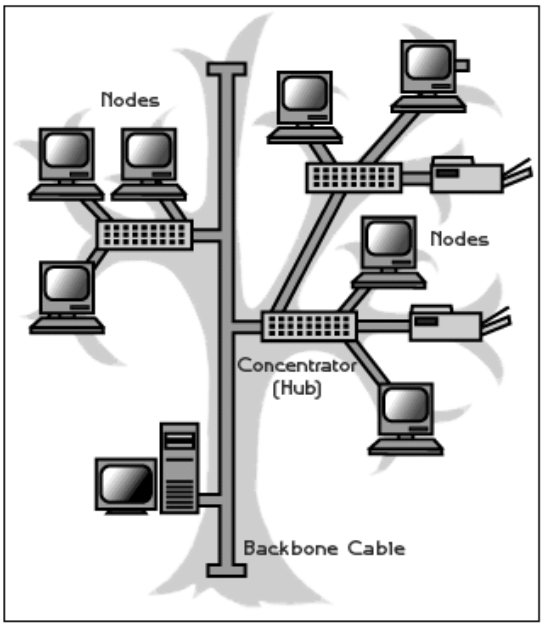


The type of network topology in which each of the nodes of the network is connected to each of the other nodes in the network with a point-to-point link – this makes it possible for data to be simultaneously transmitted from any single node to all of the other nodes.

Note: The physical fully connected mesh topology is generally too costly and complex for practical networks, although the topology is used when there are only a small number of nodes to be interconnected

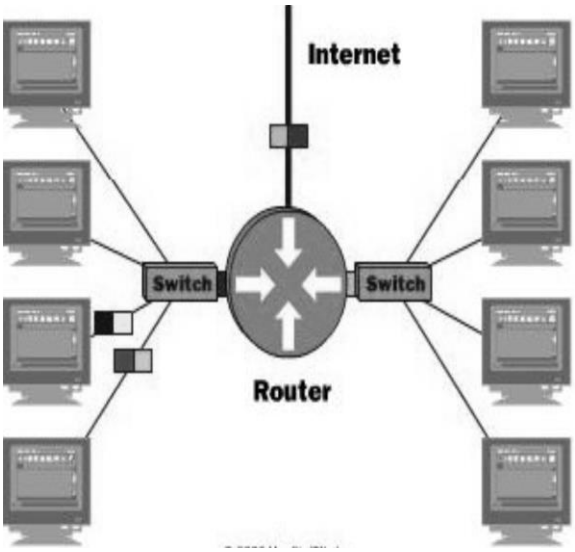
5. Hybrid/Tree Topology:-

A tree topology combines characteristics of linear bus and star topologies. It consists of groups of star-configured workstations connected to a linear bus backbone cable.



These topologies can also be mixed. For example, a bus-star network consists of a high-bandwidth bus, called the ***backbone,*** which connects a collection of slower-bandwidth star segments.

How Routers Work



Routers are the traffic cops of intranets. They make sure that all data gets sent to where it's supposed to go and that it gets sent via the most efficient route. Routers are also useful tools to make the most efficient use of the intranet. Routers are used to segment traffic and provide

redundancy of routes. Routers use encapsulation to permit different protocols to be sent across otherwise incompatible networks.

Just as routers direct traffic on the Internet, sending information to its proper destination, routers on an intranet perform the same function. Routers-equipment that is a combination of hardware and software-can send the data to a computer on the same subnetwork inside the intranet, to another network on the intranet, or outside to the Internet. They do this by examining header information in IP packets, and then sending the data on its way. Typically, a router will send the packet to the next router closest to the final destination, which in turn sends it to an even closer router, and so on, until the data reaches its intended recipient.

A router has input ports for receiving IP packets, and output ports for sending those packets toward their destination. When a packet comes to the input port, the router examines the packet header, and checks the destination in it against a routing table-a database that tells the router how to send packets to various destinations.

Based on the information in the routing table, the packet is sent to a particular output port, which sends the packet to the next closest router to the packet's destination.

If packets come to the input port more quickly than the router can process them, they are sent to a holding area called an input queue. The router then processes packets from the queue in the order they were received. If the number of packets received exceeds the capacity of the queue (called the length of the queue), packets may be lost.

In a simple intranet that is a single, completely self-contained network, and in which there are no connections to any other network or the intranet, only minimal routing need be done, and so the routing table in the router is exceedingly simple with very few entries, and is constructed automatically by a program called *ifconfig*

Conclusion: Hence ,we have demonstrate a wired LAN for four computers.

Assignment No. A2

Title: PC to PC communication

Objectives: To establish communication among the computing nodes in P2P and Client-Server architecture

Problem Statement:

Write a Program with following four options to transfer-

a. Characters separated by space
b. One Strings at a time
c. One Sentence at a time
d. One file at a time

Between two RS 232D or USB ports using C/C++. (To demonstrate Framing, Flow control, Error control).

Outcomes:

Develop Client-Server architectures and prototypes by the means of correct standards and technology.

Tools Required:

Hardwar: PC-2, RS-232 cable

Software: gcc compiler

Theory:

Introduction to RS (Recommended Standard)-232:

RS-232 standards (EIA-232) are defined by EIA/TIA (Electronic Industries Alliance /Telecommunications Industry Association). RS-232 defines both the physical and electrical characteristics of the interface. RS-232 is practically identical to ITU V.24 (signal description and names) and V.28 (electrical). RS232 is an Active LOW voltage driven interfaces and operates at +12V to -12V where:

Signal = 0 (LOW) > +3.0V (SPACE)

Signal = 1 (HIGH) < -3.0V (MARK)

1. Signal voltages in the range >-3.0V to +3.0V are regarded as being in the 'dead area' (indeterminate value) and allow for absorption of noise. For more on the use of signals and other heavy stuff.

2. The power level on RS232 pins is defined by TIA for short circuit protection to be 100mA. Most RS232 drivers will provide lower short circuit protection (especially for laptops). A

max of 50mA PER PIN may be available but the data sheet for the specific interface/chip should be consulted before committing to externally powered designs.

RS-232 standards (EIA-232) are defined by EIA/TIA. They have defined following standards

1. RS232 on DB9 and DB25 known as RS-232C
2. RS232 on DB9 and DB25 known as EIA/TIA – 574
3. RS232 on DB9 and DB25 known as RS-232D
4. RS232 on RJ45 known as RS-232D EIA/TIA-561
5. RS422,423 and 435 on DB25 Known as EIA/TIA RS-530-A

RS232 is the most known serial port used in transmitting the data in communication and interface. Even though serial port is harder to program than the parallel port, this is the most effective method in which the data transmission requires less wires that yields to the less cost. The RS232 is the communication line which enables the data transmission by only using three wire links. The three links provides 'transmit', 'receive' and common ground.

The 'transmit' and 'receive' line on this connecter send and receive data between the computers. As the name indicates, the data is transmitted serially. The two pins are TXD & RXD. There are other lines on this port as RTS, CTS, DSR, DTR, and RTS, RI. The '1' and '0' are the data which defines a voltage level of 3V to 25V and -3V to -25V respectively.

The electrical characteristics of the serial port as per the EIA (Electronics Industry Association) RS232C Standard specifies a maximum baud rate of 20,000bps, which is slow compared to today's standard speed. For this reason, we have chosen the new RS-232D Standard, which was recently released.

The RS-232D has existed in two types. i.e., D-TYPE 25 pin connector and D-TYPE 9 pin connector, which are male connectors on the back of the PC. You need a female connector on your communication from Host to Guest computer. The pin outs of both D-9 & D-25 are show below.

DTE (PC) and DCE (Modem)

Devices, which use serial cables for their communication, are split into two categories. These are DCE (Data Communications Equipment) and DTE (Data Terminal Equipment.) Data Communications Equipments are devices such as your modem, TA adapter, plotter etc while Data Terminal Equipment is your Computer or Terminal. A typical Data Terminal Device is a computer and a typical Data Communications Device is a Modem. Often people will talk about DTE to DCE or DCE to DCE speeds. DTE to DCE is the speed between your modem and computer, sometimes referred to as your terminal speed. This should run at faster speeds than the DCE to DCE speed. DCE to DCE is the link between modems, sometimes called the line speed.

Most people today will have 28.8K or 33.6K modems. Therefore, we should expect the DCE to DCE speed to be either 28.8K or 33.6K. Considering the high speed of the modem we should expect the DTE to DCE speed to be about 115,200 BPS. (Maximum Speed of the 16550a UART) . The communications program, which we use, has settings for DCE to DTE speeds. However, the speed is 9.6 KBPS, 144 KBPS etc and the modem speed.

If we were transferring that text file at 28.8K (DCE- DCE), then when the modem compresses it you are actually transferring 115.2 KBPS between computers and thus have a DCE- DTE speed of 115.2 KBPS. Thus, this is why the DCE- DTE should be much higher than the modem's connection speed. Therefore, if our DTE to DCE speed is several times faster than our DCE to DCE speed the PC can send data to your modem at 115,200 BPS.

In serial communications the terminal end (PC) is called the Data Terminal Equipment (DTE) and the modem end is called the Data Communications Equipment (DCE) as shown in the diagram below.

Figure 1.Serial Communications with a modem

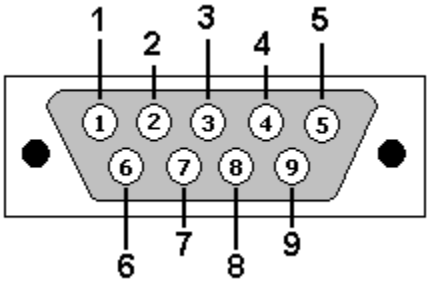
RS-232 signals have a direction (in or out) depending on whether they are with respect to a DTE or a DCE. In all the pinout diagrams below the signal direction is with respect to the DTE (PC) end.

What is NULL MODEM?

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

When PCs are connected back-to-back each end is acting as a DTE (there is no DCE in this case) and consequently certain signals may have to be looped in the connection to satisfy any input signal requirement. This is called a NULL (no) modem configuration. For example, when the DTE raises Request to Send (RTS) it typically expects Clear to Send (CTS) from the DCE. Since there is no DCE to raise CTS, the outgoing RTS signal is looped in the NULL modem cable to the incoming CTS to satisfy the DTE's need for this signal.

DB9 Male and Female Views



pin diagram

Pin No	Name	Dir	Description
1	DCD	IN	Data Carrier Detect. Raised by DCE when modem synchronized.
2	RD	IN	Receive Data (RxD, Rx). Arriving data from DCE.
3	TD	OUT	Transmit Data (TxD, Tx). Sending data from DTE.
4	DTR	OUT	Data Terminal Ready. Raised by DTE when powered on.
5	SGND	-	Ground. This is reference voltage
6	DSR	IN	Data Set Ready. Raised by DCE to indicate ready.
7	RTS	OUT	Request To Send. Raised by DTE when it wishes to send. Expects CTS from DCE.
8	CTS	IN	Clear To Send. Raised by DCE in response to RTS from DTE.
9	RI	IN	Ring Indicator. Set when incoming ring detected - used for auto-answer application. DTE raised DTR to answer.

Figure 2.DB9: View looking into male connector

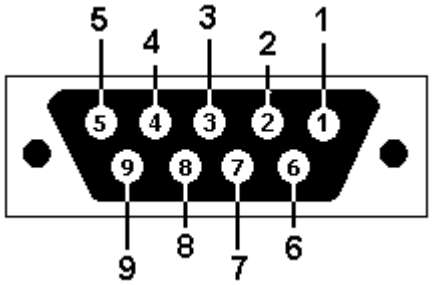


Figure 3. DB9: View looking into female connection

Framing:

To provide service to the network layer, the data link layer must use the service provided to it by the physical layer. What the physical layer does is accept a raw bit stream and attempt to deliver it to the destination. If the channel is noisy, as it is for most wireless and some wired links, the physical layer will add some redundancy to its signals to reduce the bit error rate to a tolerable level. However, the bit stream received by the data link layer is not guaranteed to be error free. Some bits may have different values and the number of bits received may be less than, equal to, or more than the number of bits transmitted. It is up to the data link layer to detect and, if necessary, correct errors. The usual approach is for the data link layer to break up the bit stream into discrete frames, compute a short token called a checksum for each frame, and include the checksum in the frame when it is transmitted. (Checksum algorithms will be discussed later in this chapter.) When a frame arrives at the destination, the checksum is recomputed. If the newly computed checksum is different from the one contained in the frame, the data link layer knows that an error has occurred and takes steps to deal with it.

Flow and Error Control

Data communication requires at least two devices working together, one to send and the other to receive. Even such a basic arrangement requires a great deal of coordination for an intelligible exchange to occur. The most important responsibilities of the data link layer are flow control and error control. Collectively, these functions are known as data link control.

Flow Control

Flow control coordinates the amount of data that can be sent before receiving an acknowledgment and is one of the most important duties of the data link layer. In most protocols, flow control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data must not be allowed to overwhelm the receiver. Any receiving device has a limited speed at which it can process incoming data and a limited amount of memory in which to store incoming data. The receiving device must be able to inform the sending device before those limits are reached and to request that the transmitting

device send fewer frames or stop temporarily. Incoming data must be checked and processed before they can be used. The rate of such processing is often slower than the rate of transmission. For this reason, each receiving device has a block of memory, called a *buffer*, reserved for storing incoming data until they are processed. If the buffer begins to fill up, the receiver must be able to tell the sender to halt transmission until it is once again able to receive.

Error Control

Error control is both error detection and error correction. It allows the receiver to inform the sender of any frames lost or damaged in transmission and coordinates the retransmission of those frames by the sender. In the data link layer, the term *error control* refers primarily to methods of error detection and retransmission. Error control in the data link layer is often implemented simply: Any time an error is detected in an exchange, specified frames are retransmitted. This process is called automatic repeat request (ARQ).

Test Cases:

1) Characters separated by space
2) One Strings at a time
3) One Sentence at a time
4) One file at a time

Conclusion: Hence we implemented program for pc to pc communication using RS 232 cable.

ASSIGNMENT-3

PROBLEM STATEMENT:

Write a program using TCP socket for wired network for following
a. Say Hello to Each other (For all students)
b. File transfer (For all students)
c. Calculator (Arithmetic) (50% students)
d. Calculator (Trigonometry) (50% students)

Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.

THEORY:

TCP:

The Transmission Control Protocol provides a communication service at an intermediate level between an application program and the Internet Protocol. It provides host-to-host connectivity at the Transport Layer of the Internet model.

The client server model

Most interprocess communication uses the client server model. These terms refer to the two processes which will be communicating with each other. One of the two processes, the client, connects to the other process, the server, typically to make a request for information. A socket is one end of an interprocess communication channel. The two processes each establish their own socket.

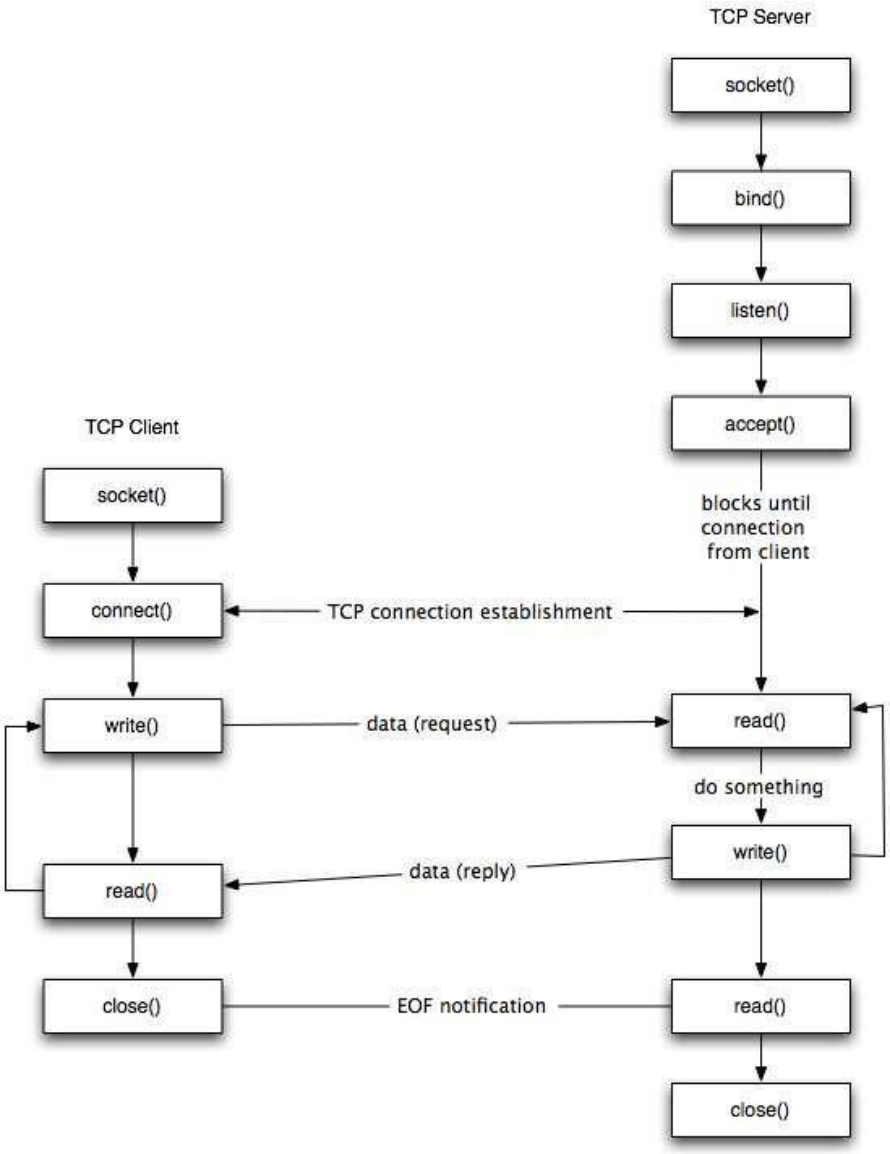
The steps involved in establishing a socket on the client side are as follows:

1. Create a socket with the socket( ) system call
2. Connect the socket to the address of the server using the connect( ) system call
3. Send and receive data. There are a number of ways to do this, but the simplest is to use the read ( ) and write ( ) system calls.

The steps involved in establishing a socket on the server side are as follows:

1. Create a socket with the socket ( ) system call
2. Bind the socket to an address using the bind ( ) system call. For a server socket on the Internet, an address consists of a port number on the host machine.
3. Listen for connections with the listen ( ) system call

4. Accept a connection with the accept ( ) system call. This call typically blocks until a client connects with the server.
5. Send and receive data



FTP:

The File Transfer Protocol (FTP) is a standard network protocol used to transfer computer files from one host to another host over a TCP-based network, such as the Internet. FTP is built on client-server architecture and uses separate control and data connections between the client and the server. FTP users may authenticate themselves using a clear-text sign-in protocol, normally

in the form of a username and password, but can connect anonymously if the server is configured to allow it. For secure transmission that protects the username and password, and encrypts the content, FTP is often secured with SSL/TLS (FTPS).

Communication and data transfer:

FTP may run in active or passive mode, which determines how the data connection is established. In both cases, the client creates a TCP control connection from a random unprivileged port N to the FTP server command port 21. In active modes, the client starts listening for incoming data connections on port N+1 from the server (the client sends the FTP command PORT N+1 to inform the server on which port it is listening). In situations where the client is behind a firewall and unable to accept incoming TCP connections, passive mode may be used. In this mode, the client uses the control connection to send a PASV command to the server and then receives a server IP address and server port number from the server, which the client then uses to open a data connection from an arbitrary client port to the server IP address and server port number received. Both modes were updated in September 1998 to support IPV6. Further changes were introduced to the passive mode at that time, updating it to extended passive mode.

The server responds over the control connection with three-digit status codes in ASCII with an optional text message. The numbers represent the code for the response and the optional text represents a human-readable explanation or request . An ongoing transfer of file data over the data connection can be aborted using an interrupt message sent over the control connection.

Login

FTP login utilizes a normal username and password scheme for granting access. The username is sent to the server using the USER command, and the password is sent using the PASS command. If the information provided by the client is accepted by the server, the server will send a greeting to the client and the session will commence. If the server supports it, users may log in without providing login credentials, but the same server may authorize only limited access for such sessions.

Anonymous FTP

A host that provides an FTP service may provide anonymous FTP access. Users typically log into the service with an 'anonymous' (lower-case and case-sensitive in some FTP servers) account when prompted for user name. Although users are commonly asked to send their email address instead of a password, no verification is actually performed on the supplied data. Many FTP hosts whose purpose is to provide software updates will allow anonymous logins.

No.	TCP	UDP
1	This Connection oriented protocol	This is connection-less protocol
2	The TCP connection is byte stream	The UDP connection is a message stream
3	It does not support multicasting and broadcasting	It supports broadcasting
4	It provides error control and flow control	The error control and flow control is not provided
5	TCP supports full duplex transmission	UDP does not support full duplex transmission
6	It is reliable service of data transmission	This is an unreliable service of data transmission
7	The TCP packet is called as segment	The UDP packet is called as user datagram.

CONCLUSION:

Thus we have successfully implemented the socket programming for TCP using C.

ASSIGNMENT-4

PROBLEM STATEMENT:

Write a program using UDP Sockets to enable file transfer (Script, Text, Audio and Video one file each) between two machines. Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.

THEORY:

UDP:

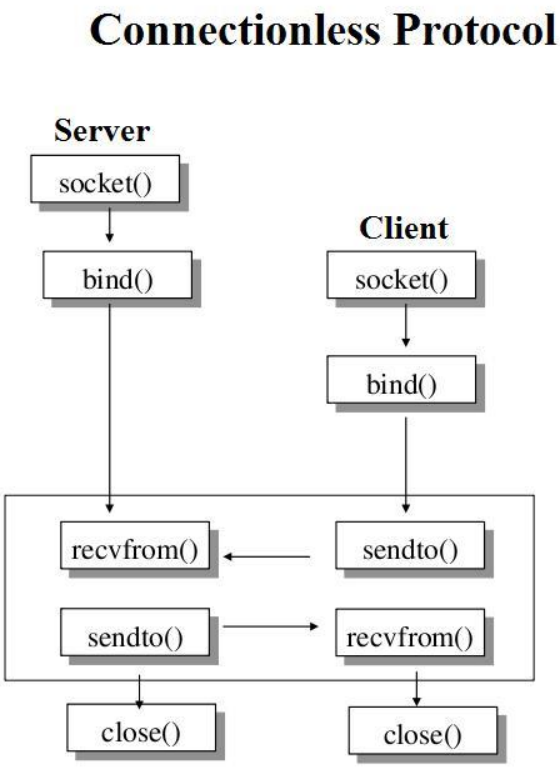
UDP (User Datagram Protocol) is a communication protocol that offers a limited amount of service when messages are exchanged between computers in a network that uses the Internet Protocol (IP). UDP is an alternative to the Transmission Control Protocol (TCP) and, together with IP, is sometimes referred to as UDP/IP. Like the Transmission Control Protocol, UDP uses the Internet Protocol to actually get a data unit (called a datagram) from one computer to another. Unlike TCP, however, UDP does not provide the service of dividing a message into packets (datagrams) and reassembling it at the other end. Specifically, UDP doesn't provide sequencing of the packets that the data arrives in. This means that the application program that uses UDP must be able to make sure that the entire message has arrived and is in the right order. Network applications that want to save processing time because they have very small data units to exchange (and therefore very little message reassembling to do) may prefer UDP to TCP. The Trivial File Transfer Protocol (TFTP) uses UDP instead of TCP.

With a UDP socket a connection is NOT made, instead the sender just issues a message to its destination and hopes it gets there! The message uses a datagram of fixed length, often termed a record. Since there is no connection between client and server the client can send a datagram to one server and then immediately send a datagram to another server using the same socket UDP is a connectionless protocol.

Trivial File Transfer Protocol (TFTP) is a simple, lock-step, file transfer protocol which allows a client to get from or put a file onto a remote host.

TFTP is a simple protocol for transferring files, implemented on top of the UDP/IP protocols using IANA registered port number 69. TFTP was designed to be small and easy to implement,

and therefore it lacks most of the advanced features offered by more robust file transfer protocols. TFTP only reads and writes files from or to a remote server. It cannot list, delete, or rename files or directories and it has no provisions for user authentication. Today TFTP is generally only used on local area networks (LAN).



CONCLUSION:

Thus we have successfully implemented the socket programming for UDP using C.

ASSIGNMENT-5

Title: Packet analysis for wired network

Objectives : To demonstrate data flow at various layer

PROBLEM STATEMENT:

Write a program to analyze following packet formats captured through Wireshark for wired network. 1. Ethernet 2. IP 3.TCP 4. UDP

Outcome: Student will able to demonstrate data flow from top-to-down and down to up for various protocol stacks at various layers and propose protocol model / framework for future network requirements

Tools Required: gcc complier and wireshark tool

THEORY:

Packet sniffer \ Packet analyzer:

A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams own across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

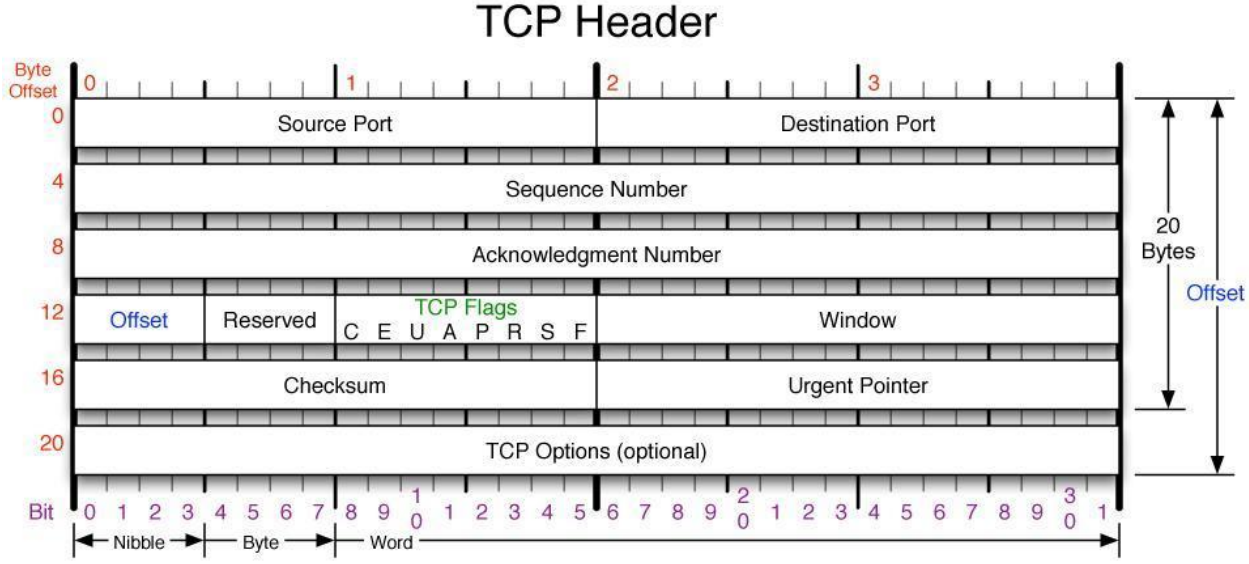
Different types of packet:

1. TCP:

The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered and error-checked delivery (or notification of failure to deliver) of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer. Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another. The protocol corresponds to the transport layer of TCP/IP suite. TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the

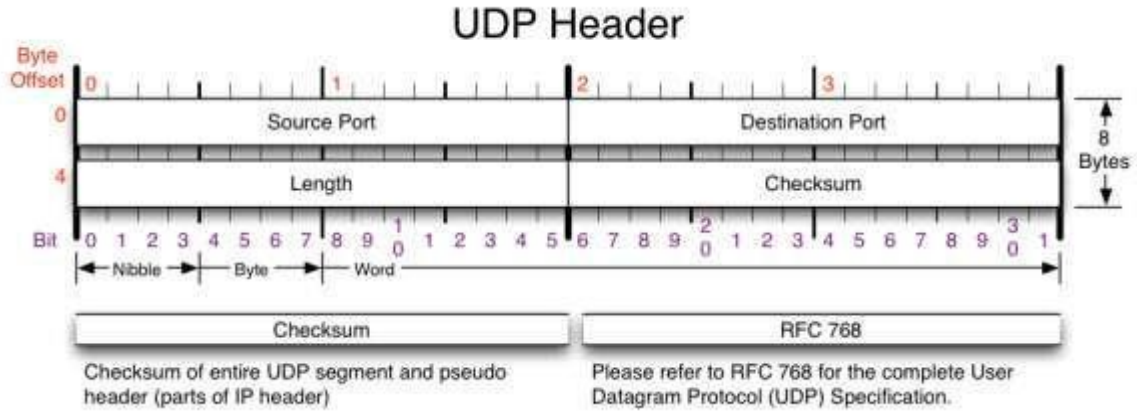
IP works by exchanging pieces of information called packets. A packet is a sequence of octets (bytes) and consists of a header followed by a body. The header describes the packet's source,

destination and control information. The body contains the data IP is transmitting. Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost, duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details. TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer over many networks is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps a record of each packet it sends. The sender also maintains a timer from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted.



2. UDP:

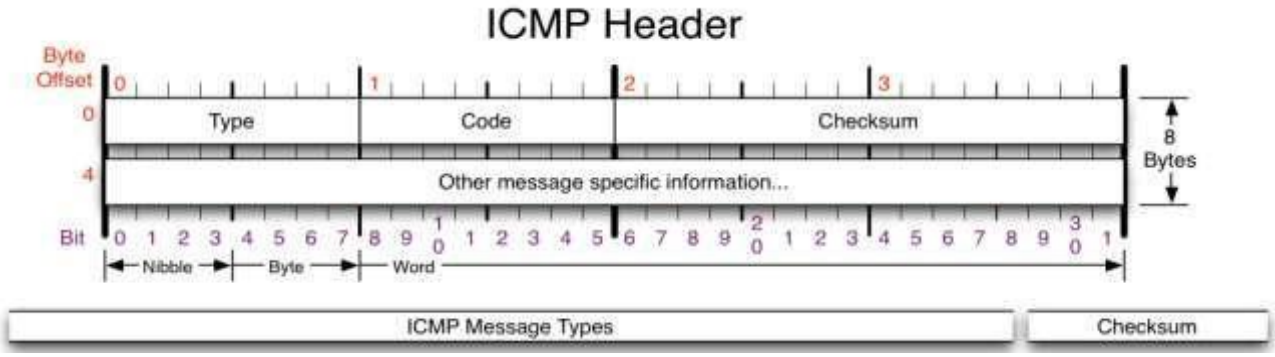
The User Datagram Protocol (UDP) is one of the core members of the Internet protocol Suite. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.



3.ICMP:

The Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

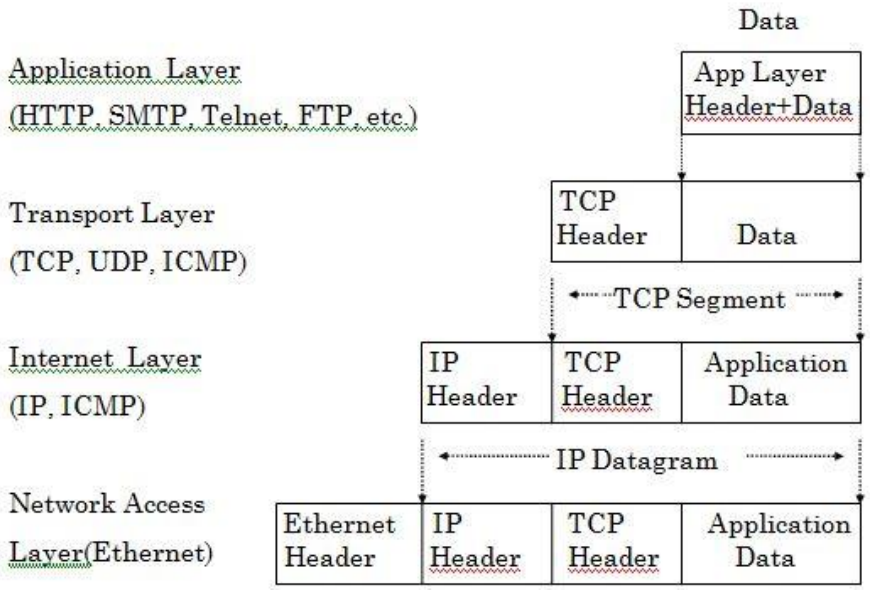
ICMP can also be used to relay query messages. It is assigned protocol number 1.ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and trace route). ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6. The Internet Control Message Protocol is part of the Internet Protocol Suite, as defined in RFC 792. ICMP messages



are typically used for diagnostic or control purposes or generated in response to errors in IP operations. ICMP errors are directed to the source IP address of the originating packet.

4.IGMP:

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast.IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. IGMP messages are carried in bare IP packets with IP protocol. There is no transport layer used with IGMP messaging, similar to the Internet Control Message Protocol. Membership Queries are sent by multicast routers to determine which multicast addresses are of interest to systems attached to its network. Routers periodically send General Queries to refresh the group membership state for all systems on its network. Group-Specific Queries are used for determining the reception state for a particular multicast address.



TCP/IP model

CONCLUSION:

Hence we have implemented packet formats captured through Wireshark for wired network. 1. Ethernet 2. IP 3.TCP 4. UDP .

ASSIGNMENT-6

Tittle: To demonstrate error detection and correction using Hamming Codes or CRC

Objectives : To implement error detection and correction techniques

Problem Statement: Write a program for error detection and correction for 7/8 bits ASCII codes using Hamming Codes or CRC. Demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.

Outcome : Demonstrate Hamming Codes or CRC with example.

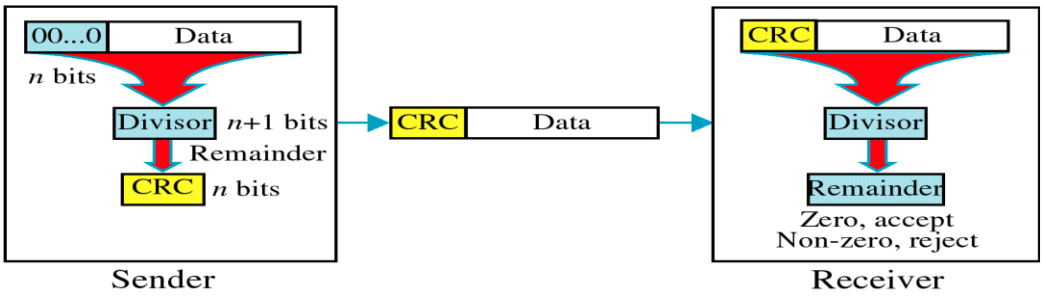
Software Requirements : Jdk and wireshark

Hardware Requirements : Open source linux operating system.

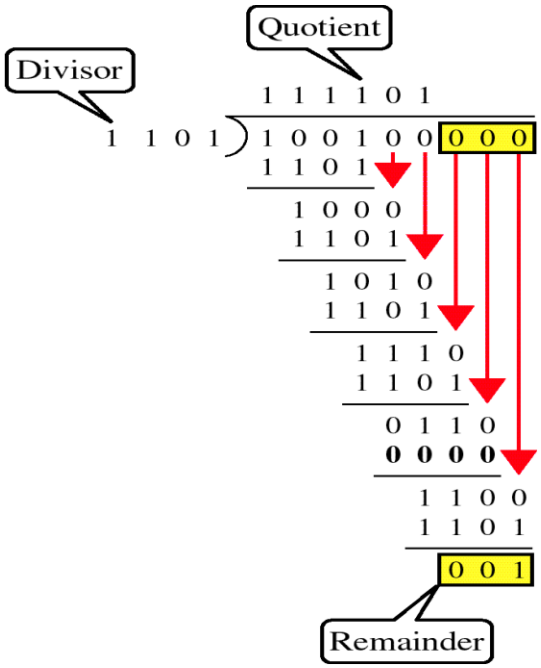
THEORY:

Cyclic Redundancy Check: CRC

- Given a k-bit frame or message, the transmitter generates an n-bit sequence, known as a *frame check sequence (FCS)*, so that the resulting frame, consisting of (k+n) bits, is exactly divisible by some predetermined number.
- The receiver then divides the incoming frame by the same number and, if there is no remainder, assumes that there was no error.



Example:



Hamming code

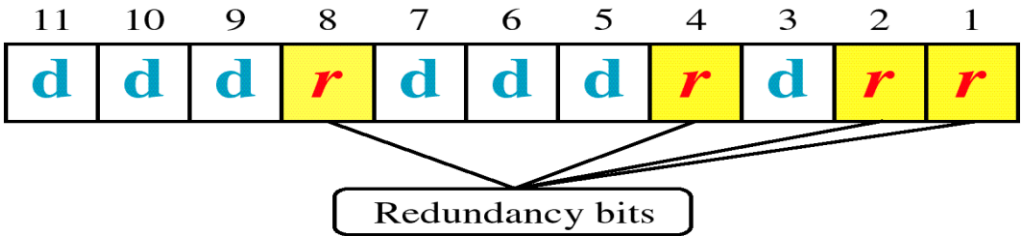
- **Hamming codes are a family of linear error-correcting codes that generalize the Hamming(7,4)-code**
- **Invented by Richard Hamming in 1950**

Hamming codes can detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors.

General algorithm

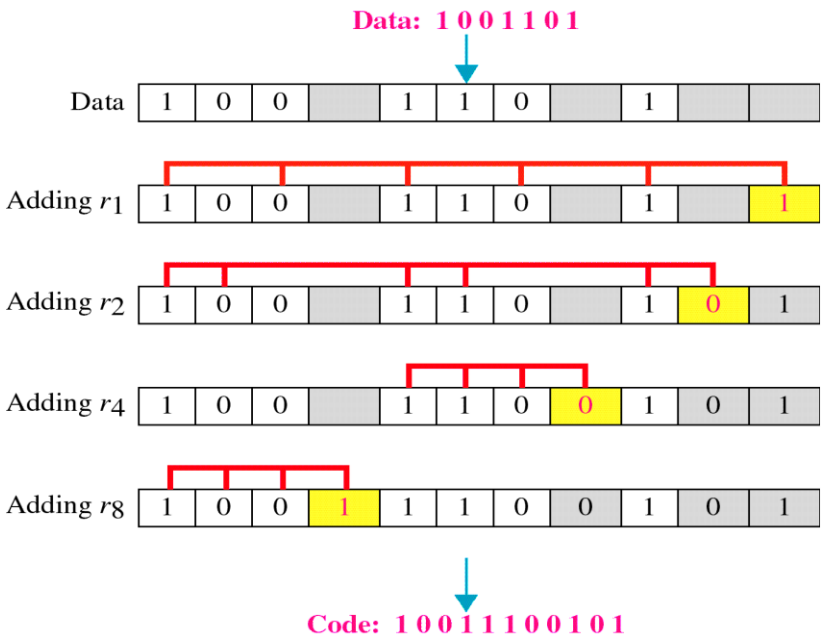
- **The following general algorithm generates a single-error correcting (SEC) code for any number of bits.**
- **Number the bits starting from 1: bit 1, 2, 3, 4, 5, etc.**
- **Write the bit numbers in binary: 1, 10, 11, 100, 101, etc.**
- **All bit positions that are powers of two (have only one 1 bit in the binary form of their position) are parity bits: 1, 2, 4, 8, etc. (1, 10, 100, 1000)**

- **All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.**
- **Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.**
- **Each data bit is included in a unique set of 2 or more parity bits, as determined by the binary form of its bit position.**
    - **Parity bit 1 covers all bit positions which have the least significant bit set: bit 1 (the parity bit itself), 3, 5, 7, 9, etc.**
    - **Parity bit 2 covers all bit positions which have the second least significant bit set: bit 2 (the parity bit itself), 3, 6, 7, 10, 11, etc.**
    - **Parity bit 4 covers all bit positions which have the third least significant bit set: bits 4–7, 12–15, 20–23, etc.**
    - **Parity bit 8 covers all bit positions which have the fourth least significant bit set: bits 8–15, 24–31, 40–47, etc.**
    - **In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.**

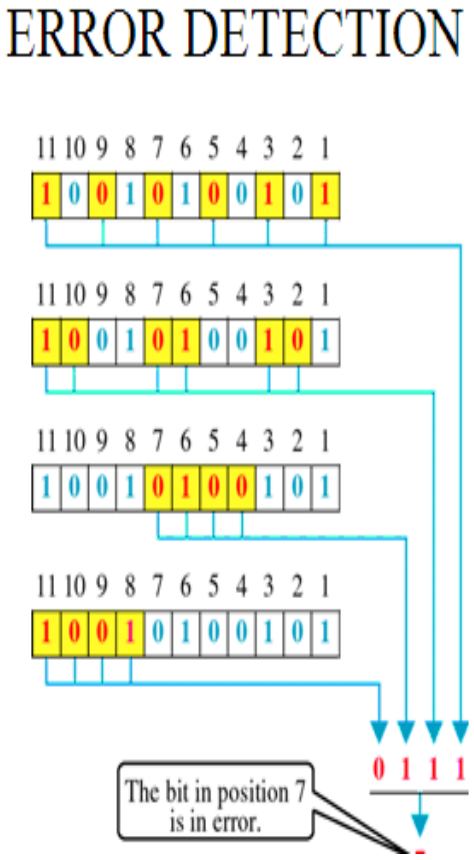


Example

Error detection



Error correction



Conclusion: Hence we have implemented CRC and Hamming code.

Assignment No. A7

Title: Implementation of sliding window protocol(Go back N and Selective Repeat**)**

Objectives: To demonstrate Go back N and Selective Repeat Modes of Sliding Window Protocol in peer to peer mode .

Problem Statement:

Write a program to simulate Go back N and Selective Repeat Modes of Sliding Window Protocol in peer to peer mode and demonstrate the packets captured traces using Wireshark Packet Analyzer Tool for peer to peer mode.

Outcomes:

Demonstrate Go back N and Selective Repeat Modes and also captured packets using Wireshark Packet Analyzer Tool for peer to peer mode.

Tools Required:

Hardwar: PC-2

Software: jdk compiler and wireshark.

Theory:

The basic idea of sliding window protocol is that both sender and receiver keep a ``window" of acknowledgment. The sender keeps the value of expected acknowledgment; while the receiver keeps the value of expected receiving frame. When it receives an acknowledgment from the receiver, the sender advances the window. When it receives the expected frame, the receiver advances the window.

In transmit flow control, sliding window is a variable-duration window that allows a sender to transmit a specified number of data units before an acknowledgement is received or before a specified event occurs.

Flow Control is a set of procedures that tells the sender how much data it can transmit before it must wait for an acknowledgment from the receiver. The flow of data should not be allowed to overwhelm the receiver. Receiver should also be able to inform the transmitter before its limits (this limit may be amount of memory used to store the incoming data or the processing power at the receiver end) are reached and the sender must send fewer frames. Hence, Flow control refers to the set of procedures used to restrict the amount of data the transmitter can send before waiting for acknowledgment.

There are two methods developed for flow control namely Stop-and-wait and Sliding-window Sliding window algorithms, used by TCP, permit multiple data packets to be in simultaneous transit, making more efficient use of network bandwidth.

Sliding Window Protocol:

With the use of multiple frames for a single message, the stop-and-wait protocol does not perform well. Only one frame at a time can be in transit. Efficiency can be greatly improved by allowing multiple frames to be in transit at the same time. Efficiency can also be improved by making use of the full-duplex line. To keep track of the frames, sender station sends sequentially numbered frames. Since the sequence number to be used occupies a field in the frame, it should be of limited size. If the header of the frame allows k bits, the sequence numbers range from 0 to 2k – 1. Sender maintains a list of sequence numbers that it is allowed to send (sender window).

The size of the sender's window is at most 2k – 1. The sender is provided with a buffer equal to the window size. Receiver also maintains a window of size 2k – 1. The receiver acknowledges a frame by sending an ACK frame that includes the sequence number of the next frame expected. This also explicitly announces that it is prepared to receive the next N frames, beginning with the

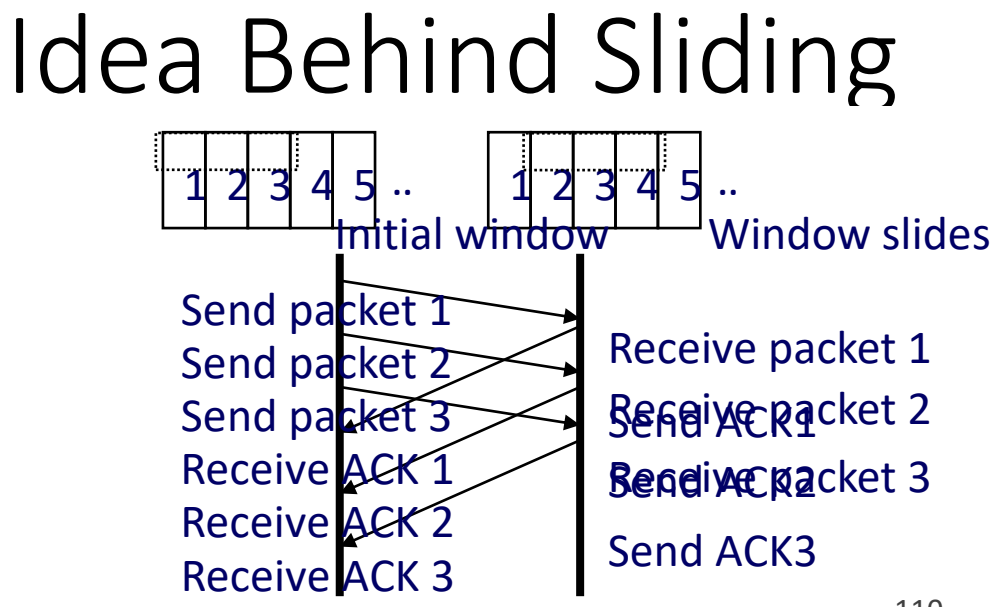
number specified. This scheme can be used to acknowledge multiple frames. It could receive frames 2, 3, 4 but withhold ACK until frame 4 has arrived. By returning an ACK with sequence number 5, it acknowledges frames 2, 3, 4 in one go. The receiver needs a buffer of size 1.

Sliding window algorithm is a method of flow control for network data transfers. TCP, the Internet's stream transfer protocol, uses a sliding window algorithm.

A sliding window algorithm places a buffer between the application program and the network data flow. For TCP, the buffer is typically in the operating system kernel, but this is more of an implementation detail than a hard-and-fast requirement.

Data received from the network is stored in the buffer, from where the application can read at its own pace. As the application reads data, buffer space is freed up to accept more input from the network. The window is the amount of data that can be "read ahead" - the size of the buffer, less the amount of valid data stored in it. Window announcements are used to inform the remote host of the current window size.

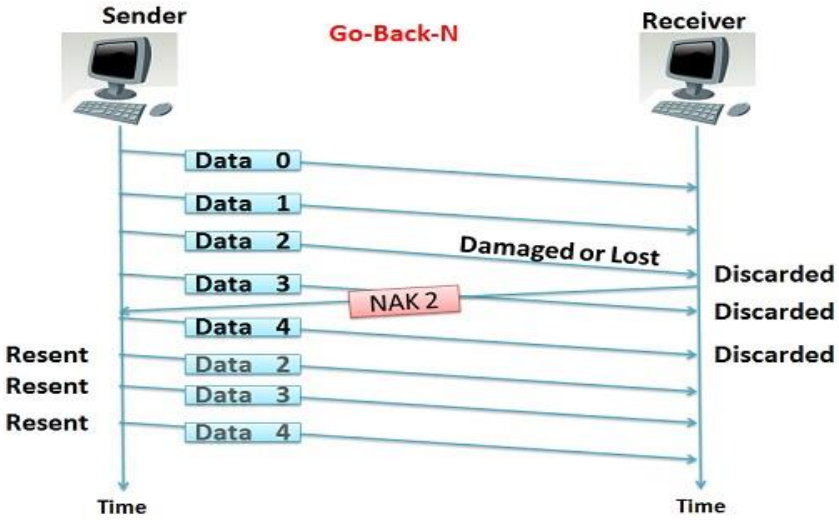
> An example of a sliding window in packet transmission is one in which, after the sender fails to receive an acknowledgement for the first transmitted packet, the sender "slides" the window, i.e. resets the window, and sends a second packet. This process is repeated for the specified number of times before the sender interrupts transmission. Sliding window is sometimes (loosely) called *acknowledgement delay period*.



Go-Back-N Protocol and "Selective Repeat Protocol" are the sliding window protocols. The sliding window protocol is primarily an error control protocol, i.e. it is a method of error detection and error correction. The basic difference between go-back-n protocol and selective repeat protocol is that the "go-back-n protocol" retransmits all the frames that lie after the frame which is damaged or lost. The "selective repeat protocol" retransmits only that frame which is damaged or lost.

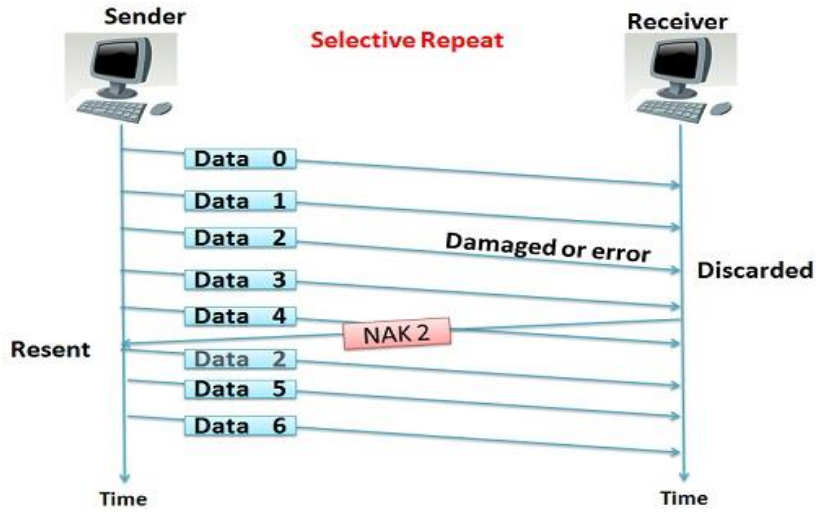
Go back N ARQ

In the Go-Back-N Protocol, the sequence numbers are modulo 1!",
where *m* is the size of the sequence number field in bits.



Selective Repeat ARQ

Go-Back-N ARQ simplifies the process at the receiver site. The receiver keeps track of only one variable, and there is no need to buffer out-of-order frames; they are simply discarded. However, this protocol is very inefficient for a noisy link. In a noisy link a frame has a higher probability of damage, which means the resending of multiple frames. This resending uses up the bandwidth and slows down the transmission. For noisy links, there is another mechanism that does not resend *N* frames when just one frame is damaged;only the damaged frame is resent. This mechanism is called Selective RepeatARQ.



Key Differences Between Go-Back-N and Selective Repeat

1. Go-Back-N protocol is design to retransmit all the frames that are arrived after the damaged or a lost frame. On the other hand, Selective Repeat protocol retransmits only that frame that is damaged or lost.
2. If the error rate is high i.e. more frames are being damaged and then retransmitting all the frames that arrived after a damaged frame waste the lots of bandwidth. On the other hand, selective repeat protocol re-transmits only damaged frame hence, minimum bandwidth is wasted.
3. All the frames after the damaged frame are discarded and the retransmitted frames arrive in a sequence from a damaged frame onwards, so, there is less headache of sorting the frames hence it is less complex. On the other hand only damaged or suspected frame is retransmitted so, extra logic has to be applied for sorting hence, it is more complicated.
4. Go-Back-N has a window size of N-1 and selective repeat have a window size <=(N+1)/2.
5. Neither sender nor receiver need the sorting algorithm in Go-Back-N whereas, receiver must be able to sort the as it has to maintain the sequence.

6. In Go-Back-N receiver discards all the frames after the damaged frame hence, it don't need to store any frames. Selective repeat protocol does not discard the frames arrived after the damaged frame instead it stores those frames till the damaged frame arrives successfully and is sorted in a proper sequence.
7. In selective repeat NAK frame refers to the damaged frame number and in Go-Back-N, NAK frame refers to the next frame expected.
8. Generally the Go-Back-N is more is use due to its less complex nature instead of Selective Repeat protocol.

Conclusion: Hence we have implemented of sliding window protocol(Go back N and Selective Repeat).

ASSIGNMENT-8

Tittle: To demonstrate subnetting and find subnet mask.

Objectives : To understand subnetting concepts and also find subnet mask of network.

Problem Statement: Write a program to demonstrate subnetting and find subnet mask.

Outcome : Demonstrate subnetting concepts with examples.

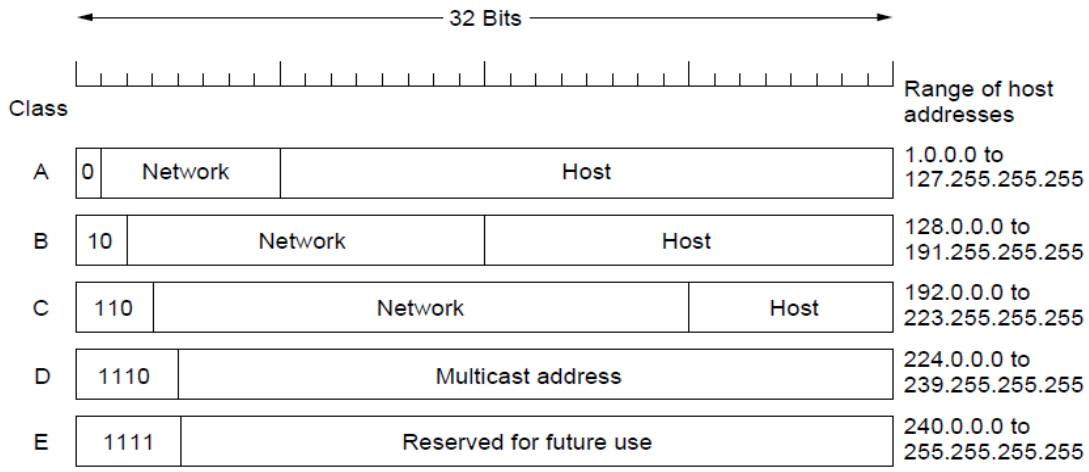
Software Requirements : Jdk and python

Hardware Requirements : Open source linux operating system.

THEORY:

What is IP address?

An Internet Protocol address (IP address) is a numerical label assigned to each device (e.g., computer, printer) participating in a computer network that uses the Internet Protocol for communication. An IP address serves two principal functions: host or network interface identification and location addressing. IP address is a 32 bit number. It is universally unique



What is subnet?

A sub network, or subnet, is a logical, visible subdivision of an IP network. The practice of dividing a network into two or more networks is called sub netting. Computers that belong to a subenet are addressed with a common identical, most-significant bit-group in their IP . This results in the logical division of an IP address into two fields, a network or routing prefix and the rest field or host identifier. The rest field is an identifier for a specific host or network interface.

For the purpose of network management, an IP address is divided into two logical parts, the network prefix and the host identifier or rest field. All hosts on a sub network have the same network prefix. This routing prefix occupies the most-significant bits of the address. The number of bits allocated within a network to the internal routing prefix may vary between subnets, depending on the network architecture. While in IPv6 the prefix must consist of a set of contiguous 1-bits, in IPv4 this is not enforced, though there is no advantage to using non-contiguous 1-bits. The host part is a unique local identification and is either a host number on the local network or an interface identifier.

What is subnet masking?

An IP address has two components, the network address and the host address. A subnet mask separates the IP address into the network and host addresses (<network><host>). Subnetting further divides the host part of an IP address into a subnet and host address (<network><subnet><host>) if additional sub network is needed. It is called a subnet mask because it is used to identify network address of an IP address by performing a bitwise AND operation on the net mask.

A Subnet mask is a 32-bit number that masks an IP address, and divides the IP address into network address and host address. Subnet Mask is made by setting network bits to all "1"s and setting host bits to all "0"s. Within a given network, two host addresses are reserved for special purpose, and cannot be assigned to hosts. The "0" address is assigned a network address and "255" is assigned to a broadcast address, and they cannot be assigned to hosts.

A mask used to determine what subnet an IP address belongs to. An IP address has two components, the network address and the host address.

For example

consider the IP address 150.215.017.009. Assuming this is part of a Class B network, the first two

numbers (150.215) represent the Class B network address, and the second two numbers (017.009) identify a particular host on this network.

Subnetting an IP network is to separate a big network into smaller multiple networks for reorganization and security purposes. All nodes (hosts) in a sub network see all packets transmitted by any node in a network. Performance of a network is adversely affected under heavy traffic load due to collisions and retransmissions.

Applying a subnet mask to an IP address separates network address from host address. The network bits are represented by the 1's in the mask, and the host bits are represented by 0's. Performing a bitwise logical AND operation on the IP address with the subnet mask produces the network address.

Conclusion:

Thus we have implemented subnetting program .

ASSIGNMENT-9

Title: Packet analysis for wired network

Objectives : To demonstrate data flow at various layer

PROBLEM STATEMENT:
Write a program to analyze following packet formats captured through Wireshark for wired network. 1. Ethernet 2. IP 3.TCP 4. UDP

Outcome: Student will able to demonstrate data flow from top-to-down and down to up for various protocol stacks at various layers and propose protocol model / framework for future network requirements
Tools Required: gcc complier and wireshark tool
THEORY:

Packet sniffer \ Packet analyzer:

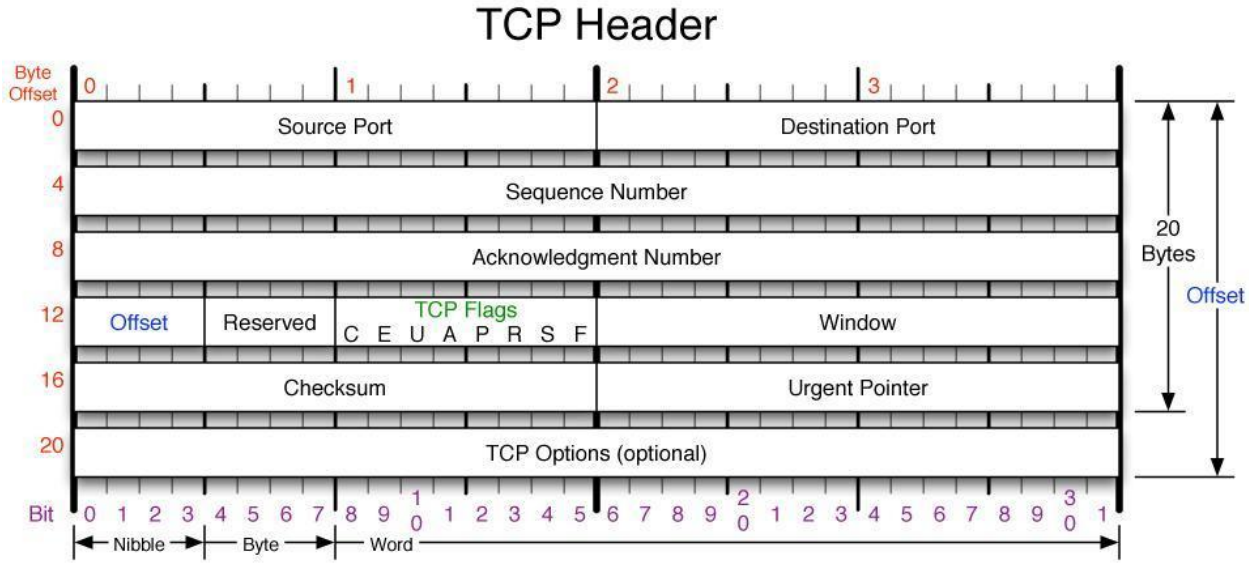
A packet analyzer (also known as a network analyzer, protocol analyzer or packet sniffer or for particular types of networks, an Ethernet sniffer or wireless sniffer) is a computer program or a piece of computer hardware that can intercept and log traffic passing over a digital network or part of a network. As data streams own across the network, the sniffer captures each packet and, if needed, decodes the packet's raw data, showing the values of various fields in the packet, and analyzes its content according to the appropriate RFC or other specifications.

Different types of packet:

1. TCP:

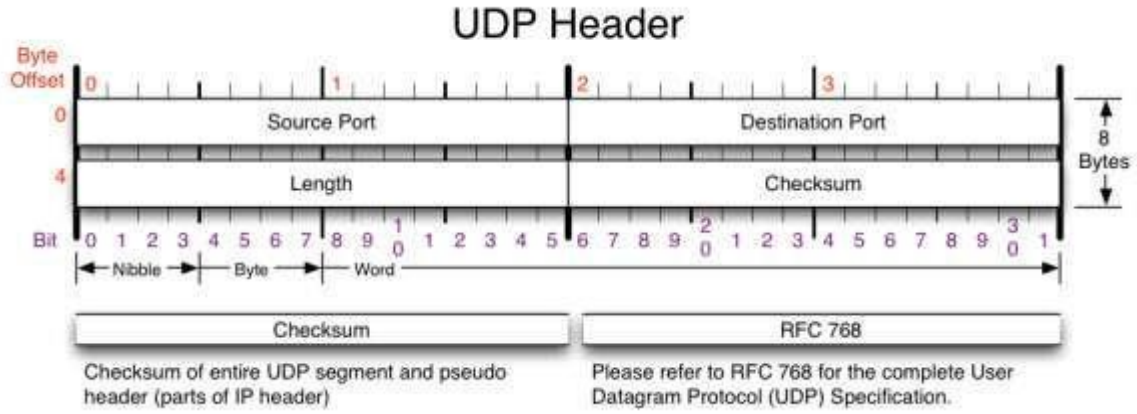
The Transmission Control Protocol (TCP) is one of the core protocols of the Internet protocol suite (IP), and is so common that the entire suite is often called TCP/IP. TCP provides reliable, ordered and error-checked delivery (or notification of failure to deliver) of a stream of octets between programs running on computers connected to a local area network, intranet or the public Internet. It resides at the transport layer. Web browsers use TCP when they connect to servers on the World Wide Web, and it is used to deliver email and transfer files from one location to another. The protocol corresponds to the transport layer of TCP/IP suite. TCP provides a communication service at an intermediate level between an application program and the Internet Protocol (IP). That is, when an application program desires to send a large chunk of data across the Internet using IP, instead of breaking the data into IP-sized pieces and issuing a series of IP requests, the software can issue a single request to TCP and let TCP handle the
IP works by exchanging pieces of information called packets. A packet is a sequence of octets (bytes) and consists of a header followed by a body. The header describes the packet's source, destination and control information. The body contains the data IP is transmitting. Due to network congestion, traffic load balancing, or other unpredictable network behavior, IP packets can be lost,

duplicated, or delivered out of order. TCP detects these problems, requests retransmission of lost data, rearranges out-of-order data, and even helps minimize network congestion to reduce the occurrence of the other problems. If the data still remains undelivered, its source is notified of this failure. Once the TCP receiver has reassembled the sequence of octets originally transmitted, it passes them to the receiving application. Thus, TCP abstracts the application's communication from the underlying networking details. TCP is a reliable stream delivery service that guarantees that all bytes received will be identical with bytes sent and in the correct order. Since packet transfer over many networks is not reliable, a technique known as positive acknowledgment with retransmission is used to guarantee reliability of packet transfers. This fundamental technique requires the receiver to respond with an acknowledgment message as it receives the data. The sender keeps a record of each packet it sends. The sender also maintains a timer from when the packet was sent, and retransmits a packet if the timer expires before the message has been acknowledged. The timer is needed in case a packet gets lost or corrupted.



2. UDP:

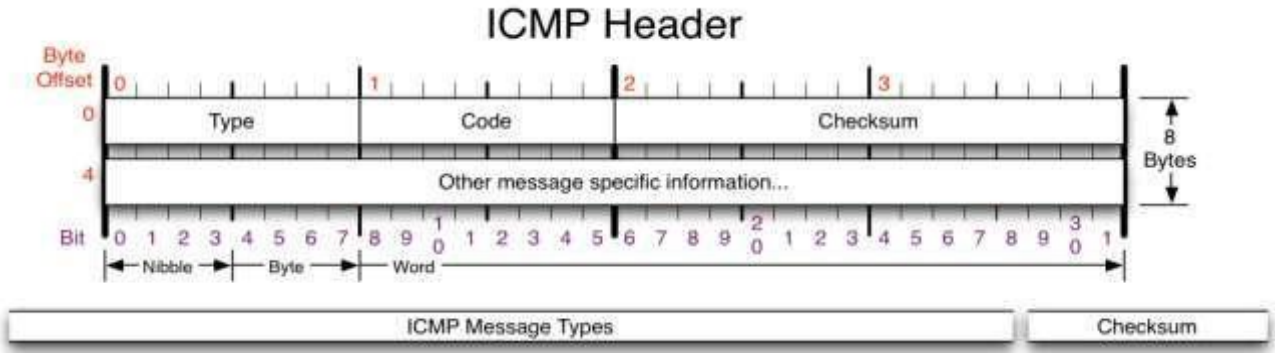
The User Datagram Protocol (UDP) is one of the core members of the Internet protocol Suite. UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. It has no handshaking dialogues, and thus exposes any unreliability of the underlying network protocol to the user's program. There is no guarantee of delivery, ordering, or duplicate protection. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. With UDP, computer applications can send messages, in this case referred to as datagrams, to other hosts on an Internet Protocol (IP) network without prior communications to set up special transmission channels or data paths. UDP is suitable for purposes where error checking and correction is either not necessary or is performed in the application, avoiding the overhead of such processing at the network interface level. Time-sensitive applications often use UDP because dropping packets is preferable to waiting for delayed packets, which may not be an option in a real-time system.



3.ICMP:

The Internet Control Message Protocol (ICMP) is one of the main protocols of the Internet Protocol Suite. It is used by network devices, like routers, to send error messages indicating, for example, that a requested service is not available or that a host or router could not be reached.

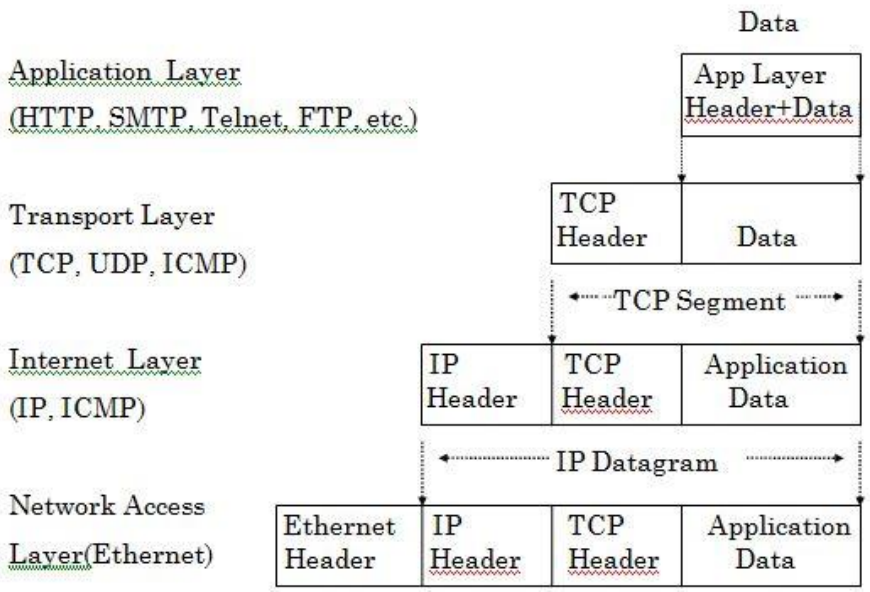
ICMP can also be used to relay query messages. It is assigned protocol number 1.ICMP differs from transport protocols such as TCP and UDP in that it is not typically used to exchange data between systems, nor is it regularly employed by end-user network applications (with the exception of some diagnostic tools like ping and trace route). ICMP for Internet Protocol version 4 (IPv4) is also known as ICMPv4. IPv6 has a similar protocol, ICMPv6. The Internet Control Message Protocol is part of the Internet Protocol Suite, as defined in RFC 792. ICMP messages



are typically used for diagnostic or control purposes or generated in response to errors in IP operations. ICMP errors are directed to the source IP address of the originating packet.

4.IGMP:

The Internet Group Management Protocol (IGMP) is a communications protocol used by hosts and adjacent routers on IP networks to establish multicast group memberships. IGMP is an integral part of IP multicast.IGMP can be used for one-to-many networking applications such as online streaming video and gaming, and allows more efficient use of resources when supporting these types of applications. IGMP messages are carried in bare IP packets with IP protocol. There is no transport layer used with IGMP messaging, similar to the Internet Control Message Protocol. Membership Queries are sent by multicast routers to determine which multicast addresses are of interest to systems attached to its network. Routers periodically send General Queries to refresh the group membership state for all systems on its network. Group-Specific Queries are used for determining the reception state for a particular multicast address.



TCP/IP model

CONCLUSION:

Hence we have implemented packet formats captured through Wireshark for wired network. 1. Ethernet 2. IP 3.TCP 4. UDP .

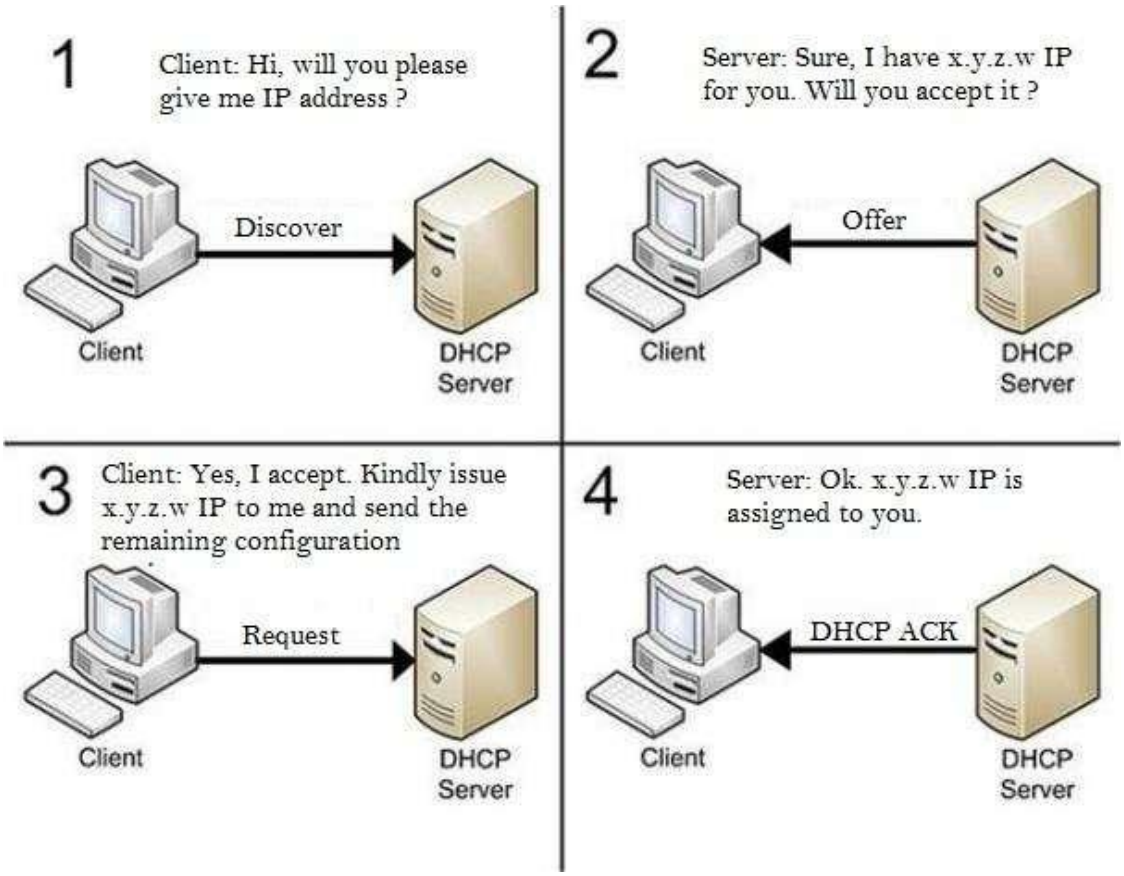
ASSIGNMENT-10

PROBLEM STATEMENT:

Installing and configure DHCP server and write a (C++/Python/Java) program to install the software on remote machine.

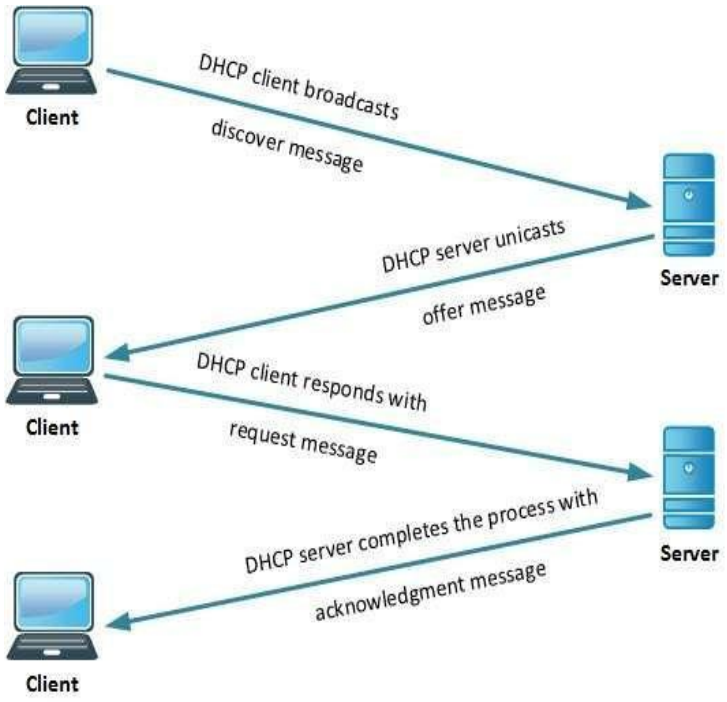
THEORY:

Dynamic Host Control Protocol (DHCP):



The Dynamic Host Configuration Protocol (DHCP) is a standardized network protocol used on Internet Protocol (IP) networks for dynamically distributing network configuration parameters, such as IP addresses for interfaces and services. With DHCP, computers request IP addresses and networking parameters automatically from a DHCP server, reducing the need for a network administrator or a user to configure these settings manually.

DHCP is based on BOOTP but can dynamically allocate IP addresses from a pool and reclaim them when they are no longer in use. It can also be used to deliver a wide range of extra configuration parameters to IP clients, including platform-specific parameters. It was first defined in RFC 1531 in October 1993; but due to errors in the editorial process was almost immediately reissued as RFC 1541. Four years later the DHCPINFORM message type and other small changes were added by RFC 2131; which as of 2014 remains the standard for IPv4 networks. Depending on implementation, the DHCP server may have three methods of allocating IP-addresses:



Dynamic allocation:

A network administrator reserves a range of IP addresses for DHCP, and each client computer on the LAN is configured to request an IP address from the DHCP server during network initialization.

The request-and-grant process uses a lease concept with a controllable time period, allowing the DHCP server to reclaim (and then reallocate) IP addresses that are not renewed

Automatic allocation:

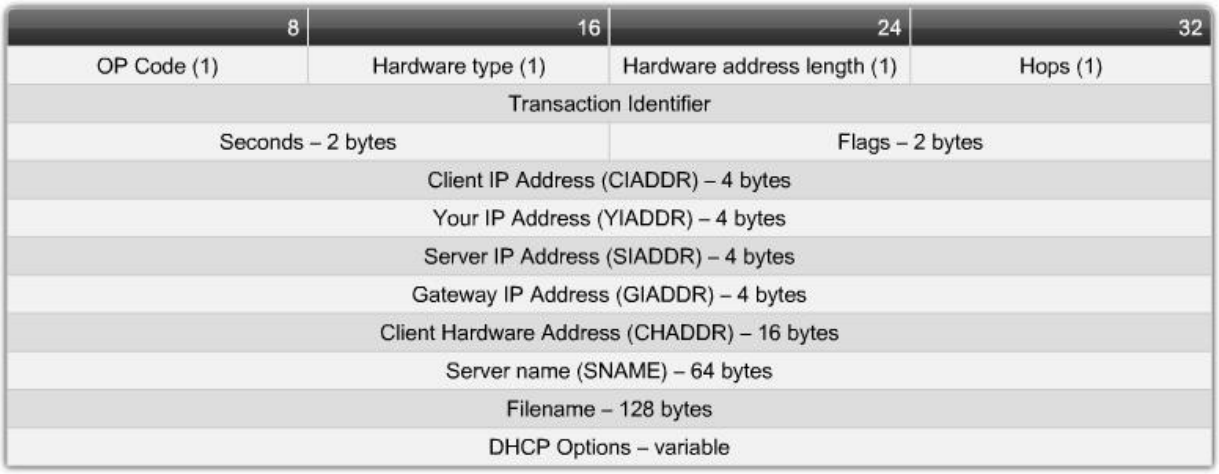
The DHCP server permanently assigns an IP address to a requesting client from the range defined by the administrator. This is like dynamic allocation, but the DHCP server keeps a table of past IP address assignments, so that it can preferentially assign to a client the same IP address that the client previously had.

Static allocation:

The DHCP server allocates an IP address based on a precon_gured mapping to each client's MAC address. This feature is called static DHCP assignment.

Working:

The DHCP employs a connectionless service model, using the User Datagram Protocol (UDP). It is implemented with two UDP port numbers for its operations which are the same as for the BOOTP protocol. UDP port number 67 is the destination port of a server, and UDP port number 68 is used by the client. DHCP operations fall into four phases: server discovery, IP lease offer, IP request, and IP lease acknowledgment. These stages are often abbreviated as DORA for discovery, offer, request, and acknowledgment.



8	16	24	32
OP Code (1)	Hardware type (1)	Hardware address length (1)	Hops (1)
Transaction Identifier			
Seconds – 2 bytes		Flags – 2 bytes	
Client IP Address (CIADDR) – 4 bytes			
Your IP Address (YIADDR) – 4 bytes			
Server IP Address (SIADDR) – 4 bytes			
Gateway IP Address (GIADDR) – 4 bytes			
Client Hardware Address (CHADDR) – 16 bytes			
Server name (SNAME) – 64 bytes			
Filename – 128 bytes			
DHCP Options – variable			

DHCP discovery

The client broadcasts messages on the network subnet using the destination address 255.255.255.255 or the specific subnet broadcast address. A DHCP client may also request its last-known IP address. If the client remains connected to the same network, the server may grant the request. Otherwise, it depends whether the server is set up as authoritative or not. An

authoritative server denies the request, causing the client to issue a new request. A non-authoritative server simply ignores the request, leading to an implementation-dependent timeout for the client to expire the request and ask for a new IP address.

DHCP offer

When a DHCP server receives a DHCPDISCOVER message from a client, which is an IP address lease request, the server reserves an IP address for the client and makes a lease offer by sending a DHCPOFFER message to the client. This message contains the client's MAC address, the IP address that the server is offering, the subnet mask, the lease duration, and the IP address of the DHCP server making the offer. The server determines the configuration based on the client's hardware address as specified in the CHADDR (client hardware address) field. DHCP request in response to the DHCP offer, the client replies with a DHCP request, broadcast to the server, requesting the offered address. A client can receive DHCP offers from multiple servers, but it will accept only one DHCP offer. Based on required server identification option in the request and broadcast messaging, servers are informed whose offer the client has accepted. When other DHCP servers receive this message, they withdraw any offers that they might have made to the client and return the offered address to the pool of available addresses.

DHCP acknowledgement

When the DHCP server receives the DHCP REQUEST message from the client, the configuration process enters its final phase. The acknowledgement phase involves sending a DHC PACK packet to the client. This packet includes the lease duration and any other configuration information that the client might have requested. At this point, the IP configuration process is completed. The protocol expects the DHCP client to configure its network interface with the negotiated parameters. After the client obtains an IP address, it should probe the newly received address (e.g. With ARP Address Resolution Protocol) to prevent address conicts caused by overlapping address pools of DHCP servers.

DHCP releasing

The client sends a request to the DHCP server to release the DHCP information and the client deactivates its IP address. As client devices usually do not know when users may unplug them from the network, the protocol does not mandate the sending of DHCP Release.

CONCLUSION:

Hence we have studied and implemented DHCP server program.