Modern Education Society's

College of Engineering, Pune – 411 001.

INDEX SHEET

Sr. No.	Title	Page No.	Date		Remarks
			Performance	Assessment	
1)	To analyse packet using wireshark and setup a wired LAN using switch	1	4/7/18	11/7/18	Yes
2)	Demonstrate error detection & correction using hamming code & CRC in C++	9	11/7/18	18/7/18	Yes
3)	Demonstrate Go-Back-N sliding window protocol in peer to peer mode in Java	14	18/7/18	25/7/18	Yes
4)	Demonstrate subnetting and find subnet mask in Java.	19	25/7/18	29/8/18	Yes
5)	Implement TCP Socket for (i) Hello message (ii) File transfer (iii) Calculator - arithmetic (iv) Trignometric calculator.	23	29/8/18	5/9/18	Yes
6)	Implement UDP socket for file transfer in peer to peer mode.	28	5/9/18	10/9/18	Yes

CERTIFICATE

This is to certify that Mr./Ms. Akshit Abhay Kedilya of Class TE Comp. I Roll No ...F161111005... Exam No. ..... has satisfactorily completed the Term-work in the subject ...Computer Network Lab... as detailed above within the four walls of the institute from ...June-18... to ...Oct-18...

Date: 17/10/18

Staff Member 17/10/18

Head of Department

INDEX SHEET

Sr. No.	Title	Page No.	Date		Remarks
			Performance	Assessment	
7.	Analyse packet formats captured through wireshark for wired network	31	10/9/18	12/9/18	Yes
8.	Identify domain name IP address from the host	35	12/9/18	22/9/18	Yes
9.	Implement TCP socket for peer to peer chat In C	42	22/9/18	26/9/18	Yes
10.	Implement UDP socket for peer to peer chat.	47	26/9/18	3/10/18	Yes
11.	Monitor traffic by given topology using NS2	52	3/10/18	15/10/18	Yes
12.	Configure RIP/OSPF/BGP protocol using packet tracer	55	15/10/18	16/10/18	Yes

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT:	Akshit Keoliya	CLASS:	TE Comp 1
SEMESTER/YEAR:	05	ROLL NO:	F16111005
DATE OF PERFORMANCE:	4/7/18	DATE OF SUBMISSION:	11/7/18
EXAMINED BY:		EXPERIMENT NO:	1

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.

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.

Questions

1) Explain the Specification & functionality of hardware components used- RJ-45 Connectors, Switch, CAT-5 Cable, Cable tester, Crimping tool.

2) What is topology? Explain different types og topologies used for designing Network.

3) Explain funcionality of Switch, bridge, Hub, Router, Brouter.

4)Write down command to install wireshark Tool. Explain importance of wireshark Tool.

Assignment - 1

Explain specification and functionality of hardware components - switch, Cat 5 cable, cable tester, crimping tool

1) RJ 45 connectors

Specification :- Physical construction, wiring, signal semantics

Functionalities :-

It is standard 8P8C telecommunication connector commonly found in computer networks such as Ethernet.

It specifies both, the plug and the socket.

2) Switch

Specification :- Std. IEEE 802.3 10 Base-T
IEEE 802.3a 100 Base-TX
Transfer method :- store and forward
Protocol :- CSMA/CD

Functionalities :-

Divides network into several isolated channels
Reduces possibility of collision
Suitable for real time applications like video conferencing.

3) CAT 5 cable

Specification :- Frequency :- 100 MHz
Attenuation :- 22 dB
Impedence :- 100 Ω
Networks supported :- 100 base-T

Functionalities :-

It is mainly used for data transmission.
It is typically used for Ethernet networks running at 10 or 100 mbps.

4) Cable testers
Specification :- Test points, test resistance, maxim voltage, maximum current.
Functionality :-
Most powerful cable testers measure cable relevant to signal transmission.

5) Crimping Tool
Specification :- Hand held
Functionalities :-
It is a special device used to attach a connector to end of a phone or network cable.
Word crimping means joining 2 metal pieces together by determining one of them. The deformed piece is 'crimp'.

Q What is Topology ? Explain different types of topologies used for designing networks.

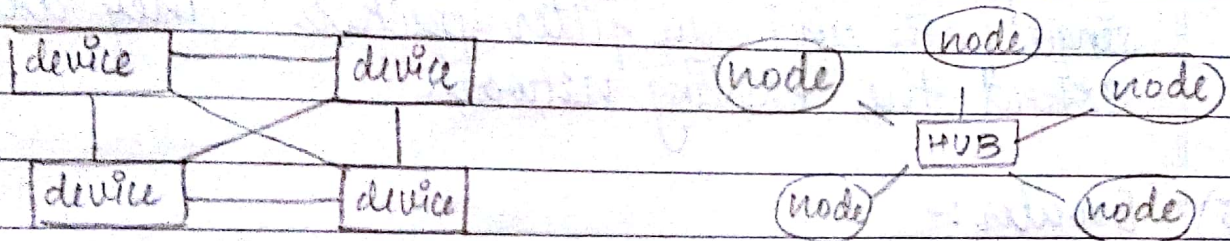
Ans Topology :- It is defined as the manner in which nodes are geometrically arranged and connected. Network topology refers to physical layout of the network.
Types of network topologies are :-

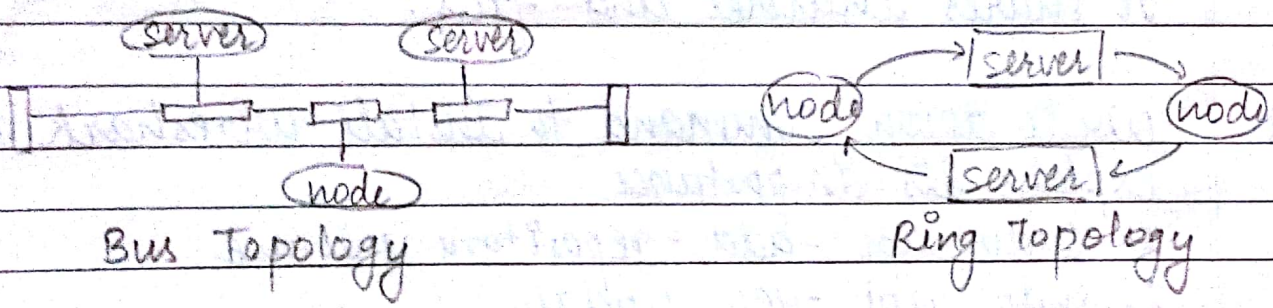
1) Mesh topology :- All devices have links to every other device. It is difficult to install as no. of devices increases This network is easy to troubleshoot.

2) Star topology :- It consists of a no. of devices connected by point to point connection to a central link (called as hub).

5) Bus topology :- In bus, multiple devices are connected one by one by means of connectors. It is a passive technology.

4) Ring topology :- Each computer is connected to next computer with last one connected to other.





Q Explain functionalities of switch, hub, router, bridge, brouter

Ans 1) Switch :-
- It is a multiport bridge with a buffer and design that can boost its efficiency and performance.
- It operates at data link layer
- It is point to point communication device.
- It uses switching table to find out correct destination
- It can be used as a repeater.

2) Hub :-
It is centrally located device to bring media segment together
It is broadcasting device operating at physical layer.

3) Router :-
It works at network layer. It routes packets based on

their logical addresses.
It connects 2 or more networks.

4) Bridge :-
It operates at data link layer. It can accomodate single path and can filter packets. They are used to extend the existing network.

5) Brouter :-
It is network bridge and plus router.
It shares Internet and files.

Q Write down command to install wireshark tool. Explain its Importance.

Ans
1. sudo apt -add - repository universe
2. sudo apt -get update
3. sudo apt get install wireshark.

Importance :-
a) It is used for network troubleshooting analysis, software and communications protocol development.
b) It is very similar to tcpdump, but has graphical front end and Integrated sorting and filtering options.
c) It lets users put network Interface controllers into promiscous mode so they can see all traffic on network
d) Port mirroring or various network taps extend capture to any point on the network.

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT:	Akshit Keoliya	CLASS:	TE comp 1
SEMESTER/YEAR:	05	ROLL NO:	F16111005
DATE OF PERFORMANCE:	11/7/18	DATE OF SUBMISSION:	18/7/18
EXAMINED BY:		EXPERIMENT NO:	2

ASSIGNMENT NO -3

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.

Questions

1)What is CRC? Explain CRC generator and checker with example.

2)What is hamming code? Generate hamming code for 7/8 bit data word.

3) Explain checksum in detail

Assignment - 3

What is CRC? Explain CRC generator & checker with example

Ans:

CRC (Cyclic Redundancy check) :-
Parity methods detect only odd/even no. of errors. To overcome this weakness, polynomial codes error detection method is used. Polynomial code involve generating check in form of cyclic redundancy code.

CRC Generator :-
CRC code requires a generator polynomial. This becomes the divisor in polynomial long division which takes message as dividend and quotient is discarded and remainder is taken as the result.

CRC Checker :-
f(x) :- polynomial with binary coefficients
d(x) :- dataword
c(x) :- codeword
s(x) :- syndrome.
g(x) :- generator
e(x) :- error

If s(x) is not zero then one or more bits are corrupted. However if c(x) is zero, either no bit is corrupted or decoder failed to detect any errors.

Example :- $g(x) = x^4 + x^3 + 1$
$= 11001$
Message = 110011

degree of g(x) = 4, therefore append 4 zero bits.
Hence d(x) = 110011 0000.

```
                1000001  → Quotient
          ↗ 11001) 110011 0000  → Dividend
Divisor
          11001↓
          000001
           00000↓
           00010
            00000↓
            00100
             00000↓
             01000
              00000↓
              10000
               11001
               01001  → Remainder
```

Remainder is appended to d(x) to give f(x)

i.e. f(x) = 110011 11001

Q What is hamming code? Generate code for 718 bit dataword

Ans Hamming code :-

Hamming bits are inserted into message at random locations.

It is a single bit error correcting code.

It is more complex from stand point of creating and interpreting the error bits.

eg :- Generate hamming codeword for 1010101. Assume even parity for hamming code.

Data :- 1010101 hamming

P_1	P_2	1	P_3	0	1	0	P_4	1	0	1

$P_1 = 1 \oplus 0 \oplus 0 \oplus 1 \oplus 1 = 1$

$P_2 = 1 \oplus 1 \oplus 0 \oplus 0 \oplus 1 = 1$

$P_3 = 0 \oplus 1 \oplus 0 = 1$

$P_4 = 1 \oplus 0 \oplus 1 \oplus 0 \oplus 0 \oplus 0 = 0$

$\therefore$ Hamming code = 1 1 1 1 0 1 0 0 1 0 1.

Q Explain checksum in details.

(i) Checksum is used in Internet by several protocols ~~algo~~ although not at datalink layer.

(ii) Checksum is based on the concept of redundancy.

(iii) Suppose that data is a list of 4 bit numbers that we want to send to a destination. In addition to sending these numbers, we send sum of the numbers.

(iv) The receiver adds the 5 members and compares the result with sum. If the two are same, the receiver assumes no error, accepts the 5 numbers and discards the sum.

(v) Otherwise there is error in data and the numbers are not accepted.

(vi) For making job of receiver easier, we send the negative of the sum called checksum.

(vii) In this way, if the sum of numbers (that are sent) and checksum results in zero, it assumes no error.

(viii) Otherwise, there is error & data is discarded.

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT:	Akshit Keoliya	CLASS:	TE Comp 1
SEMESTER/YEAR:	05	ROLL NO:	F16111005
DATE OF PERFORMANCE:	18/7/18	DATE OF SUBMISSION:	25/7/18
EXAMINED BY:		EXPERIMENT NO:	3

Assignment No. A4

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

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.

- The error rate is high i.e. more frames are being damaged and then discarding 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.

- 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.

- Go-Back-N has a window size of N-1 and selective repeat have a window size <=(N+1)/2.

- 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.

- 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.

- In selective repeat NAK frame refers to the damaged frame number and in Go-Back-N, NAK frame refers to the next frame expected.

- 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).

Questions:

1) Write note on flow control and error conrol .

2) What is sliding window protocol?

3)Explain in brief Slective repeat and Go- back N.

Assignment - A4

Q Write a note on flow control and error control

Ans (i) Flow control :-

a) In flow control, problem to be handled is what to do with computer wants to send data at a faster rate than capacity of receiver to receive them.

b) This usually happens when sender is a faster computer

c) Flow control is a set of procedures that tells sender how much data it can transmit before it must wait for ack. from receiver, otherwise there will be data overflow.

d) The rate of processing at receiver is generally slower than rate of transmission. Each receiver thus has finite memory called buffer. Incoming data is first stored in buffer and then sequentially processed.

(ii) Error control :-

a) Problem to deal during transmission of data is to make sure that all frames are delivered in proper order.

b) A positive ack. (ACK) indicates a successful and error free delivery of frame. Whenever negative ack. (NAK) means something has gone wrong and frame is to be retransmitted.

c) Due to noise burst, a frame may be lost completely & receiver does not receive anything & doesn't react at all.

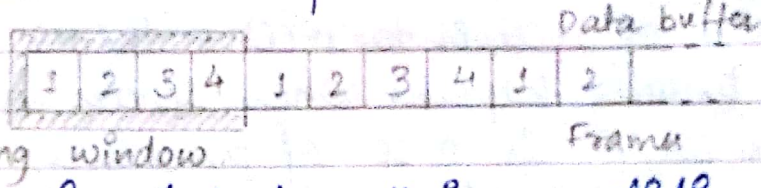
d) This problem is overcome by introducing a linear timer in data link layer.

Q What is sliding window protocol?

Sliding window protocol is feature of packet-based data transmission protocol. It is more robust and bi-directional protocols.

a) Sequence no :- Each outbound frame has a sequence ranging from 0 to max. value.

b) Sliding windows :- Imaginary boxes at transmitter and receiver and provides upper limit on no. of frames that can be transmitted before ack. is obtained.

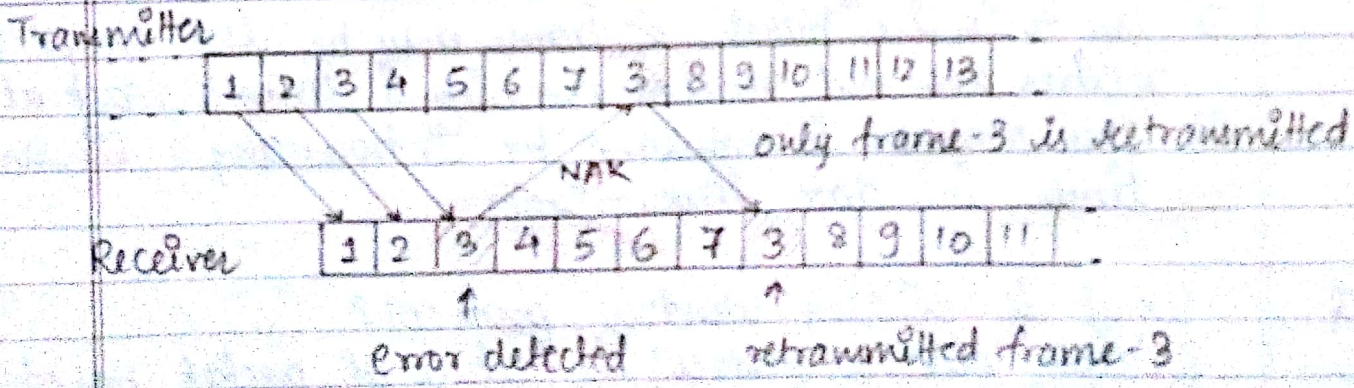


Sender & receiver both have their own sliding windows. Sender sends ack. & no of frames in its own window and waits for ack. from receiver. Receiver sends ack which includes no. of next frame that sender should send.

Q Explain in brief selective repeat and Go-back-N.

Ans (i) Selective repeat :-

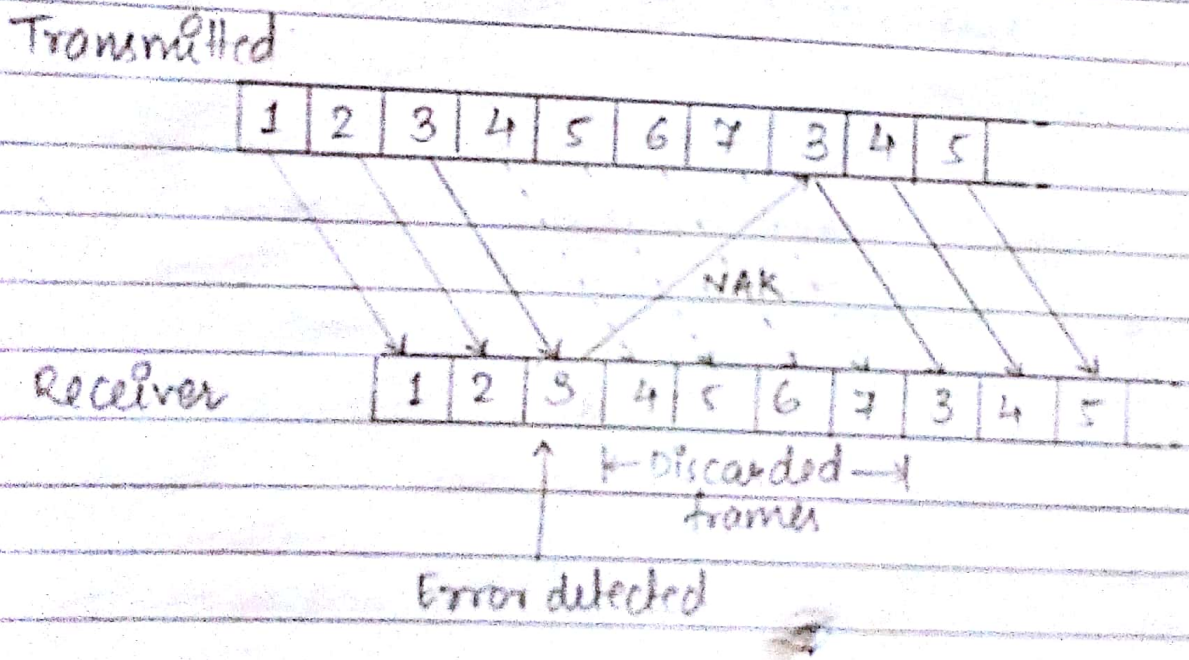
In this method, only the specified damaged or lost frames are retransmitted. Receiver can do sorting of data frames and is also able to store frames after it has sent NAK until damaged frame has been replaced.



Selective Repeat ARQ

(ii) Go-Back-N ARQ :-

In this stop and wait protocol it was assumed that transmission time required from frame to arrive at receiver plus transmicion time for ack. to come back is negligible. In Go-back-N ARQ. if one frame is damaged or lost, all frames are sent since the last frame acknowledged are retransmitted.



Go-back-N ARQ

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT:	Akshit Kholiya	CLASS:	TE Comp 1
SEMESTER/YEAR:	05	ROLL NO:	F1611005
DATE OF PERFORMANCE:	26/7/18	DATE OF SUBMISSION:	29/8/18
EXAMINED BY:		EXPERIMENT NO:	5

ASSIGNMENT NO -5

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

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 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 .

Questions

1.Explain diffrence between IP v4 and IP v6.

2.Explain Header of IP v4 with diagram.

3.Explain clasees of IP adressses.

(21)

Assignment - 5

Explain difference between IPv4 and IPv6.

IPv4	IPv6
a) There are only 2^{32} possible ways to represent addresses.	a) There are about 2^{128} possible ways to represent addresses.
b) Address is written by dotted decimal notation	b) Addresses is written in hexadecimal (4 groups).
c) Header has a checksum, which must be computed by each router	c) It has no header checksum
d) IPv4 node has only stateful auto-configuration	d) IPv6 node has both stateful and stateless address auto-configuration mechanism.
e) Source & destination addresses are 32 bits.	e) Source and destination addresses are 128 bits.
f) IPsec is option	f) IPsec support is required.

Explain header of IPv4 with diagram.

0	4	8	16	32
VER (4 bits)	HLEN (4 bits)	DS type of (8 bits) service	Total length (16 bits)	
Identification (16 bits)			Flags (3 bits)	Fragmentation offset (13 bits)
Time to live	Protocol		Header checksum (16 bits)	
Source IP address				
Destination IP address				
Options + Padding				

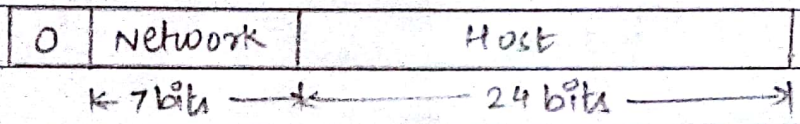
IPv4 header format.

a) VER :- (version) defines the version of IP.
b) HLEN :- (header length) defines length of datagram heaa.
c) DS :- (differential services) defines class of datagram fr. quality of service (QoS) purpose.
d) Total length :- defines total length of IP datagram. It includes length of header as well as data field.
e) Identification :- it identifies datagram originating from the source host.
f) Flags :- First bit is reserved and should be zero.
Second bit is 'Do not fragment'
Third bit is 'More Fragment Bit'
g) Fragmentation offset :- It is used to indicate relative position of fragment wrt complete datagram.
h) Time to live :- it controls maximum no. of routers visited by datagram.
i) Protocol :- defines high-level protocol which uses services of the IP layer.
j) Checksum :- A checksum in IP packet covers header only. It is verified at each point that Internet header is processed.
k) Source addr :- defines IP address of source
l) Destination addr :- defines IP address of destination.
m) Options :- Options are not required for every datagram. They are used for network testing and debugging

Q Explain classes of IP addresses.

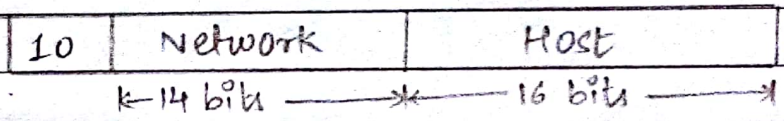
Ans The IPv4 addresses are classified in 5 types :-
a) Class A
b) Class B
c) Class C
d) Class D
e) Class E.

(i) Class A :-



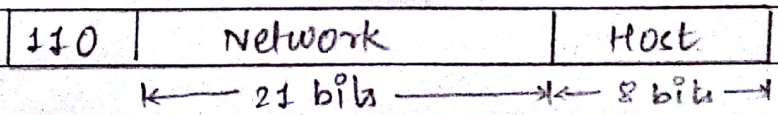
The network field is 7 bit long and host field is 24 bit. So network field can have no. between 1 to 127. Thus host no will range from 0.0.0.0 to 127.255.255.255.

(ii) Class B :-



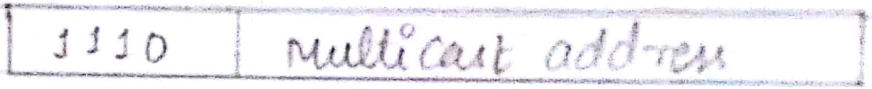
The first two fields Identify networks & no. in first field must be in 128-191 range. Host no 0.0 and 255.255 are reserved. So there can be upto 65,534 hosts.

(iii) Class C :-



The first block covers addresses from 192.0.0.0 to 192.0.0.255 and last block covers addresses from 223.255.255.0 to 223.255.255.255

(iv) Class D :-



Class D allows upto 2 million networks with upto 254 hosts each and class D format allows a multicast in which a datagram is directed to multiple host

(v) Class E :-

Class E address begins with 11110 which is reserved. Lowest IP address is 0.0.0.0 & highest is 255.255.255.255

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT: Akshit Keoliya	CLASS: TE Comp 1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 29/8/18	DATE OF SUBMISSION: 5/9/18
EXAMINED BY:	EXPERIMENT NO: 5

ASSIGNMENT-7

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

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

QUESTIONS

1) What is Socket? Explain different types of socket?

2)Differenciate between TCP & UDP.

3)Explain FTP Protocol.

4) Write down steps involved in establishing a socket on the client side & server side.

Assignment - 7.

Q What is socket? Explain different types of socket.

Ans A socket is one endpoint of a two-way communication link between two programs running on the network socket types & associated data.

Socket type		Protocol
SOCK - STREAM	-	transmission control protocol
SOCK - DGRAM	-	User datagram protocol
SOCK - RAW	-	IP, ICMP, RAW.

Q Differentiate between TCP & UDP.

	TCP	UDP
(i)	TCP is connection oriented	(i) UDP is connectionless protocol.
(ii)	As a message makes it way across Internet from computer to another, it is connection based.	(ii) In UDP, one program can send load of packets to another & that could be end of relationship.
(iii)	It is slower than UDP	(iii) It is faster than TCP.
(iv)	There is absolute guarantee that data transferred remains intact & arrives in same order in which it is send.	(iv) There is no guarantee that messages or packets sent would reach at all.
(v)	TCP header size is 20 bytes	(v) UDP header size is 8 bytes.
(vi)	TCP is more secure than UDP as it is connection oriented protocol.	(vii) UDP is less secure as it is connectionless protocol.

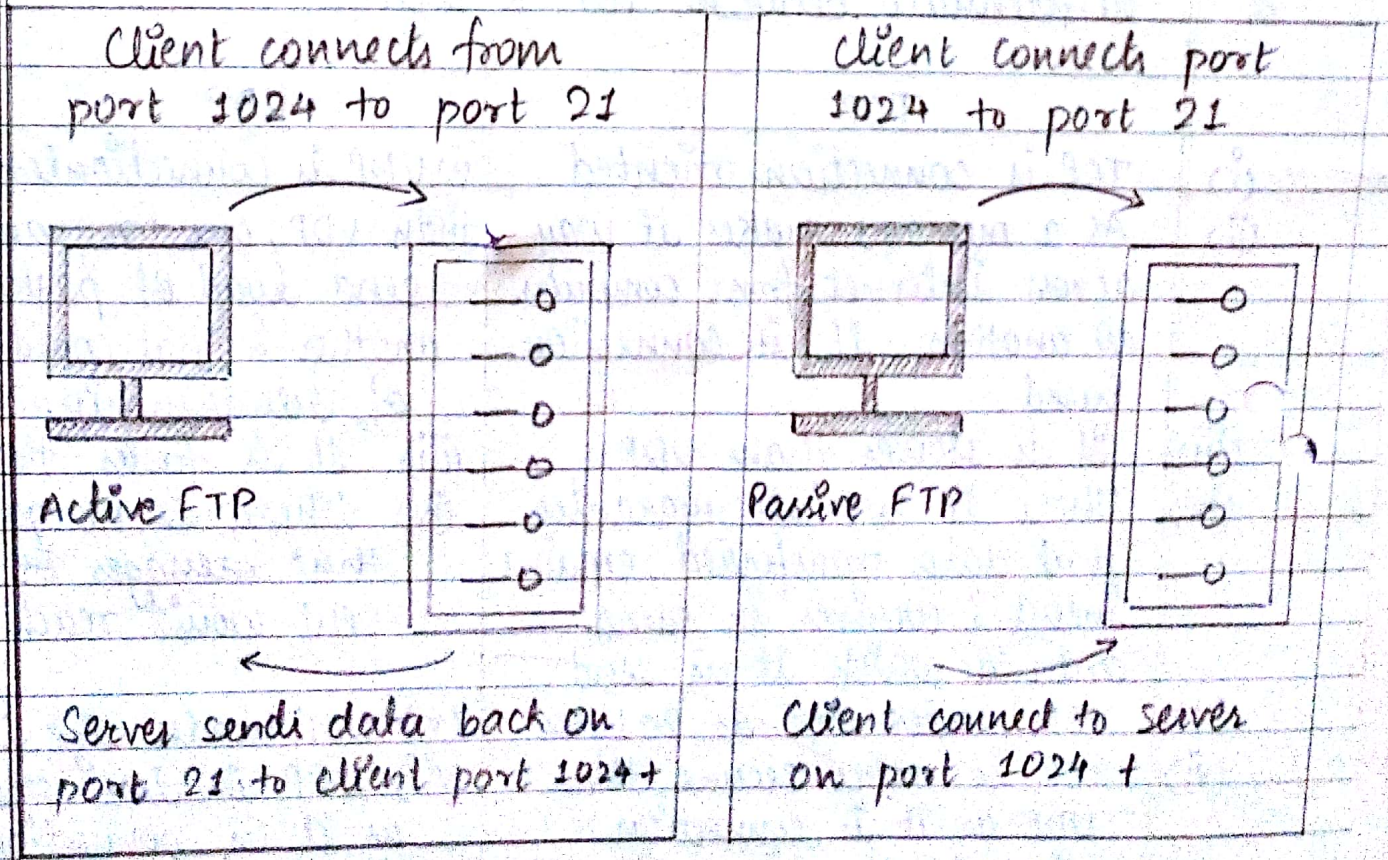
Q Explain FTP protocol.

(i) File transfer Protocol (FTP) is a standard Internet protocol for transmitting files between computers on the Internet over TCP/IP connections.

(ii) FTP is client-server protocol that relies on 2 communication channels between client and server, a command channel for controlling conversation and data channel for file transfer.

(iii) Client initiate conversation with server by requesting to download a file.

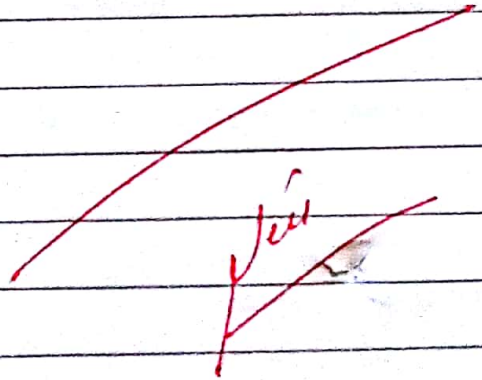
(iv) A user typically needs to login on FTP server, although some servers make some or all of their content available without login, also known as anonymous.



Q Write down steps involved in establishing a socket on the client side and server side.

Ans Following steps are involved :-

(i) Create a socket on or with the socket() system call.
(ii) Bind socket to an address using the bind() system calls, for a server socket on the Internet, an address consists of a port no. on host machine.
(iii) Listen for connection with accept() system call.



Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT: Akshit Kuliya	CLASS: TE Comp 1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 5/9/18	DATE OF SUBMISSION: 10/9/18
EXAMINED BY:	EXPERIMENT NO: 6

ASSIGNMENT-8

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.

CONCLUSION:

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

Question:

1) What is Socket? Explain system calls related to UDP SOCKET?
2)Draw and explain UDP header in detail.
3)Explain FTP Protocol.
4) Write down steps involved in establishing a UDP socket on the client side & server side.

Assignment -8

Q For each of the following applications, determine whether TCP or UDP is used as transport layer protocol and explain reasons for your choice.

(i) Watching a real time streamed video :-
UDP should be used because when watching a real-time video, delay is critical and therefore there simply isn't time to seek the transmission of errors. The simplicity of UDP is therefore required.

(ii) Web browsing :-
TCP should be used as webpages need to be delivered without error so that all the content is properly formatted and presented.

(iii) A voice over IP telephone conversation :-
VOIP could use UDP. The reason is that telephone conversation has strict timing requirements for the transfer of data & seeking retransmission of any errors would introduce too much delay.

(iv) YouTube video :-
TCP is used as video streaming adopts prefetching and buffering to achieve smooth playout.

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT: Akshit Keoliya	CLASS: TE Comp 1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 10/9/18	DATE OF SUBMISSION: 12/9/18
EXAMINED BY:	EXPERIMENT NO:

ASSIGNMENT NO -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:

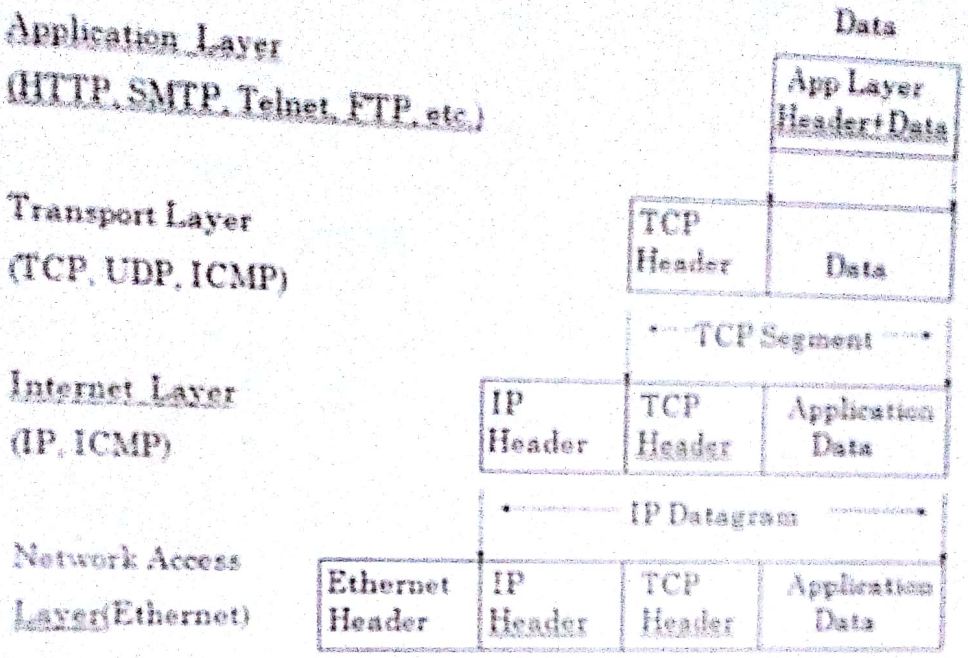
Packet sniffer \ Packet analyzer:

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



TCP/IP model

CONCLUSION:

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

Questons

1.give list of packet analyzer tool.

2.Explain Wireshark in Detail.

3.Explain steps of installation of packet analyzer tool for ubantu.

Assignment - 9

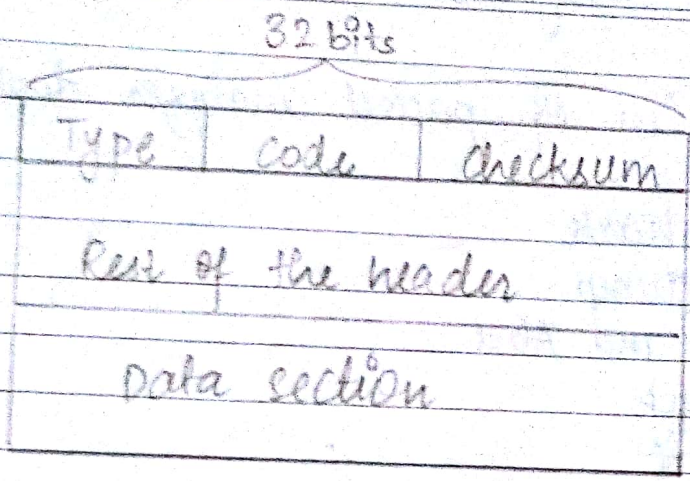
Q Give a list of packet analyzer tools.

Ans
(i) Wireshark
(ii) TCP dump
(iii) Cain and Abel
(iv) Kismet
(v) DSNiff
(vi) Netstumbler
(vii) Ettercap
(viii) Ngrep
(ix) Ntop
(x) EtherApe

Q ~~Explain~~ wireshark in detail

Q Explain ICMP in detail.

Ans
(i) The Internet control message protocol (ICMP) is one of the main protocols of Internet protocol suite.
(ii) It is used by network devices like routers, send error message indicating a requested service is not available or that host or router could not be reached.
(iii) ICMP can also be used to relay query messages. It is assigned protocol number 1.
(iv) ICMP differs from transport protocols such as TCP & UDP as it is not typically used to ~~∞~~ employ by end-user network applications.
(v) ICMP errors are directed to the source IP address of the originating packet.



ICMP

Q Explain steps of installation of packet analyzer tool for ubuntu.

Ans Steps to install packet analyzer tool for ubuntu are :-

(i) sudo ~~apt~~ add-apt-repository universe
(ii) sudo apt-get updati
(iii) sudo apt-get install wireshark.

College of Engineering, Pune

NAME:	Akshit Abhay Keoliya		
CLASS:	TE Comp1	ROLL NO:	F16111005
SEMESTER/YEAR:	05	EXAM NO:	
DATE OF PERFORMANCE:	12/9/18	DATE OF SUBMISSION:	22/9/18
EXAMINED:			

Assignment No. A11

Title : DNS Lookup for specified for domain name or IP address.

Objective : To identify DNS and display attributed related to it.

Problem Statement :

Write a program for DNS lookup. Given an IP address input, it should return URL and vice-versa.

Outcomes :

Accepting a domain name/ IP address and displaying its DNS Attributes.

Tools Required:

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

Software: A simple DNS server Program

Theory:

Introduction:-

The **Domain Name System (DNS)** is a hierarchical decentralized naming system for computers, services, or other resources connected to the Internetor a private network. It associates various information with domain namesassigned to each of the participating entities. Most prominently, it translates more readily memorized domain names to the numerical IP addressesneeded for locating and identifying computer services and devices with the underlying network protocols. By providing a worldwide, distributed directory service, the Domain Name System is an essential component of the functionality on the Internet.The Domain Name System delegates the responsibility of assigning domain names and mapping those names to Internet resources by designating authoritative name servers for each domain.

Conclusion : Learnt the basic and various functionalities of DNS. Implemented the look up for DNS specified.

Questions :

(1) What is DNS??What is main purpose of DNS server??

(2) What are DNS zone??

(3) What is round robin DNS??

Assignment - A11.

Q What is DNS ? What is main purpose of DNS server ?

Ans (i) The Domain Name system (DNS) is hierarchical decentralised naming system for computer, services or other resources connected to 'Internet' or a private network.

(ii) It associates various info. with domain name assigned to each of participating entities. Main purpose of DNS is server as 'easy to remember' name for websites & other services on Internet.

(iii) Computer access Internet devices by their IP addresses, allowing us to Internet location by its domain name.

(iv) It supports high performance, availability & scalability through use of data ~~iii~~ hierarchical data replication & coaching.

(v) DNS is used to resolve human reliable host name like www.google.com into machine reliable IP address like 256.58.196.100.

Q What are DNS zone?

Ans (i) A DNS zone is any distinct, contiguous position of domain name space in Domain Name System (DNS) for which administer responsibility has been delegated to single manner.

(ii) The domain name space of Internet is organized into hierarchical layout of sub-domain below the DNS not domain.

Q What is round robin DNS?

Ans (i) Round Robin DNS is technique of load distribution load balancing or fault tolerance provisioning multiple redundant in protocol servic host eg. web server.

(ii) FTP server by managing the Domain Name System response to address requests from client computer according to an appropriate statistical model.

(iii) A round robin DNS name, is an more occasions referred to as 'rotot' due to rotation between alternative A records.

NAME OF STUDENT: Akshit Kooliya CLASS: TE Comp 1
SEMESTER/YEAR: 05 ROLL NO: F16111005
DATE OF PERFORMANCE: 22/9/18 DATE OF SUBMISSION: 26/9/18
EXAMINED BY: EXPERIMENT NO: 8

Assignment No. B3

Title: Set up a program using TCP sockets for wired network

Objective: Set up a program using UTP sockets for wired network

Problem Statement: Write a program using TCP sockets for wired network to implement
a. Peer to peer Chat
b. Multiuser chat

Apparatus:

Tools Required:
Hardware Required: Computer, LAN cards, cables, cables testers, crimping tools, etc.

Software: Open source, OS and wireshark

Theory:

Introduction

A socket is the mechanism that most popular operating systems provide to give programs access to the network. It allows messages to be sent and received between applications (unrelated processes) on different networked machines.

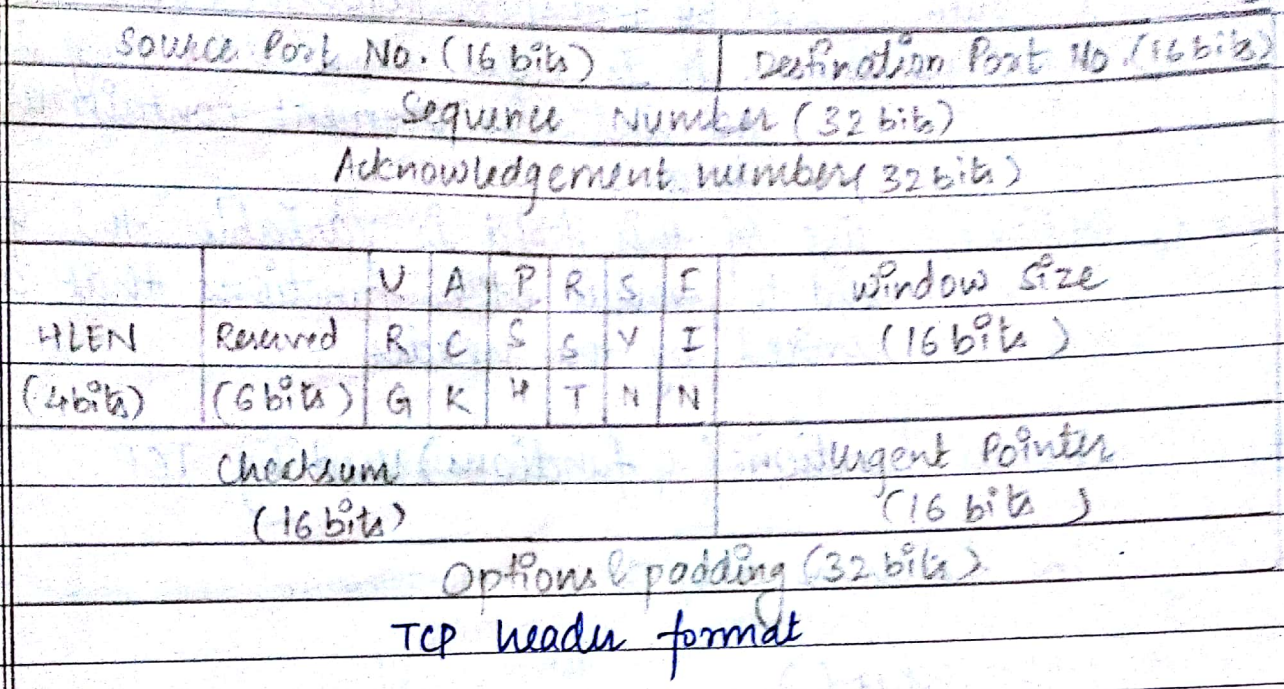
The sockets mechanism has been created to be independent of any specific type of network. IP, however, is by far the most dominant network and the most popular use of sockets. This tutorial provides an introduction to using sockets over the IP network (IPv4).

There are a few steps involved in using sockets:

1. Create the socket
2. Identify the socket
3. On the server, wait for an incoming connection
4. On the client, connect to the server's socket
5. Send and receive messages
6. Close the socket

Assignment B3

Q. Explain TCP header



TCP header format

(i) Source port :- specifies the application sending the segment.
(ii) Dest. port :- identifies receiving application port no.
(iii) Sequence no :- each byte in the stream that TCP sends is numbered
(iv) Ack. number :- it identifies sequence no. of next data.
(v) HLEN :- header length specifies the length of header in 32 bit words.
(vi) Reserved :- this field is reserved for future and must be set to zero.
(vii) URG :- urgent pointer is valid if it is set.
(viii) ACK :- it is set to 1 to denote ack. no is valid.
(ix) PSH :- Informs host data should be pushed up.
(x) RST :- Reset the connection
(xi) SYN :- Initializes the connection.
(xii) FIN :- Closes the connection.
(xiii) Window size :- specifies the no. of bytes sender is sending to accept.

(xiv) Checksum :- used by transport layer for error correction.

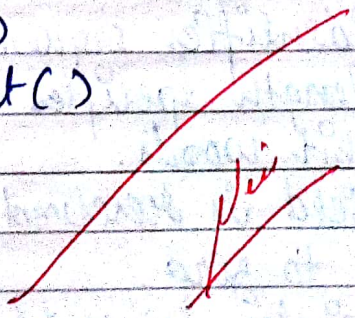
(xv) Urgent pointer :- it is valid when URG flag is set and indicates segment contain urgent data.

(xvi) Options :- size of this field is variable. this field is used to provide other functions that are not covered by the header.

Q List all functions (C functions) used by TCP.

Ans The functions are :-

(i) setsocket()
(ii) bind()
(iii) listen()
(iv) Accept()
(v) send()
(vi) recv()
(vii) connect()



NAME OF STUDENT: Akshit Keoliya	CLASS: TE Comp 1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 26/9/18	DATE OF SUBMISSION: 3/10/18
EXAMINED BY:	EXPERIMENT NO: B4

Tittle: Program using UDP socket for wired network to implement

a.Peer to Peer chat

b.Multiset Chat

Aim: To study program using UDP socket for wired network to implement

a.Peer to Peer chat

b.Multiset Chat

Apparatus:

Theory:

UDP SOCKETS

In electronic communication, the **User Datagram Protocol (UDP)** is one of the core members of the Internet protocol suite. The protocol was designed by David P. Reed in 1980 and formally defined in RFC 768. With UDP, computer applications can send messages, in this case referred to as *datagrams*, to other hosts on an Internet Protocol (IP) network. Prior communications are not required in order to set up transmission channels or data paths.

UDP uses a simple connectionless transmission model with a minimum of protocol mechanism. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. It has no handshaking dialogues, and thus exposes the user's program to any unreliability of the underlying network: there is no guarantee of delivery, ordering, or duplicate protection. If error-correction facilities are needed at the network interface level, an application may use the Transmission Control Protocol (TCP) or Stream Control Transmission Protocol (SCTP) which are designed for this purpose.

The recvfrom() Function

This function is similar to the read() function, but three additional arguments are required. The recvfrom() function is defined as follows:

The sendto() Function

This function is similar to the send() function, but three additional arguments are required. The sendto() function is defined as follows:

Questions.

1.explain deatils about protocol required for chat.

2.explain differnts function in UDP

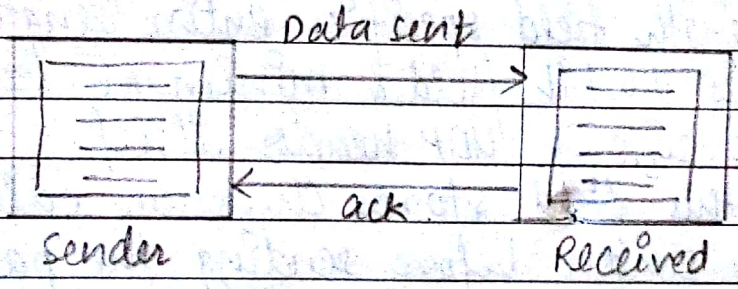
3.explain UDP header

Conclusion :- We have succesfully implemented program using UDP socket for wired network to implement
(a) Peer to peer chat
(b) Multicast chat

Assignment No. B4

Q Explain details about protocol required for chat.

Ans
(i) TCP protocol is used for chatting applications.
(ii) In TCP, the sender sends data and waits for receiver to send an acknowledgement (ack).
(iii) If no ack is received, the sender assumes that data has been lost and retransmits the data.
(iv) TCP ensures the correct order of data to be send and also ensures data to be error free.
(v) In chatting applications, this protocol is used since it provides reliable communication without error in data.



Q Explain different functions in UDP.

Ans The functions in UDP are :-
(i) bind() :- this method binds address (hostname port number pair) to socket.
(ii) listen() :- this method setups & starts TCP listener.
(iii) recvfrom() :- this method receives UDP message
(iv) sendto() :- this method transmits UDP message

Q. Explain UDP header format.

i) Source port :- This 16 bit information is used to Identify the source port of the packet.

ii) Destination port :- this 16 bit information is used to identify application level service on destination machine.

(iii) Length :- length field specifies entire length of UDP packet It is 16 bit field & minimum value is 8 byte i.e. size of UDP header itself.

(iv) Checksum :- this field stores checksum value generated by sender before sending the packet.

Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT: Akshit Keoliya	CLASS: TE Comp1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 3/10/18	DATE OF SUBMISSION: 15/10/18
EXAMINED BY:	EXPERIMENT NO: 11

ASSIGNMENT NO : B - 6

Title: Using Network simulator NS2

Objectives : To demonstrate the network simulator NS2

PROBLEM STATEMENT:

Use network simulator NS2 to implement :

1.Monitoring traffic for given topology

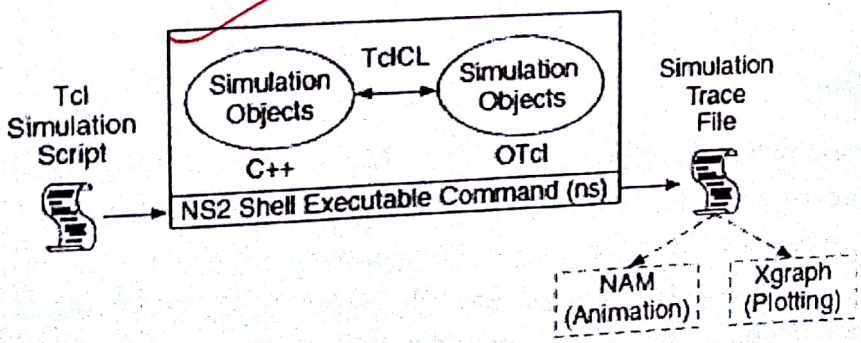
2.Analysis of CSMA and Ethernet protocols

3.Network Routing : Shortest path routing,AODV

4.Analysis of congestion control(TCP and UDP)

THEORY:

NS2 stands for Network Simulator Version 2. It is an open-source event-driven simulator designed specifically for research in computer communication networks. NS2 consists of two key languages: C++ and Object-oriented Tool Command Language (OTcl). While the C++ defines the internal mechanism (i.e., a backend) of the simulation objects, the OTcl sets up simulation by assembling and configuring the objects as well as scheduling discrete events. The C++ and the OTcl are linked together using TclCL



Basic architecture of NS.

...the network area. ...vector protocols) allow routers to work

Shortest Path Routing

Most of the practical routing algorithms are based on the idea of the shortest path between two nodes. Here, each communication link in the network is usually assigned a positive number called its length. A link can have a different length in each direction. Each path consists of a sequence of nodes. A length of the path between two nodes can be calculated by adding the lengths of its links. The shortest path routing algorithm routes each packet along a minimum length between the source and destination nodes of the packet. The shortest path is simply a path that has a minimum number of links. More generally, the transmission capacity and its projected traffic load determine the length of the link. The idea here is that the shortest path should contain relatively small number of links and the links should be uncongested and therefore be suitable for routing.

Ad hoc On-Demand Distance Vector (AODV) Routing

It is a routing protocol for mobile ad hoc networks (MANETs) and other wireless ad hoc networks. It was jointly developed on July 2003 in Nokia Research Center, University of California, Santa Barbara and University of Cincinnati by C. Perkins, E. Belding-Royer and S. Das.[1]

AODV is the routing protocol used in ZigBee - a low power, low data rate wireless ad hoc network. There are various implementations of AODV such as MAD-HOC, Kernel-AODV, AODV-UU, AODV-UCSB and AODV-UIUC.

CONCLUSION:

Hence we have implemented a program using network simulator NS2 for monitoring traffic,analysis of CSMA ,network routing and for congestion control.

Questions :

1.explain routing protcol
2.explain architecture of AODV
3.expalin network simulator tools.

Assignment - B6

Q Explain routing protocols.

Ans Routing protocols are :-

(i) It specifies how routers communicate with each other, discriminating information that enables them to select routes between any 2 nodes on computer network.

(ii) Routing algorithm determine specific choice of route

(iii) Each route has prior knowledge only of networks attached to it directly.

(iv) Routing protocol shares this info 1st throughout the network.

(v) Routers gain knowledge of topology of network.

Q Explain architecture of AODV

Ans (i) AODV protocol is reactive MANET routing protocol, means it discovers route to destination only, when required.

(ii) The algorithm is similar to distance vector algorithm that has been adapted to work in mobile environment.

(iii) Routes to destination host are discovered on demand, i.e It determines a route to some destination only when any node wants to send a data packet to that destination.

(iv) 2 nodes are said to be connected if they can communicate directly using their radio signals.

(v) The algorithm maintains a routing table of each node.

AODV

Type	Flag	Reserved	Hoplist
Broadcast_id			
Dest_addr			
Dest_sequence #			
Source_addr			
Source_sequence #			

Q Explain network simulator tools.

Ans (i) Network simulator is a software that predicts the behaviour of computer network.

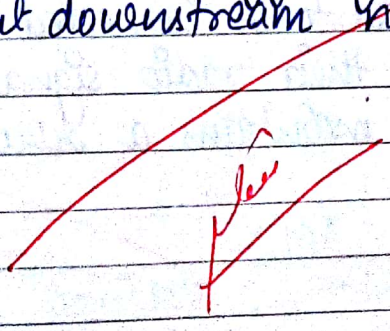
(ii) Communication networks have become too complex for traditional analytical methods to provide an acurate understanging, network simulators are used.

(iii) In simulators, computer network is modeled with devices, links, applications, etc and performance is analysed.

(iv) Simulators come with support for most popular technologies and network in use today such as wireless sensor networks, wireless LANs, mobile Ad-hoc networks, vehicle AdHoc Network, Cognitive radio network, LTE/LTE advanced networks, IOTs are some of popular technologies used today.

(vi) Most of the commercial simulators are GUI driven while some network simulators are GUI driven.

(vii) They use discrete events simulators in which a list of 'events' that are pending is stored & those events triggering future events such as events of arrival of packet at one node triggering event of arrival of that packet at downstream node.



Modern Education Society's
College of Engineering, Pune

NAME OF STUDENT: Akshit Kediya	CLASS: TE Comp 1
SEMESTER/YEAR: 05	ROLL NO: F16111005
DATE OF PERFORMANCE: 15/10/18	DATE OF SUBMISSION: 16/10/18
EXAMINED BY:	EXPERIMENT NO: 12

Assignment No. B7

Title: Configure RIP/OSPF/BGP using packet tracer wireshark.

Objectives:

Configure RIP/OSPF/BGP using packet tracer.

Problem Statement:

Configure RIP/OSPF/BGP using packet tracer.

Outcomes:

Configuration of RIP/OSPF/BGP using packet tracer using wireshark.

Tools Required:

Hardwar: PC-2

Software: jdk compiler and wireshark

peers, are established by manual configuration between routers to
A BGP speaker sends 19-byte keep-alive messages every 60 seconds to
among routing protocols, BGP is unique in using TCP as its transport protocol.

When BGP runs between two peers in the same autonomous system (AS), it is referred t
BGP (iBGP or Interior Border Gateway Protocol). When it runs between different autonomou
is called *External BGP (eBGP or Exterior Border Gateway Protocol)*. Routers on the bounda
exchanging information with another AS are called *border or edge routers* or simply *eBGP p*
connected directly, while *iBGP peers* can be interconnected through other
Other deployment topologies are also possible, such as running eBGP peering
tunnel, allowing two remote sites to exchange routing information in a secure and isolated
main difference between iBGP and eBGP peering is in the way routes that were received fro
are propagated to other peers. For instance, new routes learned from an eBGP peer
redistributed to all iBGP peers as well as all other eBGP peers (if *transit* mode is enabled on
However, if new routes are learned on an iBGP peering, then they are re-advertised only
peers. These route-propagation rules effectively require that all iBGP peers inside
interconnected in a full mesh.

How routes are propagated can be controlled in detail via the *route-maps* mechanism. This
consists of a set of *rules*. Each rule describes, for routes matching some given criteria, w
should be taken. The action could be to drop the route, or it could be to modify some attrib
route before inserting it in the routing table.

Conclusion :

Thus we have configured RIP/OSPF/BGP using packet tracer using wireshark.

Questions.

1.Explain packet Tracer

2.Explain packet tracer tools

3.Explain header format of packet tracer

4.Explain wireshark

Assignment - B7

Q. Explain packet tracer.

Ans (i) Packet tracer is a cross platform visual simulation tool designed by Cisco system that allow users to create it network topologies.

(ii) The software allows users to stimulate the configuration of Cisco routers and switches using a simulated command line Interface.

(iii) Packet tracer makes use of drag & drop UI, allowing users to add & remove network devices as they see fit.

(iv) Packet tracer allows students to design complex & large networks, which as often not feasible with physical hardware, due to cost.

Q. Explain packet tracer tools.

Ans Following are the networking tools :-

(i) GNS3 - Design & Configure
(ii) Cisco Packet tracer
(iii) Putty configure
(iv) Secure CRT - configure
(v) Microsoft vision - Design only
(vi) PRTG monitoring
(vii) Wireshark monitor
(viii) Concept Draw pro - design
(ix) Network simulator Design & monitor
(x) Free SNMP agent simulator - monitor

Q Explain Wireshark

Ans (i) Wireshark is a free & open source packet analyser. It is used for troubleshooting analysis, software & communications protocol development & education.

(ii) It is cross platform, using the Qt widget toolkit in current releases to implement its UI & pcap to capture packets. It runs on MacOS, Windows, Linux, etc.

(iii) It can also be used to capture packets from most networks simulation tools like ns-OPNET modulators & netism.

(iv) Wireshark native networks trace file format is libPcapformat, supported by libpcap and wincap, so it can exchange captured network traces with other application the uses the same format including tcpdump & CA Net Master.

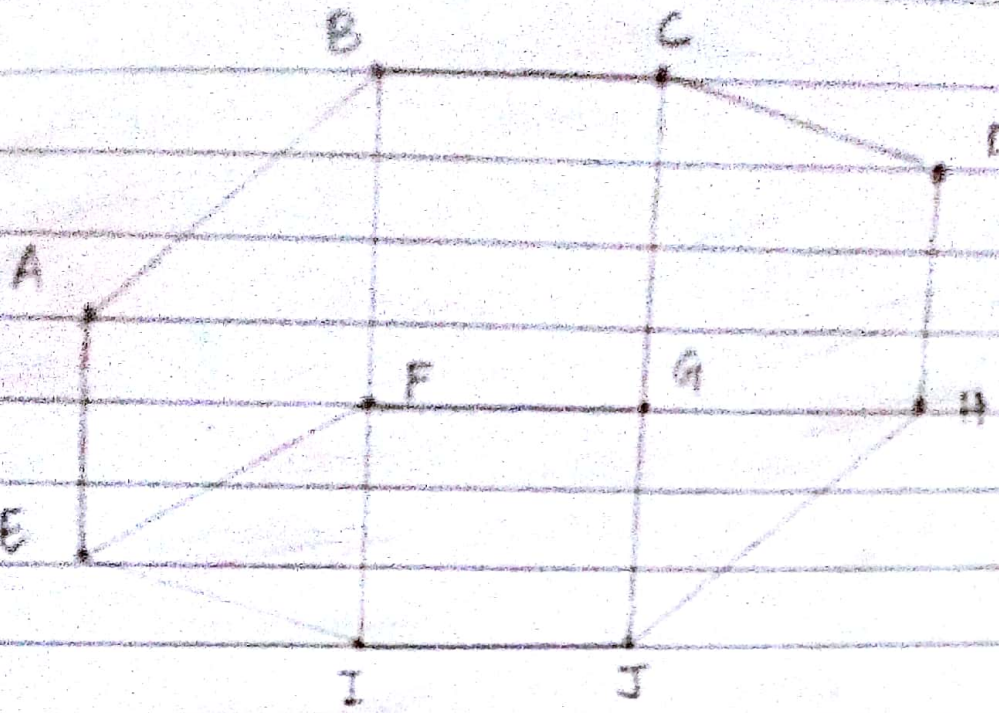
Q Explain BGP Protocol

Ans (i) BGP stands for Border Gateway Protocol is standardized exterior gateway protocol designed to exchange routing & reachability information along autonomous systems (AS) on the Internet.

(ii) The protocol is often classified as a path vector proto-l but its sometimes also classed as distance vector routing protocol

(iii) The BGP protocol makes routing, decision based on paths, network policies, or rules, sets configured by a network administrator and is involved in making core routing decisions.

(iv) As an example, consider BGP routers as shown in fig. In particular consider routing table, suppose that it uses the path EGC to get to D. When neighbours routing information, they provide their complete paths.



Information E receive from its neighbours about D

from B : I use "BCG"
from G : I use "GCD"
from I : I use "FGEN"
from E : I use "EFGCD"

(v) BGP really solves the count to infinite problem that players other distance vector routing algorithm.