Department of Computer Engineering

LAB MANUAL

Semester-V

Computer Networks

Institute Vision, Mission & Quality Policy

Vision

To foster and permeate higher and quality education with value added engineering, technology programs, providing all facilities in terms of technology and platforms for all round development with societal awareness and nurture the youth with international competencies and exemplary level of employability even under highly competitive environment so that they are innovative adaptable and capable of handling problems faced by our country and world at large.

Mission

The Institution is committed to mobilize the resources and equip itself with men and materials of excellence thereby ensuring that the Institution becomes pivotal center of service to Industry, academia, and society with the latest technology. RAIT engages different platforms such as technology enhancing Student Technical Societies, Cultural platforms, Sports excellence centers, Entrepreneurial Development Center and Societal Interaction Cell. To develop the college to become an autonomous Institution & deemed university at the earliest with facilities for advanced research and development programs on par with international standards. To invite international and reputed national Institutions and Universities to collaborate with our institution on the issues of common interest of teaching and learning sophistication.

Quality Policy

ज्ञानधीनं जगत् सर्वम।

Knowledge is supreme.

Our Quality Policy

It is our earnest endeavour to produce high quality engineering professionals who are innovative and inspiring, thought and action leaders, competent to solve problems faced by society, nation and world at large by striving towards very high standards in learning, teaching and training methodologies.

Our Motto: If it is not of quality, it is NOT RAIT!

Dr. Vijay D. Patil
President, RAES

Department Vision & Mission

Vision

To impart higher and quality education in computer science with value added engineering and technology programs to prepare technically sound, ethically strong engineers with social awareness. To extend the facilities, to meet the fast changing requirements and nurture the youths with international competencies and exemplary level of employability and research under highly competitive environments.

Mission

- To mobilize the resources and equip the institution with men and materials of excellence to provide knowledge and develop technologies in the thrust areas of computer science and Engineering.
- To provide the diverse platforms of sports, technical, co curricular and extracurricular activities for the overall development of student with ethical attitude.
- To prepare the students to sustain the impact of computer education for social needs encompassing industry, educational institutions and public service.
- To collaborate with IITs, reputed universities and industries for the technical and overall uplifment of students for continuing learning and entrepreneurship.

Index

Sr. No.	Contents	Page No.
1.	List of Experiments	1
2.	Course Outcomes and Experiment Plan	2
3.	Study and Evaluation Scheme	4
4.	Experiment No. 1	5
5.	Experiment No. 2	15
6.	Experiment No. 3	21
7.	Experiment No. 4	25
8.	Experiment No. 5	31
9.	Experiment No. 6	37
10.	Experiment No. 7	43
11.	Experiment No. 8	49
12.	Experiment No. 9	55
13.	Experiment No. 10	61
14.	Experiment No. 11	69
15	Experiment No. 12	75

List of Experiments

Sr. No.	Experiments Name
1	Study of network connecting devices
2	Implement Hamming code Error correction and detection mechanism
3	Implement CRC Error detection mechanism
4	Implement CHECKSUM Error detection Mechanism
5	Client – Server using network socket connection
6	Implement Stop and wait protocol in DLL
7	Implement Sliding window protocol in DLL
8	Write program to find out class of a given IP address ,Subnet Mask and first and last IP address of that block
9	Installation and configuration of NS-2
10	Study and implement of basic wired LAN topology in NS-2
11	Simulating networks and protocols using NS-2 DVR simulation and link failure handling
12	Study of Network Management Tool

Course Outcome & Experiment Plan

Course Objectives:

1.	To provide students with an overview of the concepts and fundamentals of data communication and computer networks
2.	To familiarize with the basic taxonomy and terminology of computer networking area.
3.	To experience the designing and managing of communication protocols while getting a good exposure to the TCP/IP protocol suite

Course Outcomes:

CO1	Conceptualize all the OSI Layers
CO2	Use appropriate network tools to build network topologies
CO3	**To provide students with in-depth knowledge of fundamental such as error detection, correction and flow control techniques; multiple access control techniques**
CO4	Install and configure an open source tool NS2
CO5	Test simple protocols in a laboratory scenario
CO6	**Allow the students to gain expertise in some specific areas of networking such as design and maintenance of individual network**

Experiment Plan:

Module No.	Week No.	Experiments Name	Course Outcome
1	W1	Study of network connecting devices	CO1
2	W2	Implement Hamming code Error correction and detection mechanism	CO3
3	W3	Implement CRC Error detection mechanism	CO3
4	W4	Implement CHECKSUM Error detection Mechanism	CO3
5	W5	Client – server using network socket connection.	CO5
6	W6	Implement Stop and wait protocol in DLL	CO3
7	W7	Implement Sliding window protocol in DLL	CO3
8	W8	Write program to find out class of a given IP	CO5

		address ,Subnet Mask and first and last IP address of that block	
9	W9	Installation and configuration of NS2	CO4
10	W10	Study and implement of basic wired LAN topology in NS2	CO2
11	W11	Simulating networks and protocols using NS 2 DVR simulation and link failure handling	CO4
12	W12	Study of network management tool	CO6

Mapping Course Outcomes (CO) - Program Outcomes (PO)

Subject Weight	Course Outcomes	Contribution to Program outcomes											
		P_a	P_b	P_c	P_d	P_e	P_f	P_g	P_h	P_i	P_j	P_k	P_l
PR 40%	**CO1**:Conceptualize all the OSI Layers	2	2	2			2				2		
	CO2:Use appropriate network tools to build network topologies	2	2			2		2		2			
	CO3: To provide students with in-depth knowledge of data link layer fundamental such as error detection, correction and flow control techniques; multiple access control techniques.	1	3	1		2			2	1			
	CO4:Install and configure an open source tool NS2		3		1			2		1	2	1	
	CO5:Test simple protocols in a laboratory scenario		3		2							2	3
	CO6:Allow the students to gain expertise in some specific areas of networking such as design and maintenance of individual network							2		2	1	2	3

Study and Evaluation Scheme

Course Code	Course Name	Teaching Scheme			Credits Assigned			
		Theory	Practical	Tutorial	Theory	Practical	Tutorial	Total
CPC504	Computer Networks	04	02	--	04	01	--	05

Course Code	Course Name	Examination Scheme		
		Term Work	Oral/Practical	Total
CPC504	Computer Networks	25	25	50

Term Work:

1. Term work assessment must be based on the overall performance of the student with every experiment graded from time to time. The grades should be converted into marks as per the Credit and Grading System manual and should be added and averaged.
2. The final certification and acceptance of term work ensures satisfactory performance of laboratory work and minimum passing marks in term work.

Practical:

Practical exam will be based on the experiments performed along with additional experiments

Computer Networks

Experiment No. : 1

Study of various Network devices

Experiment No. 1

1. **Aim:** Study of various Network devices.

2. **Objectives:** From this experiment, the student will be able to
   - Understand the concepts and fundamentals of data communication and computer networks
   - Familiarize with the basic taxonomy and terminology of computer Networking area.

3. Outcomes: The learner will be able to
   - Understand, identify, analyze the network devices.
   - Understanding of professional, ethical, legal, security and social issues and responsibilities.
   - Understand exploit gained skills and knowledge of contemporary issues.

4.Hardware / Software Required :

5.Theory:

To understand what connecting devices are, it is important to know about Backbone Networks. Backbone Network is a means of connecting 2 LAN's. It provides a transmission channel for packets from being transmitted from one LAN to the other. The individual LAN's are connected to the Backbone Network by using some types of devices such as Hubs, Repeaters, Switches, Bridges, Routers and Gateways.

Hub

A hub works in the physical layer of the OSI model. It is basically a non-intelligent device, and has no decision making capability. What a Hub basically does is take the input data from one of the ports and broadcast the information to all the other ports connected to the network.

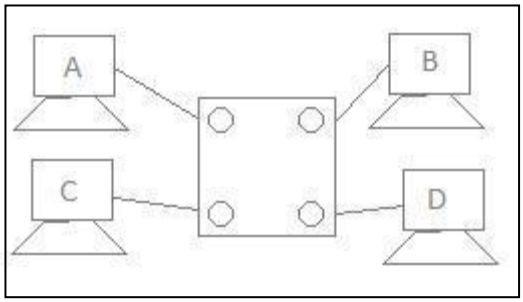

Fig 1.1 port network

To demonstrate its working, consider a 4 port network as shown in Fig 1. There are 4 computers connected to the 4 ports. Suppose, if Computer A wants to send some data to Computer B using a Hub, then, Computer A broadcasts the data on the network, and Computer B, being connected to the network, has access to the data. But, in this case all the other ports connected to the network has access to the data that is being transmitted by Computer A. This happens because, the Hub works in the Physical Layer and hence it does not know about the MAC addresses of the ports connected to the network. So, there is a lack of security in the Hub.

Repeater

A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different from the regular amplification by amplifiers. The regular amplifies everything fed into it. That means, if the input signal has noise induced into it, both the desired signal and noise signal are together amplified. But, in the case of a repeater, it regenerates the input signal, and amplifies only the desirable signal. Hence, the noise component of the signal is eliminated.

Fig 1.2: Repeater

Switch

A switch is an intelligent device that works in the data link layer. The term intelligent refers to the decision making capacity of the Switch. Since it works in the Data link layer, it has knowledge of the MAC addresses of the ports in the network.

Fig 1.3: Switch

Hence, in the Fig 1, if data has to be sent from Computer A to Computer B, then, the data is transferred to the Computer B only, and not to any other computers connected on the network. Hence, it establishes a link between the sender and the receiver based on the MAC addresses. This also means that when data is being sent from A to B, Computer C can establish a link with Computer D and communication can take place between them. So, simultaneous data transfer is possible in a switch. Also, Hub divides bandwidth, but a Switch does not.

Bridge

A bridge is also a device which works in the Data Link Layer, but is more primitive when compared to a switch. Initial bridges were used to connect only 2 LAN's, but the most recent ones perform similar operation as the switches. It also works on the principle of transfer of information using the MAC addresses of the ports.

Fig 1.4: Bridge

It can be noted is that the normal ADSL modem can be connected via bridging also. The only difference is that, when bridging is used, each time the device has to be connected to the internet, it has to dial to the internet and establish a connection. Also, a bridge alone cannot be used to connect to the internet, because, the bridge works in the Data Link Layer, and has no knowledge of the IP Addresses, which are used in the Internet.

Router

Any computer can be connected to the internet via MODEM, which performs the Modulation and the Demodulation operations. But, when there are more than one computer at home or in an organization, and you have a single internet connection, you need a Router. Router is a device which is used when multiple devices need to connect to the Internet using the same IP.

Any Internet Service Provider (ISP) provides a single IP, and especially for personal use, the IP address is assigned dynamically. This is done because, suppose, an ISP has 1000 IP addresses, it does not mean that it has 1000 customers. An ISP assumes that not all devices will be connected to the internet at the same time. Hence, when a user wants to access the internet, any IP address from the pool of IP addresses from the ISP will be assigned to connect the user to the internet.

Fig 1.5: Router

Hence, the router does the job of connecting multiple devices in a LAN to the internet using the same IP address. Since the router works in the Network Layer, it does forwarding on the basis of IP addresses.

The Wi-Fi routers that are commonly used now are the IEEE 802.11 b/g standard router, which is explained below.

IEEE 802.11

IEEE 802.11 is a standard for Wi-Fi. There are several different technologies/ generations that have been implemented. As mentioned, the recent modems are IEEE 802.11 b/g modems. The word b/g has the meaning as follows:

An IEEE 802.11 b standard uses 2.4GHz band and has a maximum transfer rate of 11 Mbps, while the IEEE 802.11 g standard uses 2.4 GHz band and has maximum transfer rate of 54 Mbps. Thus the b/g modem refers to a dual bandwidth modem, which is compatible with both the b and g standards. The standards are mainly differentiated based on the distance and speed of data transfer.

The more recent IEEE 802.11 N standard has the capability to provide speeds of over 100 Mbps. It basically uses multiple wireless signals and antennas, and has increased signal intensity in order to be able to provide network for greater distances. It employs MIMO technology, wherein spatial encoding is used. The spatial pre-coding is done at the transmitter and the post-coding is done at the receiver. Recently, Reliance Communications was in news for implementing MIMO technology to improve its 3G data transfer speeds.

Brouter

Brouter (Bridging Router) is a device which has two functions. Brouter acts as a router for known protocols (known by the router and those on the network) and hence works in the network layer. For data packets with unknown protocols, it acts as a bridge by connecting two different networks which is the function of a bridge - and this works in the data-link layer.

Gateway

The Gateway devices work in the Transport layer and above, where the different network technologies are implemented. A gateway is necessary when there are different technologies implemented by the different LAN's which are to be connected together.

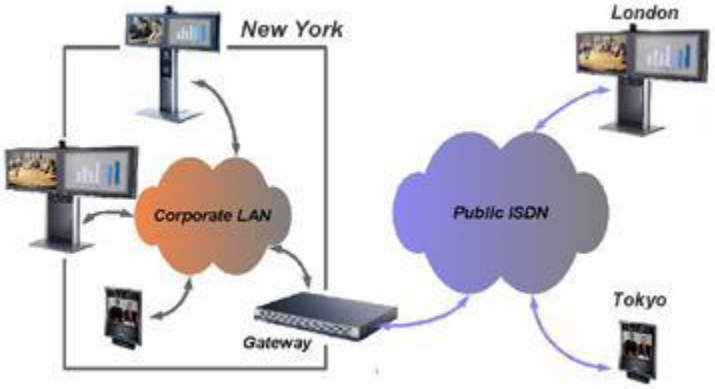

Fig 1.6: Gateway function

The Fig 1.6 shows the working of a gateway. Consider 2 networks, say in New York, and a network in London. If data has to be sent from one place to another, we need to ensure that the network technologies that are being used by both the networks are the same. If not, we need to use a Gateway.

In the more common example, we use a telephone network and internet networks, which works on different technologies. The telephone network follows the ISDN, and the Internet follows the IP. Here, 2 different technologies are being used. In this case, the router fails to work, since the router cannot understand the functionalities of both the networks. Hence, we require a Gateway, which acts as a translator in communicating between the 2 networks.

Connecting Cables

While connecting different networks, we come across different connecting cables, which are as follows:

1. RJ45/ RJ 11 Connectors: The RJ45 (Registered Jack 45) cable or the Cat 5 cable, is used to connect the two different LAN's together. This is normally confused with the RJ11 cable, which is used in the interconnections in the telephone network.
2. Crossover cables: Crossover cables are generally used when 2 different computers are to be connected together. They get the name because, in these cables, a crossover is made between the Transmitter and Receiver ports, i.e., Transmitter of one end of the cable is connected to the Receiver port at the other end and vice versa.
3. Null Modem Cables: The null modem cables are also those which are used in connecting 2 different computers to form a network. They also have a crossover, but generally, the term null modem cables are used for RS232 standard cables.
4. Optical Fibers: The optical fibers are used when gigabit Ethernet is used, and very high rates of data transmission is necessary.

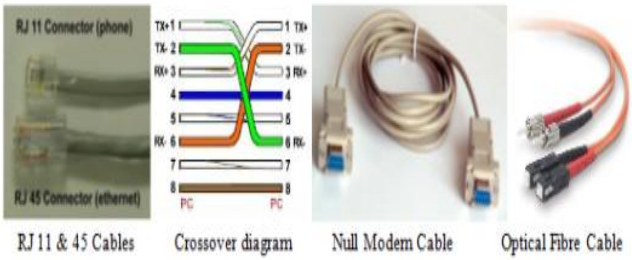

Fig 1.7: Connecting Cables

6. Conclusion:

Hence from above experiment student studied and understand about the network devices and conclude as Hubs and switches provide a mechanism to connect devices to a network created with twisted-pair cabling. Switches offer a speed advantage over hubs because they can use full-duplex communications. Bridges allow network traffic to be confined to certain network segments, thereby reducing the amount of network traffic. Routers are devices that connect networks and thereby create internetworks. A gateway is a device that translates from one data format to another; it can be a hardware device or a software application.

7. Viva Questions:

- At what OSI layer does a hub work?
- At what OSI layer does a repeater work?

- At what OSI layer does a router work?
- At what OSI layer does a switch work?
- What are the types of hubs?
- What are the types of switches?
- What are manageable switches? What are their functions?

8. References:

1. A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
2. B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 2

Implement Hamming code Error correction and detection mechanism

Experiment No. 2

1. Aim: Implement Hamming code Error correction and detection mechanism

2. Objective

From this experiment, the student will be able to

- Understand the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminology of computer Networking area.
- Implement Hamming code Error correction and detection mechanism.

3. Outcomes: The learner will be able to

- Understand, Implementation of Hamming code Error correction and detection mechanism
- Understanding of professional, ethical, legal, security and social issues and responsibilities.
- Understand exploit gained skills and knowledge of contemporary issues.

4. Hardware/Software Required: Java

5. Theory:

In telecommunication, Hamming codes are a family of linear error-correcting codes. Hamming codes can detect up to two-bit errors or correct one-bit errors without detection of uncorrected errors. By contrast, the simple parity code cannot correct errors, and can detect only an odd number of bits in error. Hamming codes are perfect codes, that is, they achieve the highest possible rate for codes with their block length and minimum distance of three.

General algorithm

The following general algorithm generates a single-error correcting (SEC) code for any number of bits.

1. Number the bits starting from 1: bit 1, 2, 3, 4, 5, etc.
2. Write the bit numbers in binary: 1, 10, 11, 100, 101, etc.
3. 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)
4. All other bit positions, with two or more 1 bits in the binary form of their position, are data bits.

5. 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.

    1. 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.
    2. 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.
    3. Parity bit 4 covers all bit positions which have the third least significant bit set: bits 4–7, 12–15, 20–23, etc.
    4. Parity bit 8 covers all bit positions which have the fourth least significant bit set: bits 8–15, 24–31, 40–47, etc.
    5. In general each parity bit covers all bits where the bitwise AND of the parity position and the bit position is non-zero.

The form of the parity is irrelevant. Even parity is simpler from the perspective of theoretical mathematics, but there is no difference in practice.

This general rule can be shown visually:

Bit position		1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20
Encoded data bits		p1	p2	d1	p4	d2	d3	d4	p8	d5	d6	d7	d8	d9	d10	d11	p16	d12	d13	d14	d15
Parity bit coverage	p1	X		X		X		X		X		X		X		X		X		X	
	p2		X	X			X	X			X	X			X	X			X	X	
	p4				X	X	X	X					X	X	X	X					X
	p8								X	X	X	X	X	X	X	X					
	p16																X	X	X	X	X

The pattern continues indefinitely

To check for errors, check all of the parity bits The pattern of errors, called the error syndrome, identifies the bit in error If all parity bits are correct, there is no error Otherwise, the sum of the

positions of the erroneous parity bits identifies the erroneous bit For example, if the parity bits in positions 1, 2 and 8 indicate an error, then bit 1+2+8=11 is in error If only one parity bit indicates an error, the parity bit itself is in error

6. Conclusion:

Student successfully Implemented Hamming code Error correction and detection mechanism and studied that Hamming code is a set of error-correction code s that can be used to detect and correct bit errors that can occur when computer data is moved or stored.

7. Viva Questions:

- Given an example calculate parity of the message
- Give the algorithm to compute parity
- Is it possible to correct errors using (n, k) Hamming code?
- How many bit errors can be detected?
- How many bit errors can be corrected?
- Given a received code check if there is any error
- Give the procedure for error detection and correction

8. References:

1. A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
2. B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 3

Implement CRC Error detection mechanism

Experiment No. 3

1. **Aim:** Implement CRC Error detection mechanism

2. **Objective**

From this experiment, the student will be able to

- Understand the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminology of computer Networking area.
- Implement CRC Error detection method

3. Outcomes: The learner will be able to

- Understand, Implementation of Implement CRC Error detection method
- Understanding of professional, ethical, legal, security and social issues and responsibilities.
- Understand exploit gained skills and knowledge of contemporary issues.

4. Hardware /Software Required: Java

5. Theory: Cyclic Redundancy Check

We can create cyclic codes to correct errors. However, the theoretical background required is beyond the scope of this book. In this section, we simply discuss a category of cyclic codes called the cyclic redundancy check (CRC) that is used in networks such as LANs and WANs.

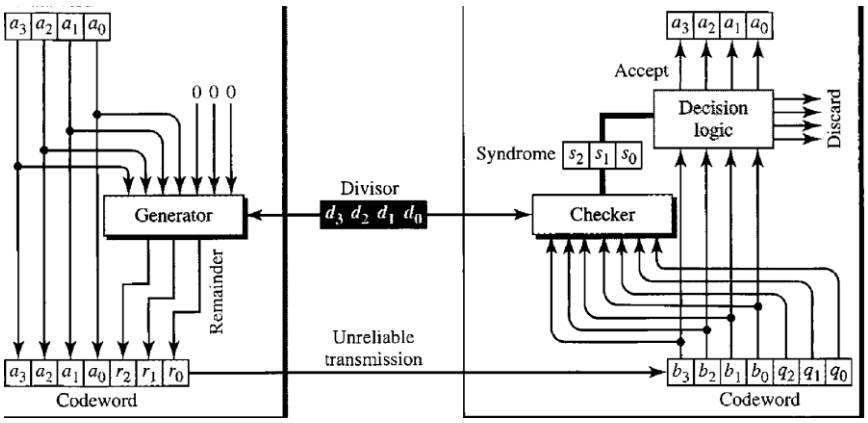

Fig 3.1 CRC encoder and decoder

In the encoder, the data word has *k* bits (4 here); the codeword has *n* bits (7 here).The size of the data word is augmented by adding *n* - *k* (3 here) Os to the right-hand side of the word. The n-bit result is fed into the generator. The generator uses a divisor of size *n* - *k* + I (4 here), predefined and agreed upon. The generator divides the augmented data word by the divisor (modulo-2 division). The quotient of the division is discarded; the remainder *(r2rl ro)* is appended to the data word to create the codeword.

The decoder receives the possibly corrupted codeword. A copy of all *n* bits is fed to the checker which is a replica of the generator. The remainder produced by the checker is a syndrome of *n* - *k* (3 here) bits, which is fed to the decision logic analyzer. The analyzer has a simple function. If the syndrome bits are all as, the 4 leftmost bits of the codeword are accepted as the data word (interpreted as no error); otherwise, the 4 bits are discarded (error).

6. Conclusion :

Student will successfully Implemented CRC Error detection technique and conclude that CRC is an error-detecting code. Its computation resembles a long division operation in which the quotient is discarded and the remainder becomes the result, with the important distinction that the arithmetic used is the carry-less arithmetic of a finite field. The length of the remainder is always less than or equal to the length of the divisor, which therefore determines how long the result can be. The definition of a particular CRC specifies the divisor to be used, among other things.

7. Viva Questions:

- Given an example calculate checksum of the message
- Give the algorithm to compute checksum
- Is it possible to correct errors using CRC method?
- How many bit errors can be detected
- How many bit errors can be corrected?
- Given a received code check if there is any error
- Give the procedure for error detection and correction

8. References

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 4

Implement CHECKSUM Error detection Mechanism

Experiment No. 4

1. Aim: Implement CHECKSUM Error detection Mechanism

2 . Objective

From this experiment, the student will be able to

- Understand the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminology of Computer Networking area.
- Implement CHECKSUM Error detection Mechanism

3. Outcomes: The learner will be able to

- Understand Implementation CHECKSUM Error detection Mechanism
- Understanding of professional, ethical, legal, security and social issues and responsibilities.
- Understand exploit gained skills and knowledge of contemporary issues.

4. Hardware /Software Required: Java

5. Theory:

Checksum is a error detection method used in the Internet by several protocols although not at the data link layer

Internet Checksum

Traditionally, the Internet has been using a 16-bit checksum. The sender calculates the checksum by following these steps.

Sender site:

1. The message is divided into 16-bit words.

2. The value of the checksum word is set to O.

3. All words including the checksum are added using one's complement addition.

4. The sum is complemented and becomes the checksum.

5. The checksum is sent with the data.

The receiver uses the following steps for error detection.

1. The message (including checksum) is divided into 16-bit words.
2. All words are added using one's complement addition.
3. The sum is complemented and becomes the new checksum.
4. If the value of checksum is 0, the message is accepted; otherwise, it is rejected.

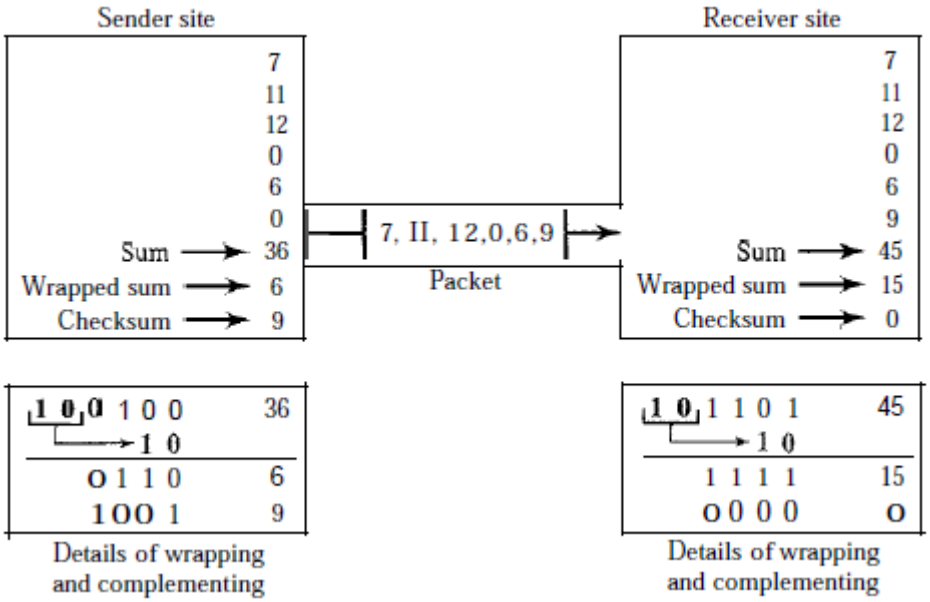

Fig: 4.1 CRC Method

Above Figure shows the process at the sender and at the receiver. The sender initializes the checksum to 0 and adds all data items and the checksum (the checksum is considered as one data item and is shown in color). The result is 36. However, 36 cannot be expressed in 4 bits. The extra two bits are wrapped and added with the sum to create the wrapped sum value 6. In the figure, we have shown the details in binary. The sum is then complemented, resulting in the checksum value 9 (15 - 6 = 9). The sender now sends six data items to the receiver including the checksum 9. The receiver follows the same procedure as the sender. It adds all data items (including the checksum); the result is 45. The sum is wrapped and becomes 15. The wrapped sum is complemented and becomes O. Since the value of the checksum is 0, this means that the data is not corrupted. The receiver drops the checksum and keeps the other data items. If the checksum is not zero, the entire packet is dropped.

6. Conclusion:

Student will successfully Implemented CHECKSUM Error detection technique and conclude that checksum is created by calculating the binary values in a packet or other block of data using

some algorithm and storing the results with the data. When the data is retrieved from memory or received at the other end of a network, a new checksum is calculated and compared with the existing checksum. A non-match indicates an error; a match does not necessarily mean the absence of errors

7. Viva Questions:

- Given an example calculate checksum of the message
- Give the algorithm to compute checksum
- Is it possible to correct errors using CRC method?
- How many bit errors can be detected
- How many bit errors can be corrected?
- Given a received code check if there is any error
- Give the procedure for error detection and correction

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 5

Client – Server using network socket connection.

Experiment No. 5

1. Aim: Client – server using network socket connection.

2. Objective

From this experiment, the student will be able to

- Understand the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminology of computer Networking area.
- Understand the use of client/server architecture in application development.

3. Outcomes:

The learner will be able to

- Understand Use network programming concepts
- Create client – server network connection.

4. Hardware /Software Required: Java

5. Theory:

Sockets are interfaces that can "plug into" each other over a network Once so "plugged in", the programs so connected communicate Normally, a server runs on a specific computer and has a socket that is bound to a specific port number The server just waits, listening to the socket for a client to make a connection request On the client-side: The client knows the hostname of the machine on which the server is running and the port number on which the server is listening To make a connection request, the client tries to rendezvous with the server on the server's machine and port The client also needs to identify itself to the server so it binds to a local port number that it will use during this connection This is usually assigned by the system .

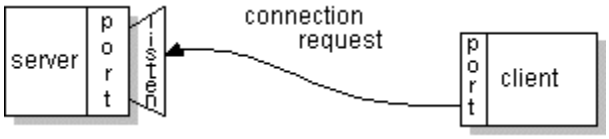

Fig. 5.1 Client to Server Connection request

If everything goes well, the server accepts the connection Upon acceptance, the server gets a new socket bound to the same local port and also has its remote endpoint set to the address and

port of the client It needs a new socket so that it can continue to listen to the original socket for connection requests while tending to the needs of the connected client

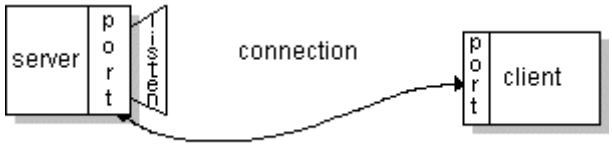

Fig 5.2 Server Response to Client Connection

On the client side, if the connection is accepted, a socket is successfully created and the client can use the socket to communicate with the server

The client and server can now communicate by writing to or reading from their sockets

Definition: A *socket* is one endpoint of a two-way communication link between two programs running on the network A socket is bound to a port number so that the TCP layer can identify the application that data is destined to be sent The java net package in the Java platform provides a class, Socket, that implements one side of a two-way connection between your Java program and another program on the network The Socket class sits on top of a platform-dependent implementation, hiding the details of any particular system from your Java program By using the java net Socket class instead of relying on native code, your Java programs can communicate over the network in a platform-independent fashion

Additionally, `java net` includes the `ServerSocket` class, which implements a socket that servers can use to listen for and accept connections to clients

1. Open a socket
2. Open an input stream and output stream to the socket
3. Read from and write to the stream according to the server's protocol
4. Close the streams
5. Close the socket

These lines establish the socket connection between the client and the server and open a `PrintWriter` and a `BufferedReader` on the socket:

```
echoSocket = new Socket("taranis", 7);
out = new PrintWriter(echoSocket getOutputStream(), true);
in = new BufferedReader(new InputStreamReader(
                    echoSocket getInputStream()));
```

The first statement in this sequence creates a new Socket object and names it echoSocket The Socket constructor used here requires the name of the machine and the port number to which you want to connect The example program uses the host name taranis This is the name of a

hypothetical machine on our local network When you type in and run this program on your machine, change the host name to the name of a machine on your network Make sure that the name you use is the fully qualified IP name of the machine to which you want to connect The second argument is the port number Port number 7 is the port on which the Echo server listens

The second statement gets the socket's output stream and opens a `PrintWriter` on it Similarly, the third statement gets the socket's input stream and opens a `BufferedReader` on it The example uses readers and writers so that it can write Unicode characters over the socket

To send data through the socket to the server, `EchoClient` simply needs to write to the `PrintWriter` To get the server's response, `EchoClient` reads from the `BufferedReader`

6. Conclusion:

Student will successfully Implemented client server connection and will study A socket is one end-point of a two-way communication link between two programs running on the network. Socket classes are used to represent the connection between a client program and a server program. The java.net package provides two classes--Socket and Server Socket--that implement the client side of the connection and the server side of the connection, respectively.

7. Viva Questions:

- Difference between TCP and UDP protocol?
- What are the most typical functional units of the Client/Server applications?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 6

Implement Stop and wait protocol in DLL

Experiment No. 6

1.Aim: Implement Stop and wait protocol in DLL

2.Objective

From this experiment, the student will be able to

- Understand the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminology of computer Networking area.
- To understand the concept of Stop and wait protocol in DLL

3.Outcomes: The learner will be able to

- Understand Use network programming concepts
- Understand the Implementation of Stop and wait protocol in DLL

4.Hardware /Software Required: Java

5.Theory:

Stop and wait protocol Stop and Wait transmission is the simplest reliability technique and is adequate for a very simple communications protocol. A stop and wait protocol transmits a Protocol Data Unit (PDU) of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if a data PDU is received correctly, and a Negative Acknowledgement (NACK) PDU if the data was not received. In practice, the receiver may not be able to reliably identify whether a PDU has been received, and the transmitter will usually also need to implement a timer to recover from the condition where the receiver does not respond.

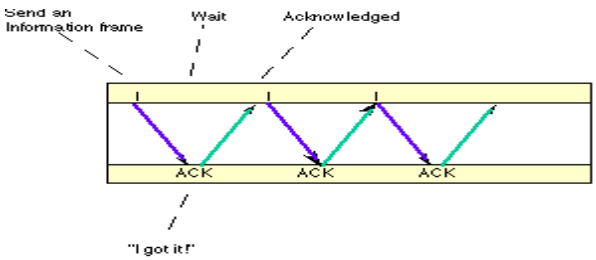

Fig 6.1 Stop and Wait ARQ - Waiting for Acknowledgment (ACK) from the remote node.

The blue arrows show the sequence of data PDUs being sent across the link from the sender (top to the receiver (bottom). A Stop and Wait protocol relies on two way transmission (full duplex or

half duplex) to allow the receiver at the remote node to return PDUs acknowledging the successful transmission. The acknowledgements are shown in green in the diagram, and flow back to the original sender. A small processing delay may be introduced between reception of the last byte of a Data PDU and generation of the corresponding ACK. When PDUs are lost, the receiver will not normally be able to identify the loss (most receivers will not receive anything, not even an indication that something has been corrupted). The transmitter must then rely upon a timer to detect the lack of a response.

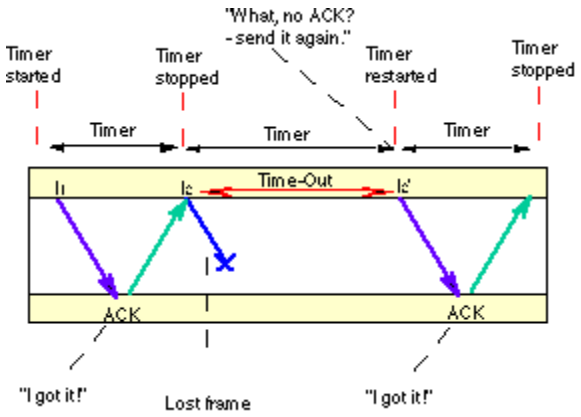

Fig 6.2 Stop and Wait ARQ - Retransmission due to timer expiry

In the diagram, the second PDU of Data is corrupted during transmission. The receiver discards the corrupted data (by noting that it is followed by an invalid data checksum). The sender is unaware of this loss, but starts a timer after sending each PDU. Normally an ACK PDU is received before this the timer expires. In this case no ACK is received, and the timer counts down to zero and triggers retransmission of the same PDU by the sender. The sender always starts a timer following transmission, but in the second transmission receives an ACK PDU before the timer expires, finally indicating that the data has now been received by the remote node.

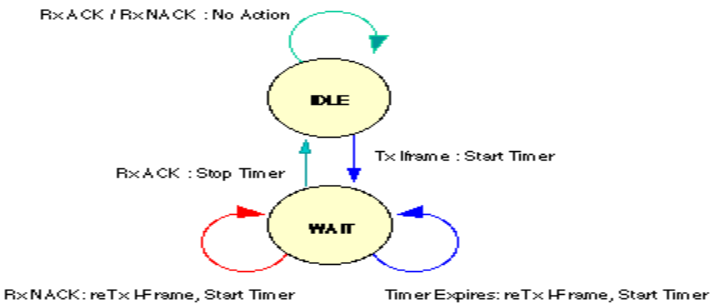

Fig 6.3 State Diagram for a simple stop and wait protocol(Green for ACK, Blue for Data, Red for NACK)

6. Conclusion:

Student will successfully Implemented Stop and wait protocol and study that A stop and wait protocol transmits a Protocol Data Unit (PDU) of information and then waits for a response. The receiver receives each PDU and sends an Acknowledgement (ACK) PDU if a data PDU is received correctly, and a Negative Acknowledgement (NACK) PDU if the data was not received.

7. Viva Questions:

- What is Stop-and-Wait Protocol?
- What is Stop-and-Wait Automatic Repeat Request?
- What is usage of Sequence Number in Relaible Transmission?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Networks

Experiment No. : 7

Implement Sliding window protocol in DLL

Experiment No. 7

1. **Aim:** Write a program to implement Sliding window protocol in DLL

2. **Objectives:** From this experiment, the student will be able to

- Get the overview of the concepts and fundamentals of data communication and computer networks
- Familiarize with the basic terminologies used in computer networks
- Design a communication protocol

3. **Outcomes:** The learner will be able to

- Understand, identify, analyze and design the problem, implement and validate the solution including software
    - Use current techniques for communication practices
    - Use this technique for lifelong learning

4. **Hardware / Software Required :** JAVA

Sliding Window Protocol:

In sliding window method, multiple frames are sent by sender at a time before needing an acknowledgment. Multiple frames sent by source are acknowledged by receiver using a single ACK frame.

Sliding window refers to an imaginary boxes that hold the frames on both sender and receiver side.

• It provides the upper limit on the number of frames that can be transmitted before requiring an acknowledgment.

• Frames may be acknowledged by receiver at any point even when window is not full on receiver side.

• Frames may be transmitted by source even when window is not yet full on sender side.

• The windows have a specific size in which the frames are numbered modulo- n, which means they are numbered from 0 to n-l. For e.g. if n = 8, the frames are numbered 0, 1,2,3,4,5,6, 7, 0, 1,2,3,4,5,6, 7, 0, 1, ...

• The size of window is n-1. For e.g. In this case it is 7. Therefore, a maximum of n-l frames may be sent before an acknowledgment.

• When the receiver sends an ACK, it includes the number of next frame it expects to receive. For example in order to acknowledge the group of frames ending in frame 4, the receiver sends an ACK containing the number 5. When sender sees an ACK with number 5, it comes to know that all the frames up to number 4 have been received.

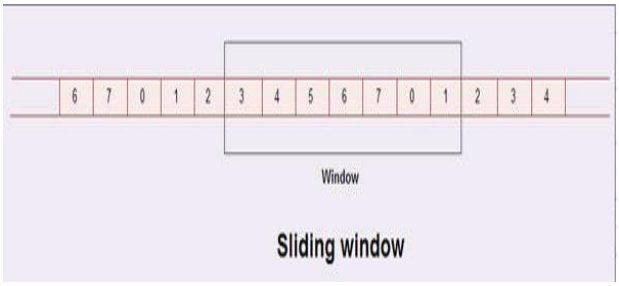

Fig 7.1 Sliding Window

Sliding Window on Sender Side

• At the beginning of a transmission, the sender's window contains n-l frames.

• As the frames are sent by source, the left boundary of the window moves inward, shrinking the size of window. This means if window size is w, if four frames are sent by source after the last acknowledgment, then the number of frames left in window is w-4.

• When the receiver sends an ACK, the source's window expand i.e. (right boundary moves outward) to allow in a number of new frames equal to the number of frames acknowledged by that ACK.

• For example, Let the window size is 7 (see diagram (a)), if frames 0 through 3 have been sent and no acknowledgment has been received, then the sender's window contains three frames - 4,5,6.

• Now, if an ACK numbered 3 is received by source, it means three frames (0, 1, 2) have been received by receiver and are undamaged.

• The sender's window will now expand to include the next three frames in its buffer. At this point the sender's window will contain six frames (4, 5, 6, 7, 0, 1)

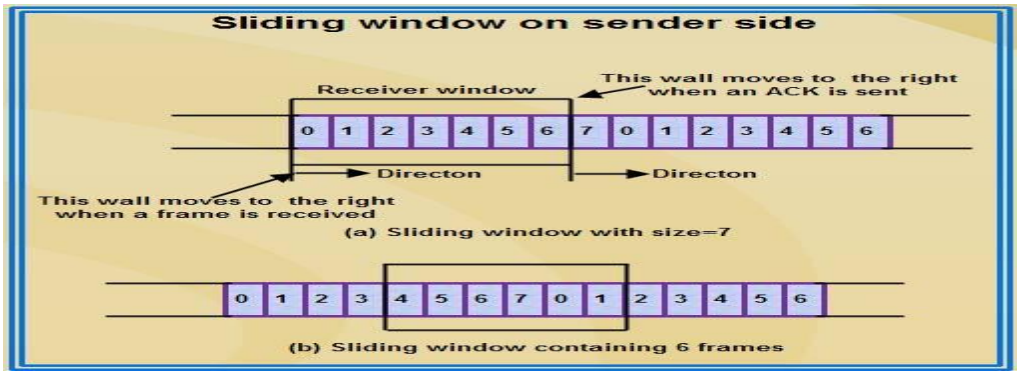

Fig 7.2 Sliding Window on Sender Side

Sliding Window on Receiver Side

• At the beginning of transmission, the receiver's window contains n-1 spaces for frame but not the frames.

• As the new frames come in, the size of window shrinks.

• Therefore the receiver window represents not the number of frames received but the number of frames that may still be received without an acknowledgment ACK must be sent.
• Given a window of size w, if three frames are received without an ACK being returned, the number of spaces in a window is w-3.
• As soon as acknowledgment is sent, window expands to include the number of frames equal to the number of frames acknowledged.
• For example, let the size of receiver's window is 7 as shown in diagram. It means window contains spaces for 7 frames.
• With the arrival of the first frame, the receiving window shrinks, moving the boundary from space 0 to 1. Now, window has shrunk by one, so the receiver may accept six more frame before it is required to send an ACK.
• If frames 0 through 3 have arrived but have DOC been acknowledged, the window will contain three frame spaces.
• As receiver sends an ACK, the window of the receiver expands to include as many new placeholders as newly acknowledged frames.
• The window expands to include a number of new frame spaces equal to the number of the most recently acknowledged frame minus the number of previously acknowledged frame. For *e.g.*, If window size is 7 and if prior ACK was for frame 2 & the current ACK is for frame 5 the window expands by three
Therefore, the sliding window of sender shrinks from left when frames of data are sending. The sliding window of the sender expands to right when acknowledgments are received.
• The sliding window of the receiver shrinks from left when frames of data are received. The sliding window of the receiver expands to the right when acknowledgement is sent.

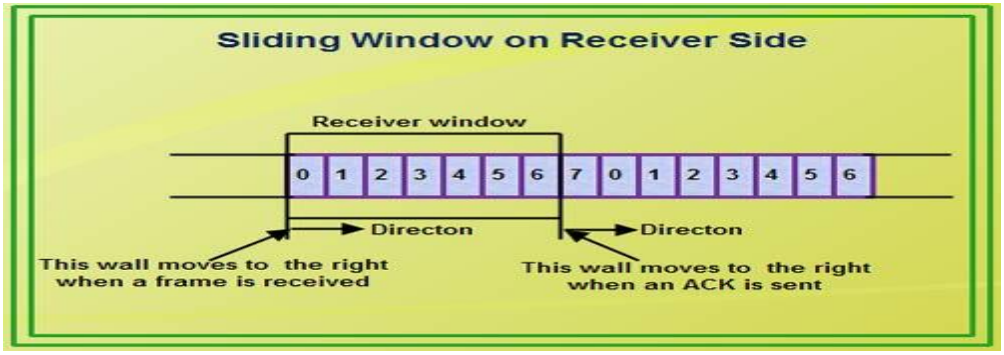

Fig 7.3 Sliding Window on Receiver Side

6.Conclusion:

Thus student will successfully implement sliding window protocol and conclude that Sliding window refers to imaginary boxes at the transmitter and receiver. This window provides the upper limit on the number of frames that can be transmitted before

acknowledgment requirement. Window holds the number of frame to provide above mention limit. The frames which are being transmitted to send are falling in sending window similarly frames to be accepted are store in the receiving window.

7.Viva Questions:

- Explain the algorithm of Sliding window protocol?
- Give an example of Sliding Window Protocol?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Network

Experiment No. : 8

Write program to find out class of a given IP address , Subnet Mask and first and last IP address of that block

Experiment No. 8

1. **Aim:** Write program to find out class of a given IP address ,Subnet Mask and first and last IP address of that block

2. **Objectives:** From this experiment, the student will be able to
   - Understand and get the overview of IP addressing
   - Design and implement IP addressing schemes
   - Understand terminologies used in addressing of computers in network

3. **Outcomes:**
   Understand, identify and implement network addressing techniques
   - the overview of the concepts and fundamentals of data communication and computer networks
   - Familiarize with the basic terminologies used in computer networks
   - Design a communication protocol

4. Hardware / Software Required : JAVA

5. Theory:

What id IP address

An IP address is a number that represents a device like a network card uniquely on the Internet or on your company's intranet. This number is actually a binary one, but for convenience it's normally written as four decimal numbers. For instance, a typical IP address would be something like 192.168.1.1. The four constituent numbers together represent the network that the computer is on and the computer (interface) itself. Let us first look at the network address part. The IP addresses for networks on the Internet are allocated by the InterNIC. If you have an Internet connection (a registered domain and a permanent link to the Internet, and not just a dial-up connection), then you would be allocated a network address by the agency that registered you, like the InterNIC. Let us assume this to be 192.6.132.0, a class C network. Then all the machines on this network would have the same network address. And the last 0 will be replaced by a number from 1 to 254 for the node address. So, nodes will have addresses 192.6.132.1, 192.6.132.2, and so on up to 192.6.132.254.It would be worth mentioning here that IP address calculations and concepts make sense only when done in binary.

Table 8.1 Types of networks and corresponding IP address

Depending on the size of the network, IP-based networks are divided into five classes

Class	1st Octet Decimal Range	1st Octet High Order Bits	Network/Host ID (N=Network, H=Host)	Default Subnet Mask	Number of Networks	Hosts per Network (Usable Addresses)
A	1 – 126*	0	N.H.H.H	255.0.0.0	126 ($2^7 - 2$)	16,777,214 ($2^{24} - 2$)
B	128 – 191	10	N.N.H.H	255.255.0.0	16,382 ($2^{14} - 2$)	65,534 ($2^{16} - 2$)
C	192 – 223	110	N.N.N.H	255.255.255.0	2,097,150 ($2^{21} - 2$)	254 ($2^8 - 2$)
D	224 – 239	1110	Reserved for Multicasting			
E	240 – 254	1111	Experimental; used for research			

Note: Class A addresses 127.0.0.0 to 127.255.255.255 cannot be used and is reserved for loopback and diagnostic functions.

Subnet Mask

In an IP network, every machine on the same physical network sees all the data packets sent out on the network. As the number of computers on a network grows, network traffic will grow many folds, bringing down performance drastically. In such a situation, you would divide your network into different sub networks and minimize the traffic across the different subnet works. between the different subnets would be provided by routers, which will only transmit data meant for another subnet across itself. To divide a given network address into two or more subnets, you use subnet masks. The default subnet masks for class A networks is 255.0.0.0, for class B is 255.255.0.0, Interconnectivity and for class C is 255.255.255.0, which signify a network without subnet

The InterNIC has (RFC 1597 Address Allocation for Private Internets) allocated particular blocks of network addresses for use in intranets. These IP addresses don't conflict with those of existing Internet hosts and will not be handed out for use on the Internet.

Table 8.2 IP Address range for the class

Class	Private Networks	Subnet Mask	Address Range
A	10.0.0.0	255.0.0.0	10.0.0.0 - 10.255.255.255
B	172.16.0.0 - 172.31.0.0	255.240.0.0	172.16.0.0 - 172.31.255.255
C	192.168.0.0	255.255.0.0	192.168.0.0 - 192.168.255.255

Dynamic IP Addressing and Static IP Addressing

In assigning IP addresses to machines, you have two choices. You can either go around typing in the individual address on each machine or you can setup one machine to assign IP addresses to the others. The second one called dynamic addressing is preferred for three reasons. First, it makes the job of administering the network such as adding new clients, avoiding IP clashes, etc a lot easier. And second, since only those machines that are switched on will need an IP address, you could potentially have more machines on your network with dynamic addressing, than you could with static addressing. Finally, mobile computing has become an everyday reality, and notebook computers have a likelihood of moving from one network to another or from one subnet to another. In such a situation, if you have static IP addressing, you have to reconfigure the machine every time you move it something that is eminently avoidable. You do dynamic addressing with DHCP (Dynamic Host Configuration Protocol). To make DHCP work on your network you have to set up a DHCP server.

6. Conclusion:

Thus we have implemented an program to find out the class of an given IP address , subnet mask and also find the start and end IP address of the block.

From above experiment student will understand the basic concept of IP address , subnet mask and start and end IP address of the block.

7.Viva Questions:

- Defne IP address?
- What are different classes of IP address?
- What is subnet mask?
- Explain CIDR?
- How to find the start and end ip address of the block?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Network

Experiment No. : 9

Installation and configuration of NS2

Experiment No. 9

1. Aim: Installation and Configuration of NS2

2. Objectives: From this experiment, the student will be able to

- To provide students overview of data communication in network
- To provide experience in installation of network simulation software
- To provide experience in designing and managing a communication protocol

3. Outcomes: The learner will be able to

- Understand ,design and analyse problem in installation of the software
- Install and Configure open source tool NS2
- Exploit gained skills and knowledge
- Engage in higher studies and life long studies

4. Hardware / Software Required : NS2,Ubuntu

5.Theory:

Network Simulator (Version 2), widely known as NS2, is simply an event driven simulation tool that has proved useful in studying the dynamic nature of communication networks. Simulation of wired as well as wireless network functions and protocols (e.g., routing algorithms, TCP, UDP) can be done using NS2. In general, NS2 provides users with a way of specifying such network protocols and simulating their corresponding behaviours.

Download NS2 from terminal using command

wget http://downloads.sourceforge.net/project/nsnam/allinone/ns-allinone-2.35/ns-allinone-2.35.tar.gz

or directly using

http://downloads.sourceforge.net/project/nsnam/allinone/ns-allinone-2.35/ns-allinone-2.35.tar.gz

•Unpack ns-allinone-2.35.tar.gz to your home directory.

tar -zxvf ns-allinone-2.35.tar.gz -C /home/yourusername

•Next you need to edit a file. Go to **/home/yourusername/ns-allinone-2.35/ns-2.35/linkstate/ directory and open ls.h file** in a text editor**.** Line 137 will be

void eraseAll() { erase(baseMap::begin(), baseMap::end()); }

Change it to

void eraseAll() { this->erase(baseMap::begin(), baseMap::end()); }

•Now install dependencies.

sudo apt-get install tcl8.5-dev tk8.5-dev

sudo apt-get install build-essential autoconf automake

sudo apt-get install perl xgraph libxt-dev libx11-dev libxmu-dev g++ xorg-dev

sudo apt-get install libperl4-corelibs-perl

•Change your directory

cd /home/yourusername/ns-allinone-2.35/

•Run the "install script" by. /**install** command. [This may take few minutes]

•After installation modify .bashrc file located in your home directory.

gedit /home/yourusername/.bashrc

Add the following lines to the end of the file.

export PATH=$PATH:/home/yourusername/ns-allinone-2.35/bin:/home/yourusername/ns-allinone-2.35/tcl8.5.10/unix:/home/yourusername/ns-allinone-2.35/tk8.5.10/unix

export LD_LIBRARY_PATH=$LD_LIBRARY_PATH:/home/yourusername/ns-allinone-2.35/otcl-1.14:/home/yourusername/ns-allinone-2.35/lib

export TCL_LIBRARY=$TCL_LIBRARY:/home/yourusername/ns-allinone-2.35/tcl8.5.10/library

Close gedit.

•To enable the path setting immediately, use.

source ~/.bashrc

•Go to directory /home/yourusername/ns-allinone-2.35/ns-2.35

cd /home/yourusername/ns-allinone-2.35/ns-2.35

and type: **./validate**

Validations tests are performed. This may also take few minutes.

•Now check ns2 working by entering the command **ns**. We should get a **"%"** prompt.

•For testing create a **sample.tcl** file in your home directory.

gedit sample.tcl

and type the following sample code

```
set ns [new Simulator]
set nf [open out.nam w]
$ns namtrace-all $nf
proc finish {} {
global ns nf
$ns flush-trace
close $nf
exec nam out.nam &
exit 0
}
set n0 [$ns node]
set n1 [$ns node]

$ns duplex-link $n0 $n1 1Mb 10ms DropTail
$ns at 3.0 "finish"
$ns run
```

•Save and close **sample.tc**l and run using

ns sample.tcl

It will display a graph with two nodes and a link between them in the NAM

GUI window.

6. Conclusion:

Thus we will install and configure open source tool NS-2 and It is aligned with the simulation needs of modern networking research. It encourages community contribution, peer review, and validation of the software

7. Viva Questions:

- What platforms does NS-2 run on and what kind of hardware do I need?
- What protocols does NS-2 support?
- What is the Full form on NS-2?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Network

Experiment No. : 10

Study and implement of basic wired LAN topology in NS2

Experiment No. 10

1. **Aim:** Study and implement of basic wired LAN topology in NS2

2. **Objectives :** From this experiment, the student will be able to
   - To provide students overview of data communication in network topology
   - To provide experience in designing topology in open source tool network simulation-2 software
   - To provide experience in designing and managing a communication protocol

3. **Outcomes:** The learner will be able to
   - Understand ,design and analyse problem in open source tool NS2
   - Exploit gained skills and knowledge
   - Engage in higher studies and life long studies

4. **Hardware / Software Required :** Ubuntu , NS2

5. **Theory:**

A network topology is the basic design of a computer network. It is very much like a map of a road. It details how key network components such as nodes and links are interconnected. A network's topology is comparable to the blueprints of a new home in which components such as the electrical system, heating and air conditioning system, and plumbing are integrated into the overall design. Taken from the Greek work "Topos" meaning "Place," Topology, in relation to networking, describes the configuration of the network; including the location of the workstations and wiring connections. Basically it provides a definition of the components of a Local Area Network (LAN). A topology, which is a pattern of interconnections among nodes, influences a network's cost and performance. There are three primary types of network topologies which refer to the physical and logical layout of the Network cabling. They are:

1. **Star Topology:** All devices connected with a Star setup communicate through a central Hub by cable segments. Signals are transmitted and received through the Hub. It is the simplest and the oldest and all the telephone switches are based on this. In a star topology, each network device has a home run of cabling back to a network hub, giving each device a separate connection to the network. So, there can be multiple connections in parallel.

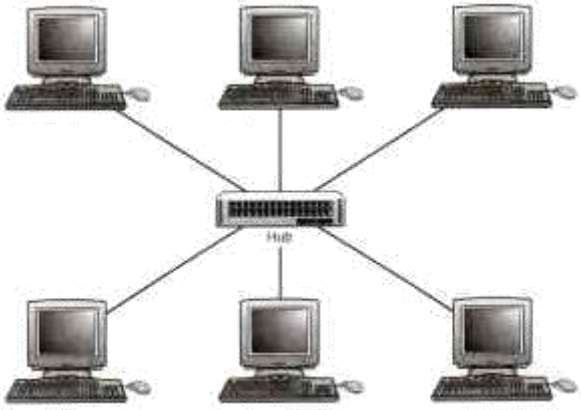

Fig 10.1 Star Topology

Advantages

- Network administration and error detection is easier because problem is isolated to central node
- Networks runs even if one host fails
- Expansion becomes easier and scalability of the network increases
- More suited for larger networks

Disadvantages

- Broadcasting and multicasting is not easy because some extra functionality needs to be provided to the central hub
- If the central node fails, the whole network goes down; thus making the switch some kind of a bottleneck
- Installation costs are high because each node needs to be connected to the central switch

2. **Bus Topology:** The simplest and one of the most common of all topologies, Bus consists of a single cable, called a Backbone, that connects all workstations on the network using a single line. All transmissions must pass through each of the connected devices to complete the desired request. Each workstation has its own individual signal that identifies it and allows for the requested data to be returned to the correct originator. In the Bus Network, messages are sent in both directions from a single point and are read by the node (computer or peripheral on the network) identified by the code with the message. Most Local Area Networks (LANs) are Bus Networks because the network will continue to function even if one computer is down. This topology works equally well for either peer to peer or client server.

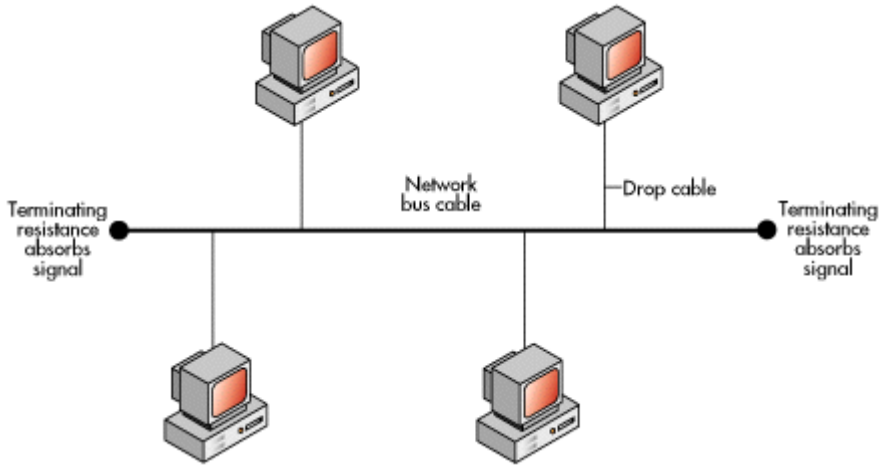

Fig 10.2 Bus Topology

The purpose of the terminators at either end of the network is to stop the signal being reflected back.

Advantages

- Broadcasting and multicasting is much simpler
- Network is redundant in the sense that failure of one node doesn't effect the network. The other part may still function properly
- Least expensive since less amount of cabling is required and no network switches are required
- Good for smaller networks not requiring higher speeds

Disadvantages

- Trouble shooting and error detection becomes a problem because, logically, all nodes are equal
- Less secure because sniffing is easier
- Limited in size and speed

3. **Ring Topology:** All the nodes in a Ring Network are connected in a closed circle of cable. Messages that are transmitted travel around the ring until they reach the computer that they are addressed to, the signal being refreshed by each node. In a ring topology, the network signal is passed through each network card of each device and passed on to the

next device. Each device processes and retransmits the signal, so it is capable of supporting many devices in a somewhat slow but very orderly fashion. There is a very nice feature that everybody gets a chance to send a packet and it is guaranteed that every node gets to send a packet in a finite amount of time.

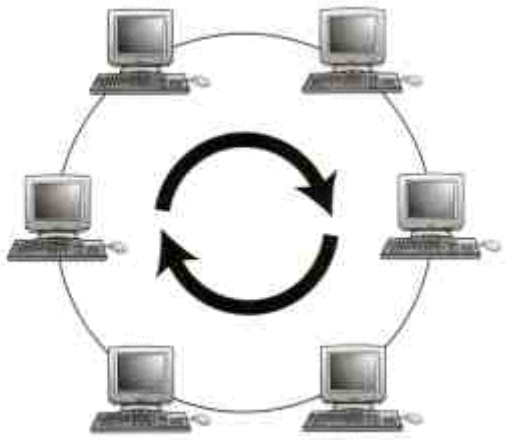

Fig 10.3 Ring Topology

Advantages

- Broadcasting and multicasting is simple since you just need to send out one message
- Less expensive since less cable footage is required
- It is guaranteed that each host will be able to transmit within a finite time interval
- Very orderly network where every device has access to the token and the opportunity to transmit
- Performs better than a star network under heavy network load

Disadvantages

- Failure of one node brings the whole network down
- Error detection and network administration becomes difficult
- Moves, adds and changes of devices can effect the network
- It is slower than star topology under normal load

Generally, a BUS architecture is preferred over the other topologies - ofcourse, this is a very subjective opinion and the final design depends on the requirements of the network more than anything else. Lately, most networks are shifting towards the STAR topology. Ideally we would like to design networks, which physically resemble the STAR topology, but behave like BUS or RING topology.

6.Conclusion:

Thus on completion of this experiment students can implement LAN topology in NS2 and also implement bus, ring and mesh topology.
They will able to study different topology and its advantages and disadvantages.

7.Viva Questions:

- What is topology?
- What are different types of topology?
- What is the advantage and disadvantage of mesh topology?
- What is the advantage and disadvantage of star topology?
- Explain LAN & VLAN?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Network

Experiment No. : 11

Simulating networks and protocols using NS 2 DVR simulation and link failure handling

Experiment No. 11

1. **Aim:** Simulating networks and protocols using NS 2 DVR simulation and link failure handling

2. **Objectives :** From this experiment, the student will be able to
   - To provide students overview of data communication and computer network
   - To provide experience in design and implementation routing protocol in NS-2
   - Getting good exposure to TCP/IP Protocol suite

3. **Outcomes:** The learner will be able to
   - Understand ,design and analyse problem in implementation of routing protocol
   - Exploit gained skills, knowledge and test simple protocol in Laboratory
   - Engage in higher studies and lifelong studies

4. **Hardware / Software Required :** NS2,Ubuntu

5. **Theory:**

A distance-vector routing protocol requires that a router inform its neighbours of topology changes periodically. Compared tolink-state protocols, which require a router to inform all the nodes in a network of topology changes, distance-vector routing protocols have less computational complexity and message overhead. The term distance vector refers to the fact that the protocol manipulates vectors (arrays) of distances to other nodes in the network.

Routers using distance-vector protocol do not have knowledge of the entire path to a destination. Instead they use two methods:

1. Direction in which router or exit interface a packet should be forwarded.
2. Distance from its destination

Distance-vector protocols are based on calculating the direction and distance to any link in a network. "Direction" usually means the next hop address and the exit interface. "Distance" is a measure of the cost to reach a certain node. The least cost route between any two nodes is the route with minimum distance. Each node maintains a vector (table) of minimum distance to every node. The cost of reaching a destination is calculated using various route metrics. RIP uses the hop count of the destination whereas IGRP takes into account other information such as node delay and available bandwidth.

Updates are performed periodically in a distance-vector protocol where all or part of a router's routing table is sent to all its neighbours that are configured to use the same distance-vector routing protocol. RIP supports cross-platform distance vector routing whereas IGRP is a Cisco Systems proprietary distance vector routing protocol. Once a router has this information it is able to amend its own routing table to reflect the changes and then inform its neighbors of the changes. This process has been described as 'routing by rumor' because routers are relying on the information they receive from other routers and cannot determine if the information is actually valid and true. There are a number of features which can be used to help with instability and inaccurate routing information.

Example:

In this network we have 4 routers A, B, C, and D:

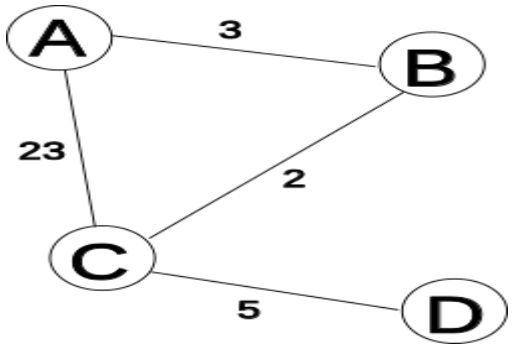

Fig 11.1 Network of four nodes

We shall mark the current time (or iteration) in the algorithm with T, and shall begin (at time 0, or T=0) by creating distance matrices for each router to its immediate neighbors. As we build the routing tables below, the shortest path is highlighted with the color green, a new shortest path is highlighted with the color yellow. Grey columns indicate nodes that are not neighbors of the current node, and are therefore not considered as a valid direction in its table. Red indicates invalid entries in the table since they refer to distances from a node to itself, or via itself.

T=0

from A	via A	via B	via C	via D
to A				
to B		3		
to C			23	
to D				

from B	via A	via B	via C	via D
to A	3			
to B				
to C			2	
to D				

from C	via A	via B	via C	via D
to A	23			
to B		2		
to C				
to D				5

from D	via A	via B	via C	via D
to A				
to B				
to C			5	
to D				

At this point, all the routers (A,B,C,D) have new "shortest-paths" for their DV (the list of distances that are from them to another router via a neighbor). They each broadcast this new DV to all their neighbors: A to B and C, B to C and A, C to A, B, and D, and D to C. As each of these neighbors receives this information, they now recalculate the shortest path using it.

For example: A receives a DV from C that tells A there is a path via C to D, with a distance (or cost) of 5. Since the current "shortest-path" to C is 23, then A knows it has a path to D that costs 23+5=28. As there are no other shorter paths that A knows about, it puts this as its current estimate for the shortest-path from itself (A) to D, via C.

T=1

from A	via A	via B	via C	via D
to A				
to B		3	25	
to C		5	23	
to D			28	

from B	via A	via B	via C	via D
to A	3		25	
to B				
to C	26		2	
to D			7	

from C	via A	via B	via C	via D
to A	23	5		
to B	26	2		
to C				
to D				5

from D	via A	via B	via C	via D
to A			28	
to B			7	
to C			5	
to D				

Again, all the routers have gained in the last iteration (at T=1) new "shortest-paths", so they all broadcast their DVs to their neighbors; This prompts each neighbor to re-calculate their shortest distances again.

For instance: A receives a DV from B that tells A there is a path via B to D, with a distance (or cost) of 7. Since the current "shortest-path" to B is 3, then A knows it has a path to D that costs 7+3=10. This path to D of length 10 (via B) is shorter than the existing "shortest-path" to D of length 28 (via C), so it becomes the new "shortest-path" to D.

T=2

from A	via A	via B	via C	via D
to A				
to B		3	25	
to C		5	23	
to D		10	28	

from B	via A	via B	via C	via D
to A	3		7	
to B				
to C	8		2	
to D	31		7	

from C	via A	via B	via C	via D
to A	23	5		33
to B	26	2		12
to C				
to D	51	9		5

from D	via A	via B	via C	via D
to A			10	
to B			7	
to C			5	
to D				

This time, only routers A and D have new shortest-paths for their DVs. So they broadcast their new DVs to their neighbors: A broadcasts to B and C, and D broadcasts to C. This causes each of the neighbors receiving the new DVs to re-calculate their shortest paths. However, since the information from the DVs doesn't yield any shorter paths than they already have in their routing tables, then there are no changes to the routing tables.

T=3

from A	via A	via B	via C	via D
to A				
to B		3	25	
to C		5	23	
to D		10	28	

from B	via A	via B	via C	via D
to A	3		7	
to B				
to C	8		2	
to D	13		7	

from C	via A	via B	via C	via D
to A	23	5		15
to B	26	2		12
to C				
to D	33	9		5

from D	via A	via B	via C	via D
to A			10	
to B			7	
to C			5	
to D				

None of the routers have any new shortest-paths to broadcast. Therefore, none of the routers *receive* any new information that might change their routing tables. The algorithm comes to a stop.

6.Conclusion:

Thus we have simulated network routing protocol DVR and also handled link failure during routing also student will get understand overview of data communication and implementation routing protocol in NS-2 with good exposure to TCP/IP Protocol suite

7.Viva Questions:

- Explain routing?
- Which are the different routing algorithms?
- Explain DVR?
- Explain how link failure is handled in DVR?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.

Computer Network

Experiment No. : 12

Study of Network Management Tool

Experiment No. 12

1. **Aim:** Study of Network Management Tool
2. **Objectives :** From this experiment, the student will be able to
    - To provide students overview of computer network and network management tools
    - To familiarize with the basic terminology of network management
    - To experience the designing and managing of network management

3. **Outcomes:** The learner will be able to
    - Allow the students to gain expertise in some specific areas of networking such as design and maintenance of individual network
    - Engage in higher studies and lifelong studies
    - Match industry requirement in network management

4. **Hardware / Software Required :** Ubuntu

5. **Theory:**
   Network Management Tools

The tremendous growth in scale and diversity of computer networks has made network management a complex and challenging task for network administrators. To manage computer networks tangibly and efficiently, specific management tools must be used to monitor the network activities and to preemptively determine the network behavior. Network management tools are usually based upon particular network management protocols. Most systems use open protocols. However, some network management tools are based upon vendor specific proprietary protocols. The network management capabilities provided with the tools are usually based upon the functionality supported by the network management protocols

Table 12.1 RMON2 MIB

RMON2 MIB Group	Functions
Protocol directory	Presents an inventory of protocol types capable of monitoring
Protocol distribution	Collects the relative amounts of octets and packets
Address mapping	Provides address translation between MAC addresses and network addresses on the interface
Network layer host	Provides network host traffic statistics
Network layer matrix	Provides traffic analysis between each pair of network hosts
Application layer host	Reports on protocol usage at the network layer or higher
Application layer matrix	Provides protocol traffic analysis between pairs of network hosts
User history collection	Provides user-specified history collection on alarm and configuration history
Probe configuration	Controls the configuration of probe parameters
RMON conformance	Describes the conformance requirements to RMON2 MIB

1. **Network Monitors**

One of the fundamental responsibilities of a network administrator is network monitoring.

Network monitors should have the ability to collect and analyze network traffic. A good system will allow you to generate log files and performance charts that detail your system's capabilities and responses. With this data, you can optimize your network configuration and be better prepared for faults. Some network monitors are designed with SNMP management capability to offer full view of the fundamental network issues. To minimize the network down-time, effective networking monitoring will alert network anomaly immediately.

2. **Network Scanners**

Network security vulnerabilities are being detected on a daily basis – over 10,000 in the last two years alone. Network scanner is one of the key element for network security. It checks network system, operating system and applications running on your network to identify vulnerabilities and possible security flaws that could expose your network to security compromise. To protect online assets and eliminate the risk to your business, some network scanners can also automate vulnerability assessment.

3. **Packet Filers**

Packet filters control access of data packets to a network by scanning the contents of the packet headers. A packet filter determines whether a packet should be allowed to go through a given point based on certain access control policies

Packet filtering is most commonly used as a first line of defense against attacks from machines outside your network. It has become a common and inexpensive method of security protection mechanism. However, packet filtering does guarantee the security of your network and internal data.

Dynamic packet filtering, also referred to as stateful inspection, is a firewall architecture that works at the network layer. Stateful inspection tracks each connection traversing all interfaces of the firewall and makes sure they are valid. A stateful firewall may examine the contents of the packet up through the application layer in order to determine more about the packet than just information about its source and destination. A stateful inspection firewall also monitors the state of the connection and compiles the information in a state table. Because of this, filtering decisions are based not only on administrator-defined rules but also on context that has been established by prior packets that have passed through the firewall.

6. Conclusion:

Thus at the end of this experiment student will able to understand Network management tools , network management protocols. However, some network management tools are based upon vendor specific proprietary protocols. The network management capabilities provided with the tools are usually based upon the functionality supported by the network management protocols.

7. Viva Questions:

- Explain network management functions?
- Explain network management protocols?
- Explain function of network management tools?
- Name two most widely used network management standards?

8. References:

- A.S. Tanenbaum, “Computer Networks”, Pearson Education, Fourth Edition.
- B.A. Forouzan, “Data Communications and Networking”, TMH, Fourth Edition.