Semester/Session	Even/ (2024-25)	Class	B.TECH VI CS1
Course Code	BCS 653	Course title	COMPUTER NETWORKING LAB
Hours	30	Hours per week	2
Faculty name		Contact details	
Course Description	The merging of computers and communications has had a profound influence. On the way computer systems are organized. The concept of the 'computer center' as a room with a large computer to which users bring their work for processing is now totally obsolete. The old model of a single computer serving all of the organization's computational needs has been replaced by one in which a large no. of separated but interconnected computers do the job. These systems are called computer networks. **Pre-Requisites**: Students should have knowledge of Computer Fundamental, Hardware, Basic of networking devices.		

Course Outcome and Bloom's Taxonomy

Course Outcomes	Bloom'sTaxonomy
CO1: Understand the concepts of different types of network topologies and transmission media, architecture of OSI and TCP/IP Model.	K1,K2
CO2: Analyze the network applications, management issues and security issues, routing algorithms.	K2,K4
CO3:Analyze and solve the IP addressing, subneting and classless addressing related problem.	K2,K3,k4
CO4: To understand the knowledge about Qos, VPN, Tunneling and to understand the wired and wireless network such as manet, wsn etc.	K2,K3,K4
CO5: Identify the security issue in the network and resolve it.To understand the knowledge of various protocols used at different layers of TCP/IP model.	K1,K4,K5,K2

Competencies/Skills to be developed

- Communication and Interpersonal skills
- Recognizing
- Problem Solving
- Critiquing
- Inventing
- Planning
- Prepare Documentation

CO-PO Mapping

Course Outcomes	Program Outcomes												Program Specific Outcomes		
	PO1	PO2	PO3	PO4	PO5	PO6	PO7	PO8	PO9	PO10	PO11	PO12	PSO1	PSO2	PSO3
CO1: Understand the concepts of different types of network topologies and transmission media, architecture of OSI and TCP/IP Model.	**3**	**-**	**-**	**2**	**1**	**-**	**-**	**-**	**-**	**-**	**-**	**-**	**2**	**3**	**-**
CO2:Analyze the network applications, management issues and security issues, routing algorithms.	**3**	-	-	**2**	-	-	-	-	-	-	-	-	**3**	**3**	-
CO3: Analyze and solve the IP addressing, subneting and classless addressing related problem.	**3**	-	-	**3**	**3**	-	-	-	-	-	-	-	**3**	**3**	-
CO4: To understand the knowledge about Qos, VPN, Tunneling and to understand the wired and wireless network such as manet,wsn etc.	**2**	-	-	**3**	**3**	-	-	-	-	-	-	-	**3**	**3**	-
CO5. Identify the security issue in the network and resolve it. To understand the knowledge of various protocols used at different layers of TCP/IP model.	**2**	-	-	**2**	-	-	-	-	-	-	-	-	**2**	**2**	-

CO-CIA Mapping

Course Outcomes	Components of Assessment					
	CIAI	CIAII	CIAIII	CIA V	CIAVI	
CO1: Understand the concepts of different types of network topologies and transmission media, architecture of OSI and TCP/IP Model.	YES	YES		YES		YES
CO2:Analyze the network applications, management issues and security issues, routing algorithms.	YES	YES		YES		YES
CO3: Analyze and solve the IP addressing, subneting and classless addressing related problem.	YES	YES		YES		YES
CO4: To understand the knowledge about Qos, VPN,	YES	YE		YES		YES

network such as manet,wsn etc.						
CO5: Identify the security issue in the network and resolve it. To understand the knowledge of various protocols used at different layers of TCP/IP model.	YES	YES		YES		YES

Course Outcomes	Components of Assessment					
	CEA I	CEAII	CEAIII	CEAIV	CEAV	CEA VI
CO1: Understand the concepts of different types of network topologies and transmission media, architecture of OSI and TCP/IP Model.	YES					
CO2:Analyze the network applications, management issues and security issues, routing algorithms.	YES					
CO3: Analyze and solve the IP addressing, subneting and classless addressing related problem.	YES					
CO4: To understand the knowledge about Qos, VPN, Tunneling and to understand the wired and wireless network such as manet,wsn etc.	YES					
CO5: Identify the security issue in the network and resolve it. To understand the knowledge of various protocols used at different layers of TCP/IP model.	YES					

LIST OF PROGRAM

S No	EXPERIMENT NAME	CO'S	DATE OF COMPLETION	FACULTY SIGNATURE
1	Study of different types of Network cables and Practically implement the cross-wired cable and straight through cable using clamping tool.	CO1		
2	Study of Network Devices in Detail.	CO2		
3	Assign the IP address for the network and also check the connectivity between the PC.	CO3		
4	Write a program to implement bit stuffing in Data Link Layer using C.	CO1		
5	Write a Program to implement Socket programming (TCP, UDP, RAW) Socket.	CO5		
6	To study the basic configuration command for router.	CO2		
7	Configure a Network using packet tracer software.	CO3		
8	Configure a Network using static routing protocol.	CO2		
9	Configure a Network using Distance Vector Routing protocol (RIP).	CO2		
10	Configure Network using Link State Routing (OSPF).	CO2		
11	Simulate and analyze Ethernet Protocols using Network Simulator 1.	CO4		
12	Simulate and analyze Token Ring mechanism using Network Simulator 1.	CO4		
13	Configuring wireless LAN access using packet tracer	CO4		
14	Write a Program to implement Remote Procedural Calls.	CO5		
15	Simulation of sliding window protocols.	CO1		

Resources

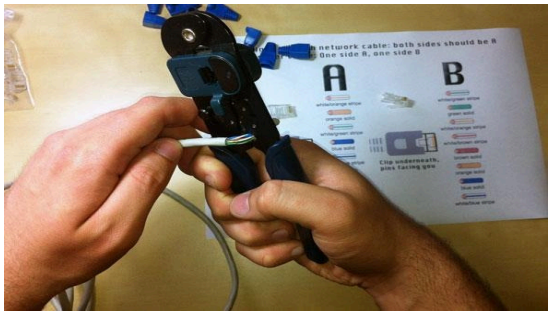
(1) Forouzen, "Data Communication and Networking", TMH
(2) A.S. Tanenbaum, Computer Networks, Pearson Education

OBJECTIVE- Study of different types of Network cables and practically implement the cross-wired cable and straight through cable using clamping tool.

APPARATUS (COMPONENTS):RJ-45 connector, Climping Tool, Twisted pair Cable

PROCEDURE:

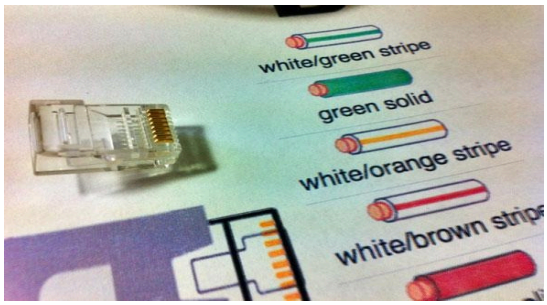
1. Strip about 1.5cm of cable shielding from both ends – your crimping tool should have a round area specifically for this task.



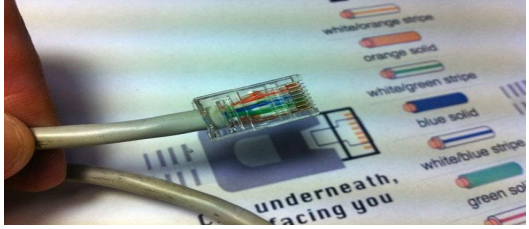
2. Untangle the wires (there should be 4 “twisted pairs”). Arrange them in the order shown on the sheet from top to bottom; one end should be in arrangement A, the other B.

©© 

3. When you’ve got the order correct, bunch them together in a line. If you have some that stick up beyond the others, use th crimping tool to crop them back to a uniform level. The hardest part is placing these into the RJ45 plug without messing up th order. Hold the plug with the clip side facing away from you; the gold pins should be facing towards you.



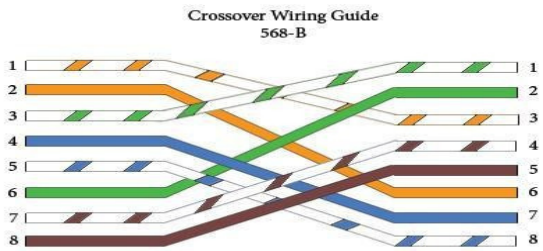
4. Push the cable right in – the notch at the end of the plug should just be over the cable shielding. If it isn’t, you stripped too much shielding off, so consider cropping the cables back a little more.



5. When the wires are sitting tightly in the plug, insert in into the end of your crimping tool and push down – in theory th crimper is shaped to the exact right size, but in practice I find pushing too hard can crack the brittle plastic plug.
crossover cable should be used when connecting hardware directly to a computer. A standard (straight through) cabl should be used when connecting hardware to a computer through an Ethernet hub or switch. A standard CAT 5 cable has

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

a 1-to-1 mapping of pins from one connector to another.



VIVA QUESTIONS

1. What is the use of straight through and cross over cable?
2. Differentiate between RJ45 and RJ11.

OBJECTIVE:Study of following Network Devices in Detail

a) Repeater
b) Hub
c) Switch
d) Bridge
e) Router
f) Gateway

APPARATUS (SOFTWARE): No software or hardware needed.

PROCEDURE: Following should be done to understand this practical.

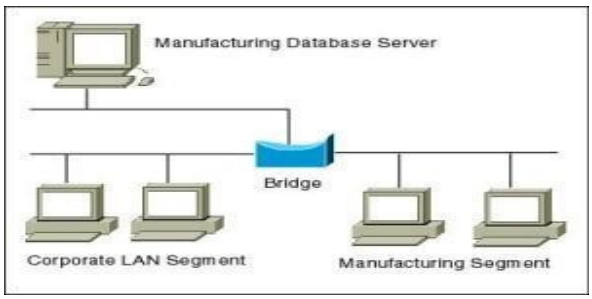
1. **REPEATER:** Functioning at Physical Layer. A repeater is a device similar to the Hub, but has additional features. It also works in the Physical layer. The repeaters are used in places where amplification of input signal is necessary. But, the kind of amplification done by the repeater is different 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.

2. **HUB:** Hub is one of the basic icons of networking devices which works at physical layer and hence connect networking devices physically together. Hubs are fundamentally used in networks that use twisted pair cabling to connect devices. They are designed to transmit the packets to the other appended devices without altering any of the transmitted packets received. They act as pathways to direct electrical signals to travel along. They transmit the information regardless of the fact if data packet is destined for the device connected or not.

3. **SWITCH:** Switches are the linkage points of an Ethernet network. Just as in hub, devices in switches are connected to them through twisted pair cabling. But the difference shows up in the manner both the devices; hub and a switch treat the data they receive. a **switch** transfers it only to that port which is connected to the destination device. A switch does so by having an in-built learning of the MAC address of the devices connected to it. Since the transmission of data signals are well defined in a **switch** hence the network performance is consequently enhanced. Switches operate in **full-duplex** mode where devices can send and receive data from the switch at the simultaneously unlike in half-duplex mode. The transmission speed in switches is double than in Ethernet hub transferring a 20Mbps connection into 30Mbps and a 200Mbps connection to become 300Mbps. Performance improvements are observed in networking with the extensive usage of switches in the modern days.

4. **BRIDGE:** A bridge is a computer networking device that builds the connection with the other bridge networks which use the same protocol. It works at the Data Link layer of the OSI Model and connects the different networks together and develops communication between them. It connects two local-area networks; two physical LANs into larger logical LAN or two segments of the same LAN that use the same protocol. Apart from building up larger networks, bridges are also used to segment larger networks into smaller portions. The bridge does so by placing itself between the two portions of two physical networks and controlling the flow of the data between them. Bridges nominate to forward the data after inspecting into the MAC address of the devices connected to every

shave been introduced that build a list of the MAC addresses on the interface by observing the traffic on the network. This is a leap in the development field of manually recording of MAC addresses.



5. **ROUTER:** Routers are network layer devices and are particularly identified as Layer- 3 devices of the OSI Model. They process logical addressing information in the Network header of a packet such as IP Addresses. Router is used to create larger complex networks by complex traffic routing. It has the ability to connect dissimilar LANs on the same protocol. It also has the ability to limit the flow of broadcasts. A router primarily comprises of a hardware device or a system of the computer which has more than one network interface and routing software.

FUNCTIONALITY:

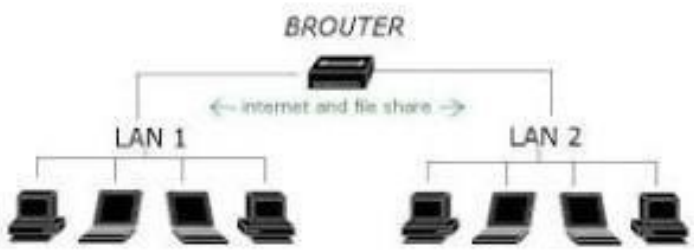
When a router receives the data, it determines the destination address by reading the header of the packet. Once the address is determined, it searches in its **routing table** to get know how to reach the destination and then forwards the packet to the higher hop on the route. The hop could be the final destination or another router.

Routing tables play a very pivotal role in letting the router makes a decision. Thus a routing table is ought to be updated and complete. The two ways through which a router can receive information are:

- **Static Routing**: In static routing, the routing information is fed into the routing tables manually. It does not only become a time-taking task but gets prone to errors as well. The manual updating is also required in case of statically configured routers when change in the topology of the network or in the layout takes place. Thus static routing is feasible for tinniest environments with minimum of one or two routers.

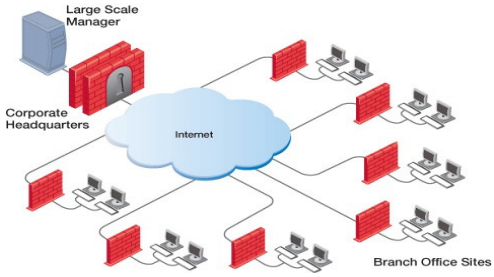
1. **Dynamic Routing**: For larger environment dynamic routing proves to be the practical solution. The process involves use of peculiar routing protocols to hold communication. The purpose of these protocols is to enable the other routers to transfer information about to other routers, so that the other routers can build their own routing tables.

2. Brouters: Brouters are the combination of both the bridge and routers. They take up the functionality of the both networking devices serving as a bridge when forwarding data between networks, and serving as a router when routing data to individual systems. Brouter functions as a filter that allows some data into the local network and redirects unknown data to the other network.Brouters are rare and their functionality is embedded into the routers functioned to act as bridge as well.



3. **GateWay:**Gateway is a device which is used to connect multiple networks and passes packets from one packet to the other network. Acting as the 'gateway' between different networking systems or computer programs, a

gateway, since it interprets data from one network protocol to another.



Others such as bridge converts the data into different forms between two networking systems. Then a software application converts the data from one format into another. Gateway is a viable tool to translate the data format, although the data itself remains unchanged. Gateway might be installed in some other device to add its functionality into another.

4. Network card: Network cards also known as Network Interface Cards (NICs) are hardware devices that connect a computer with the network. They are installed on the mother board. They are responsible for developing a physical connection between the network and the computer. Computer data is translated into electrical signals send to the network via Network Interface Cards.

They can also manage some important data-conversion function. These days network cards are software configured unlike in olden days when drivers were needed to configure them. Even if the NIC doesn't come up with the software then the latest drivers or the associated software can be downloaded from the internet as well.

VIVA QUESTIONS

1.What is the difference between switch and router?
2.in which layer gateway works?

OBJECTIVE: Assign the IP address for the network and also check the connectivity between the PC.

APPARATUS (SOFTWARE): NA

PROCEDURE:

1. Assign the IP address for the network
2. Classification of IP address
3. Sub netting

As show in figure we teach how the ip addresses are classified and when they are used.

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

Address-The unique number ID assigned to one host or interface in a network.
Subnet- A portion of a network that shares a particular subnet address
Subnet mask-A 32-bit combination used to describe which portion of an address refers to the subnet and which part refers to the host
Interface- A network connection

VIVA QUESTIONS

1.What are the different addressing schemes to identify a machine on a network?
2.What is loop back address?

OBJECTIVE : Write a program to implement bit stuffing in Data Link Layer using C.

THEORY & CONCEPT

Bit stuffing

- When data is transmitted, the transmitting node should distinguish between the start and the end of the data for the receiving node to read the data completely. This is accomplished by appending a unique pattern of bit stream before and after the data..
- Take care to ensure that this unique pattern does not occur in the data. If the pattern appears in the data, it gets broken. The process of appending a unique pattern and breaking the pattern is known as framing.
- Bit Stuffing is a framing method in which each frame begins and ends with a special bit pattern '01111110', called a flag byte.
- Whenever the sender's data link layer encounters five consecutive 1's in the data, it automatically stuffs a 0 bit into the outgoing bit stream to break the pattern.
  This is the data stream for which the Bit Stuffing works is inputted. The data should be in binary format (1or 0).

VIVA QUESTIONS

Q1. What is the difference between bit stuffing and byte stuffing?
Q2. Why stuffing of bits is required to make proper communication?

OBJECTIVE: Write a Program to implement Socket programming (TCP, UDP, RAW) Socket.

APPARATUS USED (SOFTWARE): C Language

THEORY AND CONCEPT: Sockets provide an interface for programming networks at the transport layer. Network communication using Sockets is very much similar to performing file I/O. In fact, socket handle is treated like file handle. The streams used in file I/O operation are also applicable to socket-based I/O. Socket-based communication is independent of a programming language used for implementing it. That means, a socket program written in Java language can communicate to a program written in non-Java (say C or C++) socket program. A server (program) runs on a specific computer and has a socket that is bound to a specific port. The server listens to the socket for a client to make a connection request (see Fig. 13.4a). If everything goes well, the server accepts the connection (see Fig. 13.4b). Upon acceptance, the server gets a new socket bound to a different port. It needs a new socket (consequently a different port number) so that it can continue to listen to the original socket for connection requests while serving the connected client.

Sample Program (TCP Socket)

Echo Server:

```
import java.io.*;
import java.net.*;
public class EchoServer
{
	public EchoServer(int portnum)
	{
		try
		{
			server = new ServerSocket(portnum);
		}
		catch (Exception err)
		{
			System.out.println(err);
		}
	}
	public void serve()
	{	try
		{	while (true)
			{	Socket client = server.accept();
				BufferedReader r = new BufferedReader(new InputStreamReader(client.getInputStream()));
				PrintWriter w = new PrintWriter(client.getOutputStream(), true);
				w.println("Welcome to the Java EchoServer. Type 'bye' to close.");
				String line;
				do
				{
					line = r.readLine();
					if ( line != null )
						w.println("Got: "+ line);
				}
				while ( !line.trim().equals("bye") );
				client.close();
			} }
		catch (Exception err)
		{	System.err.println(err);
```

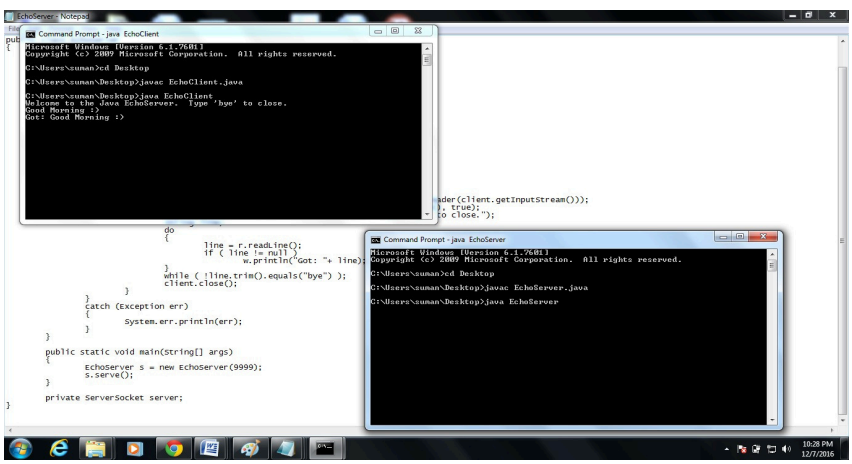
```
public static void main(String[] args)
{       EchoServer s = new EchoServer(9999);
}   private serve();ServerSocket
server;


}
```

EchoClient:

```
import java.io.*;
import java.net.*;
public class EchoClient
{
        public static void main(String[] args)
        {
                try
                {
        Socket s = new Socket("127.0.0.1", 9999);
        BufferedReader r = new BufferedReader (new InputStreamReader(s.getInputStream()));
        PrintWriter w = new PrintWriter(s.getOutputStream(), true);
        BufferedReader con = new BufferedReader(new InputStreamReader(System.in));
        String line;
                        do
                        {       line = r.readLine();
                                if ( line != null )
                                        System.out.println(line);
                                line = con.readLine();
                                w.println(line);
                        }
                        while ( !line.trim().equals("bye") );
                }
                catch (Exception err)
                {
                        System.err.println(err);
                }
        }
}
```

Output:



VIVA QUESTIONS

1.What is a socket? In which layer socket works?
2.Do we use socket in UDP?

OBJECTIVE : To study the Basic Configuration Command for Router.

APPARATUS (SOFTWARE): Cisco Packet Tracer

THEORY AND CONCEPT:

Cisco router is a device that switches data packets between two different networks. By default two different IP network cannot communicate with each other. They need a mediator device that exchanges their packets. Routers do this job successfully by taking packet from one network and delivering it to another network. This process is called routing. We need to perform some initial configurations on router before it can be used for routing. In this article we will explain these configurations. We will use Packet Tracer network simulator software for demonstration. Beside Packet Tracer You can also use any other network simulator software such as Boson, GNS or even better if you can afford, use a real Cisco device. No matter what option you choose, till this uses Cisco IOS output will be same. We have created this topology to give you a better overview of commands. You can use single router if you are unable to replicate this topology in packet tracer. Alternatively you can download this pre-created topology.

Access CLI prompt of router

Cisco IOS supports various command modes, among those followings are the main command modes.

- User EXEC Mode
- Privileged EXEC Mode
- Global Configuration Mode
- Interface Configuration Mode
- Sub Interface Configuration Mode
- Setup Mode
- ROM Monitor Mode

You need to execute specific commands to navigate from one mode to another.

Mode	Prompt	Command to enter	Command to exit
User EXEC	Router >	Default mode after booting. Login with password, if configured.	Use **exit** command
Privileged EXEC	Router #	Use **enable** command from user exec mode	Use **exit** command
Global Configuration	Router(config)#	Use **configure terminal** command from privileged exec mode	Use **exit** command
Interface Configuration	Router(config-if)#	Use **interface type number** command from global configuration mode	Use **exit** command to return in global configuration mode
Sub-Interface Configuration	Router(config-subif)	Use **interface type sub interface number** command from global configuration mode or interface configure mode	Use **exit** to return previous mode. Use **end** command to return in privileged exec mode.
Setup	Parameter[Parameter value]:	Router will automatically insert in this mode if running configuration is not present	Press **CTRL+C** to abort. Type **yes** to save configuration, or **no** to exit without saving when asked in the end of setup.

		privileged exec mode. Press **CTRL + C** key combination during the first 60 seconds of booting process	

- IOS commands are not case sensitive; you can enter them in uppercase, lowercase, or mixed case.
- Password is case sensitive. Make sure you type it in correct case.
- In any mode, you can obtain a list of commands available on that mode by entering a QUESTIONS mark (?).
- Standard order of accessing mode is
  User Exec mode => Privileged Exec mode => Global Configuration mode => Interface Configuration mode => Sub Interface Configuration mode
- Router will enter in setup mode only if it fails to load a valid running configuration.
- Router will enter in ROMMON mode only if it fails to load a valid IOS image file.
- You can manually enter in ROMMON mode for diagnostics purpose.

Enter in global configuration mode to execute following commands.
Change default router name
By default Router name is configured on routers. We can configure any desired name on router. hostname command will change the name of router. For example following command will assign LAB1name to the router.

```
Router(config)#hostname LAB1
LAB1(config)#
```

Configure password on cisco router

Router is a critical device of network. It supports multiple lines for connection. We need to secure each line [port].

Secure console port

Command	Description
Router(config)#line console 0	Move in console line mode
Router(config-line)#password console	Set console line password to CNN
Router(config-line)#login	Enable password authentication for console line

Enable telnet access on cisco router. Depending on the model number and IOS software version router may supports various number
VTY connections range from 5 to 1000. VTY is the standard name for telnet and SSH connection. By default only first five VTY
connections are enabled. But you cannot connect them. When you try to connect them remotely you will get following messag
Password required but none set This message indicates that password is not set on VTY lines. Password is required to connect VTY
Following commands set password to TELCNN on VTYs line.

Command	Description
Router(config)#line vty 0 4	Move into all five VTYs line
Router(config-line)#password TELCNN	Set password to TELCNN on all five lines
Router(config-line)#login	Configure VTYs to accept telnet connection

In above example we set password on all five lines collectively but you can do this separately if you need different passwords for different lines. Steps will be same.

1. **line vty [line number]** command will move into that specific line.
2. **password [password]** command will assign the desired password.
3. **login** command will enable that line to accept the connection.

packet tracer. You can practise with banner motd command. Both commands work in same manner. Only the difference between these commands is the place of display. MOTD banner will display before the login. An EXEC banner will display after the authentication process and before the exec mode. Both commands use delimiting character to specify the starting and ending of message. It means command parser will terminate the message on delimiting character instead of the Enter key. This feature allows us to span the message in multiple lines. Configure clock time zone Router allows us to localize the time zone. Following command will set time zone to +5 hour of EST [Eastern Standard Time].

Router(config)#clock timezone EST 05

Assign hostname to IP Address Hostname are easy to remember. We can use host name instead of their IP address while connecting with remote address. Router resolves IP address to hostname in two ways: static and dynamic. In static method we have to assign hostname to IP address. In dynamic method we have to configure an external DNS server and need to configure its IP address on router. show hosts command will display the currently configured hosts with their IP addresses. Following figure illustrate an example of static entry for hostname. Configure serial interface in router Serial interface is used to connect wan network. Following command will configure serial 0/0/0 interface.

Command	**Description**
Router(config)#interface serial 0/0/0	Enter into serial interface 0/0/0 configuration mode
Router(config-if)#description Connected to bhilwara	Optional command. It set description on interface that is locally significant
Router(config-if)#ip address 10.0.0.1 255.0.0.0	Assigns address and subnet mask to interface
Router(config-if)#clock rate 64000	DCE side only command. Assigns a clock rate for the interface
Router(config-if)#bandwidth 64	DCE side only command. Set bandwidth for the interface.
Router(config-if)#no shutdown	Turns interface on

Serial cable is used to connect serial interfaces. One end of serial cable is DCE while other end is DTE. You only need to provide clock rate and bandwidth in DCE side.

Configure Fast Ethernet Interface in router

Usually Fast Ethernet connects local network with router. Following commands will configure Fast Ethernet 0/0 interface.

Command	**Description**
Router(config)#interface fast Ethernet 0/0	Enter into the Fast Ethernet 0/0 interface.
Router(config-if)#description Development department	This command is optional. It will set description on interface.
Router(config-if)#ip address 192.168.0.1 255.255.255.0	Assigns address and subnet mask to interface
Router(config-if)#no shutdown	Turns interface on. All interfaces are set to off on startup.

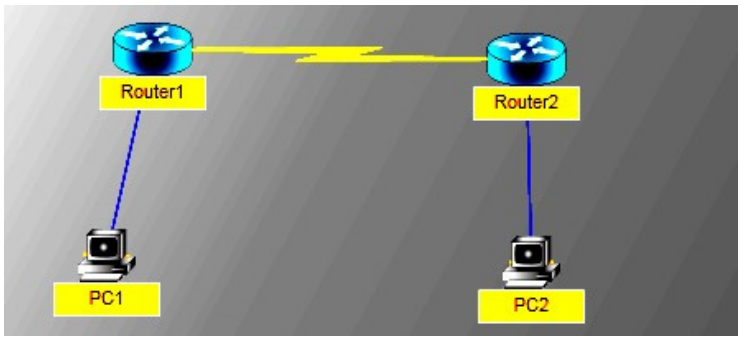
VIVA QUESTIONS

1.What is the command to configure a router?

2.In LAN configuration do we use router?

OBJECTIVE:Configure a Network using packet tracer software

LAB WORK : Configure the following network, assign the IP address to PCs and routers.



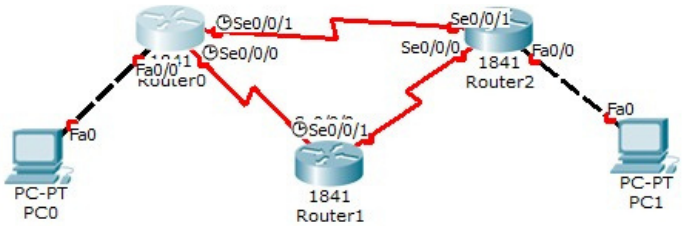
VIVA QUESTIONS

Q1. What's new in Packet Tracer 6.3?
Q2. How can I obtain Packet Tracer?

OBJECTIVE: Configure a Network using static routing protocol.

APPARATUS (SOFTWARE): Ciscopacket tracer software

THEORY AND CONCEPT: Static routing is a form of routing that occurs when a router uses a manually-configured routing entry, rather than information from a dynamic routing traffic. In many cases, static routes are manually configured by a network administrator by adding in entries into a routing table, though this may not always be the case. Unlike dynamic routing, static routes are fixed and do not change if the network is changed or reconfigured. Static routing and dynamic routing are not mutually exclusive. Both dynamic routing and static routing are usually used on a router to maximise routing efficiency and to provide backups in the event that dynamic routing information fails to be exchanged. Static routing can also be used in stub networks, or to provide a gateway of last resort.



Device	Interface	IP Configuration	Connected with
PC0	Fast Ethernet	10.0.0.2/8	Router0's Fa0/1
Router0	Fa0/1	10.0.0.1/8	PC0's Fast Ethernet
Router0	S0/0/1	192.168.1.254/30	Router2's S0/0/1
Router0	S0/0/0	192.168.1.249/30	Router1's S0/0/0
Router1	S0/0/0	192.168.1.250/30	Router0's S0/0/0
Router1	S0/0/1	192.168.1.246/30	Router2's S0/0/0
Router2	S0/0/0	192.168.1.245/30	Router1's S0/0/1
Router2	S0/0/1	192.168.1.253/30	Router0's S0/0/1
Router2	Fa0/1	20.0.0.1/30	PC1's Fast Ethernet
PC1	Fast Ethernet	20.0.0.2/30	Router2's Fa0/1

1. Assign IP address to PCs

Double click PC0 and click Desktop menu item and click IP Configuration. Assign IP address 10.0.0.2/8 to PC0. Repeat same process for PC1 and assign IP address 20.0.0.2/8.

2. Assign IP address to interfaces of routers

Double click Router0 and click CLI and press Enter key to access the command prompt of Router0.
Three interfaces FastEthernet0/0, Serial0/0/0 and Serial0/0/1 of Router0 are used in this topology. By default interfaces on router are remain administratively down during the start up.

We need to configure IP address and other parameters on interfaces before we could actually use them for routing.

Interface mode is used to assign IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

commands will assign IP address on FastEthernet0/0.

```
Router(config)#interface fastEthernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

interface fastEthernet 0/0 command is used to enter in interface mode.
ip address 10.0.0.1 255.0.0.0 command will assign IP address to interface.
no shutdown command will bring the interface up.
exit command is used to return in global configuration mode.

3. Assign IP address to serial interface.

Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface serial 0/0/0 Router(config-if)#ip address 192.168.1.249 255.255.255.252 Router(config-if)#clock rate 64000 Router(config-if)#bandwidth 64 Router(config-if)#no shutdown Router(config-if)#exit Router(config)#interface serial 0/0/1 Router(config-if)#ip address 192.168.1.254 255.255.255.252 Router(config-if)#clock rate 64000 Router(config-if)#bandwidth 64 Router(config-if)#no shutdown Router(config-if)#exit Router(config)# Router#configure terminal Command is used to enter in global configuration mode. Router(config)# interface serial 0/0/0 Command is used to enter in interface mode. Router(config-if)#ip address 192.168.1.249 255.255.255.252 Command assigns IP address to interface. For serial link we usually use IP address from /30 subnet. Router(config-if)#clock rate 64000 And Router(config-if)#bandwidth 64 In real life environment these parameters control the data flow between serial links and need to be set at service providers end. In lab environment we need not to worry about these values. We can use these values. Router(config-if)#no shutdown Command brings interface up. Router(config-if)#exit Command is used to return in global configuration mode.

We will use same commands to assign IP addresses on interfaces of remaining routers. We need to provided clock rate and bandwidth only on DCE side of serial interface. Following command will assign IP addresses on interface of

Router1.

```
Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.1.250 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.246 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
```

Command to configure the static route

We have two commands to configure the static route.

Router(config)# ip route destination_network_# [subnet_mask] IP_address_of_next_hop_neighbor [administrative_distance] [permanent]

Or

Router(config)# ip route destination_network_# [subnet_mask] interface_to_exit [administrative_distance] [permanent]

ip route.

This is the base command that adds new routes in routing table. destination_network_#[subnet_mask] This is the first parameter. It specifies the destination network address. We need to provide subnet mask if we are using sub-network. Sub-networks are the smaller network created from one large network in subnetting. If we are not using sub-network then we can omit the subnet mask value. It will parse automatically.

IP_address_of_next_hop_neighbor / interface_to_exit

This parameter provides a way to reach the destination network. Both commands use separate way to assign this value.

First command provides the IP address of next hop neighbor. It tells router that if it receives a packet for destination [that we set in previous parameter], forward that packet to this next hop neighbor IP address.

Second command also do the same job but in different way. It specifies exit interface instead of next hop IP address. It tells router that if it receives a packet for the destination specified by previous parameter then exits that packet from this interface. Device attached on other end of this interface will take care of the packet.

Configure Static Route

By default when a packet arrives in interface, router checks destination filed in packet and compare it with routing table. If it finds a match for destination network then it will forward that packet from related interface. If it does not find a match in routing table then it will discard that packet. This is the default behavior of router. We do not need to configure directly connected networks.

Run following command from global configuration mode in routers.

Router0

Router(config)#ip route 20.0.0.0 255.0.0.0 192.168.0.254

This command instructs router that when you receive a packet for 20.0.0.0 network give it to 192.168.0.254. Network 10.0.0.0 is directly connected so we do not need to configure it here.

Router1

Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.0.253

Router(config)#ip route 20.0.0.0 255.0.0.0 192.168.0.250

On this router both networks are reachable via other routers so we need to configure route for both networks 10.0.0.0 and 20.0.0.0.

Router2

Router(config)#ip route 10.0.0.0 255.0.0.0 192.168.0.249

Router(config)#ip route 20.0.0.0 255.0.0.0 192.168.0.246

Same as Router1 again we need configure route for both networks on this router.

VIVA QUESTIONS

1.Differentiate between dynamic and static routing?

2.How to implement static routing?

OBJECTIVE- Configure a Network using Distance Vector Routing protocol (RIP).

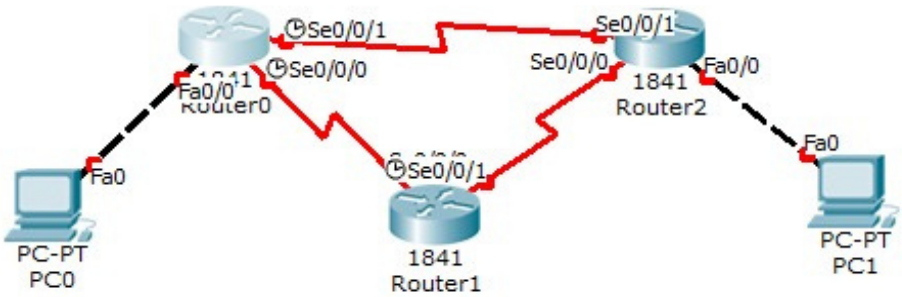
APPARATUS (SOFTWARE): Ciscopacket tracer software

THEORY:

RIP is a routing protocol which exchanges network information between routers dynamically. It uses broadcast to share routing information. Routers aware only about the networks those are directly connected with them. For example in following network R1 only aware about the 10.0.0.0/8 and 192.168.1.252/30 network.

PROCEDURE:

1. Develop a Topology shown in figure given below.
2. Configure all Routers
3. Implement RIP protocols in Router to configure Network.



Device	Interface	IP Configuration	Connected with
PC0	Fast Ethernet	10.0.0.2/8	Router0's Fa0/1
Router0	Fa0/1	10.0.0.1/8	PC0's Fast Ethernet
Router0	S0/0/1	192.168.1.254/30	Router2's S0/0/1
Router0	S0/0/0	192.168.1.249/30	Router1's S0/0/0
Router1	S0/0/0	192.168.1.250/30	Router0's S0/0/0
Router1	S0/0/1	192.168.1.246/30	Router2's S0/0/0
Router2	S0/0/0	192.168.1.245/30	Router1's S0/0/1
Router2	S0/0/1	192.168.1.253/30	Router0's S0/0/1
Router2	Fa0/1	20.0.0.1/30	PC1's Fast Ethernet
PC1	Fast Ethernet	20.0.0.2/30	Router2's Fa0/1

Assign IP address to PCs

Double click PC0 and click Desktopmenu item and click IP Configuration. Assign IP address 10.0.0.2/8 to PC0. Repeat same process for PC1 and assign IP address 20.0.0.2/8.

Assign IP address to interfaces of routers

Double click Router0and click CLI and press Enter key to access the command prompt of Router0.
Three interfaces FastEthernet0/0, Serial0/0/0 and Serial0/0/1 of Router0 are used in this topology. By default interfaces on router are remain administratively down during the start up.

We need to configure IP address and other parameters on interfaces before we could actually use them for routing.

Interface mode is used to assign IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#

From global configuration mode we can enter in interface mode. From there we can configure the interface. Following commands will assign IP address on FastEthernet0/0.

Router(config)#interface fast Ethernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#

interface fast Ethernet 0/0 command is used to enter in interface mode.
ip address 10.0.0.1 255.0.0.0 command will assign IP address to interface.
no shutdown command will bring the interface up.
exit command is used to return in global configuration mode.

Assign IP address to serial interface.

Router#configure terminal Enter configuration commands, one per line. End with CNTL/Z. Router(config)#interface serial 0/0/0 Router(config-if)#ip address 192.168.1.249 255.255.255.252 Router(config-if)#clock rate 64000 Router(config-if)#bandwidth 64 Router(config-if)#no shutdown Router(config-if)#exit Router(config)#interface serial 0/0/1 Router(config-if)#ip address 192.168.1.254 255.255.255.252 Router(config-if)#clock rate 64000 Router(config-if)#bandwidth 64 Router(config-if)#no shutdown Router(config-if)#exit Router(config)# Router#configure terminal Command is used to enter in global configuration mode. Router(config)#interface serial 0/0/0 Command is used to enter in interface mode.

Router(config-if)#ip address 192.168.1.249 255.255.255.252 Command assigns IP address to interface. For serial link
we usually use IP address from /30 subnet.

Router(config-if)#clock rate 64000 And Router(config-if)#bandwidth 64 In real life environment these parameters
control the data flow between serial links and need to be set at service providers end. In lab environment we need not to worry about these values. We can use these values.

Router(config-if)#no shutdown Command brings interface up.
Router(config-if)#exit Command is used to return in global configuration mode.

We will use same commands to assign IP addresses on interfaces of remaining routers. We need to provided clock rate and bandwidth only on DCE side of serial interface. Following command will assign IP addresses on interface of Router1.

Router>enable
Router#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0

Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.1.246 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Use same commands to assign IP addresses on interfaces of Router2.

4. Configure RIP routing protocol

- Configuration of RIP protocol is much easier than you think. It requires only two steps to configure the RIP routing.
- Enable RIP routing protocol from global configuration mode.
- Tell RIP routing protocol which networks you want to advertise. Let's configure it in Router0

Router0 Router0(config)#router rip Router0(config-router)# network 10.0.0.0 Router0(config-router)# network 192.168.1.252 Router0(config-router)# network 192.168.1.248 router rip command tell router to enable the RIP routing protocol. network command allows us to specify the networks which we want to advertise. We only need to specify the networks which are directly connected with the router. Similarly for other routers. Our network is ready to take the advantage of RIP routing. To verify the setup we will use ping command. ping command is used to test the connectivity between two devices. Access the command prompt of PC1 and use ping command to test the connectivity from PC0.

VIVA QUESTIONS

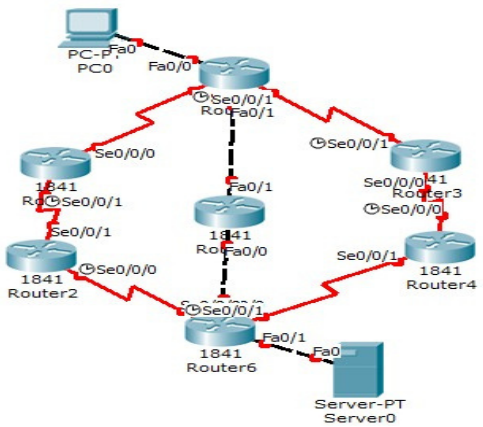
1. Which algorithm is implemented by RIP?
2.How the routing table is generated in RIP?

OBJECTIVE: Configure Network using Link State Vector Routing protocol (OSPF)

APPARATUS (SOFTWARE): Packet Tracer Software

PROCEDURE:

- Develop a Topology shown in figure given below.
- Configure all the workstations
- Configure all switches
- Configure all Routers
- Implement OSPF protocols in Router to configure Network.



Device	Interface	IP Configuration	Connected with
PC0	Fa0/0	10.0.0.2/8	Router0's Fa0/0
Router0	Fa0/0	10.0.0.1/8	PC0's Fa0/0
Router0	Fa0/1	192.168.1.1/30	Router5's Fa0/1
Router5	Fa0/1	192.168.1.2/30	Router0's Fa0/1
Router5	Fa0/0	192.168.1.5/30	Router6's F0/0
Router6	Fa0/0	192.168.1.6/30	Router5's Fa0/0
Router6	Fa0/1	20.0.0.1/8	Server0's Fa0/0
Server0	Fa0/0	20.0.0.2/8	Router6's Fa0/1
Router0	Serial 0/0/0 (DCE)	192.168.0.1/30	Router1's Se0/0/0
Router1	Serial 0/0/0	192.168.0.2/30	Router0's Se0/0/0
Router1	Serial 0/0/1 (DCE)	192.168.0.5/30	Router2's Se0/0/1
Router2	Serial0/0/1	192.168.0.6/30	Router1's Se0/0/1
Router2	Serial 0/0/0 (DCE)	192.168.0.9/30	Router6's Se0/0/0
Router6	Serial 0/0/0	192.168.0.10/30	Router2's Se0/0/0
Router0	Serial 0/0/1	192.168.2.1/30	Router3's Se0/0/1
Router3	Serial 0/0/1 (DCE)	192.168.2.2/30	Router0's Se0/0/1
Router3	Serial 0/0/0	192.168.2.5/30	Router4's Se0/0/0
Router4	Serial 0/0/0 (DCE)	192.68.2.6/30	Router3's Se0/0/0
Router4	Serial 0/0/1	192.168.2.9/30	Router6's Se0/0/1
Router6	Serial0/0/1 (DCE)	192.168.2.10/30	Router4's Se0/0/1

Double click PC0 and click Desktop menu item and click IP Configuration. Assign IP address 10.0.0.2/8 to PC0. Repeat same process for Server0 and assign IP address 20.0.0.2/8.

6. Assign IP address to interfaces of routers

Double click Router0 and click CLI and press Enter key to access the command prompt of Router0. Four interfaces FastEthernet0/0, FastEthernet0/1, Serial 0/0/0 and Serial0/0/1 of Router0 are used in this topology. By default interfaces on router are remain administratively down during the start up.

We need to configure IP address and other parameters on interfaces before we could actually use them for routing.

Interface mode is used to assign the IP address and other parameters. Interface mode can be accessed from global configuration mode. Following commands are used to access the global configuration mode.

```
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#
```

From global configuration mode we can enter in interface mode. From there we can configure the interface. Following commands will assign IP address on FastEthernet0/0 and FastEthernet0/1.

```
Router(config)#interface fast Ethernet 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface fast Ethernet 0/1
Router(config-if)#ip address 192.168.1.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#
```

interface fast Ethernet 0/0 command is used to enter in interface mode.

ip address 10.0.0.1 255.0.0.0 command would assign IP address to interface.
no shutdown command would bring the interface up.
exit command is used to return in global configuration mode.
Serial interface needs two additional parameters clock rate and bandwidth. Every serial cable has two ends DTE and DCE. These parameters are always configured at DCE end.

Now we have necessary information let's assign IP address to serial interfaces.

```
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface serial 0/0/0
Router(config-if)#ip address 192.168.0.1 255.255.255.252
Router(config-if)#clock rate 64000
Router(config-if)#bandwidth 64
Router(config-if)#no shutdown
Router(config-if)#exit
Router(config)#interface serial 0/0/1
Router(config-if)#ip address 192.168.2.1 255.255.255.252
Router(config-if)#no shutdown
Router(config-if)#exit
```

Router#configure terminal Command is used to enter in global configuration mode.

Router(config)#interface serial 0/0/0 Command is used to enter in interface mode.

usually use IP address from /30 subnet. Router(config-if)#clock rate 64000 In real life environment this parameter controls the data flow between serial links and need to be set at service provider's end. In lab environment we need not to worry about this value. We can use any valid clock rate here. Router(config-if)#bandwidth 64 Bandwidth works as an influencer. It is used to influence the metric calculation of OSPF or any other routing protocol which uses bandwidth parameter in route selection process. Serial interface has default bandwidth of 1544Kbps. To explain, how bandwidth influence route selection process we will configure (64Kbps) bandwidth on three serial DCE interfaces of our network; R0's Se0/0/0, R1's Se0/0/1 and R2's Se0/0/0.

Router(config-if)#no shutdown Command brings interface up.

Router(config-if)#exit Command is used to return in global configuration mode. We will use same commands to assign IP addresses on interfaces of remaining routers.

Command Line Interface

Router 1 Router>enable Router # configure terminal enter configuration commands, one per line. End with CNTL/Z. Router (config) #interface serial 0/0/0 Router (config-if) #ip address 192.168.0.2 255.255.255.252 Router (config-if) # exit Router (config) #interface serial 0/0/1 Router (config-if) #ip address 192.168.0.5 255.255.255.252 Router (config-if) #clock rate 64000 Router (config-if) #bandwidth 64 Router (config-if) #no shutdown Router (config-if) #exit

Router 2

Router 2

Router>enable
Router # configure terminal
enter configuration commands, one per line. End with CNTL/Z.
Router (config) #interface serial 0/0/0
Router (config-if) #ip address 192.168.0.9 255.255.255.252
Router (config-if) #clock rate 64000
Router (config-if) #no shutdown
Router (config-if) #exit
Router (config-if) #
Router (config) #interface serial 0/0/1
Router (config-if) #ip address 192.168.0.6 255.255.255.252
Router (config-if) #no shutdown
Router (config-if) #exit
Router (config-if) #

Router 6

IOS Command Line Interface

Router>enable
Router # configure terminal
enter configuration commands, one per line. End with CNTL/Z.
Router (config) #interface serial 0/0/0
Router (config-if) #ip address 192.168.0.10 255.255.255.252

Router (config-if) #exit
Router (config) #interface serial 0/0/1
Router (config-if) #ip address 192.168.2.10 255.255.255.252
Router (config-if) #clock rate 64000
Router (config-if) #no shutdown
Router (config-if) #exit
Router (config-if) #interface fastethernet 0/0
Router (config-if) #ip address 192.168.1.16 255.255.255.252
Router (config-if) #no shutdown
Router (config-if) #exit
Router (config-if) #interface fast ethernet 0/1
Router (config-if) #ip address 20.0.0.1 255.0.0.0
Router (config-if) #no shutdown
Router (config-if) #exit

Configure OSPF routing protocol

Enabling OSPF is a two steps process:-

- Enable OSPF routing protocol from global configuration mode.
- Tell OSPF which interfaces we want to include.

For these steps following commands are used respectively.
Router(config)# router ospf process_ID
Router(config-router)# network IP_network_# [wild card mask] Area Number area number

Router(config)# router ospf process ID

This command will enable OSPF routing protocol in router. Process ID is a positive integer. We can use any number from 1 to 65,535. Process ID is locally significant. We can run multiple OSPF process on same router. Process ID is used to differentiate between them. Process ID need not to match on all routers.

Router(config-router)# network IP_network_# [wildcard_mask] area [area number]

Network command allows us to specify the interfaces which we want to include in OSPF process. This command accepts three arguments network number, wildcard mask and area number.

Network number

Network number is network ID. We can use any particular host IP address or network IP address. For example we can use 192.168.1.1 (host IP address) or we can use 192.168.1.0 (Network IP address). While targeting a specific interface usually we use host IP address (configured on that interface). While targeting multiple interfaces, we use network IP address. So any interface that belongs to specified network ID will be selected.

Wildcard mask

Wildcard mask are used with network ID to filter the interfaces. Wildcard mask is different from subnet mask. Subnet mask is used to separate the network portion and host portion in IP address. While wildcard mask is used to match corresponding octet in network portion. Wildcard mask tells OSPF the part of network address that must be matched. Wildcard masks are explained with examples in access list tutorials of this category.

OSPF configuration

Router 0
Router>enable
Router # configure terminal

Router(config) #router ospf 10 Router(config-router) #network 10.0.0.0 0.255.255.255 area 0 Router(config-router) #network 192.168.0.0 0.0.0.3 area 0 Router(config-router) #network 192.168.1.0 0.0.0.3 area 0 Router(config-router) #network 192.168.2.0 0.0.0.3 area 0 Router(config-router) #exit
Router(config-router) #

Our network is ready to take the advantage of OSPF routing. To verify the setup we will use ping command. ping command is used to test the connectivity between two devices.

VIVA QUESTIONS

1.How OSPF is different from RIP?
2.How the cost matrix is calculated in OSPF?

OBJECTIVE – Simulate and analyze Ethernet Protocols using Network Simulator 1.

APPARATUS (SOFTWARE): Network Simulator 1

THEORY AND CONCEPT : Ethernet

The IEEE 802.3 standard defines Ethernet at the physical and data link layers of the OSI network model. Most Ethernet systems use the following:

1. Carrier-sense multiple-access with collision detection (CSMA/CD) for controlling access to the network media.
2. Use base band broadcasts
3. A method for packing data into data packets called frames
4. Transmit at 10Mbps, 100Mbps, and 1Gbps.

TYPES OF ETHERNET

1. 10Base5 - Uses Thick net coaxial cable which requires a transceiver with a vampire tap to connect each computer. There is a drop cable from the transceiver to the Attachment Unit Interface (AIU). The AIU may be a DIX port on the network card. There is a transceiver for each network card on the network. This type of Ethernet is subject to the 5-4-3 rule meaning there can be 5 network segments with 4 repeaters, and three of the segments can be connected to computers. It uses bus topology. Maximum segment length is 500 Meters with the maximum overall length at 2500 meters. Minimum length between nodes is 2.5 meters. Maximum nodes per segment are 100.

2. 10Base2 - Uses Thin net coaxial cable. Uses a BNC connector and bus topology requiring a terminator at each end of the cable. The cable used is RG-58A/U or RG-58C/U with an impedance of 50 ohms. RG-58U is not acceptable. Uses the 5-4-3 rule meaning there can be 5 network segments with 4 repeaters, and three of the segments can be connected to computers. The maximum length of one segment is 185 meters. Barrel connectors can be used to link smaller pieces of cable on each segment, but each barrel connector reduces signal quality. Minimum length between nodes is 0.5 meters.

3. 10BaseT - Uses Unshielded twisted pair (UTP) cable. Uses star topology. Shielded twisted pair (STP) is not part of the 10BaseT specification. Not subject to the 5-4-3 rule. They can use category 3, 4, or 5 cables, but perform best with category 5 cable. Category 3 is the minimum. Require only 2 pairs of wire. Cables in ceilings and walls must be plenum rated. Maximum segment length is 100 meters. Minimum length between nodes is 2.5 meters. Maximum number of connected segments is 1024. Maximum number of nodes per segment is 1 (star topology). Uses RJ-45 connectors.

4. 10BaseF - Uses Fiber Optic cable. Can have up to 1024 network nodes. Maximum segment length is 2000 meters. Uses specialized connectors for fiber optic. Includes three categories:

5. 10BaseFL - Used to link computers in a LAN environment, which is not commonly done due to high cost.
6. 10BaseFP - Used to link computers with passive hubs to get cable distances up to 500 meters.
7. 10BaseFB - Used as a backbone between hubs.
8. 100BaseT - Also known as fast Ethernet. Uses RJ-45 connectors. Topology is star. Uses CSMA/CD media access. Minimum length between nodes is 2.5 meters. Maximum number of connected segments is 1024. Maximum number of nodes per segment is 1 (star topology). IEEE802.3 specification.

9. 100BaseTX - Requires category 5 two pair cable. Maximum distance is 100 meters.
10. 100BaseT4 - Requires category 3 cable with 4 pair. Maximum distance is 100 meters.

12. 100VG-AnyLAN - Requires category 3 cable with 4 pair. Maximum distance is 100 meters with cat 3 or 4 cable.

The IEEE naming convention is as follows:

- The transmission speed in Mbps
- Base band (base) or Broadband data transmission
- The maximum distance a network segment could cover in hundreds of meters.

Comparisons of some Ethernet type's distances are in meters.

Ethernet Type	Cable	Min length between nodes	Max Segment length	Max overall length
10Base2	Thin net	0.5	185	925
10Base5	Thick net	2.5	500	2500
10BaseF	Fiber		2000	
10BaseT	UTP	2.5	100	

Types of Ethernet frames

1. Ethernet 802.2 - These frames contain fields similar to the Ethernet 802.3 frames with the addition of three Logical Link Control (LLC) fields. Novell NetWare 4.x networks use it. Ethernet 802.3 - It is mainly used in Novell
2. NetWare 2.x and 3.x networks. The frame type was developed prior to completion of the IEEE 802.3 specification and may not work in all Ethernet environments. Ethernet II - This frame type combines the 802.3 preamble and SFD
3. fields and include a protocol type field where the 802.3 frame contained a length field. TCP/IP networks and networks that use multiple protocols normally use this type of frames.

4. Ethernet SNAP - This frame type builds on the 802.2 frame type by adding a type field indicating what network protocol is being used to send data. This frame type is mainly used in AppleTalk networks.

The packet size of all the above frame types is between 64 and 1,518 bytes.

Ethernet Message Formats

The Ethernet data format is defined by RFC 894 and 1042. The addresses specified in the ethernet protocol are 48 bit addresses.

The types of data passed in the type field are as follows:

1. 0800 IP Datagram
2. 0806 ARP request/reply
3. 8035 RARP request/reply

There is a maximum size of each data packet for the Ethernet protocol. This size is called the maximum transmission unit (MTU). What this means is that sometimes packets may be broken up as they are passed through networks with MTUs of various sizes. SLIP and PPP protocols will normally have a smaller MTU value than Ethernet.

Carrier Sense Multiple Access (CSMA)

Carrier Sense Multiple Access (CSMA), improves performance when there is a higher medium utilization. When a Node has data to transmit, the Node first listens to the cable (using a transceiver) to see if a carrier (signal) is being transmitted by another node. This may be achieved by monitoring whether a current is flowing in the cable (each bit corresponds to 18-20 milliamps (mA)). The individual bits are sent by encoding them with a 10 (or 100 MHz for Fast Ethernet) clock using MANCHESTER ENCODING. Data is only sent when no carrier is observed (i.e. no current

same time. If two Nodes simultaneously try transmit, then both could see an idle physical medium (i.e. neither will see the other's carrier signal), and both will conclude that no other Node is currently using the medium. In this case, both will then decide to transmit and a collision will occur. The collision will result in the corruption of the frame being sent, which will subsequently be discarded by the receiver since a corrupted Ethernet frame will (with a very high probability) not have a valid 32-bit MAC CRC at the end.

Collision Detection (CD)

A second element to the Ethernet access protocol is used to detect when a collision occurs. When there is data waiting to be sent, each transmitting Node also monitors its own transmission. If it observes a collision (excess current above what it is generating, i.e. > 24 mA for coaxial Ethernet), it stops transmission immediately and instead transmits a 32-bit jam sequence. The purpose of this sequence is to ensure that any other node which may currently be receiving this frame will receive the jam signal in place of the correct 32-bit MAC CRC; this causes the other receivers to discard the frame due to a CRC error. To ensure that all Nodes start to receive a frame before the transmitting NODE has finished sending it, Ethernet defines a minimum frame size (i.e. no frame may have less than 46 bytes of payload). The minimum frame size is related to the distance which the network spans, the type of media being used and the number of repeaters which the signal may have to pass through to reach the furthest part of the LAN. Together these define a value known as the Ethernet Slot Time, corresponding to 512 bit times at 10 Mbps.

LAB WORK

Q1. Design the Ethernet network with two hubs & 4 nodes to each hub. Analyze the network performance & evaluate the bar chart for it.
Q2. Design the Ethernet network with bus topology with 5 nodes. Analyze the network performance & evaluate the bar chart for it.
Q3.Compare the throughput of these two networks through bar charts.

VIVA QUESTIONS

Q1. What is the standard of ethernet LAN??
Q2. Explain 5-4-3 rule in ethernet.

OBJECTIVE: Simulate and analyze Token Ring mechanism using Network Simulator 1.

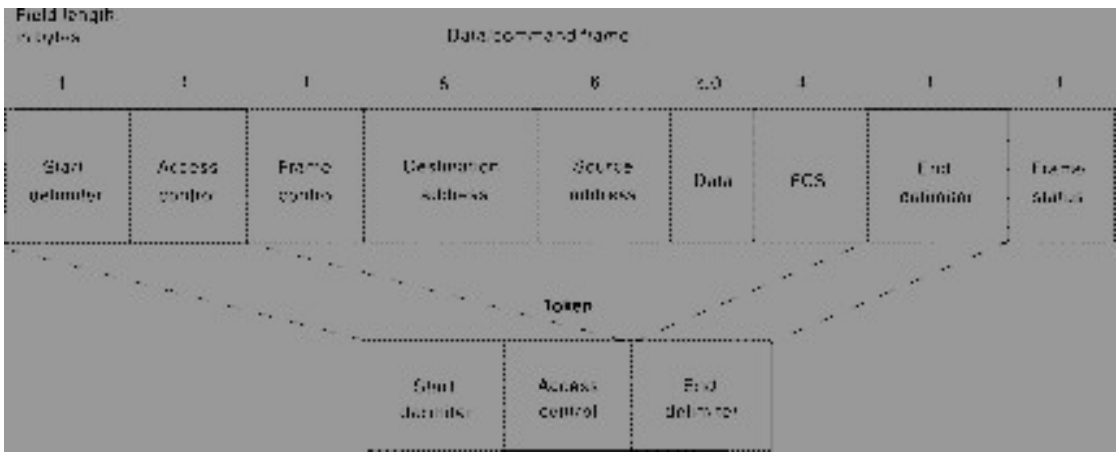
APPARATUS (SOFTWARE): Network Simulator 1

THEORY & CONCEPT Token Ring/IEEE 802.5

The Token Ring network was originally developed by IBM in the 1970s. It is still IBM's primary local-area network (LAN) technology. The related IEEE 802.5 specification is almost identical to and completely compatible with IBM's Token Ring network. In fact, the IEEE 802.5 specification was modeled after IBM Token Ring, and it continues to shadow IBM's Token Ring development. The term *Token Ring* generally is used to refer to both IBM's Token Ring network and IEEE 802.5 networks. Token Ring and IEEE 802.5 networks are basically compatible, although the specifications differ in minor ways. IBM's Token Ring network specifies a star, with all end stations attached to a device called a multi-station access unit (MSAU). In contrast, IEEE 802.5 does not specify a topology, although virtually all IEEE 802.5 implementations are based on a star. Token Ring technology was developed in the 1970s by IBM. Token-passing networks move a small frame, called a token, around the network. Possession of the token grants the right to transmit. If a node receiving the token has no information to send, it passes the token to the next end station. Each station can hold the token for a maximum period of time. If a station possessing the token does have information to transmit, it seizes the token, alters 1 bit of the token (which turns the token into a start-of-frame sequence), appends the information that it wants to transmit, and sends this information to the next station on the ring.

Frame Format

Token Ring and IEEE 802.5 support two basic frame types: tokens and data/command frames. Tokens are 3 bytes in length and consist of a start delimiter, an access control byte, and an end delimiter. Data/command frames vary in size, depending on the size of the Information field. Data frames carry information for upper-layer protocols, while command frames contain control information and have no data for upper-layer protocols. Both formats are shown in Figure.



Token Frame Fields

The three token frame fields illustrated in above Figure are summarized in the descriptions that follow:

- **Start delimiter**—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame.
- **Access-control byte**—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly).

damaged frame and identify the frame that is the last in a logical sequence.

Data/Command Frame Fields

Data/command frames have the same three fields as Token Frames, plus several others. The Data/command frame fields illustrated in above Figure are described in the following summaries:

Start delimiter—Alerts each station of the arrival of a token (or data/command frame). This field includes signals that distinguish the byte from the rest of the frame by violating the encoding scheme used elsewhere in the frame. **Access-control byte**—Contains the Priority field (the most significant 3 bits) and the Reservation field (the least significant 3 bits), as well as a token bit (used to differentiate a token from a data/command frame) and a monitor bit (used by the active monitor to determine whether a frame is circling the ring endlessly). **Frame-control bytes**—Indicates whether the frame contains data or control information. In control frames, this byte specifies the type of control information. **Destination and source addresses**—Consists of two 6-byte address fields that identify the destination and source station addresses. **Data**—indicates that the length of field is limited by the ring token holding time, which defines the maximum time a station, can hold the token. **Frame-check sequence (FCS)**—Is filed by the source station with a calculated value dependent on the frame contents. The destination station recalculates the value to determine whether the frame was damaged in transit. If so, the frame is discarded. **End Delimiter**—Signals the end of the token or data/command frame. The end delimiter also contains bits to indicate a damaged frame and identify the frame that is the last in a logical sequence. **Frame Status**—Is a 1-byte field terminating a command/data frame. The Frame Status field includes the address-recognized indicator and frame-copied indicator.

LAB WORK

Q1. Design a token ring network with 7 nodes & use optical fiber as a transmission medium. Evaluate the network performance. Give the throughput, no of collision of the network.

Q2. *Token Ring networks differ from Ethernet networks in what ways. For what types of applications is this beneficial? Evaluate the comparable bar chart for both protocol & throughput.*

VIVA QUESTIONS:

Q1. What is MAU in token ring?

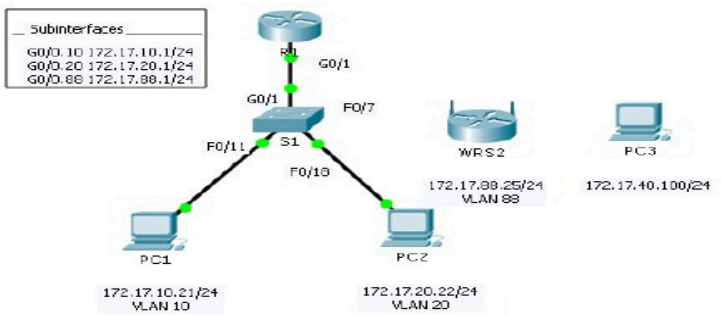
Q2. What is Beaconing?

OBJECTIVE: Configuring wireless LAN access using packet tracer

APPARATUS (SOFTWARE): Packet Tracer Software

THEORY AND CONCEPT:

In this activity, you will configure a Linksys wireless router, allowing for remote access from PCs as well as wireless connectivity with WPA2 security. You will manually configure PC wireless connectivity by entering the Linksys router SSID and password. Part 1: Configure a Wireless Router Part 2: Configure a Wireless Client Part 3: Verify Connectivity



Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
R1	G0/0.10	172.17.10.1	255.255.255.0	N/A
	G0/0.20	172.17.20.1	255.255.255.0	N/A
	G0/0.88	172.17.88.1	255.255.255.0	N/A
PC1	NIC	172.17.10.21	255.255.255.0	172.17.10.1
PC2	NIC	172.17.20.22	255.255.255.0	172.17.20.1
PC3	NIC	DHCP Assigned	DHCP Assigned	DHCP Assigned
WRS2	NIC	172.17.88.25	255.255.255.0	172.17.88.1

SAMPLE DIAGRAM

Part 1: Configure a Wireless Router

Step 1: Connect the Internet interface of WRS2 to S1.
Connect the WRS2 Internet interface to the S1 F0/7 interface.

Step 2: Configure the Internet connection type.
a. Click WRS2 > GUI tab.
b. Set the Internet Connection type to Static IP.
c. Configure the IP addressing according to the Addressing Table.

Step 3: Configure the network setup.
a. Scroll down to Network Setup. For the Router IP option, set the IP address to 172.17.40.1 and the subnet mask to 255.255.255.0.
b. Enable the DHCP server.
c. Scroll to the bottom of the page and click Save Settings.

Step 4: Configure wireless access and security.
a. At the top of the window, click Wireless. Set the Network Mode to Wireless-N Only and change the SSID to

b. Disable SSID Broadcast and click Save Settings.
c. Click the Wireless Security option.
d. Change the Security Mode from Disabled to WPA2 Personal.
e. Configure cisco123 as the passphrase.
f. Scroll to the bottom of the page and click Save Settings.

Part 2: Configure a Wireless Client

Step 1: Configure PC3 for wireless connectivity.
Because SSID broadcast is disabled, you must manually configure PC3 with the correct SSID and pass phrase to establish a connection with the router.
a. Click PC3 >Desktop >PC Wireless.
b. Click the Profiles tab.
c. Click New.
d. Name the new profile Wireless Access.
e. On the next screen, click Advanced Setup. Then manually enter the SSID of WRS_LAN on Wireless Network Name. Click Next.
f. Choose Obtain network settings automatically (DHCP) as the network settings, and then click Next.
g. On Wireless Security, choose WPA2-Personal as the method of encryption and click Next.
h. Enter the passphrase cisco123 and click Next.
i. Click Save and then click Connect to Network.

Step 2: Verify PC3 wireless connectivity and IP addressing configuration.
The Signal Strength and Link Quality indicators should show that you have a strong signal.
Click More Information to see details of the connection including IP addressing information.
Close the PC Wireless configuration window.

Part 3: Verify Connectivity

All the PCs should have connectivity with one another.
.
VIVA QUESTIONS

1.What is the use of access point?
2.What are the differences between access point and hotspot?

OBJECTIVE: Write a Program to implement Remote Procedural Calls.

APPARATUS (SOFTWARE):C Language

THEORY AND CONCEPT: Remote Procedure Call (RPC) is a protocol that provides the high-level communications paradigm used in the operating system. RPC presumes the existence of a low-level transport protocol, such as Transmission Control Protocol/Internet Protocol (TCP/IP) or User Datagram Protocol (UDP), for carrying the message data between communicating programs. RPC implements a logical client-to-server communications system designed specifically for the support of network applications.

The RPC protocol is built on top of the eXternal Data Representation (XDR) protocol, which standardizes the representation of data in remote communications. XDR converts the parameters and results of each RPC service provided.The RPC protocol enables users to work with remote procedures as if the procedures were local. The remote procedure calls are defined through routines contained in the RPC protocol. Each call message is matched with a reply message. The RPC protocol is a message-passing protocol that implements other non-RPC protocols such as batching and broadcasting remote calls. The RPC protocol also supports callback procedures and the select subroutine on the server side. RPC provides an authentication process that identifies the server and client to each other.

Sample Program-

```
//SERVER FILENAME: server.c
#include"rpc/rpc.h"
#include"square.h"
#include"stdio.h"
#include"stdlib.h"
#include"math.h"


square_out *squareproc_1_svc(square_in *inp,struct svc_req *rqstp)
{
static square_out out;
   out.res1= inp->arg1 * inp->arg1;
return(&out);
}
// CLIENT FILENAME: client.c
#include"errno.h"
#include"rpc/rpc.h"
#include"square.h"
#include"stdio.h"
#include"stdlib.h"
#include"math.h"


int main(int argc,char **argv)
{
   CLIENT *cl;
 square_in in;
 square_out *outp;
 f(argc!=3)
   {
       printf("\n\n error:insufficient arguments!!!");
       exit(-1);
```

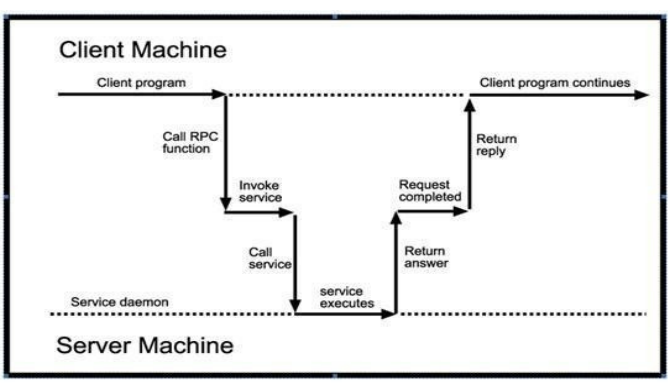
```
cl=clnt_create(argv[1],SQUARE_PROG,SQUARE_VERS,"tcp");
 in.arg1=atol(argv[2]);

if(cl==NULL)
    {    printf("\nerror:%s",strerror(errno));
         exit(-1);
    }
if((outp=squareproc_1(&in,cl))==NULL)
    {
         printf("\nerror :%s",clnt_sperror(cl,argv[1]));
         exit(-1);
    }

    printf("\n\n result is : %ld",outp->res1);
    exit(0);
}

// .h FILENAME: square.h

struct square_in
{
/*input arg*/
long arg1;
};
struct square_out
{
/*op result*/
long res1;
};
program SQUARE_PROG
{
version SQUARE_VERS
{
square_out SQUAREPROC(square_in)=1; /*proc no=1*/
}=1; /*version no*/
}=0x31230000;/*prog no*/
```



VIVA QUESTIONS

Q1. Which protocol is used by RPC procedure?
Q2. On which layer of OSI model, RPC works?

OBJECTIVE: Simulation of sliding window protocols.

THEORY AND CONCEPT:

A sliding window protocol is a feature of packet-based data transmission protocols. Sliding window protocols are used where reliable in-order delivery of packets is required, such as in the Data Link Layer (OSI model) as well as in the Transmission Control Protocol (TCP).

Conceptually, each portion of the transmission (packets in most data link layers, but bytes in TCP) is assigned a unique consecutive sequence number, and the receiver uses the numbers to place received packets in the correct order, discarding duplicate packets and identifying missing ones. The problem with this is that there is no limit on the size of the sequence number that can be required.

FEW TERMINOLOGIES:

Transmission Delay (Tt) – Time to transmit the packet from host to the outgoing link. If B is the Bandwidth of the link and D is the Data Size to transmit

$$Tt = D/B$$

Propagation Delay (Tp) – It is the time taken by the first bit transferred by the host onto the outgoing link to reach the destination. It depends on the distance d and the wave propagation speed s (depends on the characteristics of the medium).

$$Tp = d/s$$

Efficiency – It is defined as the ratio of total useful time to the total cycle time of a packet. For stop and wait protocol,

Total cycle time = Tt(data) + Tp(data) + Tt(acknowledgement) + Tp(acknowledgement)
= Tt(data) + Tp(data) + Tp(acknowledgement)
= Tt + 2*Tp

Since acknowledgements are very less in size, their transmission delay can be neglected.

Efficiency = Useful Time / Total Cycle Time
= Tt/(Tt + 2*Tp) (For Stop and Wait)
= 1/(1+2a) [Using a = Tp/Tt]

Effective Bandwidth(EB) or Throughput – Number of bits sent per second.
EB = Data Size(L) / Total Cycle time(Tt + 2*Tp)
Multiplying and dividing by Bandwidth (B),
= (1/(1+2a)) * B [Using a = Tp/Tt]
= Efficiency * Bandwidth

Capacity of link – If a channel is Full Duplex, then bits can be transferred in both the directions and without any collisions. Number of bits a channel/Link can hold at maximum is its capacity.
Capacity = Bandwidth(B) * Propagation(Tp)
For Full Duplex channels,
Capacity = 2*Bandwidth(B) * Propagation(Tp)

VIVA QUESTIONS

Q1. What is the receiver window size in Go Back N and selective reapeat protocol?
Q2. What is the Sender window size of stop and wait protocol?