SRM
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University *u/s 3 of UGC Act, 1956)*
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

COMPUTER COMMUNICATIONS LAB

(Subject Code: (18CSS202J)

B.TECH II YEAR / IV SEMESTER

NAME-

REG. No.-

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING
FACULTY OF ENGINEERING & TECHNOLOGY

SRM INSTITUTE OF SCIENCE & TECHNOLOGY,

DELHI NCR CAMPUS, MODINAGAR

SIKRI KALAN, DELHI MEERUT ROAD, DIST. – GHAZIABAD - 201204

www.srmimt.net

Even Semester (2022-23)

BONAFIDE CERTIFICATE

Registration no._____

Certified to be the bonafide record of work done by_____
Of 4th semester 2nd year B.TECH degree course in SRM INSTITUTE OF SCIENCE & TECHNOLOGY, DELHI-NCR Campus for the Department of ***Computer Science & Engineering,*** *in Computer Communications Laboratory during the academic year* ***2022-23.***

Lab In charge **Head of the department**

Submitted for end semester examination held on __/____/___ at SRM INSTITUTE OF SCIENCE & TECHNOLOGY, DELHI-NCR Campus.

Internal Examiner-I ***Internal Examiner-II***

INDEX

S.N.	Name of Experiment	Page No.	Date of Exp.	Date of Submission	Signature
1					
2					
3					
4					
5					
6					
7					
8					
9					
10					

SRM
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

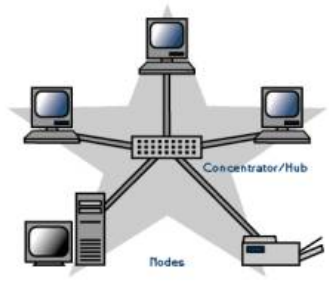
S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-1

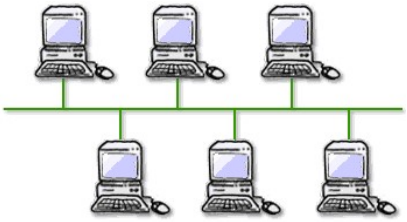
Aim: Design and analysis of Local Area Network (Wired LAN & Wireless LAN)

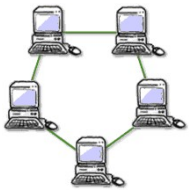
Theory: Wired networks, also called Ethernet networks, are the most common type of local area network (LAN) technology. A wired network is simply a collection of two or more computers, printers, and other devices linked by Ethernet cables. Ethernet is the fastest wired network protocol, with connection speeds of 10 megabits per second (Mbps) to 100 Mbps or higher. Wired networks can also be used as part of other wired and wireless networks. To connect a computer to a network with an Ethernet cable, the computer must have an Ethernet adapter (sometimes called a network interface card, or NIC). Ethernet adapters can be internal (installed in a computer) or external (housed in a separate case). Some computers include a built-in Ethernet adapter port, which eliminates the need for a separate adapter (Microsoft). There are three basic network topologies that are most commonly used today. (Homenthelp.com)



The star network, a general more simplistic type of topology, has one central hub that connects to three or more computers and the ability to network printers. This type can be used for small businesses and even home networks. The star network is very useful for applications where some processing must be centralized and some must be performed locally. The major disadvantage is the star network is its vulnerability. All data must pass through one central host computer and if that host fails the entire network will fail.

On the other hand the bus network has no central computer and all computers are linked on a single circuit. This type broadcasts signals in all directions and it uses special software to identify which computer gets what signal. One disadvantage with this type of network is that only one signal can be sent at one time, if two signals are sent at the same time they will collide and the signal will fail to reach its destination. One advantage is that there is no central computer so if one computer goes down others will not be affected and will be able to send messages to one another.



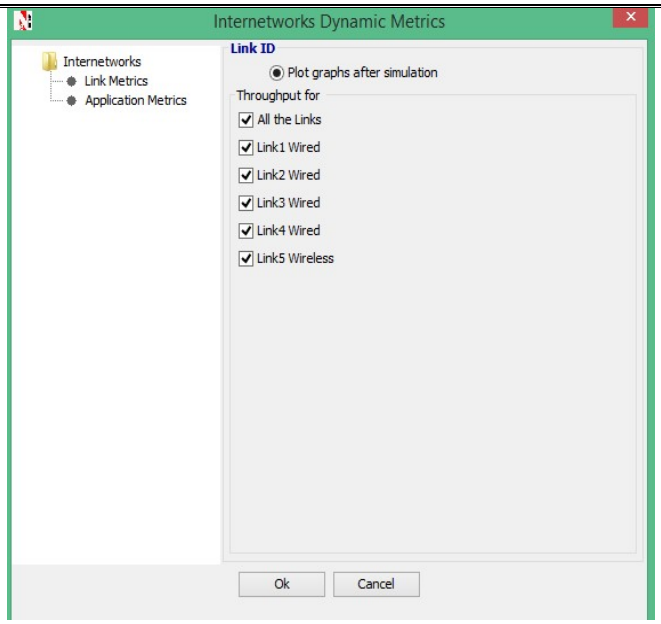


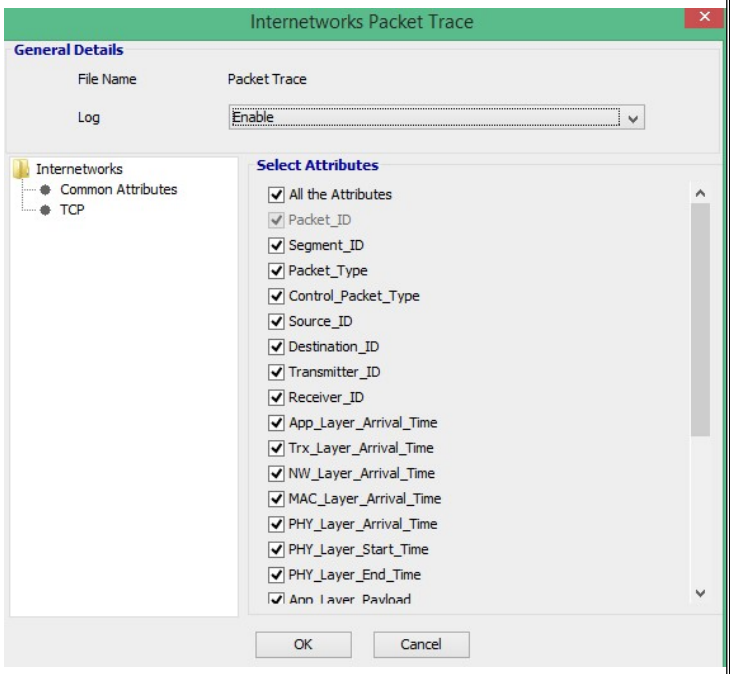
The third type of network is the ring network. Similar to the bus network, the ring network does not rely on a central host computer either. Each computer in the network can communicate directly with any other computer, and each processes its own applications independently. A ring network forms a closed loop and data is sent in one direction only and if a computer in the network fails the data is still able to be transmitted.

Typically the range of a wired network is within a 2,000-foot-radius. The disadvantage of this is that data transmission over this distance may be slow or nonexistent. The benefit of a wired network is that bandwidth is very high and that interference is very limited through direct connections. Wired networks are more secure and can be used in many situations; corporate LANs, school networks and hospitals. The biggest drawback to this type of network is that it must be rewired every time it is moved.

A wireless LAN (WLAN) is a wireless computer network that links two or more devices using wireless communication to form a local area network (LAN) within a limited area such as a home, school, computer laboratory, campus, office building etc. This gives users the ability to move around within the area and still be connected to the network. Through a gateway, a WLAN can also provide a connection to the wider Internet.

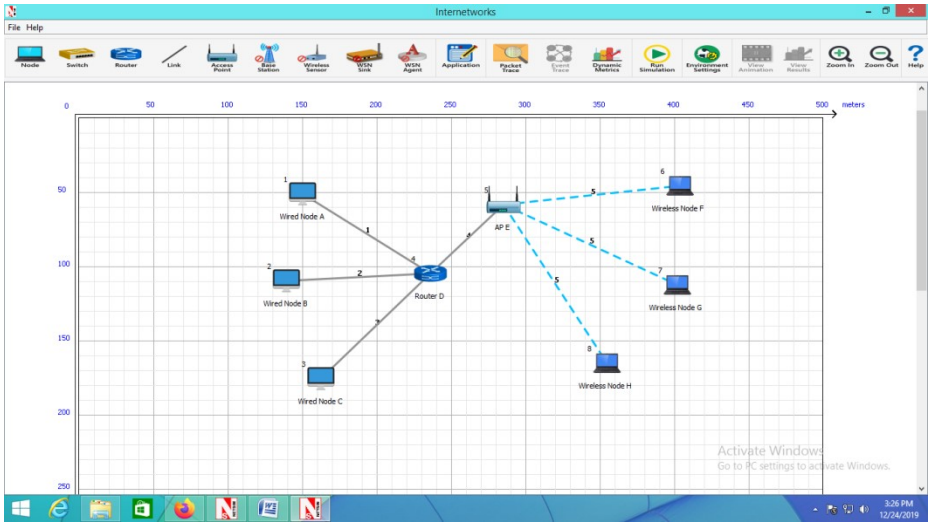
Most modern WLANs are based on IEEE 802.11 standards and are marketed under the Wi-Fi brand name. Wireless LANs have become popular for use in the home, due to their ease of installation and use. They are also popular in commercial properties that offer wireless access to their employees and customers.





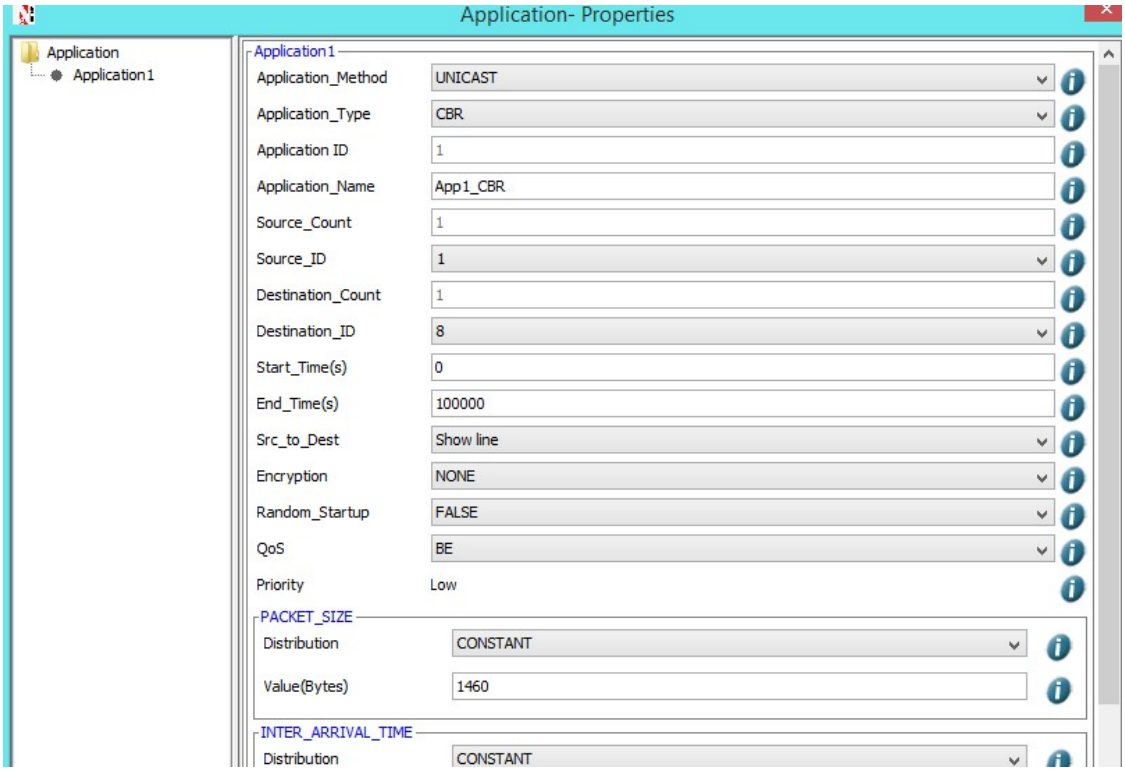
Configuration diagram:

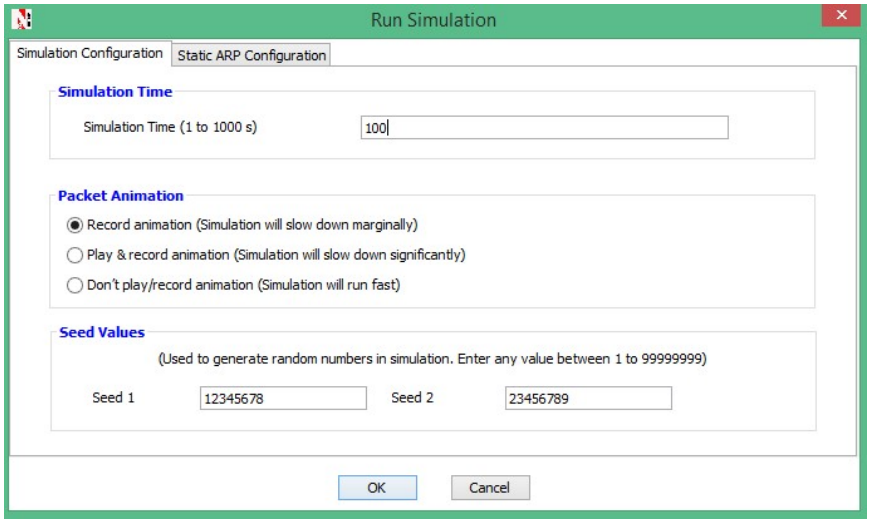
Step-1: Draw the networks



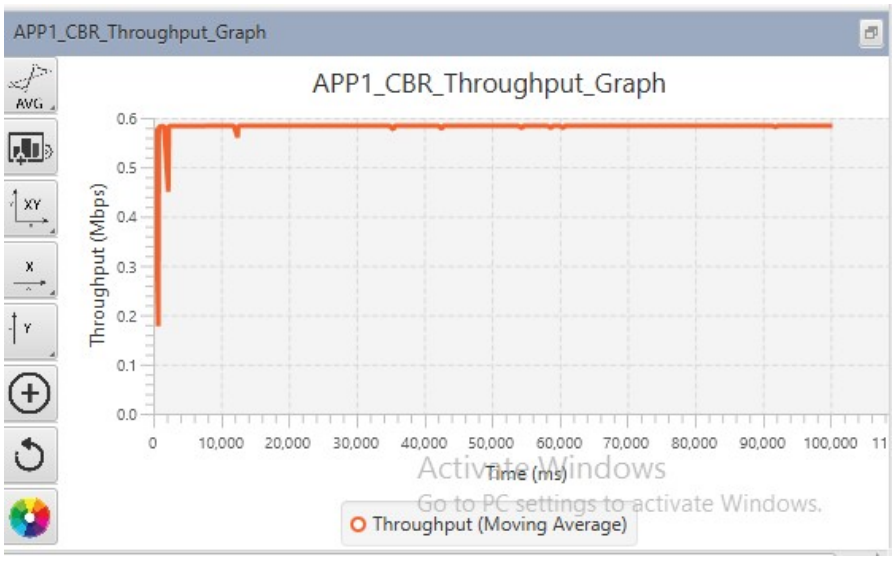
Step-2: Select the Metrics

Step-3: Set Application Properties





Step-4: Run the Simulation



Throughput of the link is increasing with respect to time and after a certain time become constant due to the Constant Bit Rate – CBR type data selection at application properties setup

Source-

Destination-

Total packet transmitted-

Packet received-

Throughput-

Result: The LAN configurations both wired and wireless are designed and the performance of the network is analyzed.

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-2

Aim: Design a network and do the IP Addressing

Theory: At the network layer, we need to uniquely identify each device on the Internet to allow global communication between all devices. This is analogous to the telephone system, where each telephone number with the country code and the area code as a part of the identifying scheme.

Introduction

The identifier used in the IP layer of the TCP/IP protocol suite to identify each device connected to the Internet is called the Internet address or IP address. An IP address is a 32-bit address that uniquely and universally defines the connection of a host or a router to the Internet. IP addresses are unique. They are unique in the sense that each address defines one, and only one, connection to the Internet. Two devices on the Internet can never have **the same address.** However, if a device has two connections to the Internet, via two networks, it has two IPv4 addresses. The IPv4 addresses are universal in the sense that the addressing system must be accepted by any host that wants to be connected to the Internet.

Address Space

A protocol like IPv4 that defines addresses has an **address space.** An address space is the total number of addresses used by the protocol. If a protocol uses n bits to define an address, the address space is 2^n because each bit can have two different values (0 or 1). IPv4 uses 32-bit addresses, which means that the address space is 232 or 4,294,967,296 (More than four billion). Theoretically, if there were no restrictions, more than 4 billion

devices could be connected to the Internet.

The address space of IPv4 is 232 or 4,294,967,296.

Notation

There are three common notations to show an IPv4 address: binary notation (base 2), dotted-decimal notation (base 256), and hexadecimal notation (base 16).

Binary Notation: Base 2

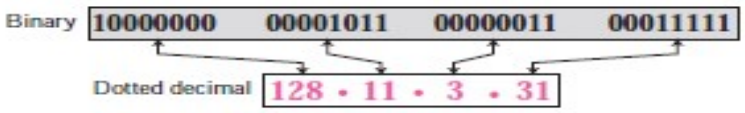
In **binary notation,** an IPv4 address is displayed as 32 bits. To make the address more readable, one or more spaces is usually inserted between each octet (8 bits). Each octet is often referred to as a byte. So it

is common to hear an IPv4 address referred to as a 32-bit address, a 4-octet address, or a 4-byte address. The following is an example of an IPv4 address in binary notation:

```
01110101 10010101 00011101 11101010
```

Dotted-Decimal Notation: Base 256

To make the IPv4 address more compact and easier to read, an IPv4 address is usually written in decimal form with a decimal point (dot) separating the bytes. This format is referred to as **dotted-decimal notation.** Figure 5.1 shows an IPv4 address in dotted decimal notation. Note that because each byte (octet) is only 8 bits, each number in the dotted-decimal notation is between 0 and 255.



Hexadecimal Notation: Base 16

We sometimes see an IPv4 address in **hexadecimal notation.** Each hexadecimal digit is equivalent to four bits. This means that a 32-bit address has 8 hexadecimal digits. This notation is often used in network programming.

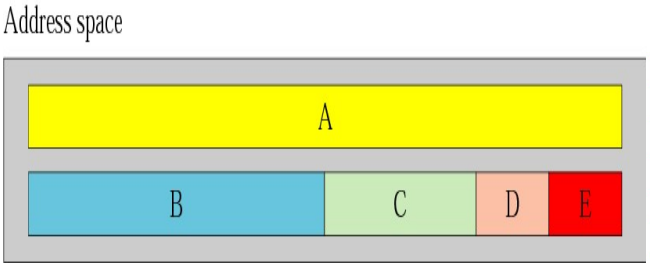
10000001 00001011 00001011 11101111 ~~0X81~~0B0BEF or 810B0BEF16

CLASSFUL ADDRESSING

IP addresses, when started a few decades ago, used the concept of classes. This architecture is called classful addressing. In the mid-1990s, a new architecture, called classless addressing, was introduced that supersedes the original architecture. However, although part of the internet is still using classful addressing.

Classes

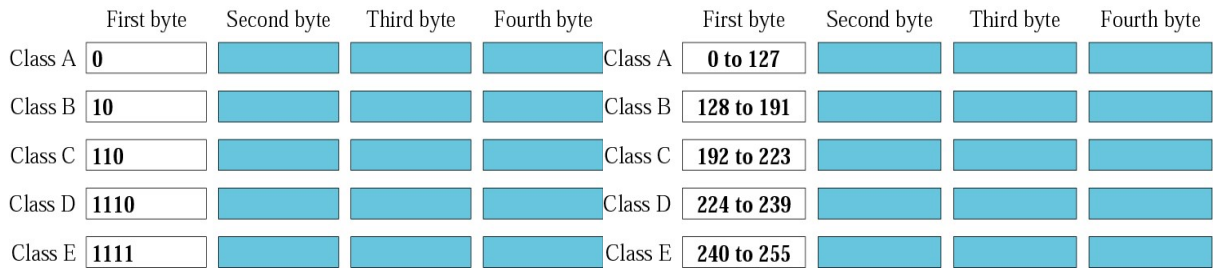
In classful addressing, the IP address space is divided into five **classes: A, B, C, D,** and **E.** Each class occupies some part of the whole address space.

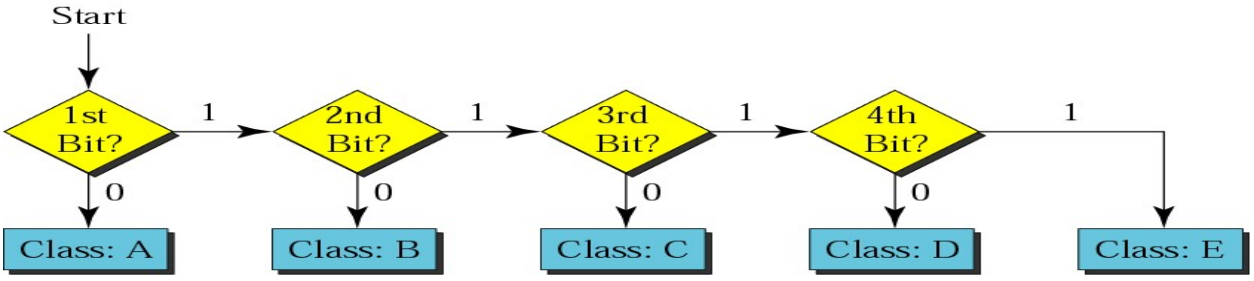


Class	*Number of Addresses*	*Percentage*
A	$2^{31} = 2{,}147{,}483{,}648$	50%
B	$2^{30} = 1{,}073{,}741{,}824$	25%
C	$2^{29} = 536{,}870{,}912$	12.5%
D	$2^{28} = 268{,}435{,}456$	6.25%
E	$2^{28} = 268{,}435{,}456$	6.25%

Recognizing Classes

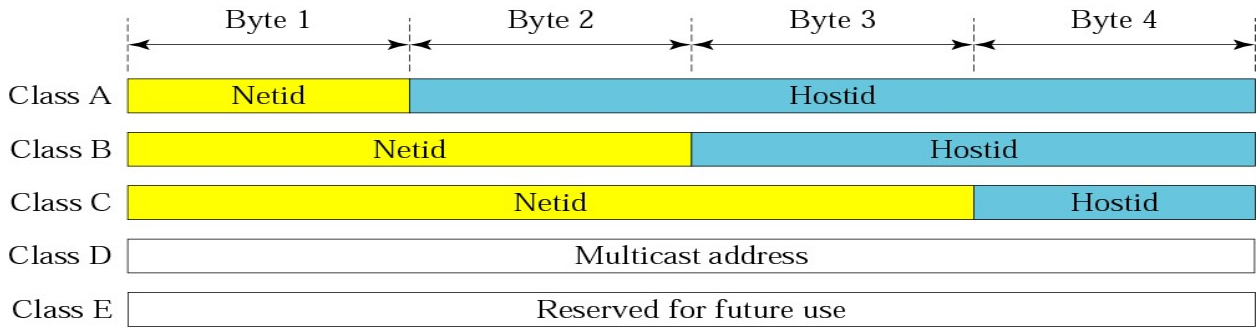
We can find the class of an address when the address is given either in binary or dotted decimal notation. In the binary notation, the first few bits can immediately tell us the class of the address; in the dotted-decimal notation, the value of the first byte can give the class of an address.



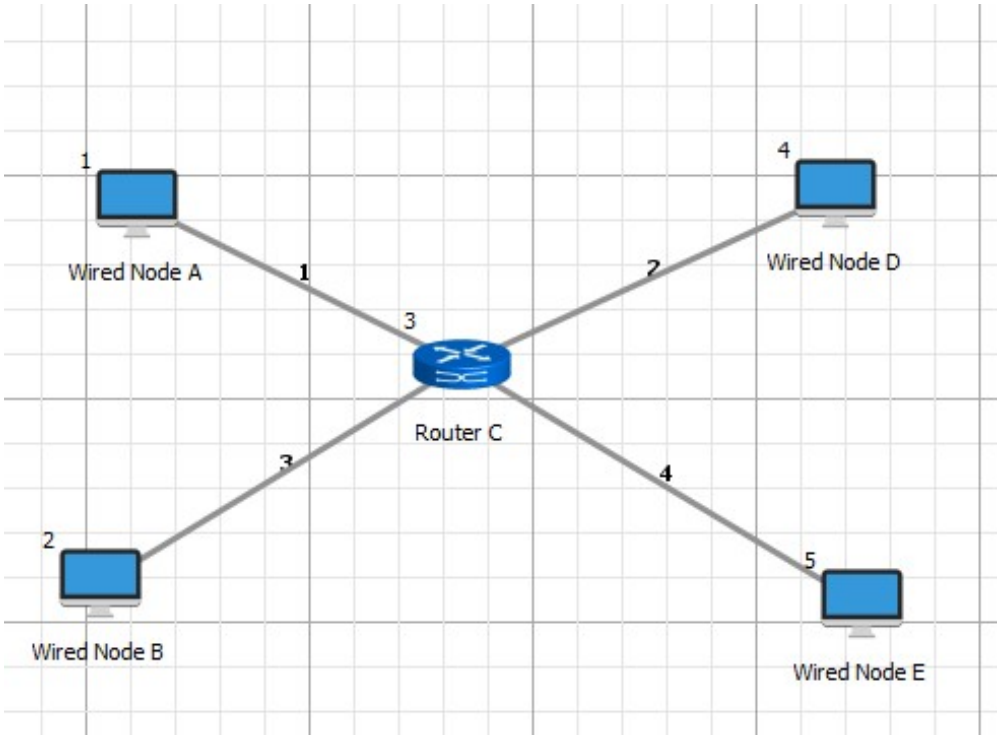


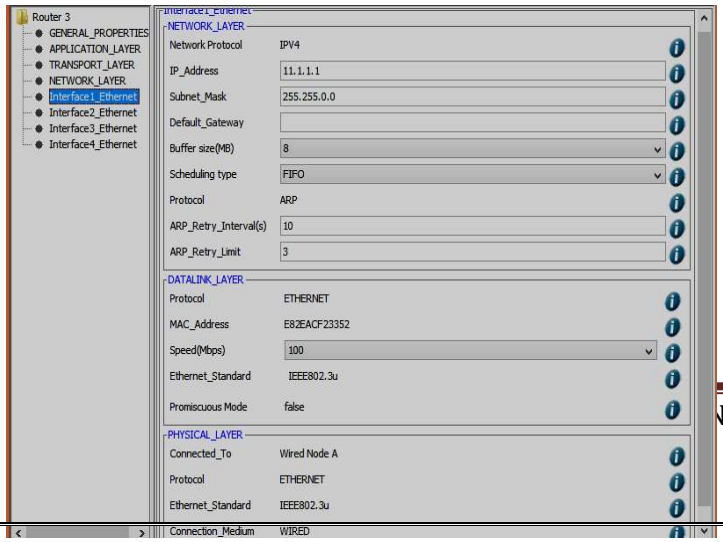
Netid and Hostid

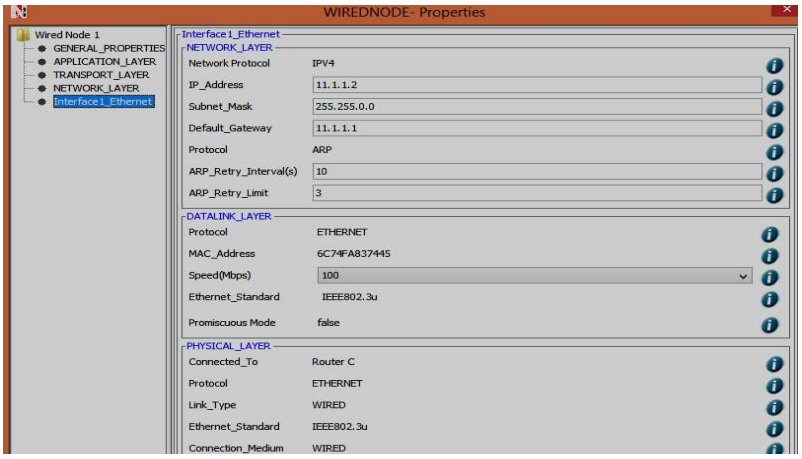
In classful addressing, an IP address in classes A, B, and C is divided into **netid** and **hostid.** These parts are of varying lengths, depending on the class of the address. Figure shows the netid and hostid bytes. Note that classes D and E are not divided into netid and hostid, for reasons that we will discuss later.

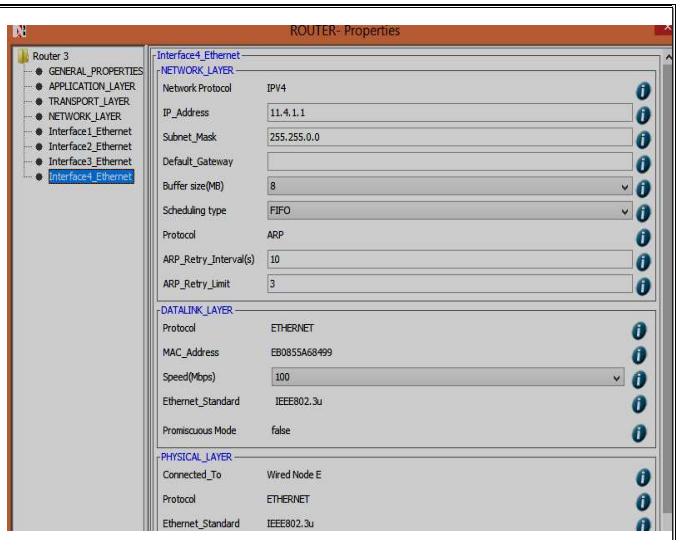


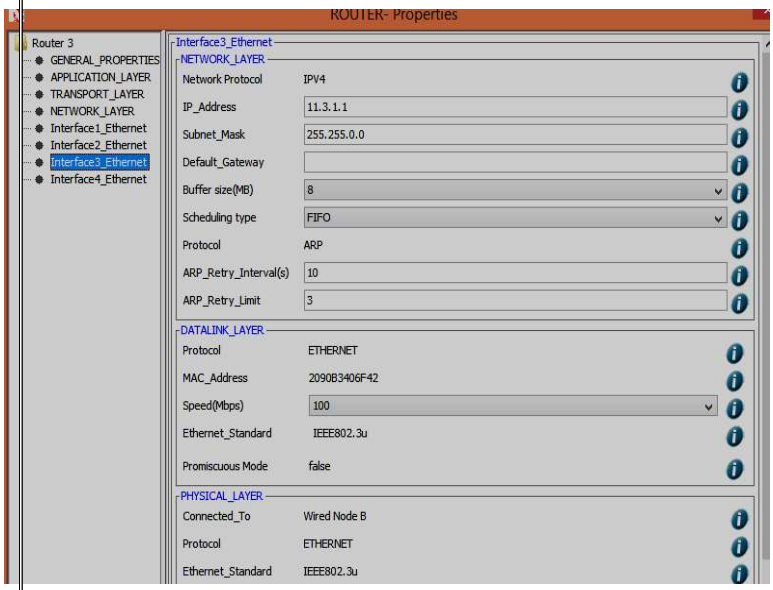
Configuration diagram:

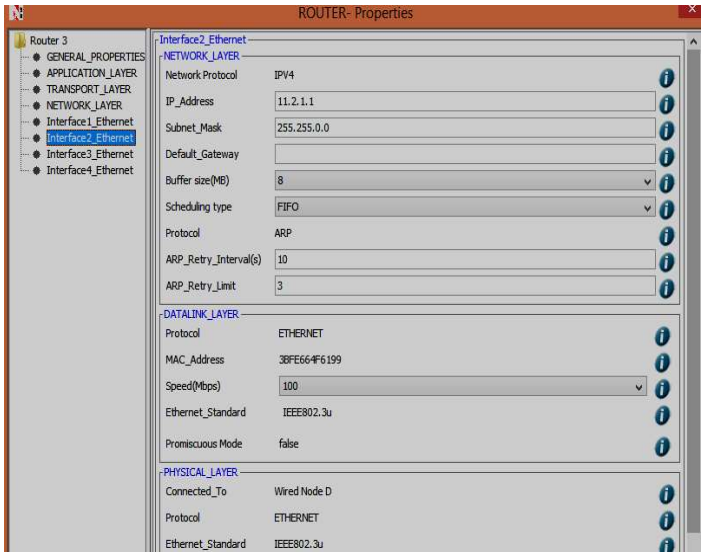












Result: Network Design and IP Addressing are performed.

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-3

Aim: Create Subnet and transfer the data.

Theory: In subnetting, a network is divided into several smaller subnetworks (subnets) with each subnetwork having its own subnetwork address.

The IP addresses were originally designed with two levels of addressing. To reach a host on the Internet, we must first reach the network and then the host. It soon became clear that we need more than two hierarchical levels, for two reasons. First, an organization that was granted a block in class A or B needed to divide its large network into several sub networks for better security and management. Second, since the blocks in class A and B were almost depleted and the blocks in class C were smaller than the needs of most organizations, an organization that has been granted a block in class A or B could divide the block into smaller sub blocks and share them with other organizations. The idea of splitting a block to smaller blocks is referred to as subnetting.

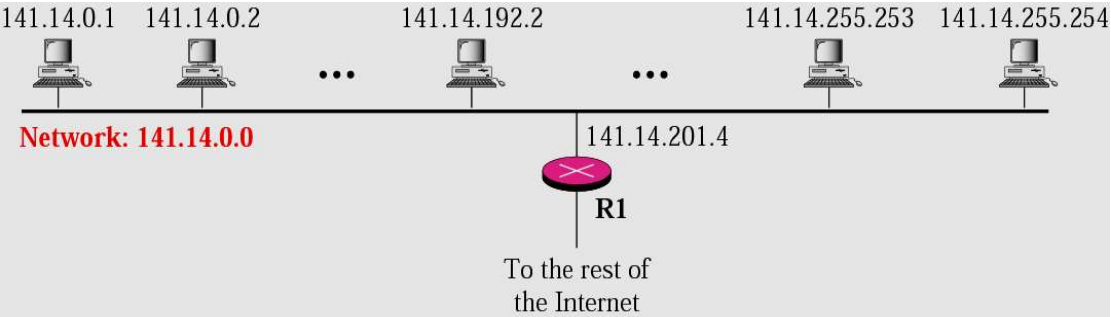


Figure: A network with two levels of hierarchy (not subnetted)

Figure shows a network using class B addresses before subnetting. We have just one network with almost 2^{16} hosts. The whole network is connected, through one single connection, to one of the routers in the Internet.

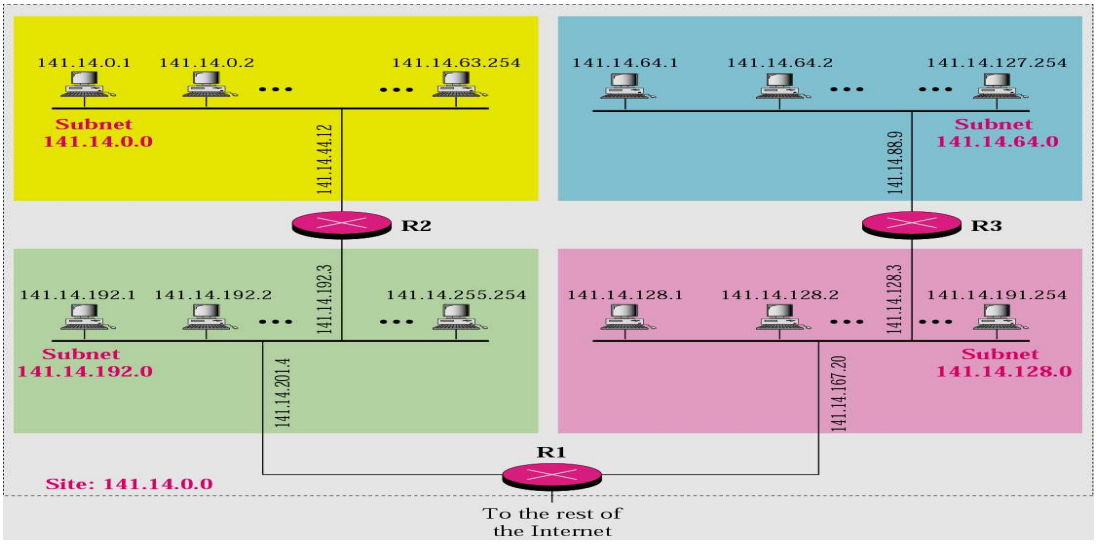
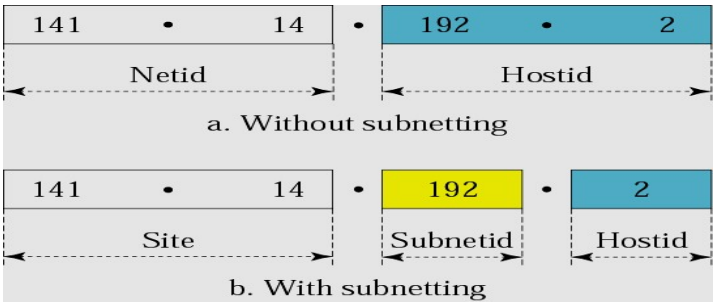


Figure: A network with three levels of hierarchy (subnetted)

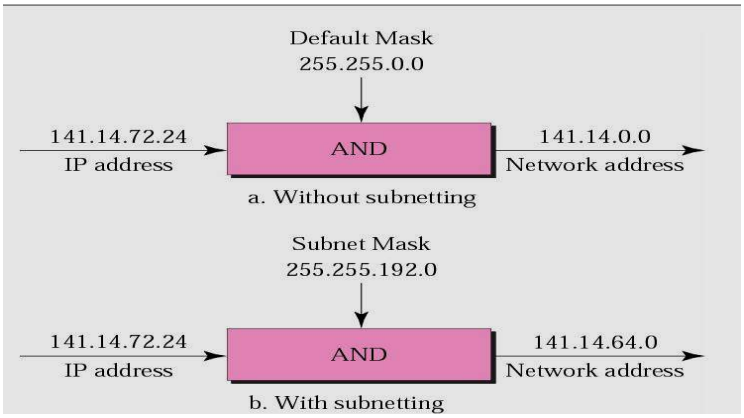
Figure shows the same network in Figure 2.2 after subnetting. The whole network is still connected to the Internet through the same router. However, the network has used a private router to divide the network into four subnetworks. The rest of the Internet still sees only one network; internally the network is made of four subnetworks. Each subnetwork can now have almost 2^{14} hosts. The network can belong to a university campus with four different schools (buildings). After subnetting, each school has its own subnetworks, but still the whole campus is one network for the rest of the Internet.

Subnet Mask

We discussed the network mask (default mask) before. The network mask is used when a network is not subnetted. When we divide a network to several subnetworks, we need to create a subnetwork mask (or subnet mask) for each subnetwork. A subnetwork has subnetid and hostid as shown in Figure.

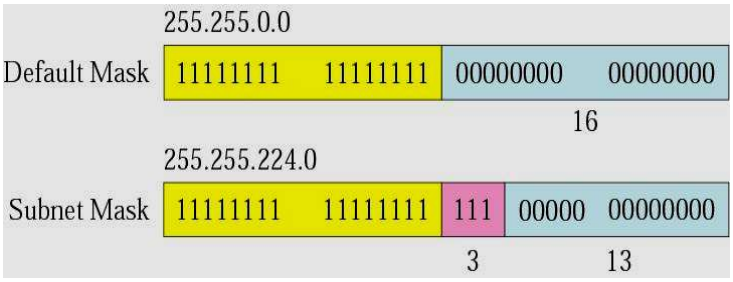


Subnetting increases the length of the netid and decreases the length of hostid. When we divide a network to s number of subnetworks, each of equal numbers of hosts, we can calculate the subnetid for each subnetwork.



- The number of 1s in a default mask is predetermined: 8, 16, or 24
- But, in a subnet mask, the number of 1s is more than the number of 1s in the corresponding default mask

Comparison of a Default Mask and a Subnet Mask



Number of Subnetworks

- Found by counting the number of extra bits that are added to the default mask in a subnet mask
- For example, in above figure
    - The number of extra 1s is 3
    - The length of subnetid = 3
    - The number of subnets is 2^3 = 8

Number of Addresses per Subnet

- Found by counting the number of 0s in the subnet mask
- For example, in above figure
    - The number of 0s is 13
    - The length of hostid = 13
    - The number of addressed in each subnet is 2^13 = 8192

Result: Subnetting of a network has been carried out.

SRM
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University *u/s 3 of UGC Act, 1956)*
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

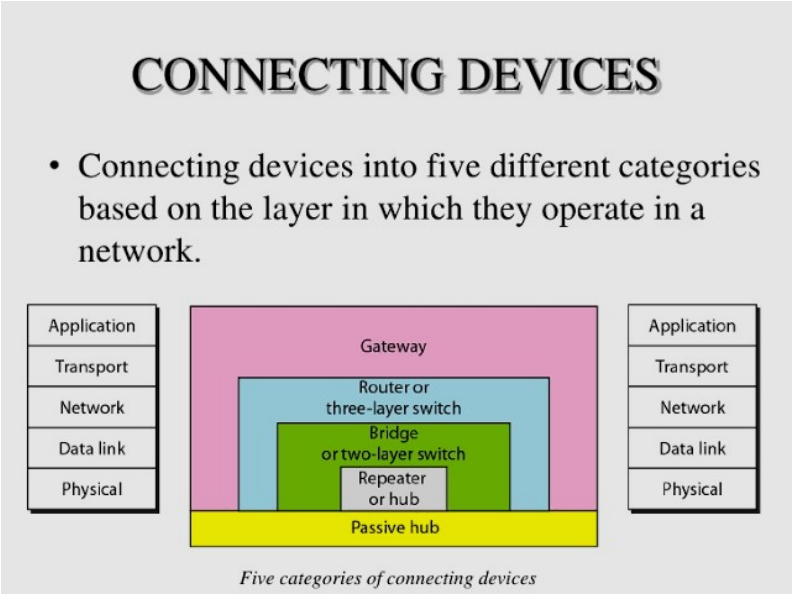
S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-4

Aim: Router Configuration (Configuring Interface)

Theory:



Five categories of connecting devices

1. Repeater: Functioning at Physical Layer. A repeater is an electronic device that receives a signal and retransmits it at a higher level and/or higher power, or onto the other side of an obstruction, so that the signal can cover longer distances. Repeater have two ports, so cannot be use to connect for more than two devices

2. Hub: An Ethernet hub, active hub, network hub, repeater hub, hub or concentrator is a device for connecting multiple twisted pair or fiber optic Ethernet devices together and making them act as a single network segment. Hubs work at the physical layer (layer 1) of the OSI model. The device is a form of multiport repeater. Repeater hubs also participate in collision detection, forwarding a jam signal to all ports if it detects a collision.

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

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

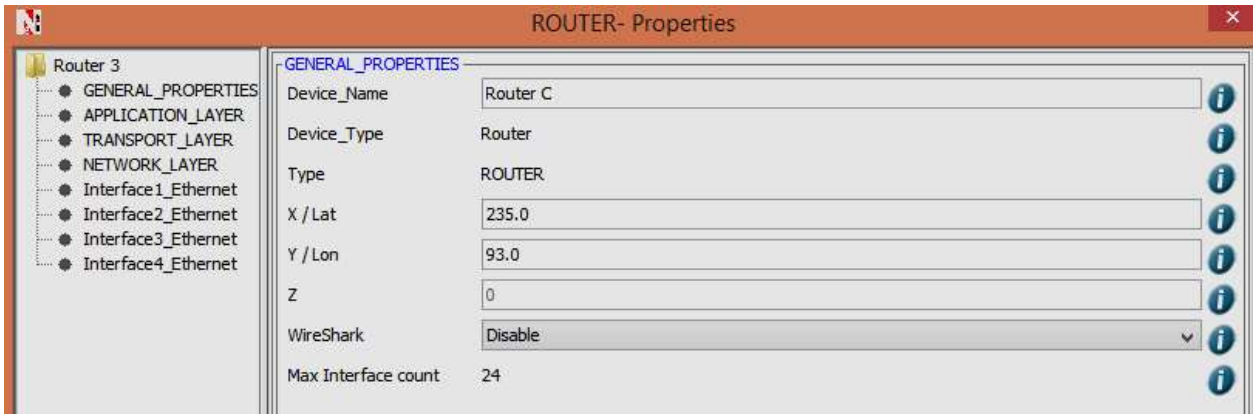
5. **Router**: A router is an electronic device that interconnects two or more computer networks, and selectively interchanges packets of data between them. Each data packet contains address information that a router can use to determine if the source and destination are on the same network, or if the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

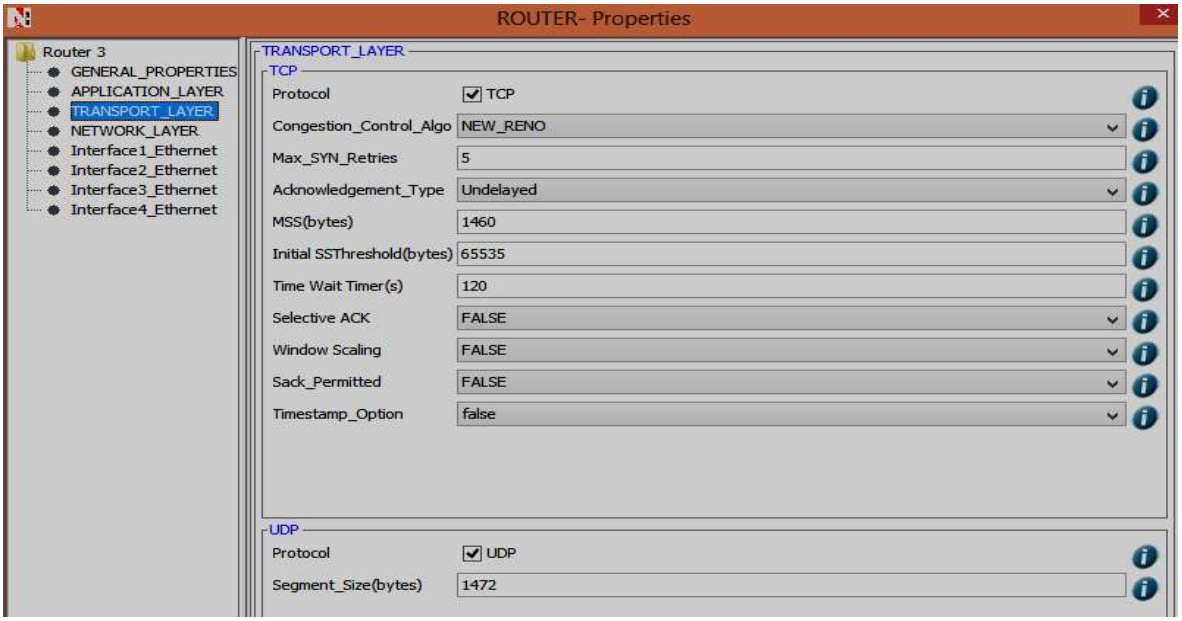
6. Gate Way: In a communications network, a network node equipped for interfacing with another network that uses different protocols.

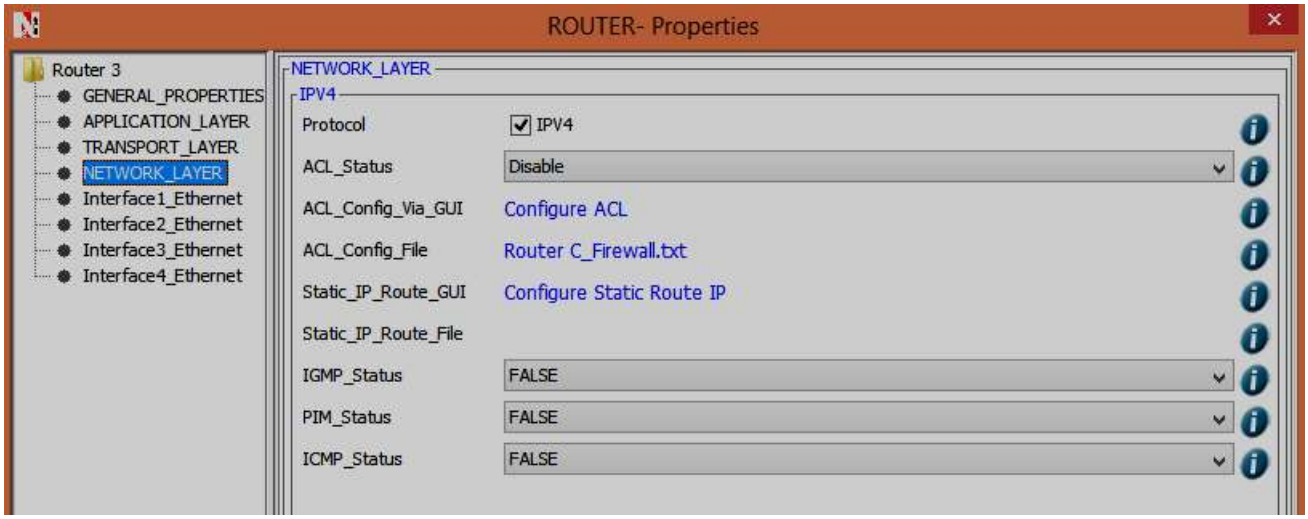
• A gateway may contain devices such as protocol translators, impedance matching devices, rate converters, fault isolators, or signal translators as necessary to provide system interoperability. It also requires the establishment of mutually acceptable administrative procedures between both networks.

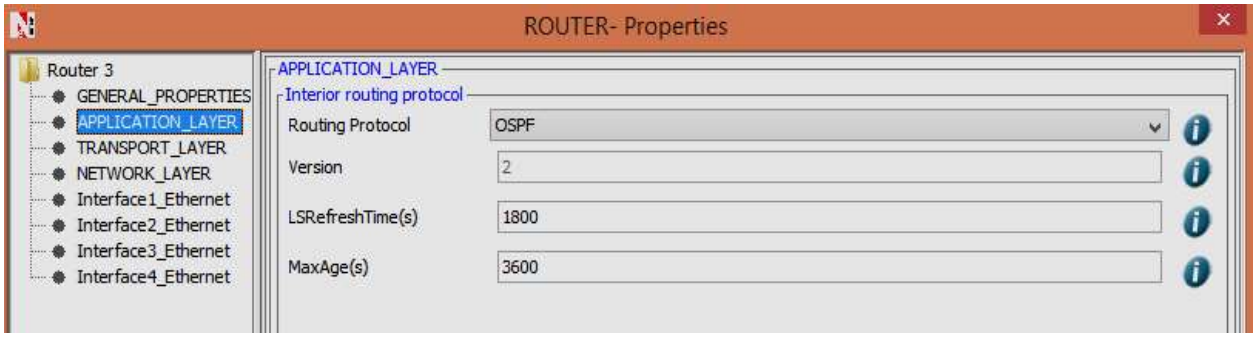
• A protocol translation/mapping gateway interconnects networks with different network protocol technologies by performing the required protocol conversions.

Configuration diagram:


ROUTER- Properties
Router 3
GENERAL_PROPERTIES
APPLICATION_LAYER
TRANSPORT_LAYER
NETWORK_LAYER
Interface1_Ethernet
Interface2_Ethernet
Interface3_Ethernet
Interface4_Ethernet
GENERAL_PROPERTIES
Device_Name
Router C
Device_Type
Router
Type
ROUTER
X / Lat
235.0
Y / Lon
93.0
Z
0
WireShark
Disable
Max Interface count
24


ROUTER- Properties
Router 3
GENERAL_PROPERTIES
APPLICATION_LAYER
TRANSPORT_LAYER
NETWORK_LAYER
Interface1_Ethernet
Interface2_Ethernet
Interface3_Ethernet
Interface4_Ethernet
TRANSPORT_LAYER
TCP
Protocol
TCP
Congestion_Control_Algo
NEW_RENO
Max_SYN_Retries
5
Acknowledgement_Type
Undelayed
MSS(bytes)
1460
Initial SSThreshold(bytes)
65535
Time Wait Timer(s)
120
Selective ACK
FALSE
Window Scaling
FALSE
Sack_Permitted
FALSE
Timestamp_Option
false
UDP
Protocol
UDP
Segment_Size(bytes)
1472


ROUTER- Properties
Router 3
GENERAL_PROPERTIES
APPLICATION_LAYER
TRANSPORT_LAYER
NETWORK_LAYER
Interface1_Ethernet
Interface2_Ethernet
Interface3_Ethernet
Interface4_Ethernet
NETWORK_LAYER
IPV4
Protocol
IPV4
ACL_Status
Disable
ACL_Config_Via_GUI
Configure ACL
ACL_Config_File
Router C_Firewall.txt
Static_IP_Route_GUI
Configure Static Route IP
Static_IP_Route_File
IGMP_Status
FALSE
PIM_Status
FALSE
ICMP_Status
FALSE



Result: Router is configured with different type of Interface

SRM
INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University *u/s 3 of UGC Act, 1956)*
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

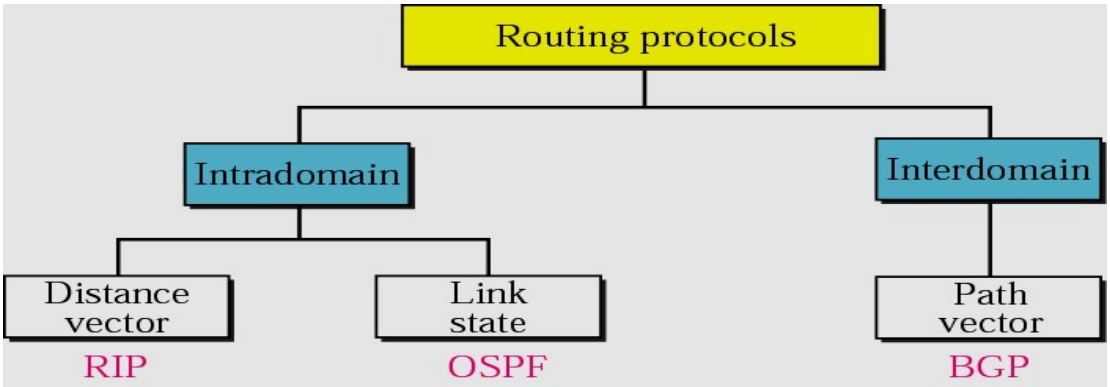
S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-5

Aim: Create a network for data transfer through Routing Information Protocol (RIP).

Theory:



DISTANCE VECTOR ROUTING

- In this type of routing a router can normally be represented by a node and a network by a link connecting two nodes
- This method sees an AS, with all routers and networks, as a graph, a set of nodes and lines (edges) connecting the nodes.
- The graph theory used an algorithm called **Bellman-Ford** (also called Ford-Fulkerson) for a while to find the shortest path between nodes in a graph given the distance between nodes

LINK STATE ROUTING

Link state routing has a different philosophy from that of distance vector routing. In link state routing, if each node in the domain has the entire topology of the domain— the list of nodes and links, how they are connected including the type, cost (metric), and the condition of the links (up or down)—the node can use the **Dijkstra algorithm** to build a routing table.

RIP:

RIP is intended to allow hosts and gateways to exchange information for computing routes through an IP-based network. RIP is a distance vector protocol which is based on Bellman Ford algorithm. This algorithm has been used for routing computation in the network. Distance vector algorithms are based on the exchange of only a small amount of information using RIP messages.

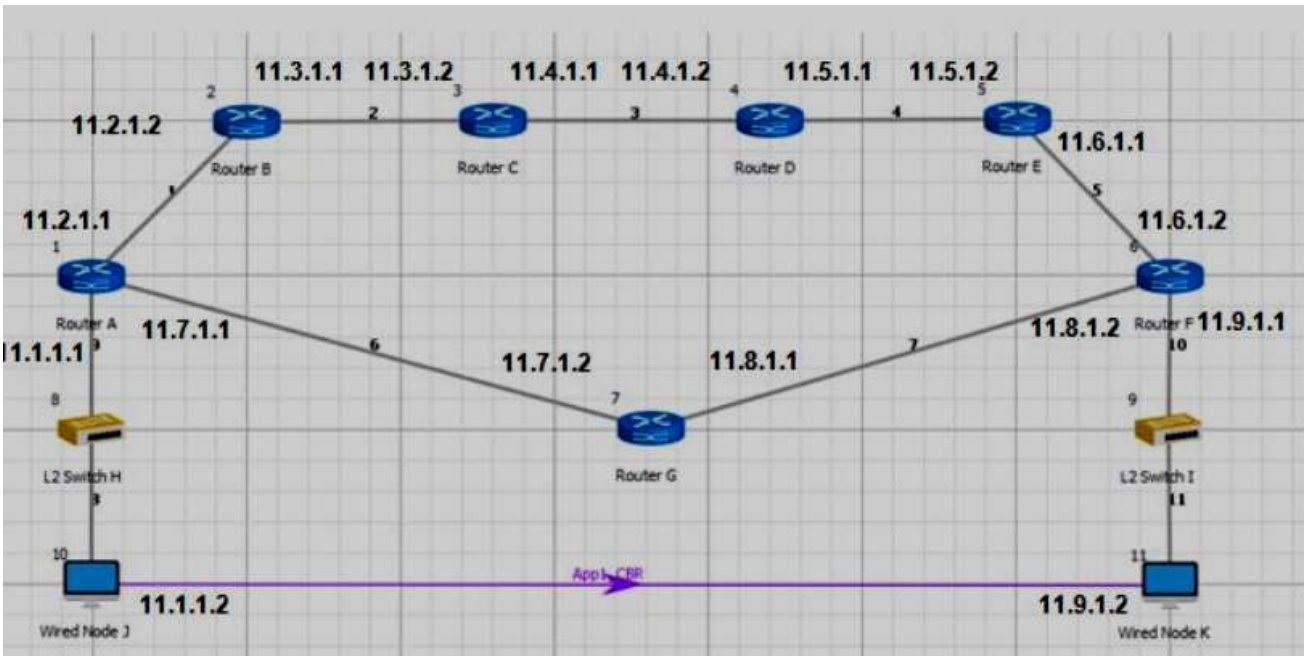
Each entity (router or host) that participates in the routing protocol is assumed to keep information about all of the destinations within the system. Generally, information about all entities connected to one network is summarized by a single entry, which describes the route to all destinations on that network. This summarization is possible because as far as IP is concerned, routing within a network is invisible. Each entry in this routing database includes the next router to which datagram's destined for the entity should be sent. In addition, it includes a "metric" measuring the total distance to the entity. Distance is a somewhat generalized concept, which may cover the time delay in getting messages to the entity, the dollar cost of sending messages to it, etc. Distance vector algorithms get their name from the fact that it is possible to compute optimal routes when the only information exchanged is the list of these distances. Furthermore, information is only exchanged among entities that are adjacent, that is, entities that share a common network.

Procedure

Sample 1:

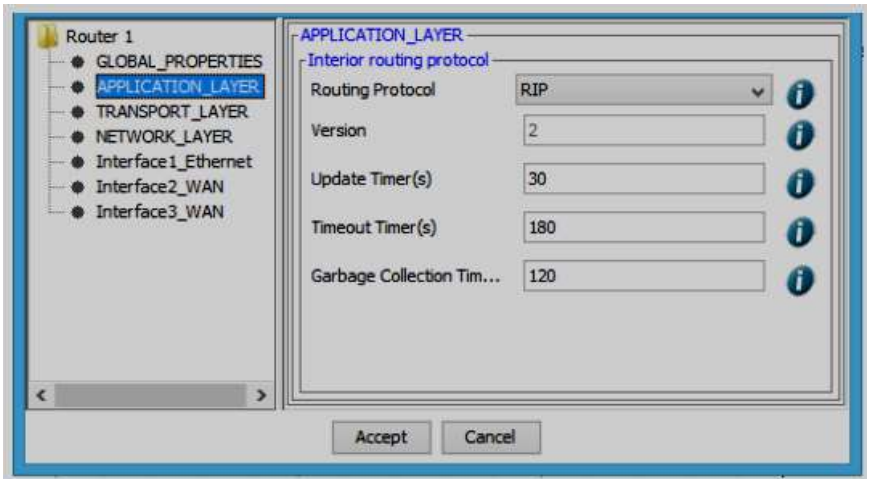
Step 1: Go to, New ◊ Internetworks

Step2: Click & drop Routers, Switches and Nodes onto the Simulation Environment and link them
as shown:



Step 3:

These properties can be set only after devices are linked to each other as shown above.



Set the properties of the Router 1 as follows:

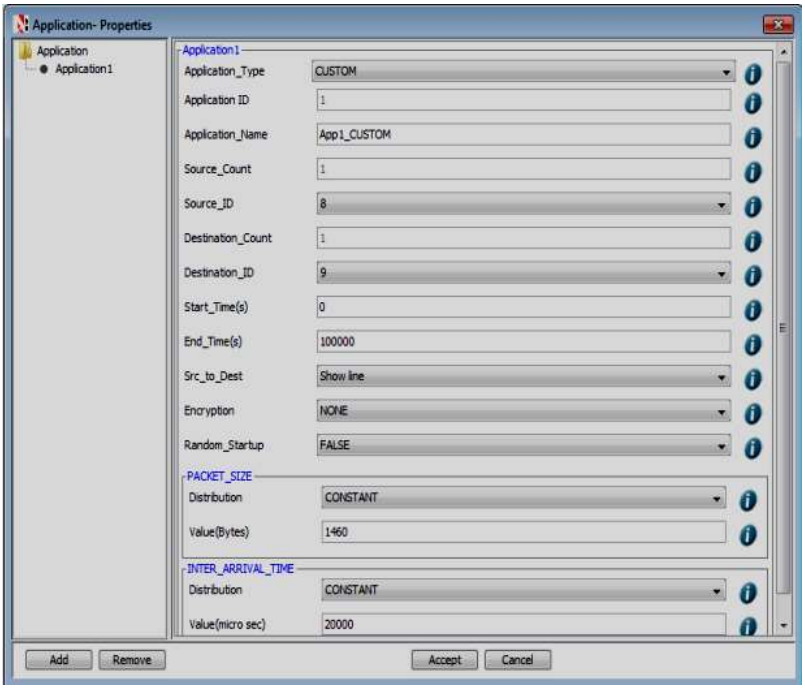
Node Properties: In Wired Node J, go to Transport Layer and set TCP as Disable

Switch Properties: Accept default properties for Switch.

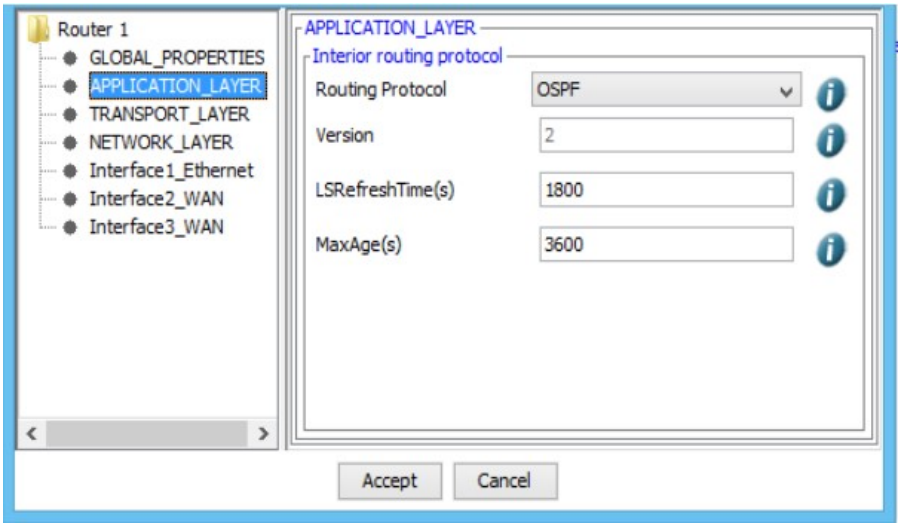
Link Properties:

Link Properties	Link 1	Link 2	Link 3	Link 4	Link 5	Link 6	Link 7
Uplink Speed	100	100	100	100	100	100	100
Downlink Speed	100	100	100	100	100	100	100

Application Properties: Click and drop the Application icon and set properties as follows:



SimulationTime-100Sec. After Simulation is performed, save the experiment. **Sample 2:** To model a scenario, follow the same steps as given in Sample1 and set the Router A properties as given below:



Application Properties: Click and drop Application icon and set properties as in Sample 1.

Simulation Time- 100 Sec

Output and Inference:

RIP

In Distance vector routing, each router periodically shares its knowledge about the entire network with its neighbors. The three keys for understanding the algorithm:

1. Knowledge about the whole network

Router sends all of its collected knowledge about the network to its neighbors

2. Routing only to neighbors

Each router periodically sends its knowledge about the network only to those routers to which it has direct links. It sends whatever knowledge it has about the whole network through all of its ports. This information is received and kept by each neighboring router and used to update that router's own information about the network.

3. Information sharing at regular intervals

For example, every 30 seconds, each router sends its information about the whole network to its neighbors. This sharing occurs whether or not the network has changed since the last time information was exchanged

In NetSim the Routing table Formation has 3 stages

Initial Table: This table will show the direct connections made by each Router.

Intermediate Table: The Intermediate table will have the updates of the Network in every 30 seconds

Final Table: This table is formed when there is no update in the Network.

The data should be forwarded using Routing Table with the shortest distance.

The RIP table in NetSim

• After running Sample1, click IP Forwarding table in Simulation Analysis screen. Then click the respective router to view the Routing table.

• We have shown the routing table for Router A and G which take part in routing the packets from source to destination.

• The destination node has the IP address 11.9.1.2 and belongs to the network 11.9.0.0

ROUTER A_Table

ROUTER A ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.3.0.0	255.255.0.0	11.2.1.2	11.2.1.1	1	RIP
11.8.0.0	255.255.0.0	11.7.1.2	11.7.1.1	1	RIP
11.4.0.0	255.255.0.0	11.2.1.2	11.2.1.1	2	RIP
11.6.0.0	255.255.0.0	11.7.1.2	11.7.1.1	2	RIP
11.9.0.0	255.255.0.0	11.7.1.2	11.7.1.1	2	RIP
11.5.0.0	255.255.0.0	11.2.1.2	11.2.1.1	3	RIP
11.1.0.0	255.255.0.0	on-link	11.1.1.1	300	LOCAL
11.7.0.0	255.255.0.0	on-link	11.7.1.1	300	LOCAL
11.2.0.0	255.255.0.0	on-link	11.2.1.1	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.2.1.1 11.7.1.1 11.1.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.2.1.1 11.7.1.1 11.1.1.1	306	MULTICAST
255.255.255.255	255.255.255.255	on-link	11.1.1.1	999	BROADCAST

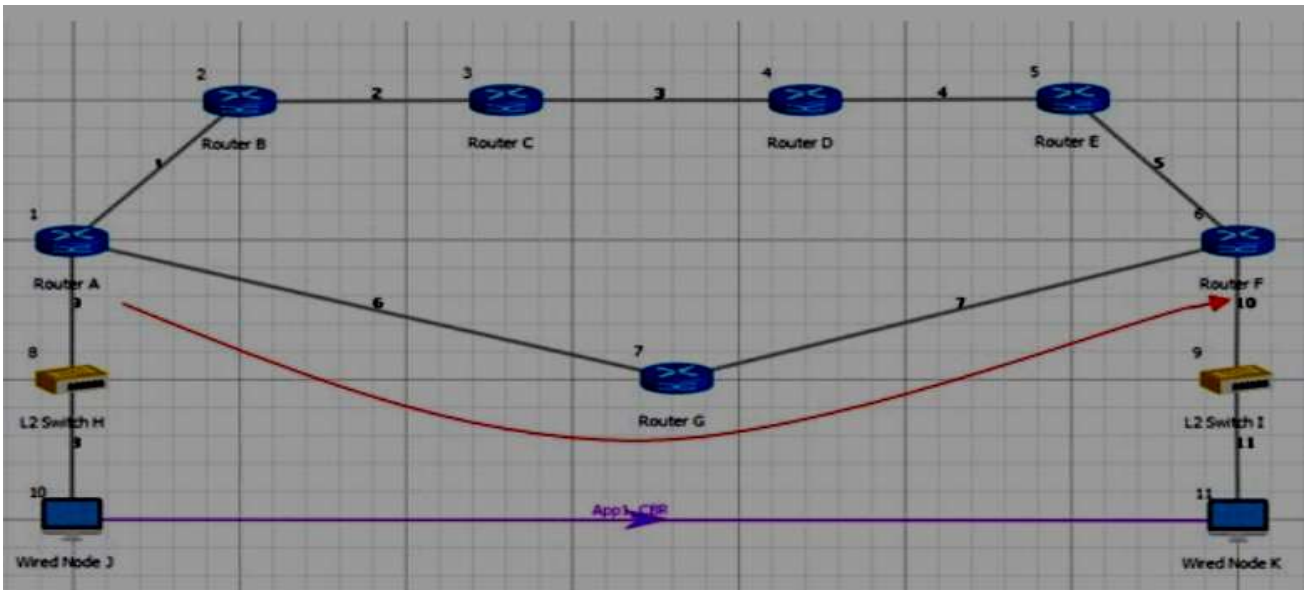
From the IP Forwarding table of Router A, it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router G with interface IP 11.7.1.1

ROUTER G_Table

ROUTER G ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.2.0.0	255.255.0.0	11.7.1.1	11.7.1.2	1	RIP
11.1.0.0	255.255.0.0	11.7.1.1	11.7.1.2	1	RIP
11.6.0.0	255.255.0.0	11.8.1.2	11.8.1.1	1	RIP
11.9.0.0	255.255.0.0	11.8.1.2	11.8.1.1	1	RIP
11.3.0.0	255.255.0.0	11.7.1.1	11.7.1.2	2	RIP
11.5.0.0	255.255.0.0	11.8.1.2	11.8.1.1	2	RIP
11.4.0.0	255.255.0.0	11.8.1.2	11.8.1.1	3	RIP
11.8.0.0	255.255.0.0	on-link	11.8.1.1	300	LOCAL
11.7.0.0	255.255.0.0	on-link	11.7.1.2	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.7.1.2 11.8.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.7.1.2 11.8.1.1	306	MULTICAST

From the IP Forwarding table of Router G it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router F with interface IP 11.8.1.1



Shortest Path from Wired Node H to Wired Node I in RIP (Use Packet Animation to view) is **Wired Node J->L2 Switch H->Router A->Router G->Router F->L2 Switch I->Wired Node K.** RIP chooses the lower path (number of hops is less) to forward packets from source to destination since it is based on hop count.

Result: Network created and the data transferred through Routing Information Protocol (RIP)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-6

Aim: Create a network for data transfer through Open Shortest Path First (OSPF) protocol.

Theory: In OSPF, the Packets are transmitted through the shortest path between the source and destination

Shortest path: OSPF allows administrator to assign a cost for passing through a link. The total cost of a particular route is equal to the sum of the costs of all links that comprise the route. A router chooses the route with the shortest (smallest) cost.

In OSPF, each router has a link state database which is tabular representation of the topology of the network (including cost). Using dijkstra algorithm each router finds the shortest path between source and destination.

Formation of OSPF Routing Table

1. OSPF-speaking routers send Hello packets out all OSPF-enabled interfaces. If two routers sharing a common data link agree on certain parameters specified in their respective Hello packets, they will become neighbors.

2. Adjacencies, which can be thought of as virtual point-to-point links, are formed between some neighbors. OSPF defines several network types and several router types. The establishment of an adjacency is determined by the types of routers exchanging Hellos and the type of network over which the Hellos are exchanged.

3. Each router sends link-state advertisements (LSAs) over all adjacencies. The LSAs describe all of the router's links, or interfaces, the router's neighbors, and the state of the links. These links might be to stub networks (networks with no other router attached), to other OSPF routers, or to external networks (networks learned from another routing process). Because of the varying types of link-state information, OSPF defines multiple LSA types.

4. Each router receiving an LSA from a neighbor records the LSA in its link-state database and sends a copy of the LSA to all of its other neighbors.

5. By flooding LSAs throughout an area, all routers will build identical link-state databases.
6. When the databases are complete, each router uses the SPF algorithm to calculate a loop-free graph describing the shortest (lowest cost) path to every known destination, with itself as the root. This graph is the SPF tree.

7. Each router builds its route table from its SPF tree

******Network Design: Follow the design procedure of RIP as Exp-5**

OSPF

The main operation of the OSPF protocol occurs in the following consecutive stages and leads to the convergence of the internetworks:

1. Compiling the LSDB

2. Calculating the Shortest Path First (SPF) Tree.
3. Creating the routing table entries.

Compiling the LSDB

The LSDB is a database of all OSPF router LSAs. The LSDB is compiled by an ongoing exchange of LSAs between neighbouring routers so that each router is synchronized with its neighbour. When the Network converged, all routers have the appropriate entries in their LSDB.

Calculating the SPF Tree Using Dijkstra's Algorithm

Once the LSDB is compiled, each OSPF router performs a least cost path calculation called the Dijkstra algorithm on the information in the LSDB and creates a tree of shortest paths to each other router and network with themselves as the root. This tree is known as the SPF Tree and contains a single, least cost path to each router and in the Network. The least cost path calculation is performed by each router with itself as the root of the tree

Calculating the Routing Table Entries from the SPF Tree

The OSPF routing table entries are created from the SPF tree and a single entry for each network in the AS is produced. The metric for the routing table entry is the OSPF-calculated cost, not a hop count.

Link Properties:

Link Properties	Link 1	Link 2	Link 3	Link 4	Link 5	Link 6	Link 7
Uplink Speed	100	100	100	100	100	10	10
Downlink Speed	100	100	100	100	100	10	10

The OSPF table in NetSim

• After running Sample 2, click IP Forwarding table in Simulation Analysis screen. Then click the router to view the Routing table

We have shown the routing table for Router A, B, C, D and E which take part in routing the data packets from source to destination.

ROUTER A_Table

ROUTER A ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.3.0.0	255.255.0.0	11.2.1.2	11.2.1.1	2	OSPF
11.4.0.0	255.255.0.0	11.2.1.2	11.2.1.1	3	OSPF
11.5.0.0	255.255.0.0	11.2.1.2	11.2.1.1	4	OSPF
11.6.0.0	255.255.0.0	11.2.1.2	11.2.1.1	5	OSPF
11.9.0.0	255.255.0.0	11.2.1.2	11.2.1.1	6	OSPF
11.8.0.0	255.255.0.0	11.2.1.2	11.2.1.1	15	OSPF
11.1.0.0	255.255.0.0	on-link	11.1.1.1	300	LOCAL
11.7.0.0	255.255.0.0	on-link	11.7.1.1	300	LOCAL
11.2.0.0	255.255.0.0	on-link	11.2.1.1	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.2.1.1 11.7.1.1 11.1.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.2.1.1 11.7.1.1 11.1.1.1	306	MULTICAST
255.255.255.255	255.255.255.255	on-link	11.1.1.1	999	BROADCAST

From the IP Forwarding table of Router A it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router B with interface IP 11.2.1.1

ROUTER B_Table

ROUTER B ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.1.0.0	255.255.0.0	11.2.1.1	11.2.1.2	2	OSPF
11.4.0.0	255.255.0.0	11.3.1.2	11.3.1.1	2	OSPF
11.5.0.0	255.255.0.0	11.3.1.2	11.3.1.1	3	OSPF
11.6.0.0	255.255.0.0	11.3.1.2	11.3.1.1	4	OSPF
11.9.0.0	255.255.0.0	11.3.1.2	11.3.1.1	5	OSPF
11.7.0.0	255.255.0.0	11.2.1.1	11.2.1.2	11	OSPF
11.8.0.0	255.255.0.0	11.3.1.2	11.3.1.1	14	OSPF
11.3.0.0	255.255.0.0	on-link	11.3.1.1	300	LOCAL
11.2.0.0	255.255.0.0	on-link	11.2.1.2	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.2.1.2 11.3.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.2.1.2 11.3.1.1	306	MULTICAST

From the IP Forwarding table of Router B it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router C with interface IP 11.3.1.1

ROUTER C_Table

ROUTER C ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.5.0.0	255.255.0.0	11.4.1.2	11.4.1.1	2	OSPF
11.2.0.0	255.255.0.0	11.3.1.1	11.3.1.2	2	OSPF
11.6.0.0	255.255.0.0	11.4.1.2	11.4.1.1	3	OSPF
11.1.0.0	255.255.0.0	11.3.1.1	11.3.1.2	3	OSPF
11.9.0.0	255.255.0.0	11.4.1.2	11.4.1.1	4	OSPF
11.7.0.0	255.255.0.0	11.3.1.1	11.3.1.2	12	OSPF
11.8.0.0	255.255.0.0	11.4.1.2	11.4.1.1	13	OSPF
11.4.0.0	255.255.0.0	on-link	11.4.1.1	300	LOCAL
11.3.0.0	255.255.0.0	on-link	11.3.1.2	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.3.1.2 11.4.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.3.1.2 11.4.1.1	306	MULTICAST

From the IP Forwarding table of Router C it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router D with interface IP 11.4.1.1

ROUTER D_Table

ROUTER D ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.6.0.0	255.255.0.0	11.5.1.2	11.5.1.1	2	OSPF
11.3.0.0	255.255.0.0	11.4.1.1	11.4.1.2	2	OSPF
11.2.0.0	255.255.0.0	11.4.1.1	11.4.1.2	3	OSPF
11.9.0.0	255.255.0.0	11.5.1.2	11.5.1.1	3	OSPF
11.1.0.0	255.255.0.0	11.4.1.1	11.4.1.2	4	OSPF
11.8.0.0	255.255.0.0	11.5.1.2	11.5.1.1	12	OSPF
11.7.0.0	255.255.0.0	11.4.1.1	11.4.1.2	13	OSPF
11.5.0.0	255.255.0.0	on-link	11.5.1.1	300	LOCAL
11.4.0.0	255.255.0.0	on-link	11.4.1.2	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.4.1.2 11.5.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.4.1.2 11.5.1.1	306	MULTICAST

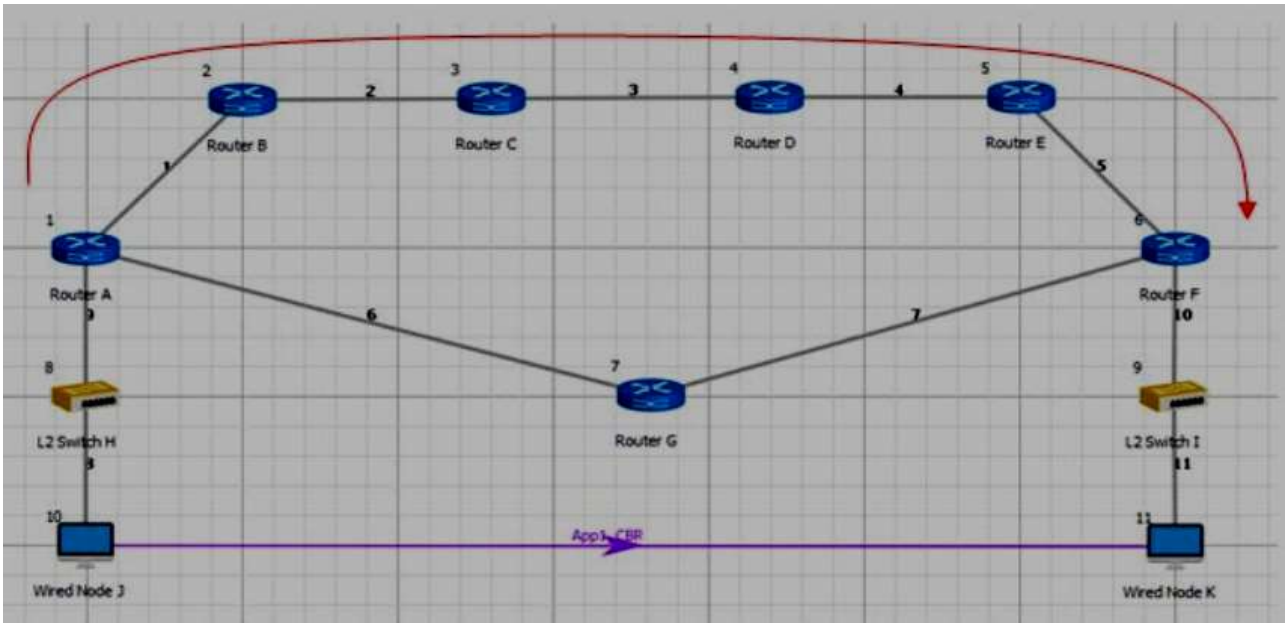
From the IP Forwarding table of Router D it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router E with interface IP 11.5.1.1

ROUTER E_Table

ROUTER E ☑ Detailed View

Network Destination	Netmask/Prefix len	Gateway	Interface	Metrics	Type
11.9.0.0	255.255.0.0	11.6.1.2	11.6.1.1	2	OSPF
11.4.0.0	255.255.0.0	11.5.1.1	11.5.1.2	2	OSPF
11.3.0.0	255.255.0.0	11.5.1.1	11.5.1.2	3	OSPF
11.2.0.0	255.255.0.0	11.5.1.1	11.5.1.2	4	OSPF
11.1.0.0	255.255.0.0	11.5.1.1	11.5.1.2	5	OSPF
11.8.0.0	255.255.0.0	11.6.1.2	11.6.1.1	11	OSPF
11.7.0.0	255.255.0.0	11.5.1.1	11.5.1.2	14	OSPF
11.6.0.0	255.255.0.0	on-link	11.6.1.1	300	LOCAL
11.5.0.0	255.255.0.0	on-link	11.5.1.2	300	LOCAL
224.0.0.1	255.255.255.255	on-link	11.5.1.2 11.6.1.1	306	MULTICAST
224.0.0.0	240.0.0.0	on-link	11.5.1.2 11.6.1.1	306	MULTICAST

From the IP Forwarding table of Router E it is evident that all packets destined to the network 11.9.0.0 are forwarded to the Router F with interface IP 11.6.1.1



Shortest Path from Wired Node H to Wired Node I in OSPF (Use Packet Animation to view) **Wired Node J->L2 Switch H->Router A->Router B->Router C->Router D->Router E->Router F->L2 Switch I->Wired Node K.** OSPF chooses the upper path (cost is less-5) since OSPF is based on cost.

Note: The Cost is calculated by using the following formula

$$Cost = \frac{ReferenceBandwidth}{LinkSpeedUp}$$

Reference Bandwidth = 100 Mbps

For Example,

Let us take, Link Speed UP = 100 Mbps

$$Cost = \frac{100\ (ReferenceBandwidth)}{100\ (LinkSpeedUP)} = 1$$

Note: The device / link numbering and IP Address setting in NetSim is based on order in which in the devices are dragged & dropped, and the order in which links are connected. Hence if the order in which a user executes these tasks is different from what is shown in the screen shots, users would notice different tables from what is shown in the screen shots.

Result: Network created and the data transferred through Open Shortest Path First (OSPF)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-7

Aim: Create a network for data transfer through Border Gateway Protocol (BGP).

Theory: In BGP, the Packets are transmitted between the Autonomous system using Path vector Routing.

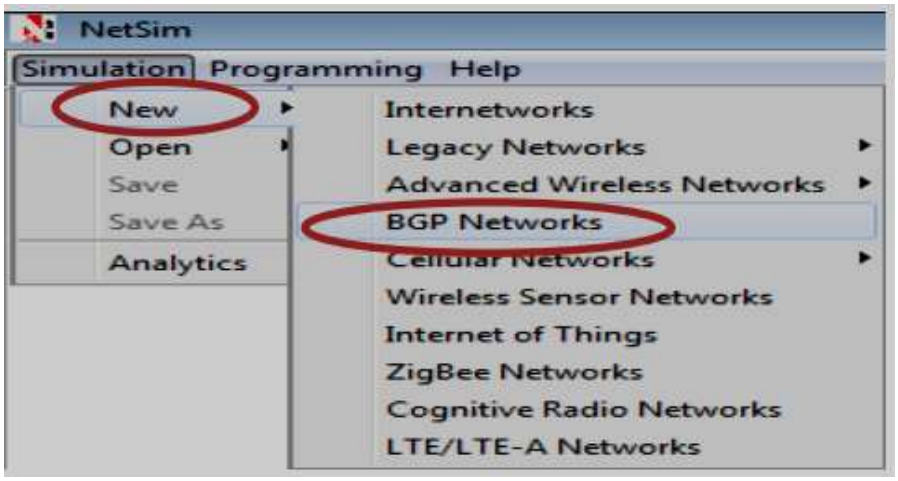
Path Vector Routing:

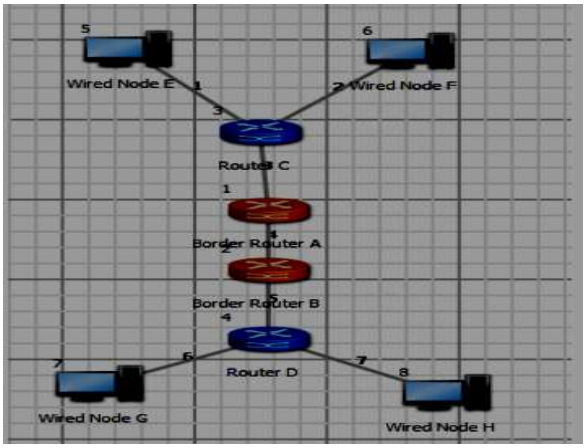
Path vector routing is used for inter-domain routing. It is similar to distance vector routing. In path vector routing we assume that there is one Router (there can be many) in each autonomous system which acts on behalf of the entire autonomous system. This Router is called the Border Router. The Border Router in one Autonomous System creates a routing table and advertises it to neighboring Border Router which belongs to neighboring autonomous systems. The idea is same as distance vector routing except that only Border Routers in each autonomous system can communicate with each other. The Border Routers advertises the path, not the metric, in its autonomous system or other autonomous systems.

Procedure:

Step 1:

Go to Simulation → New → BGP Networks





Sample Inputs:

Follow the steps given in the different samples to arrive at the objective.

- Total no of nodes used: 4
- Total number of Internal Routers used: 2
- Total number of Border Routers used: 2

The devices are interconnected as given below,

- Wired Node E and Wired Node F are connected by Link 1 and Link 2 to Router C.
- Internal Router C and Border Router A are connected by Link 3.
- Border Router A and Border Router B are connected by Link4.
- Border Router B and Router D are connected by Link 5.
- Router D is connected by Link 6 and Link 7to Wired Node G and Wired Node H respectively.

Set the properties for each device by following the tables

Application Properties	Application 1	Application 2
Application_Type	CUSTOM	CUSTOM
Source_Id	5	6
Destination_Id	7	8
Application Data size		
Distribution	Constant	Constant
Application Data size (bytes)	1472	1472
Inter Arrival Time		
Distribution	Constant	Constant
Mean Inter Arrival Time (µs)	20000	20000

Link Properties	Link 1	Link 2	Link 3	Link 4	Link 5	Link 6	Link 7
Bit Error Rate (BER)	0	0	0	0	0	0	0
Downlink Speed (Mbps)	8.448	8.448	10	1000	10	8.448	8.448
Uplink Speed (Mbps)	8.448	8.448	10	1000	10	8.448	8.448

Sample 1:

If selected internal gateway protocol is RIP then Router properties are as follows:

Router Properties	Border_ Router A		Border_ Router B	
	Interior Routing table	Exterior Routing table	Interior Routing table	Exterior Routing table
Protocol Type	RIP	BGP	RIP	BGP
Update Timer	30	-	30	-
Timeout Timer	180	-	180	-
Garbage Collection Timer	120	-	120	-

Router Properties	Router C	Router D
Routing Protocol	RIP	RIP
Update Timer	30	30
Timeout Timer	180	180
Garbage Collection Timer	120	120

Simulation Time - 10 Sec

(*Note:* *The Simulation Time can be selected only after doing the following two tasks,)*

- *Set the properties of Routers*
- *Then click on Run Simulation button**).***

After simulation save the experiment.

Sample 2:

If you want to select your internal gateway protocol as OSPF then here is the information you need to fill in for Router properties:

Router Properties	Border_ Router A		Border_ Router B	
	Interior Routing table	Exterior Routing table	Interior Routing table	Exterior Routing table
Protocol Type	OSPF	BGP	OSPF	BGP
LSRefreshTime	1800	-	1800	-
MaxAge	3600	-	3600	-

Router Properties	Router C	Router D
Routing Protocol	OSPF	OSPF
LSRefreshTime	1800	1800
MaxAge	3600	3600

Simulation Time - 10 Sec

(*Note:* *The Simulation Time can be selected only after doing the following two tasks,)*

- *Set the properties of Routers*
- *Then click on Run Simulation button**).***

Output:

After running this scenario, in Performance Metrics screen, routing tables are obtained in BGP table and RIP metrics.

If you click over the RIP metrics, you will get the RIP routing table for internal routers. If you click over the BGP table, you will get the routing table for Border routers. We have shown the routing tables for Border Router 1 and 2

Router1

PeerState	PeerLocalPort	PeerRemoteAddr	PeerRemotePort	PeerInUpdates	PeerOutUpdates	PeerInTotalMessages	PeerOutTotalMessages	NextHop
Internal	41	11.3.0.0	179	6	6	8	8	11.3.1.2
Internal	18467	12.2.0.0	179	6	6	8	8	12.2.1.1
Established	14604	13.2.0.0	179	6	6	8	8	12.2.1.2
Established	292	11.1.0.0	179	6	6	8	8	11.3.1.1
Established	17421	11.2.0.0	179	6	6	8	8	11.3.1.1
Established	17035	14.2.0.0	179	6	6	8	8	12.2.1.2
Established	23811	14.3.0.0	179	6	6	8	8	12.2.1.2

Router2

PeerState	PeerLocalPort	PeerRemoteAddr	PeerRemotePort	PeerInUpdates	PeerOutUpdates	PeerInTotalMessages	PeerOutTotalMessages	NextHop
Internal	6334	12.2.0.0	179	6	6	8	8	12.2.1.2
Internal	26500	13.2.0.0	179	6	6	8	8	13.2.1.1
Established	4827	11.3.0.0	179	6	6	8	8	12.2.1.1
Established	19718	14.2.0.0	179	6	6	8	8	13.2.1.2
Established	5447	14.3.0.0	179	6	6	8	8	13.2.1.2
Established	14771	11.1.0.0	179	6	6	8	8	12.2.1.1
Established	19912	11.2.0.0	179	6	6	8	8	12.2.1.1

The Border Routers stores the node's remote address in its Routing Table as shown in the above Tables under ―Peer Remote Address column.

Output: (Sample 2)

After running this scenario, in Performance Metrics screen, routing tables are obtained in BGP table and OSPF metrics.

If you click over the OSPF metrics, you will get the OSPF routing table for internal routers. If you click over the BGP table, you will get the routing table for Border routers. We have shown the routing tables for Border Router 1 and 2.

Router1

PeerState	PeerLocalPort	PeerRemoteAddr	PeerRemotePort	PeerInUpdates	PeerOutUpdates	PeerInTotalMessages	PeerOutTotalMessages	NextHop
Internal	41	11.3.0.0	179	6	6	8	8	11.3.1.2
Internal	18467	12.2.0.0	179	6	6	8	8	12.2.1.1
Established	14604	13.2.0.0	179	6	6	8	8	12.2.1.2
Established	19718	11.1.0.0	179	6	6	8	8	11.3.1.1
Established	5447	11.2.0.0	179	6	6	8	8	11.3.1.1
Established	14771	14.2.0.0	179	6	6	8	8	12.2.1.2
Established	19912	14.3.0.0	179	6	6	8	8	12.2.1.2

Router2								
PeerState	PeerLocalPort	PeerRemoteAddr	PeerRemotePort	PeerInUpdates	PeerOutUpdates	PeerInTotalMessages	PeerOutTotalMessages	NextHop
Internal	6334	12.2.0.0	179	6	6	8	8	12.2.1.2
Internal	26500	13.2.0.0	179	6	6	8	8	13.2.1.1
Established	4827	11.3.0.0	179	6	6	8	8	12.2.1.1
Established	292	14.2.0.0	179	6	6	8	8	13.2.1.2
Established	17421	14.3.0.0	179	6	6	8	8	13.2.1.2
Established	17035	11.1.0.0	179	6	6	8	8	12.2.1.1
Established	23811	11.2.0.0	179	6	6	8	8	12.2.1.1

Inference:

First the internal Routing tables (RIP/OSPF table) are formed among all the Routers. The Border Routers contains the network address of the next hop and the destination nodes as represented in the routing table. Border Routers communicate with each other by passing their Routing tables resulting in the formation of external Routing tables (BGP table). Then actual packet transmission takes place from Source to Destination.

Result: Network created and the data transferred through Border Gateway Protocol (BGP).

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)
DELHI-NCR CAMPUS, GHAZIABAD (U.P.)

SRM INSTITUTE OF SCIENCE & TECHNOLOGY

DELHI-NCR CAMPUS MODINAGAR

DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING

18CSS202J-Computer Communications Laboratory

Title of Experiment :
Name of the candidate : Registration Number : Date of Experiment : Date of submission :

S. No.	Marks split up	Max. Marks (10)	Marks Obtained
1	Preparation of Record	03	
2	Execution of Experiment	02	
3	Observations and Result	02	
4	Viva questions	03	
Total			

Signature of Examiner

Experiment-8

Aim: Create a network with Network address translation (NAT)

Theory:

Public Address:

A public IP address is assigned to every computer that connects to the Internet where each IP is unique. Hence there cannot exist two computers with the same public IP address all over the Internet. This addressing scheme makes it possible for the computers to "find each other" online and exchange information. User has no control over the IP address (public) that is assigned to the computer. The public IP address is assigned to the computer by the Internet Service Provider as soon as the computer is connected to the Internet gateway.

Private Address:

An IP address is considered private if the IP number falls within one of the IP address ranges reserved for private networks such as a Local Area Network (LAN). The Internet Assigned Numbers Authority (IANA) has reserved the following three blocks of the IP address space for private networks (local networks):

Class	Starting IP address	Ending IP address	No. of hosts
A	10.0.0.0	10.255.255.255	16,777,216
B	172.16.0.0	172.31.255.255	1,048,576
C	192.168.0.0	192.168.255.255	65,536

Private IP addresses are used for numbering the computers in a private network including home, school and business LANs in airports and hotels which makes it possible for the computers in the network to communicate with each other. For example, if a network A consists of 30 computers

each of them can be given an IP starting from **192.168.0.1 to 192.168.0.30.**

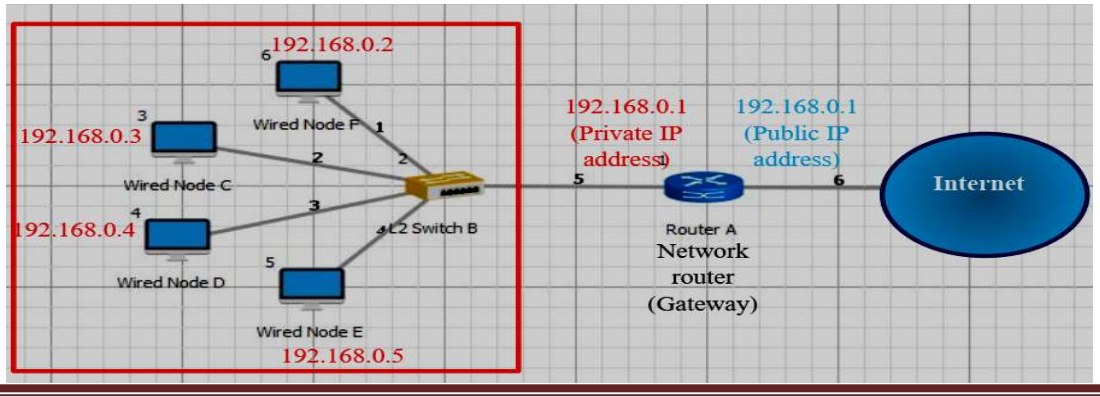
Devices with private IP addresses cannot connect directly to the Internet. Likewise, computers outside the local network cannot connect directly to a device with a private IP. It is possible to interconnect two private networks with the help of a router or a similar device that supports Network Address Translation.

If the private network is connected to the Internet (through an Internet connection via ISP) then each computer will have a private IP as well as a public IP. Private IP is used for communication within the network whereas the public IP is used for communication over the Internet.

Network address translation (NAT)

A NAT (Network Address Translation or Network Address Translator) is the virtualization of Internet Protocol (IP) addresses. NAT helps to improve security and decrease the number of IP addresses an organization needs.

A device that is configured with NAT will have at least one interface to the inside network and one to the outside network. In a typical environment, NAT is configured at the exit device between a stub domain (inside network) and the backbone. When a packet leaves the domain, NAT translates the locally significant source address into a globally unique address. When a packet enters the domain, NAT translates the globally unique destination address into a local address. If more than one exit point exists, each NAT must have the same translation table. NAT can be configured to advertise to the outside world only one address for the entire network. This ability provides additional security by effectively hiding the entire internal network behind that one address. If NAT cannot allocate an address because it has run out of addresses, it drops the packet and sends an Internet Control Message Protocol (ICMP) host unreachable packet to the destination.



NAT is

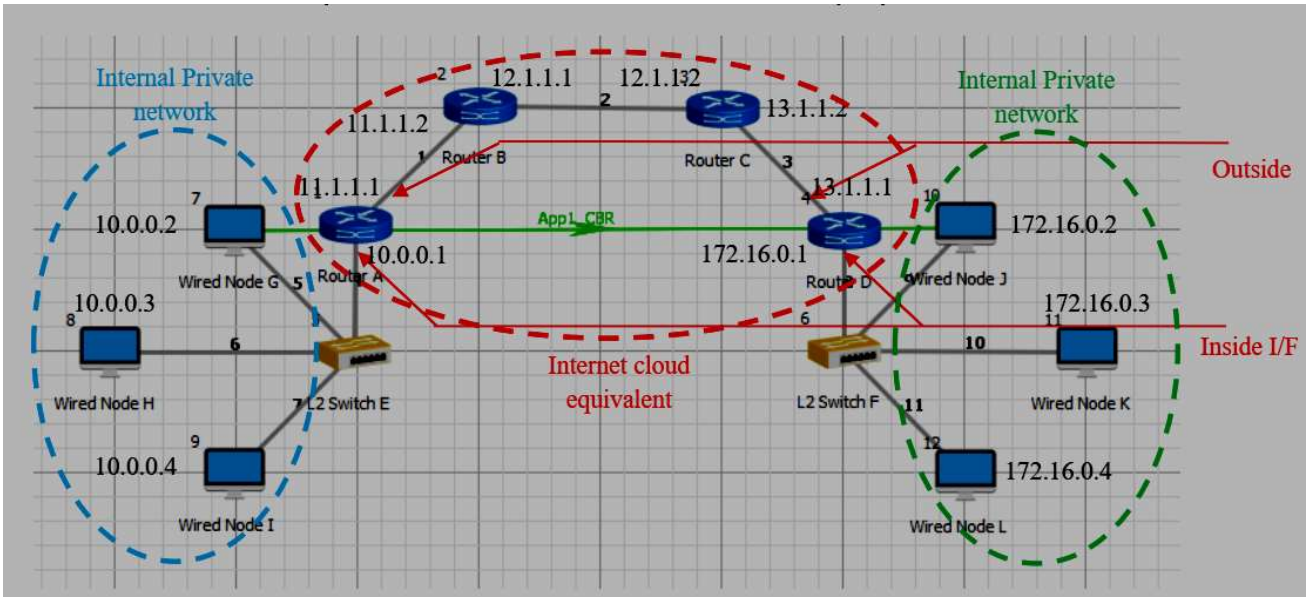
secure since it hides network from the Internet. All communications from internal private network are handled by the NAT device, which will ensure all the appropriate translations are performed and provide a flawless connection between internal devices and the Internet.

In the above figure, a simple network of 4 hosts and one router that connect this network to the Internet. All hosts in the network have a private Class C IP Address, including the router's private interface (192.168.0.1), while the public interface that's connected to the Internet has a real IP Address (203.31.220.134). This is the IP address the Internet sees as all internal IP addresses are hidden.

Network Setup

Working of NAT in NetSim:

Create a scenario as per the above screenshot and set the properties shown below:



Wired node Properties:

Wired Node	IP address	Subnet mask
G	10.0.0.2	255.0.0.0
H	10.0.0.3	255.0.0.0
I	10.0.0.4	255.0.0.0
J	172.16.0.2	255.255.0.0
K	172.16.0.3	255.255.0.0
L	172.16.0.4	255.255.0.0

Router Properties:

Router	Interface	IP address	Subnet mask
Router A	Interface1_WAN	11.1.1.1	255.0.0.0
	Interface2_Ethernet	10.0.0.1	255.0.0.0
Router B	Interface1_WAN	11.1.1.2	255.0.0.0
	Interface2_WAN	12.1.1.1	255.0.0.0
Router C	Interface1_WAN	12.1.1.2	255.0.0.0
	Interface2_WAN	13.1.1.2	255.0.0.0
Router D	Interface1_WAN	13.1.1.1	255.0.0.0
	Interface2_Ethernet	172.16.0.1	255.255.0.0

Enable Packet trace and run simulation for 10 seconds. After simulation open packet trace and filter Packet Id to 1

Inference

1	PACKET	SEGME	PACKET	CONTROL	SOURC	DESTINATION	SOURCE_IP	DESTINATION_IP	GATEWAY_IP	NEXT_HOP_IP
76	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	10.0.0.1	10.0.0.2	10.0.0.1
77	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	10.0.0.1	10.0.0.2	10.0.0.1
78	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	13.1.1.1	11.1.1.1	11.1.1.2
79	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	13.1.1.1	12.1.1.1	12.1.1.2
80	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	13.1.1.1	13.1.1.2	13.1.1.1
81	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	172.16.0.2	172.16.0.1	172.16.0.2
82	1	0	CBR	APP1_CBR	NODE-7	NODE-10	10.0.0.2	172.16.0.2	172.16.0.1	172.16.0.2

SOURCE_IP – source node IP (Node)

DESTINATION_IP – gateway IP (Router/ Node)

GATEWAY_IP – IP of the device which is transmitting a packet (Router/ Node)

NEXT_HOP_IP – IP of the next hop (Router/ Node)

Source node 7 (10.0.0.2) wouldn't know how to route to the destination and hence its default gateway is Router A with interface IP (10.0.0.1). So, the first line in the above screenshot specifies packet flow from Source Node 7 to L2 Switch E with SOURCE_IP (10.0.0.2), DESTINATION_IP (10.0.0.1), GATEWAY_IP (10.0.0.2) and NEXT_HOP_IP (10.0.0.1). Since Switch is Layer2 device there is no change in the IPs in second line. Third line specifies the packet flow from Router A to Router B with SOURCE_IP (10.0.0.2), DESTINATION_IP (13.1.1.1- IP of the router connected to destination. Since OSPF is running, the router is looks up the route to its destination from routing table), GATEWAY_IP (11.1.1.1) and NEXT_HOP_IP (11.1.1.2) and so on.

Result: Network created with Network address translation (NAT)