IT304 Lab1
Introduction to TCP/IP suite and Netsim

1 Networking devices

1. NIC(Network Interface Card)
   A network card, network adapter, or NIC (network interface card) is a piece of computer hardware designed to allow computers to communicate over a computer network. It provides physical access to a networking medium and often provides a low-level addressing system through the use of MAC addresses.

2. Hub
   A network hub contains multiple ports. When a packet arrives at one port, it is copied unmodified to all ports of the hub for transmission. The destination address in the frame is not changed to a broadcast address.

3. Switch
   A network switch is a device that forwards and filters chunk of data communication between ports (connected cables) based on the MAC addresses in the packets, is distinct from a hub in that it only forwards the frames to the ports involved in the communication rather than all ports connected. A switch breaks the collision domain but represents itself as a broadcast domain. Switches make forwarding decisions of frames on the basis of MAC addresses. A switch normally has numerous ports, facilitating a star topology for devices, and cascading additional switches.

4. Router
   A router is a 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. A router is a networking device whose software and hardware are customized to the tasks of routing and forwarding

information. A router has two or more network interfaces, which may be to different physical types of network (such as copper cables, fiber, or wireless) or different network standards.

2 Introduction to Netsim

NetSim is a network simulation tool that allows you to create network scenarios, model traffic, and study performance metrics. NetSim provides simulation of various protocols working in various networks as follows: Inter-networks, Legacy Networks, BGP Networks, Advanced Wireless Networks, Cellular Networks, Wireless Sensor Networks, Personal Area Networks, LTE/LTE-A Networks, Cognitive Radio Networks, Internet of Things and VANETs. Users can open the experiments and save the experiments as desired. The different experiments can also be analyzed using the analytic option in the simulation menu.

Network simulator enables users to design a virtual network along with its components like switch, router, links etc. It also helps user to study behavior and performance of the network. Applications:

- Protocol performance analysis
- Application modeling and analysis
- Network design and planning
- Research and development of new networking technologies
- Test and verification

Performing a network simulation in Netsim involves four steps:

1. 1. Design a network from GUI
2. Configure the network
3. Model traffic
4. Analysis

There are three versions of NetSim available. Firstly, Academic used for lab experimentation in teaching. Secondly, Standard version is used for R D at educational institute. NetSim Pro version addresses the needs of defense and industry.

3 Implementing a simple scenario in Netsim

1. To begin with click on new→Internetwork
2. Model the network by dragging and dropping the devices and links as shown below

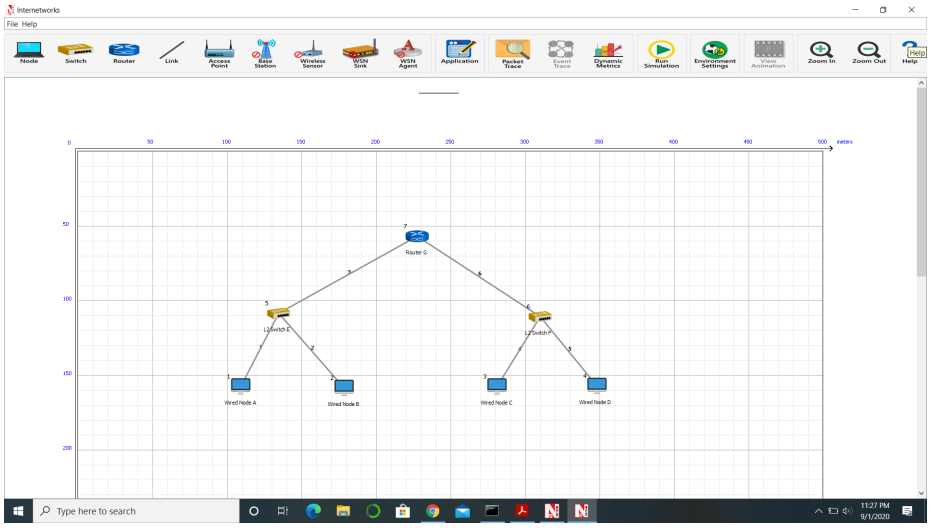
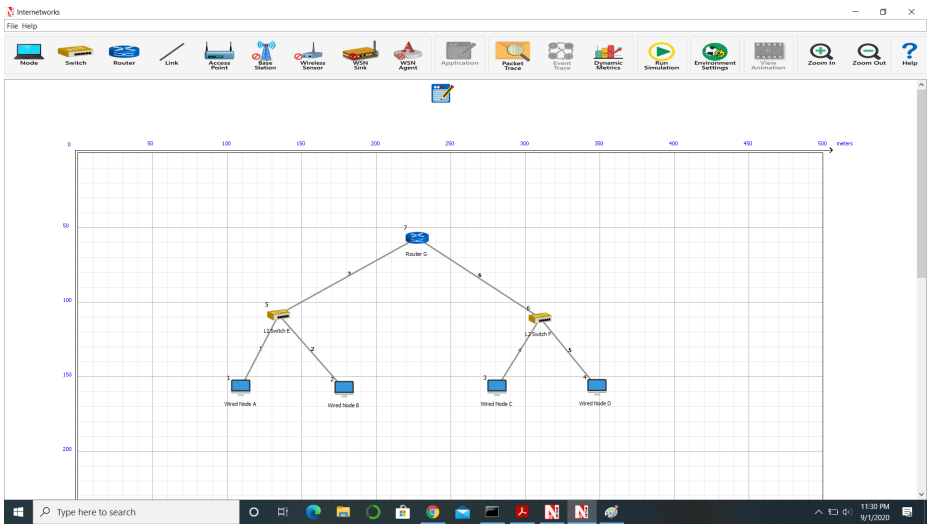


Figure 1: Caption

3. Properties of wired node, link,switch,router can be set by right click on it. (Currently keep the default values)

4. Drag the application icon and put in the area between the menu bar and grid.



5. By right clicking on application you can set properties of application.

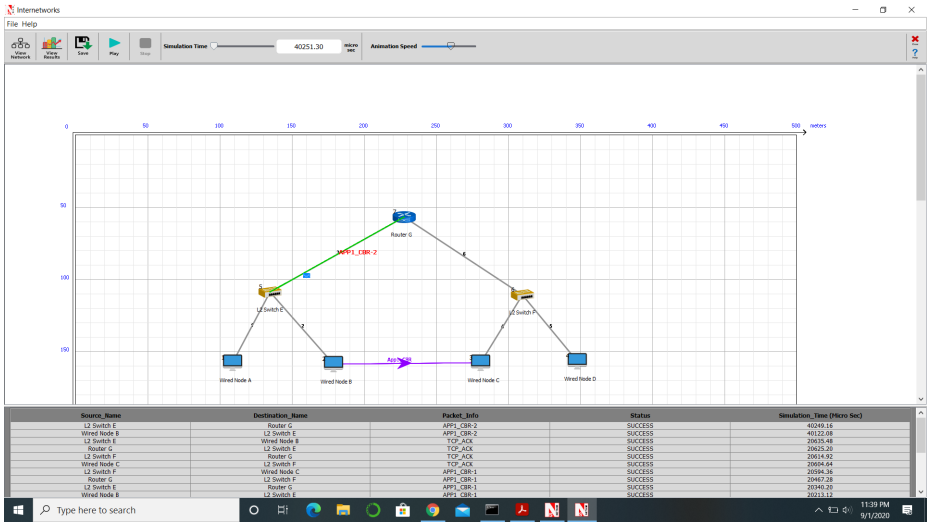
(Currently keep default parameters)

6. Click on Packet trace icon to enable packet trace. Select required attributes.(currently select all of them)

7. Click on Dynamic Metrics icon to generate various plots. Select required attributes.(currently select all of them)

8. Run the simulation set the time interval of 10 s. Select play and record simulation option.

9. Packet animation window will be opened as shown in following figure:



10. Also there will be other window which will show all statistical results.

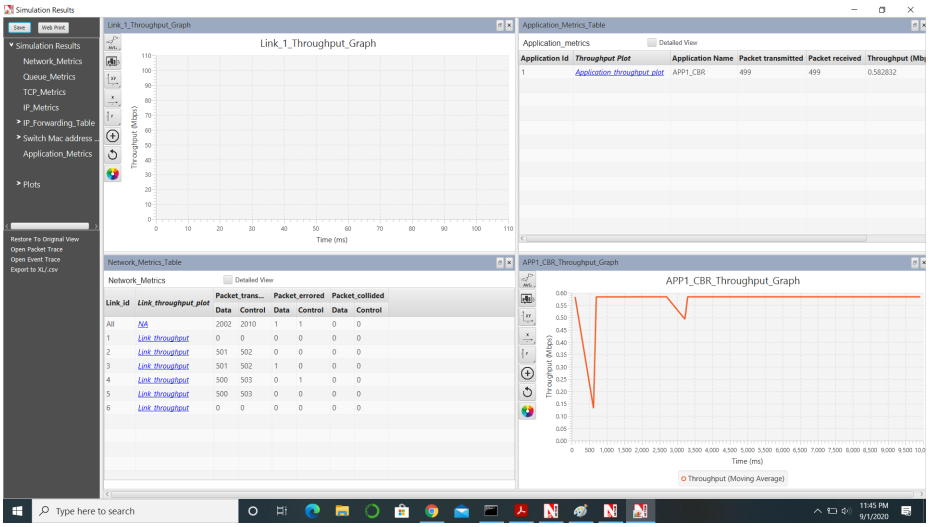


Figure 2: Caption

3.1 Exercise:Application analysis in Netsim

Configuration:

1. Devices:
   - 10 wired nodes
   - 1 L2 switch
2. Topology: Star topology(All the wired nodes connected to switch)
3. Implement 5 different applications between every disjoint pair of wired nodes(i.e. 1-2,3-4,5-6,7-8,9-10) with following properties:
   (a) HD video: This is a video application which sends 30 frames per second and every frames contains 10^5 pixels. It uses normal distribution to generate bits per pixel with $\mu = 0.52$ and $\sigma = 0.23$
   (b) You tube: This is a video application which sends 20 frames per second and every frames contains 104 pixels. It uses normal distribution to generate bits per pixel with $\mu = 0.52$ and $\sigma = 0.23$
   (c) Gmail: This is an EMAIL application which sends and receives mail of 30000 bytes at every 2s.
   (d) Browsing: This is a HTTP application in which server sends 3 pages, each of size 25000 bytes at every 2 s.
   (e) Database: This is a database application in which a transaction of size 104 bytes are sent at every $10^5\mu$ s.

4. Link properties: Set propagation delay=5ms

Results:

1. Find throughput of every application.
2. Find average throughput of video applications
3. Find average throughput of all the applications.

4 How to do addressing in a network

4.1 Types of addresses

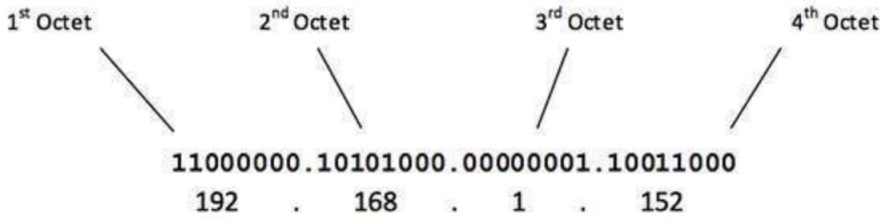
MAC(Media Access Control) address It is 48 bit (6 byte) Address given to each network interface card which is unique worldwide given by the manufacturer of the hardware. Sometimes it is also called hardware address or physical address.

IP address IP address stands for internet protocol address; it is an identifying number that is associated with a specific computer or computer network. When connected to the internet, the IP address allows the computers to send and receive information. An example of an IP address would be: 192.168.1.152

4.2 How addresses are allocated

As MAC addresses are permanent. MAC addresses are given by the manufacturing companies. And IP addresses are allocated according to requirements of number of networks and host. Internet Protocol hierarchy contains several classes of IP Addresses to be used efficiently in various situations as per the requirement of hosts per network. Broadly, the IPv4 Addressing system is divided into five classes of IP Addresses. All the five classes are identified by the first octet of IP Address as shown in fig 4.2.

The first octet referred here is the left most of all. The octets numbered as follows depicting dotted decimal notation of IP Address −



The number of networks and the number of hosts per class can be derived by this formula −

Number of networks	= 2^network_bits
Number of Hosts/Network	= 2^host_bits − 2

When calculating hosts' IP addresses, 2 IP addresses are decreased because they cannot be assigned to hosts, i.e. the first IP of a network is network number and the last IP is reserved for Broadcast IP.

Figure 3: Example of class

Class A Address

The first bit of the first octet is always set to 0 (zero). Thus the first octet ranges from 1 – 127, i.e.

00000001 – 01111111
1 – 127

Class A addresses only include IP starting from 1.x.x.x to 126.x.x.x only. The IP range 127.x.x.x is reserved for loopback IP addresses.

The default subnet mask for Class A IP address is 255.0.0.0 which implies that Class A addressing can have 126 networks (2^7-2) and 16777214 hosts (2^{24}-2).

Class A IP address format is thus: **0NNNNNNN**.HHHHHHHH.HHHHHHHH.HHHHHHHH

Figure 4: Class A addressing

Class B Address

An IP address which belongs to class B has the first two bits in the first octet set to 10, i.e.

10000000 – **10**111111
128 – 191

Class B IP Addresses range from 128.0.x.x to 191.255.x.x. The default subnet mask for Class B is 255.255.x.x.

Class B has 16384 (2^{14}) Network addresses and 65534 (2^{16}-2) Host addresses.

Class B IP address format is: **10NNNNNN.NNNNNNNN**.HHHHHHHH.HHHHHHHH

Figure 5: Class B addressing

Class C Address

The first octet of Class C IP address has its first 3 bits set to 110, that is −

11000000 – **110**11111
192 – 223

Class C IP addresses range from 192.0.0.x to 223.255.255.x. The default subnet mask for Class C is 255.255.255.x.

Class C gives 2097152 (2^{21}) Network addresses and 254 (2^{8}-2) Host addresses.

Class C IP address format is: **110NNNNN.NNNNNNNN.NNNNNNNN**.HHHHHHHH

Figure 6: Class C addressing

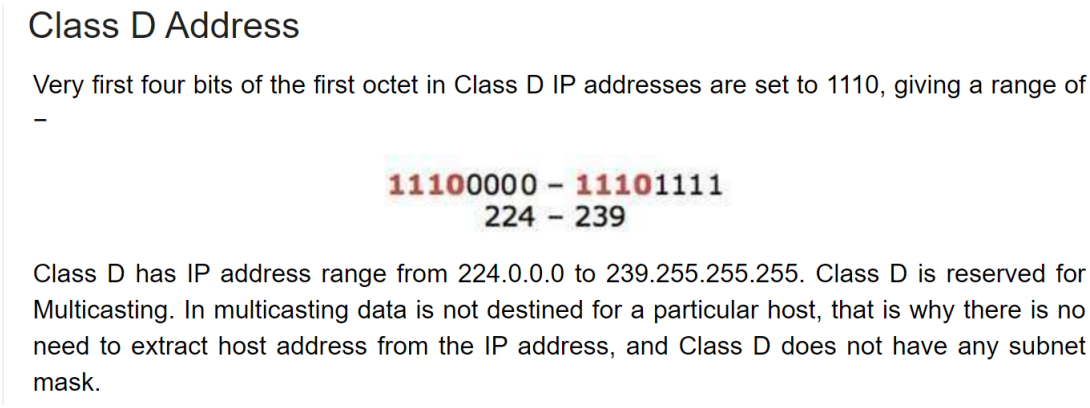
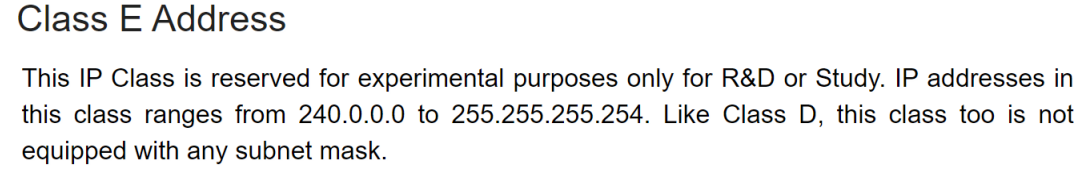


Figure 7: Class D addressing



4.3 Exercise 1: allocating IP addresses

1. Open new internetwork in Netsim.
2. Design topology as shown in figure 8 using drag and drop function on the icon of node and switch.
3. Change the ip address to "192.168.10.80" and subnet mask "255.255.255.0" of the wired node A. You may find the Interface1 ethernet property in the properties wired node, where you can edit the ip address and subnet mask.
4. Run the simulator for 10 second.

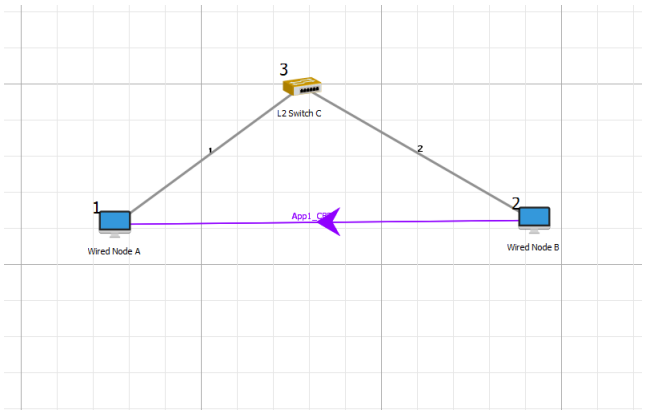


Figure 8: Exercise:allocating IP addressing

4.3.1 Questions ex1: allocating IP addresses

1. Write down the Ip address and subnet mask of both the node.
2. Write down the number of packet transmitted using simulation results.
3. How many packets have been received? Why?

4.4 Exercise 2: allocating IP addresses

1. Edit the experiment of exercise 1.
2. Change the Ip address of wired node B to "192.168.10.81" and subnet mask "255.255.255.0".
3. Run the simulation for 10 second.

4.4.1 Questions ex2: allocating IP addresses

1. How many packets have been received?
2. What is the difference between the Exercise between 1 and 2?

5 Basic networking commands

5.1 Exercise 1:Know your PC

1. Open the command prompt of your PC by writing cmd in the start menu.
2. write down the command "ipconfig /all"
3. press enter.

5.1.1 Questions

1. Search for the field of physical address and write down the values.
2. How many physical addresses have you find? why ?
3. Search for the field ip address and subnet mask and write down the value.

5.2 Exercise 2

1. Write down the command on cmd "route PRINT" Observe the results, this command will give you the routing table of your own PC.
2. Write down the command on cmd "ping daiict.ac.in", here you can see the packets transmission between your PC and daiict network. write down the packet transmitted, received and maximum,minimum and average time.
3. Try the ping command with your friend's ip adress. "ping x.x.x.x" where x.x.x.x would be the ip address of your friend. write down the packet transmitted, received and maximum, minimum and average time.
4. Compare the result of last two operation. What is the difference between two. Why there is a difference according to you.
5. Write "tracert google.com" in cmd. Observe the results. Tracert command gives the number of minimum hop between you and the destination.
6. Try the "tracert" command with another website and write down the results. For instance, 1) daiict.ac.in 2)amazon.in 3)facebook.com and observe the difference. Why there is difference according to you.

6 Submission guidelines

Submit a pdf file which contains answers of all questions asked in exercise. Submission should be done individually.