SRM INSTITUTE OF SCIENCE & 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. (CoMpUTEr sCiENCE ANd ENGiNEEriNG) - i

ii YEAr / iV sEMEsTEr

Name - Ananya Gupta

Registration Number - RA1911003030265

Experiment-8 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

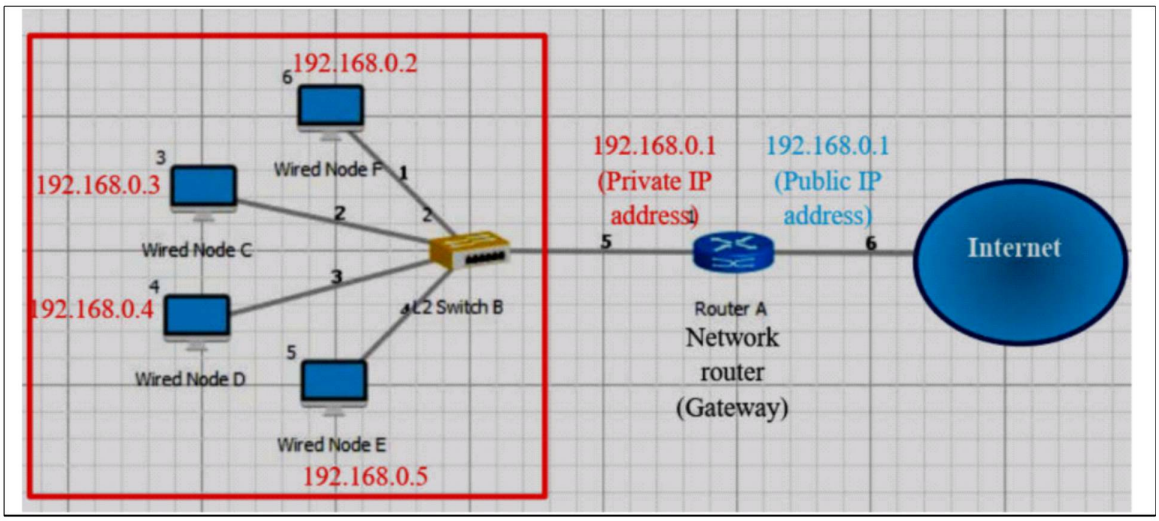
Translation.

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.



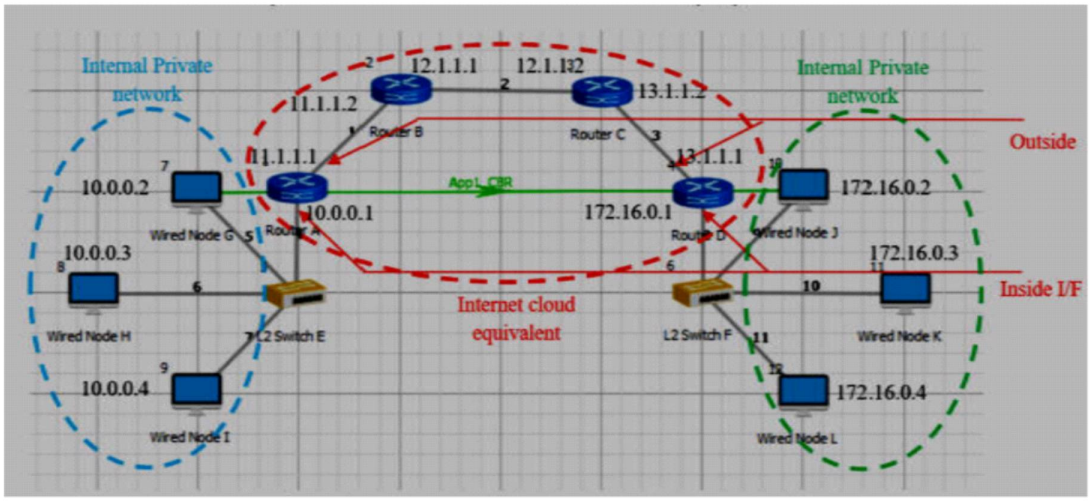
NAT is secure since it hides network from the Internet. All communications from internal private network are handled by the NAT device, which will ensure all the appropriate translations are performed and provide a flawless connection between internal devices and the Internet.

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:

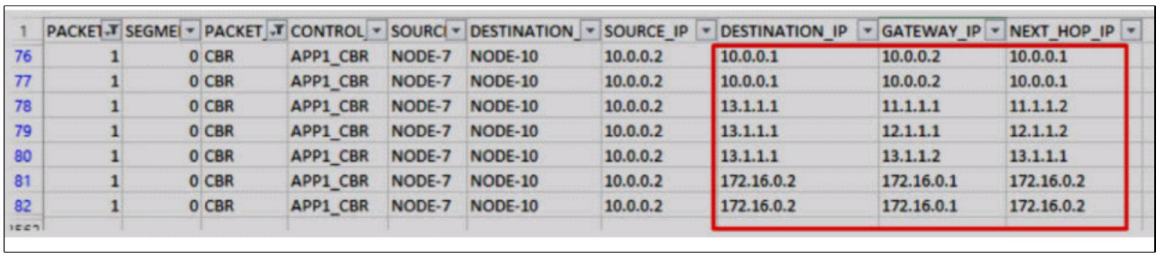
Wired Node	IP address	Subnet mask
G	10.0.0.2	255.0.0.0
H	10.0.0.3	255.0.0.0
I	10.0.0.4	255.0.0.0
J	172.16.0.2	255.255.0.0
K	172.16.0.3	255.255.0.0
L	172.16.0.4	255.255.0.0

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



	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)