RESEARCH ARTICLE   OPEN ACCESS

Simulation and Analysis of Network Address Translation (NAT) & Port Address Translation (PAT) Techniques

[1]Anchit Bansal, [2]Priyanka Goel
[1,2]*Department of Electronics & Communication Engineering SITE, SVSU, Meerut (U.P), India*

ABSTRACT
Advancements in Internet lead to the shortage of available IPV4 addresses. The main long-term solution to the IP address scalability problem was to increase the size of the IP address. To subside this problem temporarily, a specific subset of IPV4 address was termed as private. The size of routing table can be managed using certain techniques. Instead of holding information about whole route, the routing table holds information which results in next hop in next hop routing technique. Using network specific routing technique searching process is simplified as only one entry in routing table is used which defines the address of complete network. In this paper we will stimulate the network address translation and port address translation routing technique.
Keywords: Static NAT, Dynamic NAT, PAT, Hosts, Private Address, Public Address

I. INTRODUCTION

Devices accessing the internet must be configured with public addresses. A public address can be routed on the Internet. Internet Assigned Numbers Authority (IANA) allocates public addresses. Private addresses can never be routed on the Internet. When forming a private network that will have no Internet connectivity, IP network numbers called private internets are used. Network Address Translation (NAT) makes it possible to translate between private and public addresses. NAT allows a host configured with a private address to be stamped with a public address, thus allowing that host to communicate across the Internet. While referring to the term inside, it implies to the internal network interface receiving egress traffic which may or may not be using private address. The term outside implies to the external-facing network interface, bound to receive ingress traffic.

II. NETWORK ADDRESS TRANSLATION

Hosts that do not have a valid, globally registered unique IP address can communicate with other hosts through internet with the help of NAT which allows these addresses which are not internet ready to connect to hosts around the world. This process is achieved by NAT by using a valid registered IP address to represent the private address to the rest of the Internet. The router, performing NAT, changes the packet's source IP address when the packet leaves the private organization and changes the destination address in each packet that is forwarded back into the private network. A NAT gateway can provide the following benefits:
➢ Protocol-level protection.
➢ Automatic client computer configuration control.

➢ Packet level filtering and routing.

Port mapping table is used by NAT gateway which stores information regarding the ports renumbered for each client's outgoing packets. This table relates the client's real local IP address and source port along with its translated source port number to a destination address and port. The NAT gateway can thus reverse the process for returning packets and route them back to the correct clients. When any remote server replies to an NAT client, all incoming packets arriving at the NAT gateway will all have same destination address, but the destination Port number will be the unique Source Port number that was assigned by the NAT. The NAT gateway searches in its port mapping table to know which "real" client address and port number a packet is destined for, and these numbers are replaced before passing the packet on to the local client. This process is completely dynamic. When a packet is received from an internal client, NAT looks for the matching source address and port in the port mapping table. If the entry is not found, a new one is created, and a new mapping port allocated to the client.

III. NAT TERMINOLOGY

Various elements of Network Address Translation Scheme can be described using specific terms. Consider the following topology.
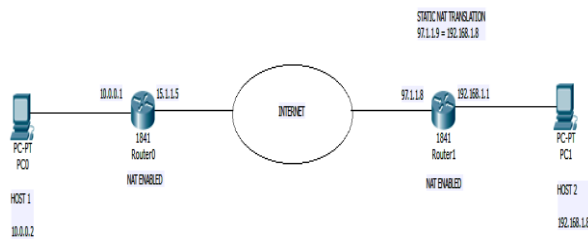
Figure 1: Nat Terminology Example

➢ **Inside Local-** The term inside refers to an address used for host inside an enterprise. This refers to set of network nodes whose IP address is subject to translation. These IP addresses are usually not globally unique. In the above figure the inside local address is 10.0.0.2

➢ **Inside Global-** This refers to the address that identifies an inside host to the outside world (usually a public address). Essentially, this is the dynamically or statically-assigned public address assigned to a private host. In the above figure the inside global address is 15.1.1.5

➢ **Outside Global-** The term outside refers to an address used for host outside an enterprise. An outside global address is the actual IP address assigned to the hosts that resides in the outside network (Internet), usually a public address. In the above figure the outside global address is 97.1.1.9

➢ **Outside Local-** This refers to the address that identifies an outside host to the inside network. This is usually the same address as the Outside Global. However, it is occasionally necessary to translate an outside (usually public) address to an inside (usually private) address. In the above figure the outside local address is 97.1.1.9

        To simplify, global addresses are associates with public addresses, and local addresses are associated with private addresses generally.

IV. TOPOLOGY FOR CONFIGURING STATIC NAT

        The NAT router simply configures a one-to-one mapping between the private address and the registered address that is used on its behalf while using static NAT. To support a second IP host with static NAT a second static one-to-one mapping using a second IP address in the public address range is required. Using NAT terminology, the enterprise network that uses private addresses, needs NAT, is the "inside" part of the network. The Internet side of the NAT function is the "outside" part of the network. A host that needs NAT has the IP address it uses inside the network, and similarly it needs an IP address to represent it in the outside network. The topology consists of three pc's (PC0,

PC1 &PC2), one switch (2950-24), two routers (1841) and connecting wires. R0 is assumed to be connected to ISP & R1 on the WAN side.
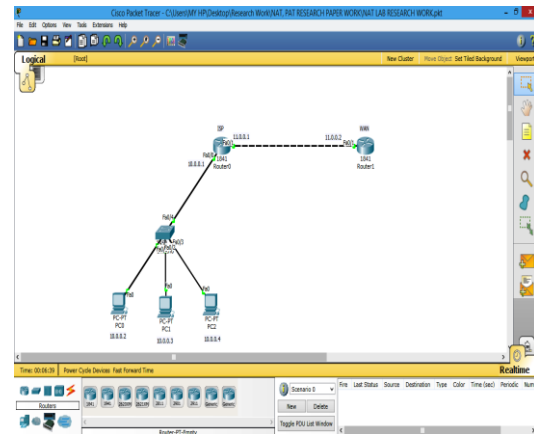

Figure 2: Topology for Configuring Static Nat

V. CONFIGURATION OF STATIC NAT FOR THE CONSIDERED TOPOLOGY

        After constructing the network and making connections as described in the above figure, ip addresses will be assigned to the pc's (end devices). The procedure for the same is given as:
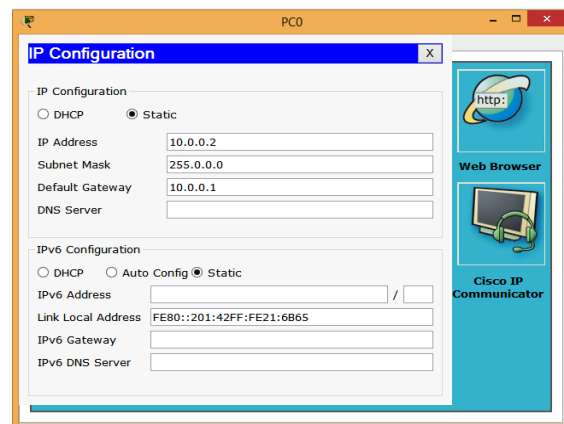

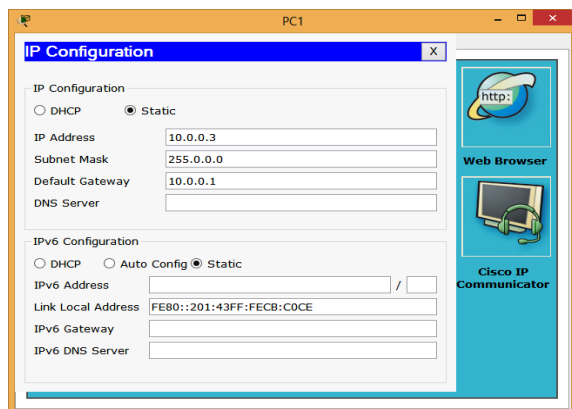**Figure 3:** Assigning IP Address for PC0

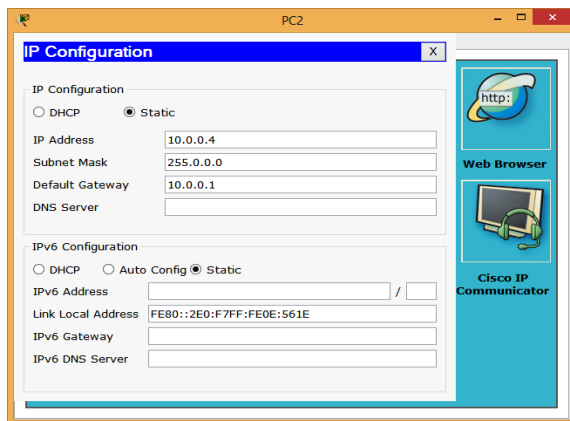**Figure 4:** Assigning IP Address for PC1

Figure 5: Assigning IP Address for PC2

Now NAT configurations on router on the LAN side will be done after assigning ip addresses on routers on LAN and WAN side respectively.

A. Router 0 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router(config)#ip nat inside source static 10.0.0.2 11.0.0.7
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#^Z
Router#

%SYS-5-CONFIG_I: Configured from console by console
Router(config)#ip nat inside source static 10.0.0.3 11.0.0.8
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#ip nat inside source static 10.0.0.4 11.0.0.9
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

B. Router 1 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.2 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#write
Building configuration...
[OK]

After configuring the topology as per the instructions written above, the routing of packets is checked in simulation mode in packet tracer.

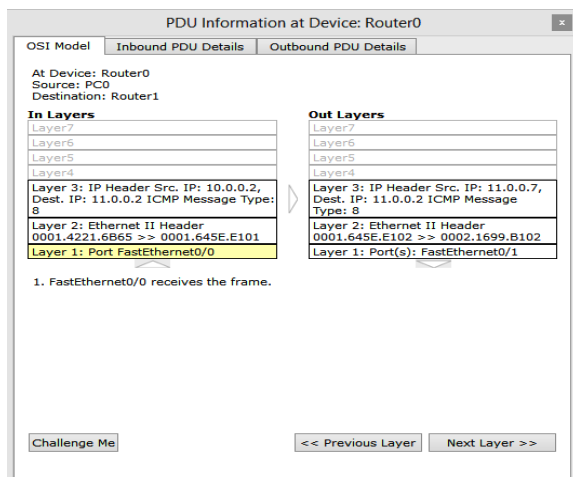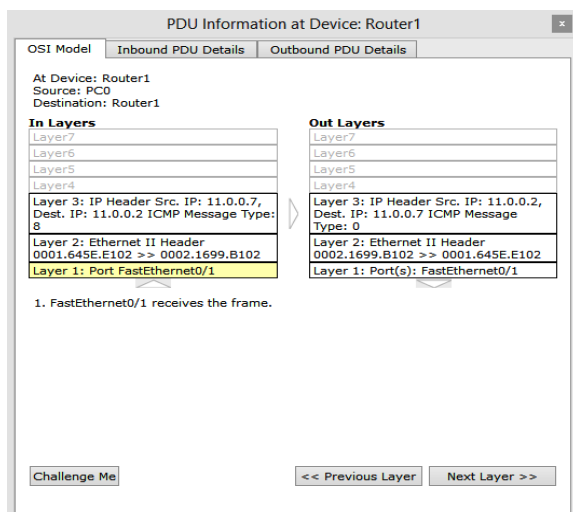**Figure 6:** PDU Information at Router0 for PC0

Figure 7: PDU Information at Router1 for PC0

The above figures indicate how the source and destination IP addresses get changed at various stages. The following information can be checked y clicking on the message packet at router0 (ISP) and at router 1 (WAN). Similarly the PDU information for PC1 & PC2 can be verified.

VI. CONFIGURATION OF DYNAMIC NAT FOR THE CONSIDERED TOPOLOGY

Dynamic NAT utilizes a pool of global addresses to dynamically translate the outbound traffic of clients behind a NAT enabled device. The router is provided with pool of IPs that contains global IPs, so every time when a user tries to access a public network it will be provided with an IP from the pool. Consider the topology as defined in figure 2. After making the connections and assigning the ip address on PC's, the configuration of dynamic NAT will be done on Router0 (ISP). The process is as follows:

A.   Router 0 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.1 255.0.0.0
Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router(config)#ip nat inside source list 1 pool networking
Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
Router(config)#ip nat pool networking 11.0.0.10 11.0.0.60 netmask 255.0.0.0
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

B.   Router 1 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.2 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

Anchit Bansal. Int. Journal of Engineering Research and Application
ISSN : 2248-9622, Vol. 7, Issue 7, (Part -2) July 2017, pp.50-56

www.ijera.com

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#write
Building configuration...
[OK]

After the topology is configured with the instructions given, the routing of packets is check in simulation mode for different PC's.
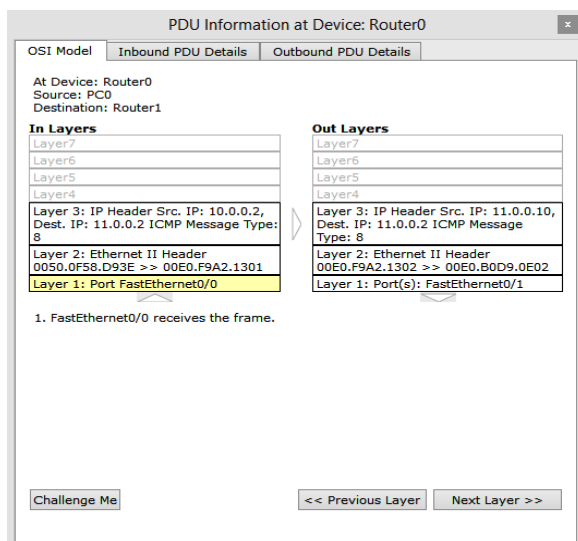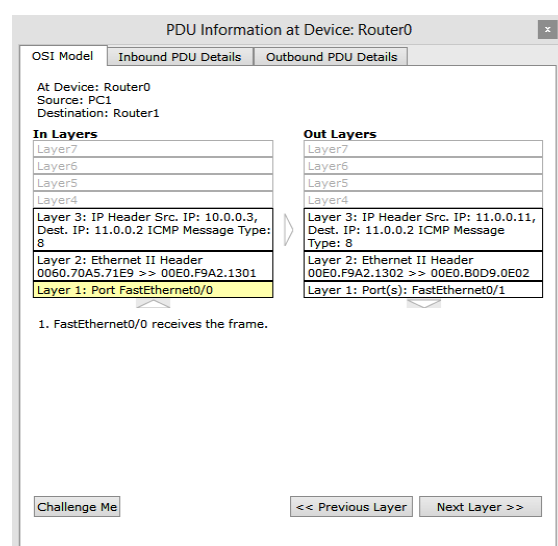

Figure 8: PDU Information at Router0 for PC0

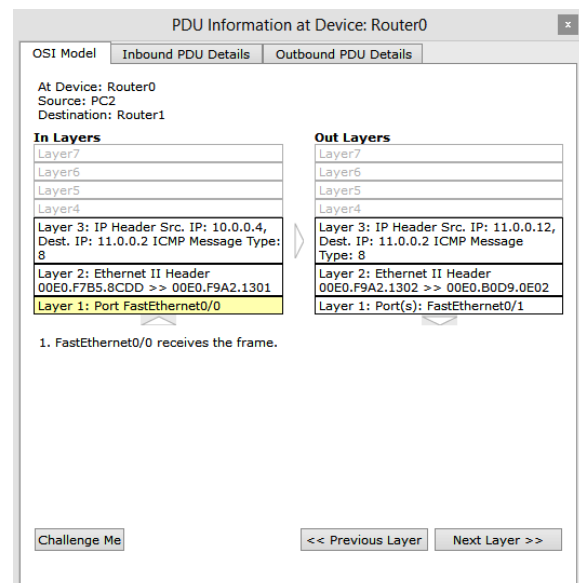**Figure 9:** PDU Information at Router0 for PC1

Figure 10: PDU Information at Router0 for PC2

VII. CONFIGURATION OF PAT FOR THE CONSIDERED TOPOLOGY

Some networks need to have most, IP hosts to access the Internet. If this network uses private IP addresses, the NAT router needs a very large set of registered IP addresses. Dynamic NAT lessens the problem to some degree, because every single host in an internetwork rarely need to communicate with the Internet at the same time. The NAT Overload feature, also called Port Address Translation (PAT), translates the outbound traffic of clients to unique port numbers of a single global address. Overloading allows NAT to scale to support many clients with only a few public IP addresses. Consider the topology as defined in figure 2. After making the connections and assigning the ip address on PC's, the configuration of dynamic NAT will be done on Router0 (ISP). The process is as follows:

A.   Router 0 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/0
Router(config-if)#ip address 10.0.0.1 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up
Router(config-if)#exit
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.1 255.0.0.0

Router(config-if)#no shutdown
Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 10.0.0.0
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router(config)#ip nat inside source list 1 pool networking overload
Router(config)#access-list 1 permit 10.0.0.0 0.255.255.255
Router(config)#ip nat pool networking 11.0.0.10 11.0.0.10 netmask 255.0.0.0
Router(config)#int fa 0/0
Router(config-if)#ip nat inside
Router(config-if)#int fa 0/1
Router(config-if)#ip nat outside
Router(config-if)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console

B. Router 1 Configuration:
--- System Configuration Dialog ---
Continue with configuration dialog? [yes/no]: n
Press RETURN to get started!
Router>enable
Router# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#int fa 0/1
Router(config-if)#ip address 11.0.0.2 255.0.0.0
Router(config-if)#no shutdown
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up
Router(config-if)#exit
Router(config)#router rip
Router(config-router)#network 11.0.0.0
Router(config-router)#^Z
Router#
%SYS-5-CONFIG_I: Configured from console by console
Router#write
Building configuration...
[OK]

After the topology is configured with the instructions given, the routing of packets is check in simulation mode for different PC's.
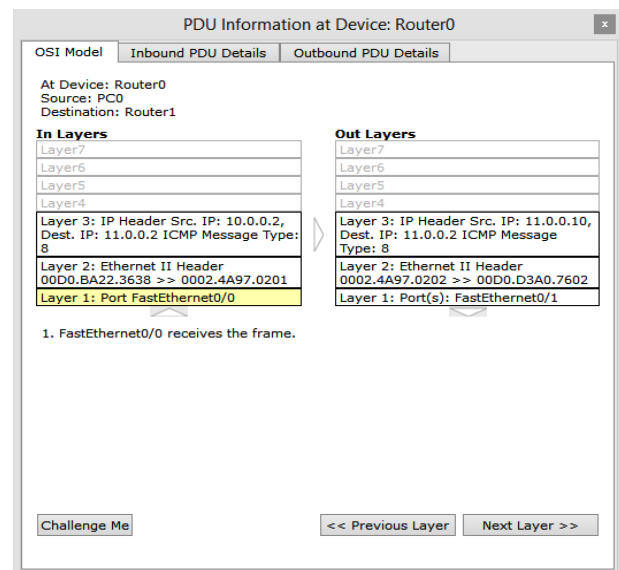

Figure 11: PDU Information at Router0 for PC0

It is clear from the figure that the packet has header source IP of 10.0.0.2 on the IN Layers and the same packet has source IP as 11.0.0.10 on the out layer once it reaches the router of the ISP. The same scenario will be repeated for pc1 and pc2 respectively. This establishes the PAT overload NAT technique. Any inside host with a source that matches access-list 1 will be translated with overload to the IP address configured on the fa 0/1 interface.
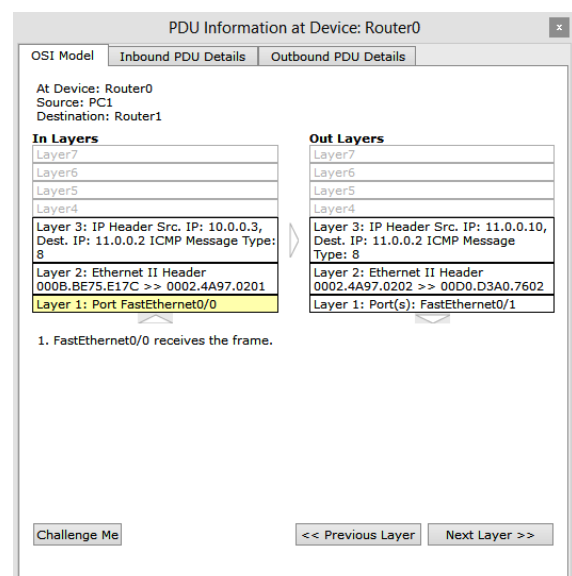

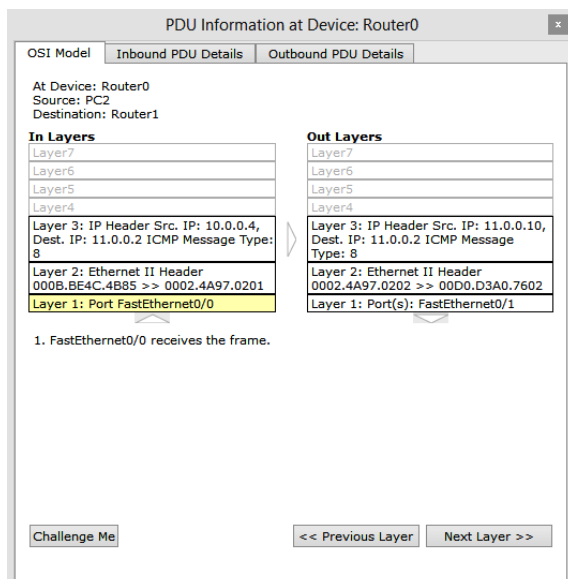
Figure 12: PDU Information at Router0 for PC1

Figure 13: PDU Information at Router0 for PC2

VIII. CONCLUSION

Technically, NAT is a firewall. Dynamic NAT is natural firewall between private network and public networks/Internet. NAT offers a fast and effective way to expand secure Internet access into existing and new private networks. NAT can reuse Ipv4 addresses. Hosts in private network can share limited public IP addresses. It also delays the deployment of IPv6. NAT breaks end-to-end connectivity model. NAT offers greater administrative flexibility and performance than the alternative application-level proxies

REFERENCES

[1]. Network Address Translation (NAT) - Router Alley. [Online].Available:http://www.routeralley.com/ra/docs/nat.pdf.

[2]. Introduction to Network Address Translation, [Online].Available:http://www.cisco.com/networkers/nw00/pres/2211.pdf.

[3]. Jeff Tyson, How Network Address Translation Works http://computer.howstuffworks.com/nat.htm

[4]. Private Networks and NAT Module. [Online]. Availablehttp://www.cs.virginia.edu/~itlab/book/slides/module17-nat.ppt.

[5]. A.S.Tanenbaum.ComputerNetworks.Prentice-Hall,2002.

[6]. Introduction to Dynamic Routing Protocols. [Online]. Available:http://ptgmedia.pearsoncmg.com/images/9781587132063/samplechapter/1587132060_03.pdf.

[7]. GertDe L. and Gert S.,Network Security Fundamentals, Publisher Cisco Press, 2004.

[8]. Geoff Huston, Anatomy: A Look Inside Network Address Translators http://www.cisco.com/web/about/ac123/ac147/archived_issues/ipj_7-3/anatomy.html

[9]. S. Biagi, "Virtual LANs," Network VAR v4 n1 p. 10-12, January 1996, *An Overview of VLAN's, advantages, and disadvantages.*

[10]. Configuring Network Address Translation, [Online]. Available:http://www.net130.com/book/cisco/typical/Cisco%20-%20Configuring%20NAT.pdf