

HACETTEPE UNIVERSITY
COMPUTER ENGINEERING DEPARTMENT
COMPUTER NETWORKS LABORATORY

EXPERIMENT

NAT (Network Address Translation)

AIM

In this lab you will learn Network Address Translation on Routers. Your aim is to configure NAT on your router and translate your PC's IP address in your group to a single IP from your subnet.

INTRODUCTION

You should read Chapter 4 - Network Layer from the course textbook, especially **NAT** Section for theoretical background.

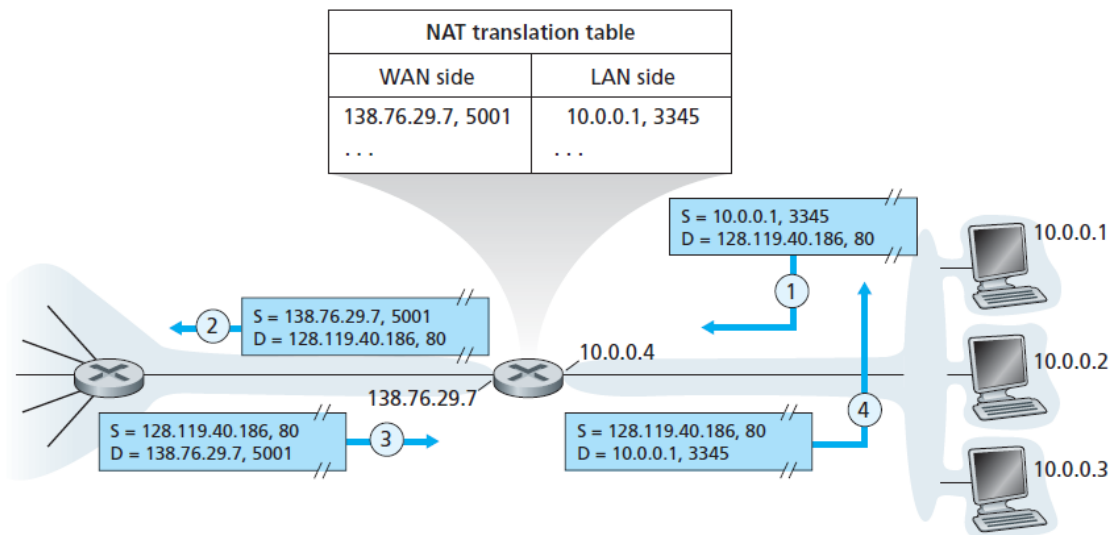


Figure 4.22 ♦ Network address translation

Types of NAT

Static NAT: In the static address translation method, the unregistered source address in the outgoing packet is changed with a registered IP address within the organization. For each unregistered IP address, there is an individual, one-to-one, registered address. Inbound packets are also reversed.

Dynamic NAT: In dynamic address translation (Dynamic NAT), the unregistered source address in the outbound packet is replaced with one that is not currently being used from the set of

registered IP addresses within the organization. The Router keeps its session-based information about which registered address it uses against the unregistered IP address in its lookup table created for this purpose. When it sees the registered address in the incoming packages as the target address, it also changes this address to the corresponding unregistered address and forwards it to the corporate network.

The same registered address is used in place of a different unregistered address in another session. In this way, it is possible for the institution to represent all unregistered addresses with a limited number of registered addresses on the Internet.

Overloading: The dynamic address translation method also has a derivation known as overloading. With this method, all the unregistered addresses are translated to a single registered address (the IP address of the router) while the packets generated in the corporate network are routed to the Internet. However, in order to be able to distinguish between computers and determine which system the incoming packets are forwarded to, the port numbers are used on the TCP / UDP datagrams carried by the packet.

In this context, for each unregistered address, a port number is specified, based on the session. The source IP address in the outgoing packet (packet header) is changed with the IP address of the router, and the source port number in the TCP / UDP datagram header is also changed with this determined number. This port number is stored in a table along with the unregistered address that is relevant.

EXPERIMENT STEPS

1. Your aim is to configure NAT on your router and translate your PC's IP address in your group to a single IP from your subnet. After translation process, you will be able to test your address translation with pinging to new IP addresses and using show commands. Another way to test your configuration is to connect remotely to another group's router and running `show user` command to see logged in users on that router.

Basic Router Configurations

2. You are going to use telnet for remote connection. To be able to use telnet, you have to configure necessary password steps for security restrictions. For example try to telnet (from your PC) to another group's Router (IP address of Serial interface), and understand why you are not able connect to the Router.
3. You have to set enable password and telnet password for remote connection.

```
Router1(config)#enable password cisco
Router1(config)#line vty 0 4
Router1(config-line)#password ciscot
Router1(config-line)#login
Router1(config-line)#end
```

4. Display your configuration changes on `running-config` and try logout from Router using `disable` command and then enable again.
5. You should observe that all text passwords can be easily seen in config file. That is also a security bug. You should use encryption service for encrypting password texts.

```
Router1(config)#service password-encryption
```

6. Now you are ready to telnet (from your PC) to another remote Routers. Enter their telnet and enable passwords and login to their router. Use `show user` command to display logged-in connections on the router in this session. Observe your IP address of your client. The * shows your connection.

NOTE: If you jump from that Router to another one, that is called reverse telnet. You can use `exit` command for terminating the telnet session.

Router NAT Configurations

7. If a router supports address translation (if it has an address translation software), then the connection interfaces to which the address translation is to be applied, must be specified and defined as inside or outside. This is done using the `ip nat [inside | outside]` command while in the sub-configuration mode.

```
router1(config)# interface fastEthernet 0/0
router1(config-if)# ip nat inside
router1(config-if)# exit
router1(config)# interface serial0/0/0
router1(config-if)# ip nat outside
router1(config-if)# exit
router1(config)#
```

Static NAT

Example Static NAT configuration commands are described in below. You are not going to run Static NAT configurations, so just learn the usage scenario for static NAT.

```
router_1(config)#interface fastEthernet 0/0
router_1(config-if)#ip nat inside source static <unregisteredIP>
<registeredIP>
```

The above commands are used if you want to use static address translation on any interface of the router .

After this last command is executed, a packet carrying an unregistered address as the source IP address is sent to the Internet by translating the source address into the registered address. In the same way, a packet arriving at the IP address registered from the Internet is redirected to the ethernet connection (corporate network) by replacing the destination address with the unregistered address.

Dynamic NAT

To use dynamic address translation, it is first necessary to introduce the "set of registered addresses" to be used in response to unregistered addresses. In the config mode:

```
ip nat pool <poolName> <beginningIP> <endingIP> netmask <mask>
```

is used. After this command, it is necessary to determine which registered addresses are used for the unregistered addresses in the translation:

```
access-list <listNo> permit <net/subnet IP> <ACL mask>
```

After previous steps, the translation process is initiated for the router's corresponding interface, using the command:

```
ip nat inside source list <listNo> pool <poolName>
```

Overloading NAT

8. You are going to configure dynamic overloading NAT. Commands are same as dynamic NAT configuration with overload command at the end. You should translate your client IP to another IP from your subnet (for example: 10.100.X.99) using dynamic overloading NAT commands:

```
router1 (config) #ip nat pool <poolName> <beginningIP> <endingIP> netmask  
<mask>  
router1 (config) #access-list <listNo> permit <net/subnet IP> <ACL mask>  
router1 (config) #ip nat inside source list <listNo> pool <poolname>
```

9. After NAT configuration, try to ping other groups client IP addresses and translated IP addresses. Discuss the results.
10. Use `show ip nat translation` command to show translated IP addresses and port numbers. Discuss each column on the table (inside/outside, local/global). If you didn't see any output, you should successfully ping remote clients and also your PC should be pinged from outside.
11. Finally, connect to other remote Routers using telnet, and display connected users and observe your IP address.

REFERENCES

- Computer Networks: A top-down approach, Kurose and Ross, 6th Edition, Addison-Wesley
- http://www.cisco.com/c/en/us/td/docs/ios-xml/ios/ipaddr_nat/configuration/15-mt/nat-15-mt-book/iadnat-addr-consv.html