Communication Protocols
2021-2022

Lab Assignment 2 – Network Address Translation

Objectives and organisation

The objective of this lab assignment is to explore the configuration and use of Network Address Translation (NAT). NAT is an extremely important topic in IPv4 networks, as it is at the basis of the preservation of the shrinking IPv4 address space.

The assignment can be prepared using the GNS3 router emulator before executing it in the lab. There are guided exercises, for which the commands/actions to execute are presented and explained, and proposed exercises that should be done autonomously by the students.

The following topics are addressed in the lab assignment:

- Configuration and use of NAT in Cisco-based networks

Throughout the execution of the lab assignment, commands output and configuration files should be kept for inspection by the teacher. Special attention should be given to their interpretation and explanation.

The current lab assignment may require cooperation between groups in order to setup the scenarios under study. More than the sheer configuration of individual routers, it is important to interpret, explain and understand the behaviour in the overall network scenario. This is a key element for evaluation.

The following aspects will be taken into account when evaluating the work:

- Preparation of the lab assignment – 10%
- Knowledge of the aspects under consideration – 30%
- Exercises execution – 50%
- Group autonomy – 10%

1. Network Address Translation

Network Address Translation (NAT) was defined in RFC 1631 (http://www.ietf.org/rfc/rfc1631.txt) with the objective of providing an answer to the shortage of IPv4 addresses. The basic idea behind NAT is to allow machines using private IP addresses defined in RFC 1918 (http://www.ietf.org/rfc/rfc1918.txt) to be able to communicate with the Internet at large. To do so, the intermediate system (router or firewall) that connects the network to the Internet must map the private IP address into a public IP address.

NAT is built on the following concepts: 'inside', 'outside', 'local address' and 'global address'. The 'outside' normally corresponds to the public address Internet, although it is possible to perform NAT between two or more networks using private addresses (as it will be done in the course of the current lab assignment).

Inside local addresses are used by hosts on the local network for communication among themselves. Whenever an internal machine wants to communicate with an external machine, its inside local address must be mapped into an outside local address. If an external machine wants to communicate with an internal machine it must use an inside global destination address. External machines communicate among themselves using outside global addresses.

It should be highlighted that the inside→outside address mapping can be one-to-one, N-to-one, N-to-M, static or dynamic. In a given router configuration there may exist various types of mappings, as we shall see below.

1.1 Basic NAT configuration

Analyse the following example of NAT configuration in a Cisco router.

```
R1#config t
R1(config)#access-list 25 permit 192.168.100.0 0.0.0.255
R1(config)#ip nat inside source list 25 interface Ethernet0 overload
R1(config)#interface FastEthernet0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#exit
R1(config)#interface Ethernet0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#end
R1#
```

An 'access list' is used to control which machines get their inside local address mapped into an outside local address. In this example, all the machines belonging to network 192.168.100.0/24 will be subject to address translation.

In addition, the 'ip nat inside source list 25 interface Ethernet0 overload' command specifies that the address to use on the outside is that of the Ethernet0 interface (i.e., 172.16.1.1) and that all inside local addresses will be mapped into a single outside local address (again, in this case, 172.16.1.1). This is specified by the 'overload' keyword. As there is 'overload', the router will distinguish between different internal machines through the use of different ports. This is called Port Address Translation (PAT).

Still in the example, the FastEthernet0 interface is declared to be the 'inside' interface, and the Ethernet0 interface is declared to be the 'outside' interface.

Exercise 1 – Based on the provided example, add the basic NAT configuration to your router, according to the scenario presented in Figure 1, and using the following:

- Ask the teacher the values of the X and N variables, where N is the number of your group.
- The 'inside' network should have the following address: 192.168.X.0/24.
- The Ethernet0 interface of your router should be the 'inside' interface, and should have the following address: 192.168.X.254;
- The FastEthernet0 interface of your router should be the 'outside' interface, and should have the following address: 10.254.0.N. This interface should be connected to the lab network, which has the following address: 10.254.0.0/24;
- The access list should allow all the machines in the local network to access the NAT pool;
- A single 'outside local' address should be used;
- Connect your computer to the 'inside' network and manually configure it with the following address: 192.168.X.100.
- Check the connectivity of your computer with the outside network, using the ping command. The ping should be done to the lab server, whose IP address is 10.254.0.254. Check the 'outside local' IP address used by your machine in the console of the lab server.
- Based on your observations, explain the actions performed by the router in terms of addressing when it receives and forwards the ICMP packets generated by the 'ping' program.

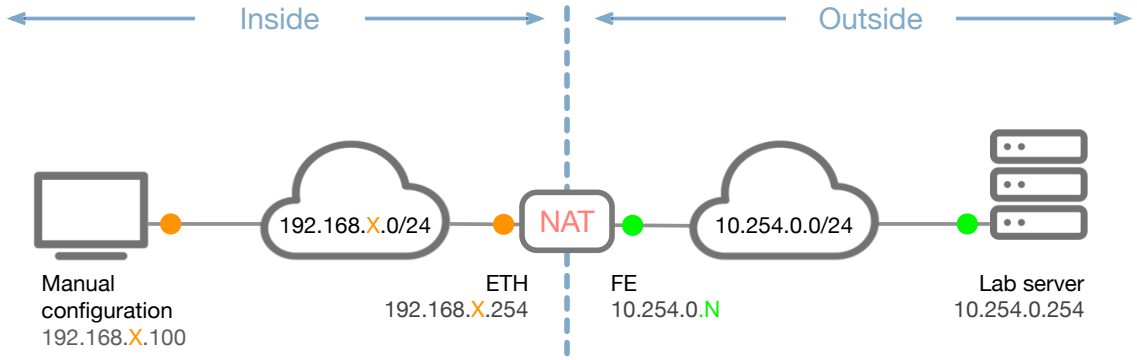

Figure 1 – Basic NAT scenario

1.2 Static and dynamic address assignment

Analyse the following NAT configuration example, in which some of the addresses are statically assigned and other are dynamically assigned:

```
R1#config t
R1(config)#access-list 25 deny 192.168.100.35 0.0.0.0
R1(config)#access-list 25 deny 192.168.100.36 0.0.0.0
R1(config)#access-list 25 permit 192.168.100.0 0.0.0.255
R1(config)#ip nat inside source static 192.168.100.35 172.16.1.50
R1(config)#ip nat inside source static 192.168.100.36 172.16.1.51
R1(config)#ip nat pool POOLB 172.16.1.100 172.16.1.120 netmask
255.255.255.0
R1(config)#ip nat inside source list 25 pool POOLB overload
R1(config)#interface FastEthernet0
R1(config-if)#ip address 192.168.100.1 255.255.255.0
R1(config-if)#ip nat inside
R1(config-if)#exit
```

```
R1(config)#interface Ethernet0
R1(config-if)#ip address 172.16.1.1 255.255.255.0
R1(config-if)#ip nat outside
R1(config-if)#end
R1#
```

The access list starts by excluding the addresses that are going to be statically mapped. Note that this is not necessary, as static NAT mapping has precedence over dynamic NAT mapping. Nevertheless, this is usually done for the sake of clarity. Next, the static mappings are specified.

Dynamic mapping is specified through the use of an address pool (172.16.1.100 to 172.16.1.120) that can be overloaded. This means that if the addresses in the pool are all used up they can be reused. Reused addresses will be sorted out by using the PAT mechanism.

Exercise 2 – Change the NAT configuration developed in the previous exercise, so that static and dynamic mappings are defined according to the following:

- The machine with the 'inside local' IP address 192.168.X.200 should be statically mapped to the outside 10.254.0.(N*16+1) address;
- Define an address pool named net-TEST, with addresses 10.254.0.(N*16+2) to 10.254.0.(N*16+5). This pool should be of type 'overload'.
- All machines with an inside local address different from 192.168.X.200 should be mapped to the net-TEST pool.
- Configure your PC with the static inside local address which you have defined (192.168.X.200). Execute the ping command, targeting the lab server, whose IP address is 10.254.0.254. In the console of this server check the outside IP address used by your machine.
- Re-configure your PC with one address that is not the static 'inside local' address and repeat the ping command. What is the outside IP address used by your machine?

1.3 NAT with the client's public addresses

In both of the previous exercises, the outside local addresses belonged to the lab backbone address range. This means that in a real scenario, they would be addresses belonging to the ISP address space. In this case, represented in Figure 2a), the client machines would appear to the outside world as machines belonging to the ISP network and not to the client network.

In certain cases, ISP clients have their own public address ranges and want that their machines to appear to the outside world as machines belonging to the client (and not to the ISP). This is represented in Figure 2b). In this case, the NAT pool to be used by the router should be an address pool using the client's public address space, and not using the ISP's public address space.

In the following example it is possible to see the static NAT, dynamic NAT and DHCP configurations, in which the client's private addresses are mapped to public addresses also belonging to the client. The following are the used address ranges:

- 192.168.0.0/24 – client inside network.
- 172.16.1.0/27 – client public address range (Note: for the purpose of illustration we consider that these addresses are 'public' although, in fact, they are RFC 1918 addresses).
- 10.254.0.0/24 – ISP network.

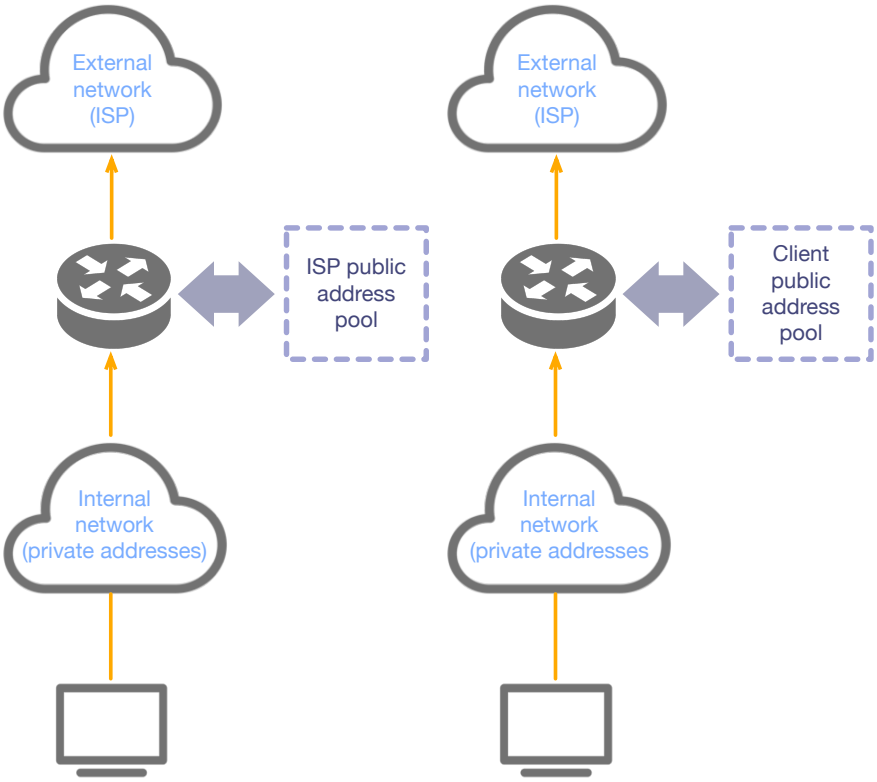

Figure 2 – NAT with public addresses belonging to (a) the ISP or (b) the client

```
!
! R1: Static NAT and Dynamic NAT configurations
! ================================================================================
!
! Inside network: 192.168.0.0/255.255.255.0
!      Fixed inside addresses: 192.168.0.1 to 192.168.0.24
!
! Outside local addresses:  172.16.0.0/255.255.255.224
!      Fixed outside local addresses: 172.16.0.1 to 172.16.0.28
!      Dynamic outside local address pool: 172.16.0.29 a 172.16.0.30
!
! DHCP configuration

interface f0
   desc This is the inside network
   ip address 192.168.0.1 255.255.255.0
   ip nat inside

interface e0
   desc This is the outside network
   ip address 10.0.0.1 255.0.0.0
   ip nat outside
   ip access-group 120 in


!
! NAT/PAT configuration
!
ip nat pool net-TESTE 172.16.0.29 172.16.0.30 netmask 255.255.255.0
ip nat inside source list 1 pool net-TESTE overload
access-list 1 permit 192.168.X.0 0.0.0.255
```

In the previous example we can see that the outside local addresses belong to the client (network 172.16.0.0/24) and not to the ISP (network 10.0.0.0/24).

Exercise 3 – Adapt the previous example to the scenario of your internal network, according to the following:

- As the client's valid network use 172.16.(X+N).0/24.
- The client's private network should be 192.168.X.0/24, as in the previous exercises.
- As ISP network use the existing lab network, that is, 10.254.0.0/24, as in the previous exercises.
- ping the lab server and check the 'outside local' IP address used by your machine.
- Explain what is happening in terms of address translation in your scenario.

1.4 State and debugging information

There are several NAT-related commands that provide useful state and debugging information. Some examples are:

```
R1#show ip nat translation

R1#clear ip nat translation *

R1#show ip nat statistics

R1#clear ip nat statistics

R1#debug ip nat

R1#debug ip nat detailed
```

Exercise 4 – Try these commands. Analyse and interpret their output.
