Lab – Configuring Dynamic and Static NAT

Topology



1. Addressing Table

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default Gateway** |
| **Gateway** | **G0/1** | 192.168.1.1 | 255.255.255.0 | N/A |
|  | **S0/1/1** | 209.165.201.18 | 255.255.255.252 | N/A |
| **ISP** | **S0/1/0 (DCE)** | 209.165.201.17 | 255.255.255.252 | N/A |
|  | **Lo0** | 192.31.7.1 | 255.255.255.255 | N/A |
| **PC-A (Simulated Server)** | **NIC** | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| **PC-B** | **NIC** | 192.168.1.21 | 255.255.255.0 | 192.168.1.1 |



1. Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

1. Background / Scenario

**Network Address Translation (NAT)** is the process where a network device, such as a Cisco router, assigns a public address to host devices inside a private network. The main reason to use NAT is to reduce the number of public IP addresses that an organization uses because the number of available IPv4 public addresses is limited.

In this lab, an ISP has allocated the public IP address space of **209.165.200.224/27** to a company. This provides the company with 30 public IP addresses. The addresses, **209.165.200.225 to 209.165.200.241**, are for static allocation and **209.165.200.242 to 209.165.200.254** are for dynamic allocation. A static route is used from the ISP to the gateway router, and a default route is used from the gateway to the ISP router. The ISP connection to the Internet is simulated by a loopback address on the ISP router.

1. Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

* 1. Configure PC hosts.
  2. Initialize and reload the routers and switches as necessary.
  3. Configure basic settings for each router.
     1. Console into the router and enter global configuration mode.
     2. Copy the following basic configuration and paste it to the running-configuration on the router.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

* + 1. Configure the host name as shown in the topology.
    2. Configure the IPv4 addresses on the router as shown in the topology. (AGREGAR)
    3. Set the DCE serial interfaces with a clock rate of 128000.
  1. Configure static routing.
     1. Create a static route from the ISP router to the Gateway router using the assigned public network address range 209.165.200.224/27.

ISP(config)# **ip route 209.165.200.224 255.255.255.224 209.165.201.18**

* + 1. Create a default route from the Gateway router to the ISP router.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

* 1. Verify network connectivity.
     1. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping results** (Fail / Success) |
| **PC-A** | **Gateway G0/1** | 192.168.1.1 |  |
| **PC-B** | **Gateway G0/1** | 192.168.1.1 |  |

* + 1. Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

1. Configure and Verify Static NAT

Static NAT uses a one-to-one mapping of local and global addresses, and these mappings remain constant. Static NAT is particularly useful for web servers or devices that must have static addresses that are accessible from the Internet.

* 1. Configure a static mapping.

A static map is configured to tell the router to translate between the private inside server address 192.168.1.20 and the public address 209.165.200.225. This allows a user from the Internet to access PC-A. PC-A is simulating a server or device with a constant address that can be accessed from the Internet.

Gateway(config)# **ip nat inside source static 192.168.1.20 209.165.200.225**

* 1. Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

Gateway(config)# **interface g0/1**

Gateway(config-if)# **ip nat inside**

Gateway(config-if)# **interface s0/0/1**

Gateway(config-if)# **ip nat outside**

* 1. Test the configuration.
     1. Display the static NAT table by issuing the **show ip nat translations** command.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

What is the translation of the Inside local host address?

192.168.1.20 = \_\_\_\_ **209.165.200.225**

The Inside global address is assigned by?

**The router from the NAT pool.**

The Inside local address is assigned by?

**The administrator for the workstation.**

* + 1. From **PC-A**, ping the **Lo0** interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:5 192.168.1.20:5 192.31.7.1:5 192.31.7.1:5

icmp 209.165.200.225:6 192.168.1.20:6 192.31.7.1:6 192.31.7.1:6

icmp 209.165.200.225:7 192.168.1.20:7 192.31.7.1:7 192.31.7.1:7

icmp 209.165.200.225:8 192.168.1.20:8 192.31.7.1:8 192.31.7.1:8

--- 209.165.200.225 192.168.1.20 --- ---

A NAT entry was added to the table with ICMP listed as the protocol when PC-A sent an ICMP request (ping) to 192.31.7.1 on ISP.

**Básicamente, los paquetes ICMP secuenciales se traducen en números de puerto, toda esta información se almacena en la memoria, lo que permite que cada paquete sea redirigido a su cliente.**

What port number was used in this ICMP exchange? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **5,6,7,8**

**Note**: It may be necessary to disable the PC-A firewall for the ping to be successful.

* + 1. From **PC-A**, telnet to the **ISP Lo0** interface and display the NAT table.

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:1 192.168.1.20:1 192.31.7.1:1 192.31.7.1:1

tcp 209.165.200.225:1034 192.168.1.20:1034 192.31.7.1:23 192.31.7.1:23

--- 209.165.200.225 192.168.1.20 --- ---

**Note**: The NAT for the ICMP request may have timed out and been removed from the NAT table. **(se haya agotado el tiempo de espera y haya sido removido de la table de NAT)**

What was the protocol used in this translation? \_\_\_\_\_\_\_\_\_\_\_\_ **tcp**

What are the port numbers used?

Inside global / local: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **1025**

Outside global / local: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ **23**

* + 1. Because static NAT was configured for **PC-A**, verify that pinging from **ISP** to PC-A at the static NAT public address **(209.165.200.225**) is successful.
    2. On the Gateway router, display the NAT table to verify the translation.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:1 192.168.1.20:1 209.165.201.17:1 209.165.201.17:1

icmp 209.165.200.225:2 192.168.1.20:2 209.165.201.17:2 209.165.201.17:2

icmp 209.165.200.225:3 192.168.1.20:3 209.165.201.17:3 209.165.201.17:3

icmp 209.165.200.225:4 192.168.1.20:4 209.165.201.17:4 209.165.201.17:4

icmp 209.165.200.225:5 192.168.1.20:5 209.165.201.17:5 209.165.201.17:5

--- 209.165.200.225 192.168.1.20 --- ---

tcp 209.165.200.225:1025 192.168.1.20:1025 192.31.7.1:23 192.31.7.1:23

Notice that the Outside local and Outside global addresses are the same. This address is the ISP remote network source address. For the ping from the ISP to succeed, the Inside global static NAT address 209.165.200.225 was translated to the Inside local address of PC-A (192.168.1.20).

* + 1. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat statistics**

Total translations: 7 (1 static, 6 dynamic, 6 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 74 Misses: 10

Expired translations: 4

Dynamic mappings:

**Note**: This is only a sample output. Your output may not match exactly.

1. Configure and Verify Dynamic NAT

Dynamic NAT uses a pool of public addresses and assigns them on a first-come, first-served basis. When an inside device requests access to an outside network, dynamic NAT assigns an available public IPv4 address from the pool. Dynamic NAT results in a many-to-many address mapping between local and global addresses.

* 1. Clear NATs.

Before proceeding to add dynamic NATs, clear the NATs and statistics from Part 2.

Gateway# **clear ip nat translation \***

Gateway# **clear ip nat statistics**

* 1. Define an access control list (ACL) that matches the LAN private IP address range.

ACL 1 is used to allow 192.168.1.0/24 network to be translated.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

* 1. Verify that the NAT interface configurations are still valid.

Issue the **show ip nat statistics** command on the Gateway router to verify the NAT configurations.

Gateway# **show ip nat statistics**

Total active translations: 1 (1 static, 0 dynamic; 0 extended)

Peak translations: 0

Outside interfaces:

Serial0/0/1

Inside interfaces:

FastEthernet0/1

Hits: 0 Misses: 0

CEF Translated packets: 0, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

* 1. Define the pool of usable public IP addresses.

Gateway(config)# **ip nat pool public\_access 209.165.200.242 209.165.200.254 netmask 255.255.255.224**

* 1. Define the NAT from the inside source list to the outside pool.

**Note**: Remember that NAT pool names are case-sensitive and the pool name entered here must match that used in the previous step.

Gateway(config)# **ip nat inside source list 1 pool public\_access**

* 1. Test the configuration.
     1. From PC-B, ping the Lo0 interface (192.31.7.1) on ISP. If the ping was unsuccessful, troubleshoot and correct the issues. On the Gateway router, display the NAT table.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

--- 209.165.200.225 192.168.1.20 --- ---

icmp 209.165.200.242:5 192.168.1.21:5 192.31.7.1:5 192.31.7.1:5

icmp 209.165.200.242:6 192.168.1.21:6 192.31.7.1:6 192.31.7.1:6

icmp 209.165.200.242:7 192.168.1.21:7 192.31.7.1:7 192.31.7.1:7

icmp 209.165.200.242:8 192.168.1.21:8 192.31.7.1:8 192.31.7.1:8

--- 209.165.200.242 192.168.1.21 --- ---

What is the translation of the Inside local host address for PC-B?

192.168.1.21 = **\_\_\_\_\_\_\_\_\_\_\_\_\_\_ 209.165.200.242**

A dynamic NAT entry was added to the table with ICMP as the protocol when PC-B sent an ICMP message to 192.31.7.1 on ISP.

What port number was used in this ICMP exchange? \_\_\_\_\_\_\_\_\_\_\_\_\_\_**5, 6, 7, 8**

* + 1. Verify NAT statistics by using the **show ip nat statistics** command on the Gateway router.

Gateway# **show ip nat statistics**

Total translations: 1 (1 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 81 Misses: 14

Expired translations: 13

Dynamic mappings:

-- Inside Source

access-list 1 pool public\_access refCount 0

pool public\_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13 , allocated 0 (0%), misses 0

**Note**: This is only a sample output. Your output may not match exactly.

* 1. Remove the static NAT entry.

In Step 7, the static NAT entry is removed and you can observe the NAT entry.

* + 1. Remove the static NAT from Part 2. Enter **yes** when prompted to delete child entries.

Gateway(config)# **no ip nat inside source static 192.168.1.20 209.165.200.225**

Static entry in use, do you want to delete child entries? [no]: **yes**

* + 1. Clear the NATs and statistics.
    2. Ping the ISP (192.31.7.1) from both hosts.

Gateway# **show ip nat translation**

* + 1. Display the NAT table and statistics.

Gateway# **show ip nat translation**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.243:13 192.168.1.20:13 192.31.7.1:13 192.31.7.1:13

icmp 209.165.200.243:14 192.168.1.20:14 192.31.7.1:14 192.31.7.1:14

icmp 209.165.200.243:15 192.168.1.20:15 192.31.7.1:15 192.31.7.1:15

icmp 209.165.200.243:16 192.168.1.20:16 192.31.7.1:16 192.31.7.1:16

icmp 209.165.200.244:13 192.168.1.21:13 192.31.7.1:13 192.31.7.1:13

icmp 209.165.200.244:14 192.168.1.21:14 192.31.7.1:14 192.31.7.1:14

icmp 209.165.200.244:15 192.168.1.21:15 192.31.7.1:15 192.31.7.1:15

icmp 209.165.200.244:16 192.168.1.21:16 192.31.7.1:16 192.31.7.1:16

**Note**: This is only a sample output. Your output may not match exactly.

Gateway# **show ip nat statistics**

Total translations: 8 (0 static, 8 dynamic, 8 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 97 Misses: 30

Expired translations: 21

Dynamic mappings:

-- Inside Source

access-list 1 pool public\_access refCount 8

pool public\_access: netmask 255.255.255.224

start 209.165.200.242 end 209.165.200.254

type generic, total addresses 13 , allocated 2 (15%), misses 0

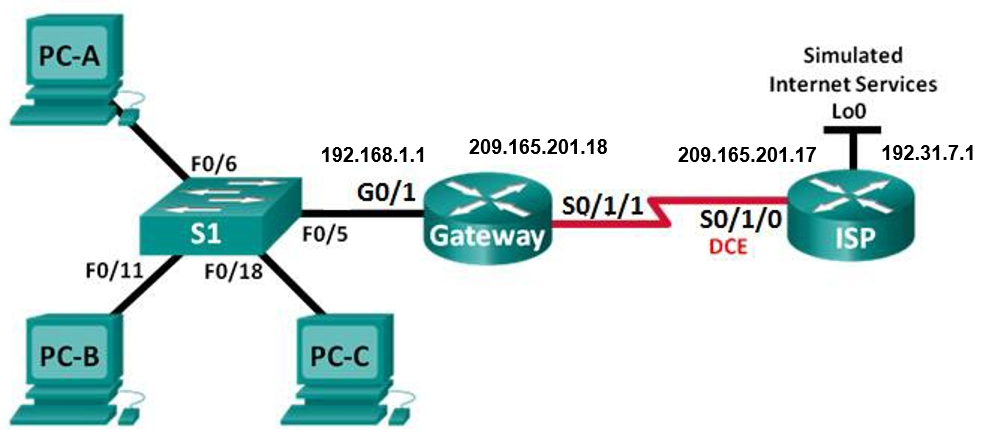
1. Reflection
   1. Why would NAT be used in a network?

Answers will vary, but should include: whenever there are not enough public IP addresses and to avoid the cost of purchasing public addresses from an ISP. NAT can also provide a measure of security by hiding internal addresses from outside networks.



**Cuando no tenemos suficientes direcciones IP públicas y para evitar el costo de comprar direcciones públicas de un ISP. NAT también puede proporcionar una medida de seguridad al ocultar las direcciones internas de las redes externas.**

Lab – Configuring Port Address Translation (PAT)



|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Device** | **Interface** | **IP Address** | **Subnet Mask** | **Default gateway** |
| **Gateway** | G0/1 | 192.168.1.1 | 255.255.255.0 | N/A |
|  | S0/1/1 | 209.165.201.18 | 255.255.255.252 | N/A |
| **ISP** | S0/1/0 (DCE) | 209.165.201.17 | 255.255.255.252 | N/A |
|  | Lo0 | 192.31.7.1 | 255.255.255.255 | N/A |
| **PC-A** | NIC | 192.168.1.20 | 255.255.255.0 | 192.168.1.1 |
| **PC-B** | NIC | 192.168.1.21 | 255.255.255.0 | 192.168.1.1 |
| **PC-C** | NIC | 192.168.1.22 | 255.255.255.0 | 192.168.1.1 |

1. Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify NAT Pool Overload

Part 3: Configure and Verify PAT

1. Background / Scenario

In the first part of the lab, your company is allocated the public IP address range of 209.165.200.224/29 by the ISP. This provides the company with six public IP addresses. Dynamic NAT pool overload uses a pool of IP addresses in a many-to-many relationship. The router uses the first IP address in the pool and assigns connections using the IP address plus a unique port number. After the maximum number of translations for a single IP address have been reached on the router (platform and hardware specific), it uses the next IP address in the pool. NAT pool overload is a form port address translation (PAT) that overloads a group of public IPv4 addresses.

In Part 2, the ISP has allocated a single IP address, 209.165.201.18, to your company for use on the Internet connection from the company Gateway router to the ISP. You will use the PAT to convert multiple internal addresses into the one usable public address. You will test, view, and verify that the translations are taking place, and you will interpret the NAT/PAT statistics to monitor the process.

1. Build the Network and Verify Connectivity

In Part 1, you will set up the network topology and configure basic settings, such as the interface IP addresses, static routing, device access, and passwords.

* 1. Configure PC hosts.
  2. Initialize and reload the routers and switches.
  3. Configure basic settings for each router.
     1. Console into the router and enter global configuration mode.
     2. Copy the following basic configuration and paste it to the running-configuration on the router.

no ip domain-lookup

service password-encryption

enable secret class

banner motd #

Unauthorized access is strictly prohibited. #

Line con 0

password cisco

login

logging synchronous

line vty 0 4

password cisco

login

* + 1. Configure the host name as shown in the topology.
    2. Copy the running configuration to the startup configuration.
  1. Configure static routing.
     1. Create a static route from the ISP router to the Gateway router.

ISP(config)# **ip route 209.165.200.224 255.255.255.248 209.165.201.18**

* + 1. Create a default route from the Gateway router to the ISP router.

Gateway(config)# **ip route 0.0.0.0 0.0.0.0 209.165.201.17**

* 1. Verify network connectivity.
     1. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
     2. Verify that the static routes are configured correctly on both routers.

1. Configure and Verify NAT Pool Overload

In Part 2, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the six usable addresses in the 209.165.200.224/29 range.

* 1. Define an access control list that matches the LAN private IP addresses.

ACL 1 is used to allow the 192.168.1.0/24 network to be translated.

Gateway(config)# **access-list 1 permit 192.168.1.0 0.0.0.255**

* 1. Define the pool of usable public IP addresses.

Gateway(config)# **ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

* 1. Define the NAT from the inside source list to the outside pool.

Gateway(config)# **ip nat inside source list 1 pool public\_access overload**

* 1. Specify the interfaces.

Issue the **ip nat inside** and **ip nat outside** commands to the interfaces.

Gateway(config)# **interface g0/1**

Gateway(config-if)# **ip nat inside**

Gateway(config-if)# **interface s0/0/1**

Gateway(config-if)# **ip nat outside**

* 1. Verify the NAT pool overload configuration.
     1. From each PC host, ping the 192.31.7.1 address on the ISP router.
     2. Display NATs on the Gateway router.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:13 192.168.1.22:13 192.31.7.1:13 192.31.7.1:13

icmp 209.165.200.225:14 192.168.1.22:14 192.31.7.1:14 192.31.7.1:14

icmp 209.165.200.225:15 192.168.1.22:15 192.31.7.1:15 192.31.7.1:15

icmp 209.165.200.225:16 192.168.1.22:16 192.31.7.1:16 192.31.7.1:16

icmp 209.165.200.225:17 192.168.1.21:17 192.31.7.1:17 192.31.7.1:17

icmp 209.165.200.225:18 192.168.1.21:18 192.31.7.1:18 192.31.7.1:18

icmp 209.165.200.225:19 192.168.1.21:19 192.31.7.1:19 192.31.7.1:19

icmp 209.165.200.225:20 192.168.1.21:20 192.31.7.1:20 192.31.7.1:20

icmp 209.165.200.225:21 192.168.1.20:21 192.31.7.1:21 192.31.7.1:21

icmp 209.165.200.225:22 192.168.1.20:22 192.31.7.1:22 192.31.7.1:22

icmp 209.165.200.225:23 192.168.1.20:23 192.31.7.1:23 192.31.7.1:23

icmp 209.165.200.225:24 192.168.1.20:24 192.31.7.1:24 192.31.7.1:24

* + 1. Display NAT statistics on the Gateway router.

Gateway# **show ip nat statistics**

Total translations: 12 (0 static, 12 dynamic, 12 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 36 Misses: 36

Expired translations: 20

Dynamic mappings:

-- Inside Source

access-list 1 pool public\_access refCount 12

pool public\_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

type generic, total addresses 6 , allocated 1 (16%), misses 0

**Note**: Depending on how much time has elapsed since you performed the pings from each PC, you may not see all three translations. ICMP translations have a short timeout value.

**Nota: Dependiendo de cuánto tiempo haya transcurrido desde que realizó los pings desde cada PC, es posible que no vea las tres traducciones. Las traducciones ICMP tienen un valor de tiempo de espera breve.**

How many Inside local IP addresses are listed in the sample output above? \_\_\_\_\_\_\_\_3\_\_

How many Inside global IP addresses are listed? \_\_\_\_\_\_\_\_\_1\_

How many port numbers are paired with the Inside global addresses? \_\_\_\_\_\_\_12\_\_

What would be the result of pinging the Inside local address of **PC-A** from the **ISP** router? Why?

**El ping fallaría porque el enrutador conoce la ubicación de la dirección global interna en su tabla de enrutamiento, pero la dirección local interna no se anuncia.**

1. Configure and Verify PAT

In Part 3, you will configure PAT by using an interface instead of a pool of addresses to define the outside address. Not all of the commands in Part 2 will be reused in Part 3.

* 1. Clear NATs and statistics on the Gateway router.

**Gateway# clear ip nat translation \***

* + 1. Verify that statistics have been cleared.
    2. Verify that the outside and inside interfaces are configured for NATs.
    3. Verify that the ACL is still configured for NATs.

Gateway# **sh ip nat statistics**

Total translations: 0 (0 static, 0 dynamic, 0 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 36 Misses: 36

Expired translations: 32

Dynamic mappings:

-- Inside Source

access-list 1 pool public\_access refCount 0

pool public\_access: netmask 255.255.255.248

start 209.165.200.225 end 209.165.200.230

type generic, total addresses 6 , allocated 0 (0%), misses 0

* 1. Remove the NAT translation from inside source list to outside pool.

Gateway(config)# **no ip nat inside source list 1 pool public\_access overload**

* 1. Remove the pool of useable public IP addresses.

Gateway(config)# **no ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248**

* 1. Associate the source list with the outside interface.

Gateway(config)# **ip nat inside source list 1 interface serial 0/1/1 overload**

* 1. Test the PAT configuration.
     1. From **each PC**, **ping** the **192.31.7.1** address on the **ISP** router.

|  |  |  |  |
| --- | --- | --- | --- |
| **From** | **To** | **IP Address (To)** | **Ping results** (Fail / Success) |
| **PC-A** | **ISP Lo0** | **192.31.7.1** |  |
| **PC-B** | **ISP Lo0** | **192.31.7.1** |  |
| **PC-C** | **ISP Lo0** | **192.31.7.1** |  |

* + 1. Display NAT statistics on the **Gateway** router.

Gateway# **show ip nat statistics**

Total translations: 12 (0 static, 12 dynamic, 12 extended)

Outside Interfaces: Serial0/1/1

Inside Interfaces: GigabitEthernet0/1

Hits: 48 Misses: 48

Expired translations: 32

Dynamic mappings:

* + 1. Display NAT translations on **Gateway**.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.201.18:17 192.168.1.22:17 192.31.7.1:17 192.31.7.1:17

icmp 209.165.201.18:18 192.168.1.22:18 192.31.7.1:18 192.31.7.1:18

icmp 209.165.201.18:19 192.168.1.22:19 192.31.7.1:19 192.31.7.1:19

icmp 209.165.201.18:20 192.168.1.22:20 192.31.7.1:20 192.31.7.1:20

icmp 209.165.201.18:21 192.168.1.21:21 192.31.7.1:21 192.31.7.1:21

icmp 209.165.201.18:22 192.168.1.21:22 192.31.7.1:22 192.31.7.1:22

icmp 209.165.201.18:23 192.168.1.21:23 192.31.7.1:23 192.31.7.1:23

icmp 209.165.201.18:24 192.168.1.21:24 192.31.7.1:24 192.31.7.1:24

icmp 209.165.201.18:25 192.168.1.20:25 192.31.7.1:25 192.31.7.1:25

icmp 209.165.201.18:26 192.168.1.20:26 192.31.7.1:26 192.31.7.1:26

icmp 209.165.201.18:27 192.168.1.20:27 192.31.7.1:27 192.31.7.1:27

icmp 209.165.201.18:28 192.168.1.20:28 192.31.7.1:28 192.31.7.1:28

1. Reflection

What advantages does PAT provide?

**PAT minimiza la cantidad de direcciones públicas necesarias para proporcionar acceso a Internet, y que PAT, como NAT, sirve para "ocultar" direcciones privadas de redes externas.**

**=POTENCIA(2, 16)**

**65 536 puertos**