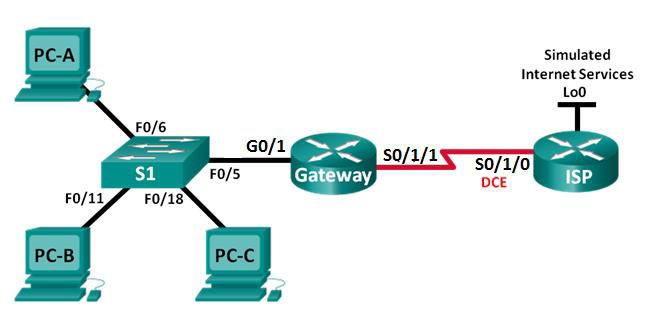


**Lab 9.2.3.7 – Configuring Port Address Translation (PAT)**



**209.165.201.17**

**192.168.1.1**

**192.31.7.1**

**209.165.201.18**

**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** | 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 |

## Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify NAT Pool Overload

Part 3: Configure and Verify PAT

**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. Configure basic settings for each router (Gateway and ISP).
     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.
    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 / 29**.

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.

|  |  |  |  |
| --- | --- | --- | --- |
| **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** |  |
| **PC-C** | **Gateway G0/1** | **192.168.1.1** |  |

* + 1. Verify that the static routes (**sh ip route**) are configured correctly on both routers.

# Part 2: 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 s0/1/1**

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.

|  |  |  |  |
| --- | --- | --- | --- |
| **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 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.

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

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

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

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

# Part 3: 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 the configuration for NAT.
     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?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_