Lab – Configuring Port Address Translation (PAT) (Instructor Version)

**Instructor Note**: Red font color or Gray highlights indicate text that appears in the instructor copy only.

1. 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 |
|  | S0/0/1 | 209.165.201.18 | 255.255.255.252 | N/A |
| ISP | S0/0/0 (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.

**Note**: The routers used with CCNA hands-on labs are Cisco 1941 Integrated Services Routers (ISRs) with Cisco IOS Release 15.2(4)M3 (universalk9 image). The switches used are Cisco Catalyst 2960s with Cisco IOS Release 15.0(2) (lanbasek9 image). Other routers, switches and Cisco IOS versions can be used. Depending on the model and Cisco IOS version, the commands available and output produced might vary from what is shown in the labs. Refer to the Router Interface Summary Table at the end of this lab for the correct interface identifiers.

**Note**: Make sure that the routers and switch have been erased and have no startup configurations. If you are unsure, contact your instructor.

**Instructor Note**: Refer to the Instructor Lab Manual for the procedures to initialize and reload devices.

1. Required Resources
* 2 Routers (Cisco 1941 with Cisco IOS Release 15.2(4)M3 universal image or comparable)
* 1 Switch (Cisco 2960 with Cisco IOS Release 15.0(2) lanbasek9 image or comparable)
* 3 PCs (Windows 7, Vista, or XP with terminal emulation program, such as Tera Term)
* Console cables to configure the Cisco IOS devices via the console ports
* Ethernet and serial cables as shown in the topology
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. Cable the network as shown in the topology.
	2. Configure PC hosts.
	3. Initialize and reload the routers and switches.
	4. Configure basic settings for each router.
		1. Disable DNS lookup.
		2. Configure IP addresses for the routers as listed in the Addressing Table.
		3. Set the clock rate to **128000** for DCE serial interface.
		4. Configure device name as shown in the topology.
		5. Assign **cisco** as the console and vty passwords.
		6. Assign **class** as the encrypted privileged EXEC mode password.
		7. Configure **logging synchronous** to prevent console messages from interrupting the command entry.
	5. 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 NAT statistics on the Gateway router.

Gateway# **show ip nat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:25 ago

Outside interfaces:

 Serial0/0/1

Inside interfaces:

 GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 1] access-list 1 pool public\_access refcount 3

 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

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

* + 1. Display NATs on the Gateway router.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.200.225:0 192.168.1.20:1 192.31.7.1:1 192.31.7.1:0

icmp 209.165.200.225:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1

icmp 209.165.200.225:2 192.168.1.22:1 192.31.7.1:1 192.31.7.1:2

**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? \_\_\_\_\_\_\_\_\_\_ 3

How many Inside global IP addresses are listed? \_\_\_\_\_\_\_\_\_\_ 1

How many port numbers are used paired with the Inside global addresses? \_\_\_\_\_\_\_\_\_ 3

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

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

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

The ping would fail because the router knows the location of the Inside global address in its routing table but the Inside local address is not advertised.

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.
	2. 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.

What command did you use to confirm the results from steps a to c?

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

Gateway# **show ip nat statistics**

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

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

* 1. Test the PAT configuration.
		1. From each PC, ping the 192.31.7.1 address on the ISP router.
		2. Display NAT statistics on the Gateway router.

Gateway# **show ip nat statistics**

Total active translations: 3 (0 static, 3 dynamic; 3 extended)

Peak translations: 3, occurred 00:00:19 ago

Outside interfaces:

 Serial0/0/1

Inside interfaces:

 GigabitEthernet0/1

Hits: 24 Misses: 0

CEF Translated packets: 24, CEF Punted packets: 0

Expired translations: 0

Dynamic mappings:

-- Inside Source

[Id: 2] access-list 1 interface Serial0/0/1 refcount 3

Total doors: 0

Appl doors: 0

Normal doors: 0

Queued Packets: 0

* + 1. Display NAT translations on Gateway.

Gateway# **show ip nat translations**

Pro Inside global Inside local Outside local Outside global

icmp 209.165.201.18:3 192.168.1.20:1 192.31.7.1:1 192.31.7.1:3

icmp 209.165.201.18:1 192.168.1.21:1 192.31.7.1:1 192.31.7.1:1

icmp 209.165.201.18:4 192.168.1.22:1 192.31.7.1:1 192.31.7.1:4

1. Reflection

What advantages does PAT provide?

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

Answers will vary, but should include that PAT minimizes the number of public addresses needed to provide Internet access, and that PAT, like NAT, serves to “hide” private addresses from outside networks.

1. Router Interface Summary Table

|  |
| --- |
| Router Interface Summary |
| Router Model | Ethernet Interface #1 | Ethernet Interface #2 | Serial Interface #1 | Serial Interface #2 |
| 1800 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 1900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2801 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/1/0 (S0/1/0) | Serial 0/1/1 (S0/1/1) |
| 2811 | Fast Ethernet 0/0 (F0/0) | Fast Ethernet 0/1 (F0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| 2900 | Gigabit Ethernet 0/0 (G0/0) | Gigabit Ethernet 0/1 (G0/1) | Serial 0/0/0 (S0/0/0) | Serial 0/0/1 (S0/0/1) |
| **Note**: To find out how the router is configured, look at the interfaces to identify the type of router and how many interfaces the router has. There is no way to effectively list all the combinations of configurations for each router class. This table includes identifiers for the possible combinations of Ethernet and Serial interfaces in the device. The table does not include any other type of interface, even though a specific router may contain one. An example of this might be an ISDN BRI interface. The string in parenthesis is the legal abbreviation that can be used in Cisco IOS commands to represent the interface. |

1. Device Configs
2. Router Gateway (After Part 2)

Gateway# show run

Building configuration...

Current configuration : 1790 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Gateway

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

!

!

!

!

!

!

no ip domain lookup

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

 no ip address

 shutdown

!

interface GigabitEthernet0/0

 no ip address

 shutdown

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 ip address 192.168.1.1 255.255.255.0

 ip nat inside

 ip virtual-reassembly in

 duplex auto

 speed auto

!

interface Serial0/0/0

 no ip address

 shutdown

!

interface Serial0/0/1

 ip address 209.165.201.18 255.255.255.252

 ip nat outside

 ip virtual-reassembly in

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip nat pool public\_access 209.165.200.225 209.165.200.230 netmask 255.255.255.248

ip nat inside source list 1 pool public\_access overload

ip route 0.0.0.0 0.0.0.0 209.165.201.17

!

access-list 1 permit 192.168.1.0 0.0.0.255

!

!

!

control-plane

!

!

!

line con 0

 password cisco

 logging synchronous

 login

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport input all

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 password cisco

login

 transport input all

!

scheduler allocate 20000 1000

!

end

1. Router Gateway (After Part 3)

Gateway# show run

Building configuration...

Current configuration : 1711 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname Gateway

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 15

!

!

!

!

!

!

!

no ip domain lookup

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

!

interface Embedded-Service-Engine0/0

 no ip address

 shutdown

!

interface GigabitEthernet0/0

 no ip address

 shutdown

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 ip address 192.168.1.1 255.255.255.0

 ip nat inside

 ip virtual-reassembly in

 duplex auto

 speed auto

!

interface Serial0/0/0

 no ip address

 shutdown

!

interface Serial0/0/1

 ip address 209.165.201.18 255.255.255.252

 ip nat outside

 ip virtual-reassembly in

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip nat inside source list 1 interface Serial0/0/1 overload

ip route 0.0.0.0 0.0.0.0 209.165.201.17

!

access-list 1 permit 192.168.1.0 0.0.0.255

!

!

!

Control-plane

!

!

!

line con 0

 password cisco

 logging synchronous

 login

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport input all

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 password cisco

login

 transport input all

!

scheduler allocate 20000 1000

!

end

1. Router ISP

ISP# **show run**

Building configuration...

Current configuration : 1487 bytes

!

version 15.2

service timestamps debug datetime msec

service timestamps log datetime msec

no service password-encryption

!

hostname ISP

!

boot-start-marker

boot-end-marker

!

!

enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2

!

no aaa new-model

memory-size iomem 10

!

!

!

!

!

!

!

no ip domain lookup

ip cef

no ipv6 cef

multilink bundle-name authenticated

!

!

!

!

!

!

!

!

!

!

interface Loopback0

 ip address 192.31.7.1 255.255.255.255

!

interface Embedded-Service-Engine0/0

 no ip address

 shutdown

!

interface GigabitEthernet0/0

 no ip address

 shutdown

 duplex auto

 speed auto

!

interface GigabitEthernet0/1

 no ip address

 shutdown

 duplex auto

 speed auto

!

interface Serial0/0/0

 ip address 209.165.201.17 255.255.255.252

 clock rate 128000

!

interface Serial0/0/1

 no ip address

 shutdown

!

ip forward-protocol nd

!

no ip http server

no ip http secure-server

!

ip route 209.165.200.224 255.255.255.224 209.165.201.18

!

!

!

!

control-plane

!

!

!

line con 0

 password cisco

 logging synchronous

 login

line aux 0

line 2

 no activation-character

 no exec

 transport preferred none

 transport input all

 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh

 stopbits 1

line vty 0 4

 password cisco

login

 transport input all

!

scheduler allocate 20000 1000

!

end