Port Address Translation (PAT)

Topology
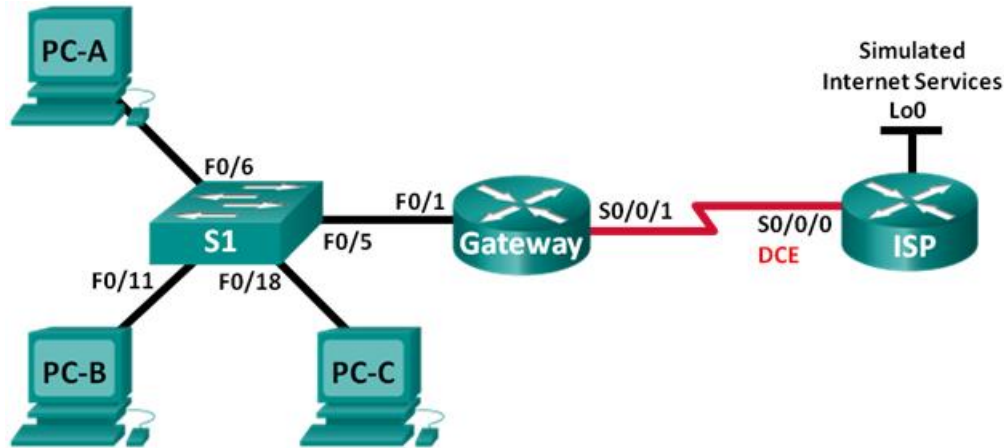
Addressing Table

Device	Interface	IP Address	Subnet Mask	Default Gateway
Gateway	F0/1	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

Introduction

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

Required Resources

- 2 Routers
- 1 Switch
- 3 PCs
- Console cables to configure the Cisco IOS devices via the console ports
- Ethernet and serial cables as shown in the topology

Part 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.

Step 1:   Cable the network as shown in the topology.

Step 2:   Configure PC hosts.

Step 3:   Initialize and reload the routers and switches if necessary.

Step 4:   Configure basic settings for each router.

a. Console into the router and enter global configuration mode.

b. Do the following basic configuration on the router.

```
no ip domain-lookup
service password-encryption
enable secret pass
banner motd #
Unauthorized access is strictly prohibited. #
Line con 0
password pass
login
logging synchronous
line vty 0 4
password pass
login
```

c. Configure the host name as shown in the topology.

d. Copy the running configuration to the startup configuration.

Step 5:   Configure static routing.

a. 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**

b. 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**

Step 6:   Verify network connectivity.

a. From the PC hosts, ping the F0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.

b. Verify that the static routes 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.

Step 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
```

Step 2:   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
```

Step 3:   Define the NAT from the inside source list to the outside pool.

```
Gateway(config)# ip nat inside source list 1 pool public_access overload
```

Step 4:   Specify the interfaces.

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

```
Gateway(config)# interface f0/1
Gateway(config-if)# ip nat inside
Gateway(config-if)# interface s0/0/1
Gateway(config-if)# ip nat outside
```

Step 5:   Verify the NAT pool overload configuration.

a. From each PC host, ping the 192.31.7.1 address on the ISP router.

b. 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:
  FastEthernet0/1
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
```

c. 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? _____

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.

Step 1:   Clear NATs and statistics on the Gateway router.

Step 2:   Verify the configuration for NAT.

a. Verify that statistics have been cleared.

b. Verify that the outside and inside interfaces are configured for NATs.

c. Verify that the ACL is still configured for NATs.

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

_____

Step 3:   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
```

Step 4:   Remove the NAT translation from inside source list to outside pool.

```
Gateway(config)# no ip nat inside source list 1 pool public_access overload
```

Step 5:   Associate the source list with the outside interface.

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

Step 6:   Test the PAT configuration.

a. From each PC, ping the 192.31.7.1 address on the ISP router.

b. 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:
  FastEthernet0/1
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
```

c. 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
```

What advantages does PAT provide?

_____