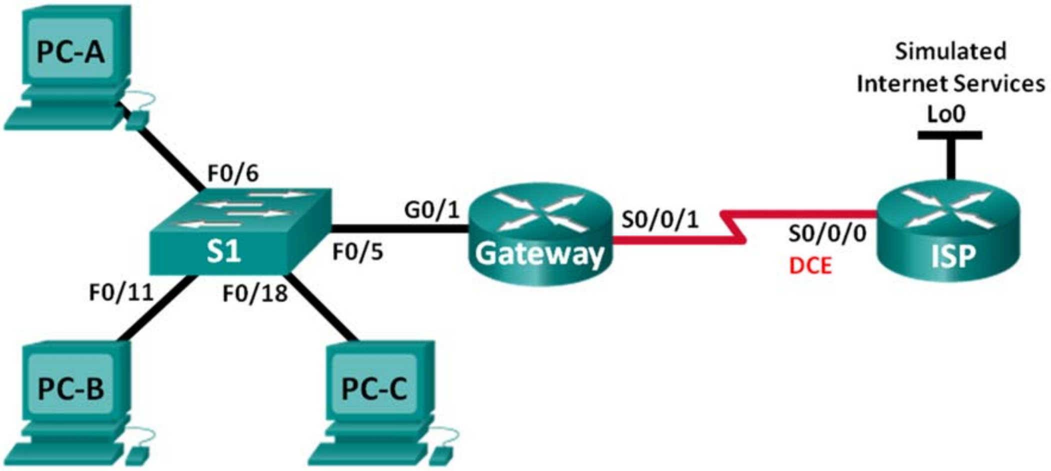
Lab 8 – Configuring Dynamic, Static NAT, and NAT Pool Overload

Topology



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

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

Part 4: Configure and Verify NAT Pool Overload

Part 5: Configure and Verify PAT

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 209.165.200.239, are for static allocation and 209.165.200.240 to 209.165.200.254 are for dynamic allocation.

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.

In Part 4, the ISP has allocated a single IP address, 209.165.201.18, to the company for use on the Internet connection from the company Gateway router to the ISP. You will use the Port Address Translation (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.

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.

Note: Make sure that the routers and switch have been erased and have no startup configurations.

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.

Attach the devices as shown in the topology diagram, and cable as necessary.

Step 2: Configure PC hosts.

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

Step 4: Configure basic settings for each router.

- Disable DNS lookup.
- Configure IP addresses for the routers as listed in the Addressing Table.
- Set the clock rate to **128000** for the DCE serial interfaces.
- Configure device name as shown in the topology.
- Assign **cisco** as the console and vty passwords.
- Assign **class** as the encrypted privileged EXEC mode password.
- Configure **logging synchronous** to prevent console messages from interrupting the command entry.

Step 5: Create a simulated web server on ISP.

- Create a local user named **webuser** with an encrypted password of **webpass**.

```
ISP(config)# username webuser privilege 15 secret webpass
```

- Enable the HTTP server service on ISP.

```
ISP(config)# ip http server
```

- Configure the HTTP service to use the local user database.

```
ISP(config)# ip http authentication local
```

Step 6: Configure static routing.

- 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
```

- 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 7: Save the running configuration to the startup configuration.

Step 8: Verify network connectivity.

- From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- Display the routing tables on both routers to verify that the static routes are in the routing table and configured correctly on both routers.

Part 2: 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.

Step 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
```

Step 2: 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
```

Step 3: Test the configuration.

- 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 = ……………………………………………

The Inside global address is assigned by? ………………………………………………………………………

The Inside local address is assigned by?

……

- 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 209.165.200.225:1 192.168.1.20:1     192.31.7.1:1       192.31.7.1:1
--- 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.

What port number was used in this ICMP exchange? ……………………….

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

- 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.

What was the protocol used in this translation? ……………………………

What are the port numbers used?

Inside global / local: ……………………………….

Outside global / local: ……………………………….

- 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.
- 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 209.165.200.225:12 192.168.1.20:12    209.165.201.17:12  209.165.201.17:12
--- 209.165.200.225      192.168.1.20       ---                ---
```

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).

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

```
Gateway# show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 1 extended)
Peak translations: 2, occurred 00:02:12 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 39  Misses: 0
CEF Translated packets: 39, CEF Punted packets: 0
Expired translations: 3
.............. <output omitted>
```

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

Part 3: 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.

Step 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
```

Step 2: 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
```

Step 3: 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.

Step 4: Define the pool of usable public IP addresses.

```
Gateway(config)# ip nat pool public_access 209.165.200.240 209.165.200.254
netmask 255.255.255.224
```

Step 5: 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
```

Step 6: Test the configuration.

- 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 209.165.200.240:1 192.168.1.21:1     192.31.7.1:1       192.31.7.1:1
--- 209.165.200.240    192.168.1.21       ---                ---
```

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

192.168.1.21 = …………………………………..

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? ……………………………

- From PC-B, open a browser and enter the IP address of the ISP-simulated web server (Lo0 interface). When prompted, log in as **webuser** with a password of **webpass**.
- Display the NAT table.

```
Pro Inside global        Inside local       Outside local      Outside global
--- 209.165.200.225      192.168.1.20       ---                ---
tcp 209.165.200.240:1038 192.168.1.21:1038 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.240:1039 192.168.1.21:1039 192.31.7.1:80     192.31.7.1:80
.............. <output omitted>
tcp 209.165.200.240:1051 192.168.1.21:1051 192.31.7.1:80     192.31.7.1:80
tcp 209.165.200.240:1052 192.168.1.21:1052 192.31.7.1:80     192.31.7.1:80
--- 209.165.200.240    192.168.1.22       ---                ---
```

What protocol was used in this translation? ………………………………..

What port numbers were used?

Inside: …………………………………………………………

outside: ………………………………

What well-known port number and service was used? ………………….

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

```
Gateway# show ip nat statistics
Total active translations: 3 (1 static, 2 dynamic; 1 extended)
Peak translations: 17, occurred 00:06:40 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
.............. <output omitted>
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
 pool public_access: netmask 255.255.255.224
        start 209.165.200.240 end 209.165.200.254
        type generic, total addresses 13, allocated 1 (7%), misses 0

.............. <output omitted>
```

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

Step 7: Remove the static NAT entry.

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

- 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
```

- Clear the NATs and statistics.
- Ping the ISP (192.31.7.1) from both hosts.
- Display the NAT table.

```
Gateway# show ip nat translation
Pro Inside global      Inside local       Outside local      Outside global
icmp 209.165.200.241:512 192.168.1.20:512 192.31.7.1:512     192.31.7.1:512
--- 209.165.200.241    192.168.1.20       ---                ---
icmp 209.165.200.240:512 192.168.1.21:512 192.31.7.1:512     192.31.7.1:512
```

```
--- 209.165.200.240    192.168.1.21       ---                ---
```

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

Part 4: Configure and Verify NAT Pool Overload

In Part 4, you will configure the Gateway router to translate the IP addresses from the 192.168.1.0/24 network to one of the usable addresses in the 209.165.200.224/29 range.

Step 1: Remove the dynamic NAT pool of usable public IP addresses.

```
Gateway(config)# no ip nat pool public_access 209.165.200.240 209.165.200.254
netmask 255.255.255.224
```

Step 2: Remove the previous static route and configure a new one.

```
ISP(config)# no ip route 209.165.200.224 255.255.255.224 209.165.201.18
```

- Create a new 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
```

Step 3: Define the new 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 4: 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 5: Verify the NAT pool overload configuration.

- From each PC host, ping the 192.31.7.1 address on the ISP router.
- 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
.............. <output omitted>
-- 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
.............. <output omitted>
```

- 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 used 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 5: Configure and Verify PAT

In Part 5, you will configure PAT by using an interface instead of a pool of addresses to define the outside address.

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

Step 2: Verify the configuration for NAT.

- Verify that statistics have been cleared.
- Verify that the outside and inside interfaces are configured for NATs.
- Verify that the ACL is still configured for NATs.

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

……

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.

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