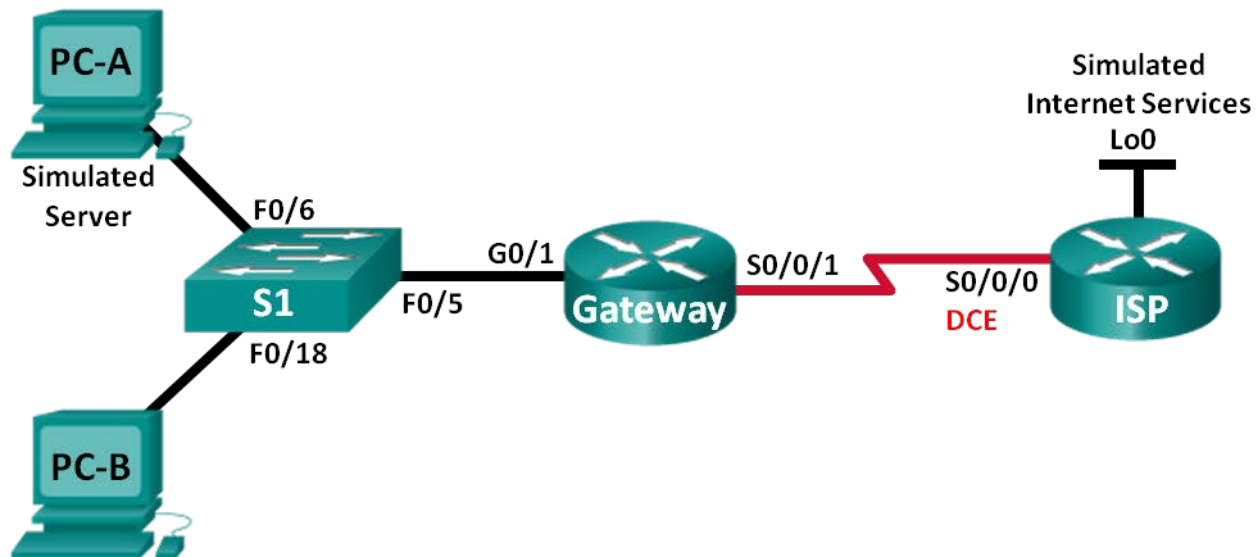


Lab – Configuring Dynamic and Static NAT

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 (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

Objectives

Part 1: Build the Network and Verify Connectivity

Part 2: Configure and Verify Static NAT

Part 3: Configure and Verify Dynamic NAT

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.

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.

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)
- 2 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

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.

- a. Console into the router and enter global configuration mode.
- b. 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
```

- c. Configure the host name as shown in the topology.
- d. Copy the running configuration to the startup configuration.

Step 5: Create a simulated web server on ISP.

- a. Create a local user named **webuser** with an encrypted password of **webpass**.
`ISP(config)# username webuser privilege 15 secret webpass`
- b. Enable the HTTP server service on ISP.
`ISP(config)# ip http server`
- c. Configure the HTTP service to use the local user database.
`ISP(config)# ip http authentication local`

Step 6: Configure static routing.

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

Step 8: Verify network connectivity.

- a. From the PC hosts, ping the G0/1 interface on the Gateway router. Troubleshoot if the pings are unsuccessful.
- b. 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.

- a. 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?

- b. 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.

- c. 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:

- d. 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.
- e. 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).

- f. 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
Dynamic mappings:

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

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 209.165.200.242 209.165.200.254
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	209.165.200.242:1	192.168.1.21:1	192.31.7.1:1	192.31.7.1:1
---	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 =

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	209.165.200.242:1038	192.168.1.21:1038	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1039	192.168.1.21:1039	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1040	192.168.1.21:1040	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1041	192.168.1.21:1041	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1042	192.168.1.21:1042	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1043	192.168.1.21:1043	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1044	192.168.1.21:1044	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1045	192.168.1.21:1045	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1046	192.168.1.21:1046	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1047	192.168.1.21:1047	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1048	192.168.1.21:1048	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1049	192.168.1.21:1049	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1050	192.168.1.21:1050	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1051	192.168.1.21:1051	192.31.7.1:80	192.31.7.1:80
tcp	209.165.200.242:1052	192.168.1.21:1052	192.31.7.1:80	192.31.7.1:80
---	209.165.200.242	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
Hits: 345 Misses: 0
CEF Translated packets: 345, CEF Punted packets: 0
Expired translations: 20
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 2
  pool public_access: netmask 255.255.255.224
    start 209.165.200.242 end 209.165.200.254
    type generic, total addresses 13, allocated 1 (7%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

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.

- a. 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
```

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

```
Gateway# show ip nat statistics
Total active translations: 4 (0 static, 4 dynamic; 2 extended)
Peak translations: 15, occurred 00:00:43 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  GigabitEthernet0/1
Hits: 16 Misses: 0
CEF Translated packets: 285, CEF Punted packets: 0
Expired translations: 11
Dynamic mappings:
-- Inside Source
[Id: 1] access-list 1 pool public_access refcount 4
  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

Total doors: 0
```

Lab – Configuring Dynamic and Static NAT

```
Appl doors: 0
Normal doors: 0
Queued Packets: 0
```

Gateway# **show ip nat translation**

```
Pro Inside global      Inside local      Outside local      Outside global
icmp 209.165.200.243:512 192.168.1.20:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.243      192.168.1.20      ---                ---
icmp 209.165.200.242:512 192.168.1.21:512 192.31.7.1:512    192.31.7.1:512
--- 209.165.200.242      192.168.1.21      ---                ---
```

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

Reflection

1. Why would NAT be used in a network?
2. What are the limitations of NAT?

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.				