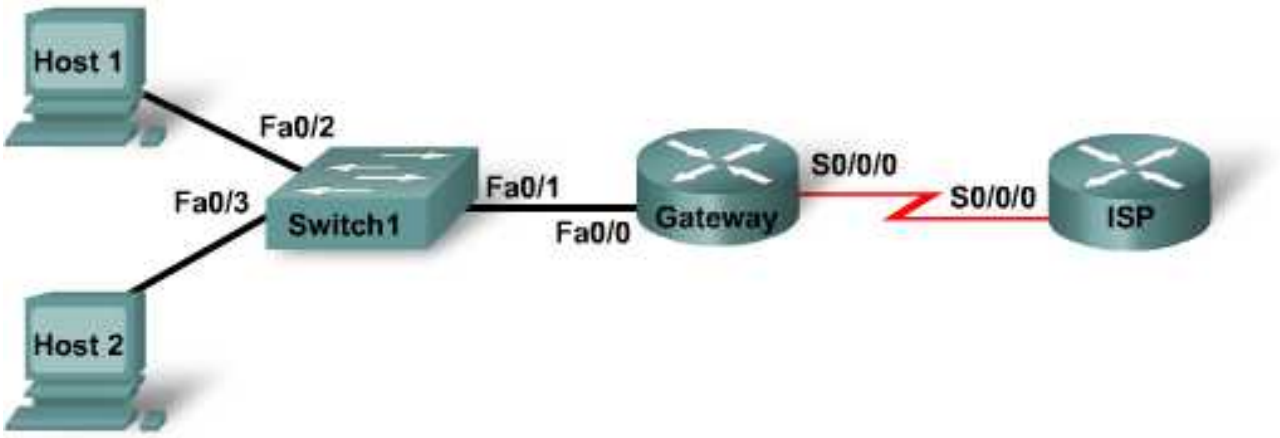
Lab 4.4.3 Configuring and Verifying Dynamic NAT



Device	Host Name	Fast Ethernet 0/0/ IP Address	Interface Type	Serial 0/0/0 IP Address	Loopback 0 Address / mask	Enable Secret Password	Enable, vty, and Console Password
Router 1	Gateway	10.10.10.1/24	DTE	209.165.201.33/30		cisco	class
Router 2	ISP	N/A	DCE	209.165.201.34/30	172.16.1.1/32	cisco	class
Switch 1	Switch1					cisco	class

Objectives

- Configure a router to use network address translation (NAT) to convert internal IP addresses, typically private addresses, into outside public addresses.
- Verify connectivity.
- Verify NAT statistics.

Background / Preparation

An ISP has allocated a company the public classless interdomain routing (CIDR) IP address 209.165.200.224/27. This provides them with 30 public IP addresses. Because the company has an internal requirement for more than 30 addresses, the IT manager decides to implement NAT. 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. Routing will be done between the ISP and the gateway router used by the company. A static route will be used between the ISP and the gateway router, and a default route will be used between the gateway and the ISP router. The ISP connection to the Internet will be represented by a loopback address on the ISP router.

This lab focuses on the basic configuration of the Cisco 2800 router, or comparable router, using Cisco IOS commands. The information in this lab applies to other routers; however, command syntax may vary. Depending on the router model, the interfaces may differ. For example, on some routers Serial 0 may be Serial 0/0 or Serial 0/0/0 and Ethernet 0 may be FastEthernet 0/0. The Cisco Catalyst 2960 switch comes preconfigured and only needs to be assigned basic security information before being connected to a network.

The following resources are required:

- One Cisco 2960 switches or other comparable switch
- Two routers, each with a serial connection and one Ethernet interface to connect to the switch
- Two Windows-based PCs for hosts, one with a terminal emulation program
- At least one RJ-45-to-DB-9 connector console cable to configure the router and switches
- Three straight-through Ethernet cables to connect from the router to Switch 1 and to connect both hosts to the switch
- One serial cable to connect from Router 1 to Router 2

NOTE: Make sure that the routers and the switches have been erased and have no startup configurations. Instructions for erasing both switch and router are provided in the Lab Manual, located on Academy Connection in the Tools section.

NOTE: SDM Enabled Routers – If the startup-config is erased in an SDM enabled router, SDM will no longer come up by default when the router is restarted. It will be necessary to build a basic router configuration using IOS commands. The steps provided in this lab use IOS commands and do not require the use of SDM. If you wish to use SDM, refer to the instructions in the Lab Manual, located on the Academy Connection in the Tools section or contact your instructor if necessary.

Step 1: Connect the equipment

a. Connect Router 1 Serial 0/0/0 interface to Router 2 Serial 0/0/0 interface using a serial cable.

b. Connect Router 1 Fa0/0 interface to Switch 1 Fa0/1 interface using a straight-through cable.

c. Connect a PC with a console cable to perform configurations on the routers and switch.

d. Connect both hosts to Fa0/2 and Fa0/3 on the switch using straight-through cables.

Step 2: Perform basic configurations on Router 2

a. Connect a PC to the console port of Router 2 to perform configurations using a terminal emulation program.

b. Configure Router 2 with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 3: Configure the gateway router

Perform basic configuration on Router 1 as the Gateway router with a hostname, interfaces, console, Telnet, and privileged passwords according to the table diagram. Save the configuration.

Step 4: Configure Switch 1

Configure Switch 1 with a hostname, console, Telnet, and privileged passwords according to the table diagram.

Step 5: Configure the hosts with the proper IP address, subnet mask, and default gateway

a. Configure each host with the proper IP address, subnet mask, and default gateway. Host 1 should be assigned 10.10.10.2 /24 and Host 2 should be assigned 10.10.10.3 /24. The default gateway should be 10.10.10.1.

b. Each workstation should be able to ping the attached router. If the ping was not successful, troubleshoot as necessary. Check and verify that the workstation has been assigned a specific IP address and default gateway.

Step 6: Verify that the network is functioning

From the attached hosts, ping the FastEthernet interface of the default gateway router.

Was the ping from Host 1 successful? _____

Was the ping from Host 2 successful? _____

If the answer is no for either question, troubleshoot the router and host configurations to find the error. Ping again until they are both successful.

Step 7: Create a static route

Create a static route from the ISP to the Gateway router. Addresses 209.165.200.224/27 have been allocated for Internet access outside of the company. Use the **ip route** command to create the static route.

```
ISP(config)#ip route 209.165.200.224 255.255.255.224 209.165.201.33
```

Is the static route in the routing table? _____

What command checks the routing table contents? _____

If the route was not in the routing table, give one reason why this might be so?

_____

Step 8: Create a default route

a. From the Gateway router to the ISP router, create a static route to network 0.0.0.0 0.0.0.0, using the **ip route** command. This will forward any unknown destination address traffic to the ISP by setting a Gateway of Last Resort on the Gateway router.

```
Gateway(config)#ip route 0.0.0.0 0.0.0.0 209.165.201.34
```

Is the static route in the routing table? _____

b. Try to ping from one of the workstations to the ISP serial interface IP address.

Was the ping successful? _____

Why? _____

Step 9: Define the pool of usable public IP addresses

To define the pool of public addresses, use the **ip nat pool** command.

```
Gateway(config)#ip nat pool public_access 209.165.200.242
209.165.200.254 netmask 255.255.255.224
```

Step 10: Define an access list that will match the inside private IP addresses

To define the access list to match the inside private addresses, use the **access-list** command.

```
Gateway(config)#access-list 1 permit 10.10.10.0 0.0.0.255
```

Step 11: Define the NAT translation from inside list to outside pool

To define the NAT translation, use **the ip nat inside source** command.

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

Step 12: Specify the interfaces

The active interfaces on the router need to be specified as either inside or outside interfaces with respect to NAT. To do this, use the **ip nat inside** or **ip nat outside** command.

```
Gateway(config)#interface fastethernet 0/0
Gateway(config-if)#ip nat inside
Gateway(config-if)#interface serial 0/0/0
Gateway(config-if)#ip nat outside
```

Step 13: Test the configuration

From Host 1 PC, ping 172.16.1.1. Open multiple command prompt windows on each workstation and telnet to the 172.16.1.1 address in each window. When successful, look at the NAT translation on the Gateway router, using the command **show ip nat translations**.

What is the translation of the inside local host addresses?

_____ = _____

The inside global address is assigned by? _____

The inside local address is assigned by? _____

Step 14: Verify NAT statistics

To view the NAT statistics type the **show ip nat statistics** command at the privileged EXEC mode prompt.

How many active translations have taken place? _____

How many addresses are in the pool? _____

How many addresses have been allocated so far? _____

Step 15: Reflection

Why would NAT be used in a network? _____

_____

_____

_____