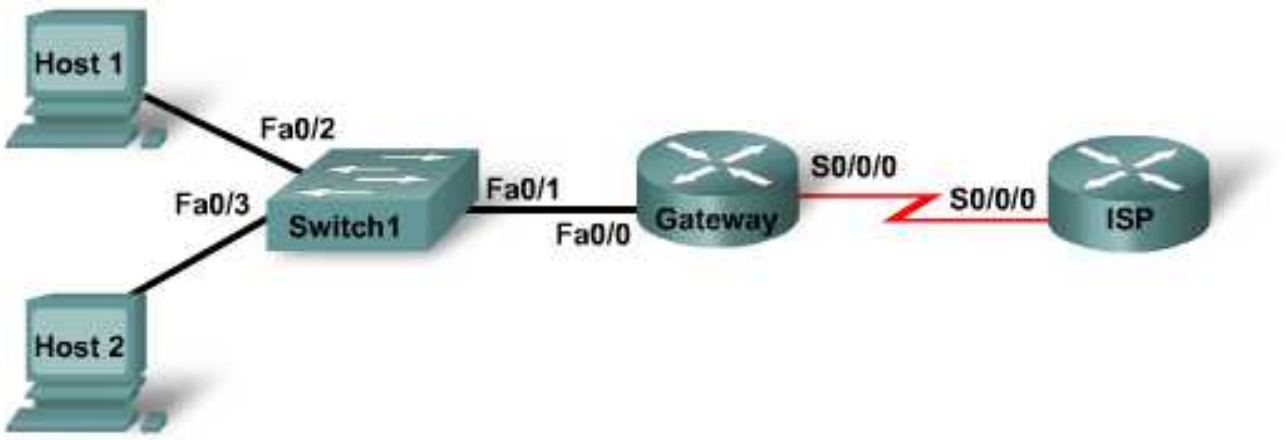
Lab 4.4.4.3 Configuring and Verifying PAT



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

Objectives

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

Background / Preparation

An ISP has allocated to a company a single IP address, 209.165.201.33, to be used on the Internet connection from the company gateway router to the ISP. 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.

In this lab, you will configure the gateway router to use 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.

The following resources are required:

- One Cisco 2960 switch or other comparable switch
- Two routers, each with a serial connection and one Ethernet interface to connect to the switch
- Two Windows-based PCs, one with a terminal emulation program, and both set up as hosts
- 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 the 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 ports 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

Configure each host with the proper IP address, subnet mask, and default gateway. Both hosts should receive IP addresses in the 10.10.10.0/24 network. The default gateway should be the FastEthernet interface IP address of the Gateway router.

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.

Predict: If you attempted to ping the loopback IP address on ISP, would the ping be successful? Explain your answer.

_____

_____

Step 7: 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
```

b. View the routing table on the Gateway router to verify the default route.

Is the static route in the routing table? _____

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

Was the ping successful? _____

Why? _____

Step 8: 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 209.165.201.33 209.165.201.33
netmask 255.255.255.252
```

Step 9: 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 10: 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 overload
```

Step 11: 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 12: Generate traffic from Gateway to the ISP

From Host 1 PC, ping 172.16.1.1. Open multiple DOS windows on each workstation and Telnet to the 172.16.1.1 address.

Step 13: Verify that NAT/PAT is working

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

How many active translations have taken place? _____

How many addresses are in the pool? _____

How many addresses have been allocated so far? _____

b. When successful, look at the NAT translation on the Gateway router, using the command **show ip nat translations**.

```
Gateway#show ip nat translations
Pro  Inside global      Inside local     Outside local     Outside global
icmp 209.165.201.33:2   10.10.10.10:2    172.16.1.1:2      172.16.1.1:2
icmp 209.165.201.33:3   10.10.10.10:3    172.16.1.1:3      172.16.1.1:3
icmp 209.165.201.33:4   10.10.10.10:4    172.16.1.1:4      172.16.1.1:4
icmp 209.165.201.33:5   10.10.10.10:5    172.16.1.1:5      172.16.1.1:5
icmp 209.165.201.33:6   10.10.10.10:6    172.16.1.1:6      172.16.1.1:6
```

How can you tell that PAT is using a single IP address for all translations? _____

_____

What feature of the translation chart illustrates how PAT is able to keep each data translation separate from the others? _____

_____

Step 14: Adjust the Gateway configuration to use an alternate PAT approach

a. Clear the NAT translation table.

```
Gateway#clear ip nat translation *
```

b. Remove the command that created a NAT pool.

```
Gateway(config)#no ip nat pool public_access 209.165.201.33
209.165.201.33 netmask 255.255.255.252
```

c. Remove the command that associated the pool with your ACL.

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

d. Enter a command that associates the source list with the outside interface.

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

e. Verify that this alternate approach works by generating traffic from the hosts to the loopback, and then by using the **show ip nat statistics** and **show ip nat translations** commands. Results should be similar to those achieved using the NAT pool.

Step 15: Reflection

What advantages does PAT provide? _____

_____