Configuring Network Address Translation (NAT)

Objective
Configure a router to use Network Address Translation (NAT) to convert internal IP addresses, typically private addresses, into outside public addresses.
Configure static IP mapping to allow outside access to an internal PC.

Theory
The two most compelling problems facing the IP Internet are IP address depletion and scaling in routing. Network Address Translation (NAT) takes advantage of the fact that a very small percentage of hosts in a stub domain are communicating outside of the domain at any given time. (A stub domain is a domain, such as a corporate network, that only handles traffic originated or destined to hosts in the domain). Indeed, many (if not most) hosts never communicate outside of their stub domain. Because of this, only a subset of the IP addresses inside a stub domain, need be translated into IP addresses that are globally unique when outside communications is required. The huge advantage of this approach is that it can be installed incrementally, without changes to either hosts or routers.
NAT's basic operation is as follows. The addresses inside a stub domain can be reused by any other stub domain. For instance, a single Class A address could be used by many stub domains. At the exit point between a stub domain and backbone, NAT is installed. For instance, consider a case where both stubs A and B internally use class A address 10.0.0.0. Stub A's NAT is assigned the class C address 198.76.29.0, and Stub B's NAT is assigned the class C address 198.76.28.0. The class C addresses are globally unique no other NAT boxes can use them.
When stub A host 10.33.96.5 wishes to send a packet to stub B host 10.81.13.22, it uses the globally unique address 198.76.28.4 as destination, and sends the packet to it's primary router. The stub router has a static route for net 198.76.0.0 so the packet is forwarded to the WAN-link. However, NAT translates the source address 10.33.96.5 of the IP header with the globally unique 198.76.29.7

Background/Preparation for the Lab exercise
An ISP has allocated a company the public classes Interdomain Routing (CIDR) IP address 199.99.9.32/27. This is equivalent to 30 public IP addresses. Since the company has an internal requirement for more than 30 addresses, the IT manager has decided to implement NAT. The addresses 199.99.9.33-199.99.9.39 for static allocation and 199.99.9.40-199.99.9.62 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 router and the ISP. The ISP connection to the Internet will be represented by a loopback address on the ISP router.
Note: Refer to the command syntax provided at the end of the lab exercise.
Equipment required for each group

If your class has 10 or less students you may work in pairs, otherwise work in groups of three.

- Two additional straight through network cables per group.
- Two serial cables per group (for console connections).
- One DTE/smart serial cable and one DCE/smart serial cable per group.
- One Cisco switch per group.
- Two Cisco routers per group.

Cable a network similar to the one in the diagram below. Please refer to the handout to correctly identify the interface identifiers to be used based on the equipment in the lab. The configuration output used in this exercise is produced from 1721 series Cisco routers. Any other router used may produce slightly different output.

<table>
<thead>
<tr>
<th>Router Designation</th>
<th>Router Name</th>
<th>FastEthernet 0 Address/subnet Mask</th>
<th>Interface Type</th>
<th>Serial Address/Subnet Mask</th>
<th>Loopback Address/Subnet Mask</th>
<th>Enable Secret</th>
<th>Enable/VTY/Console Password</th>
</tr>
</thead>
<tbody>
<tr>
<td>Router 1</td>
<td>Gateway</td>
<td>10.10.10.1/24</td>
<td>DCE</td>
<td>200.2.2.18/30</td>
<td>NA</td>
<td>class</td>
<td>cisco</td>
</tr>
<tr>
<td>Router 2</td>
<td>ISP</td>
<td>NA</td>
<td>DTE</td>
<td>200.2.2.17/30</td>
<td>172.16.1.1/32</td>
<td>class</td>
<td>cisco</td>
</tr>
</tbody>
</table>

Procedure

Start a HyperTerminal session.

Reset the routers: Erasing and reloading the router

Note: You must perform these steps on all routers in this lab exercise before continuing. Note: Please refer to the meaning and structure of the command syntax provided at the end of the exercise.

Step 1: Enter into the global configuration mode (privileged EXEC mode) by typing the following:
Router> enable

**Step 2:** At the privileged EXEC mode, enter the following command:

Router# erase startup-config

The responding prompt will be:

**Erasing the nvram filesystem will remove all files! Continue?**

[confirm]

Press **Enter** to confirm

The response should be:

**Erase of nvram: complete**

**Step 3:** Now at the privileged EXEC mode, enter the following command:

Router# reload

The responding prompt line will be:

**System configuration has been modified. Save? [yes/no]: n**

**Proceed with reload? [confirm]**

Press **Enter** to confirm

The Corresponding line prompt will be:

**Proceed with reload? [confirm]**

Press **Enter** to confirm.

In the first line of the response will be:

**Reload requested by the console.**

After the router has reloaded, the line prompt will be:

**Would you like to enter the initial configuration dialog?**

[yes/no]: n

*If you are asked...*

Would you like to terminate autoinstall? [yes]: y

The responding line prompt will be:

Press **Return** to get started!

Press **Enter**.
Now the router is ready for the assigned lab exercise to be performed.

Exercise: Configuring NAT

Step 1: Configure the routers.
Configure the routers according to the chart in handout:
  • The hostname.
  • The console.
  • The virtual terminal.
  • The enable passwords.
  • The interfaces.
If problems occur during this configuration, refer to the handout’s configuration reference information for help.

Connect the network
  • Connect the network cables.
  • Power-up the switches.
  • Reset the switches

Step 2: Save the configuration.
Enter into the global configuration mode by typing the following command:

```
Router> enable
```

At the privileged EXEC mode prompt, on both routers, type the command:

```
Router# copy running-config startup-config
```

Step 3: Configure the hosts with the proper IP address, subnet mask, and default gateway.
Each workstation must be able to ping to the attached router. If for some reason this is not the case, troubleshoot as necessary. If running Windows 2000 or higher, check using `ipconfig` in the command prompt (DOS window).

Step 4: Verify that the network is functioning.
From the attached hosts, ping the FastEthernet interface of the default gateway router.

```
Ping 10.10.10.1
```
Was the ping from the first and the second host successful? If the answer is no then you may need to troubleshoot the router and host configurations to find the error. Then ping again until they both are successful.

Step 5: Create a static route
Create a static route from the ISP to the gateway router. Addresses 199.99.9.32/27 have been allocated for Internet access outside of the company. Use the following command to create the static route:
In the Privileged mode, type the following command:

ISP# configuration t or conf t

This changes the prompt to ISP(config)#.

ISP(config)# ip route 199.99.9.32 255.255.255.224 200.2.2.18

**Step 6: Create a default route**
Add a default route from the gateway router to the ISP router. This will forward any unknown destination address traffic to the ISP.
At the gateway router, enter into the privileged mode by typing in the following command:

Gateway> enable

At the privileged mode (privileged EXEC mode), enter the following command:

Gateway# configuration t or conf t

This changes the prompt to Gateway(config)#. Type in the following command:

Gateway (Config)# ip route 0.0.0.0 0.0.0.0 200.2.2.17

**Step 7: Define a pool of usable public IP addresses**
To define the pool of public addresses, use the following command:

Gateway (config)# ip nat pool public-access 199.99.9.40 199.99.9.62 netmask 255.255.255.224

**Note:** To define a pool of IP addresses for Network Address Translation (NAT), use the ip nat pool command in global configuration mode.

This command defines a NAT pool named public-access with a range of addresses 199.99.9.40 - 199.99.9.62.

**Step 8: 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 following command:

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

**Step 9: Define the NAT translation from the inside list to outside pool**
To define the NAT translation, use the following command:
Gateway (Config)# ip nat inside source list 1 pool public-access

**Note:** To enable Network Address Translation (NAT) of the inside source address, use the **ip nat inside source** command in global configuration mode. This command does the following:
- Translates the source of IP packets that are traveling inside to outside.
- Translates the destination of the IP packets that are traveling outside to inside.

This command indicates that any packets received on the inside interface that are permitted by access-list 1 will have the source address translated to an address out of the NAT pool "public-access".

**Step 10: 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 following commands:

```
Gateway (config)# interface fastethernet 0 or inte0
```

This changes the prompt to: **Gateway (config-if)#**

At the prompt, type the following command:

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

IP NAT Inside/Outside: Designates the inside and outside interfaces; traffic originating from or destined for the interface is examined by the NAT. The fast Ethernet represents the inside interface whereas the serial interface represents the outside interface.

**Step 11: Testing the configuration**
Configure a workstation on the internal LAN with the IP address 10.10.10.10/24 and a default gateway 10.10.10.1. From the PC, ping 172.16.1.1. If successful, look at the NAT translation on the gateway router, using the following command:

```
Gateway (config-if)# Show ip nat translations
```

**Note:** This command is used to display active Network Address Translation (NAT) translations

Optionally the following command can be issued:

```
Gateway (config-if)# Show ip nat translations verbose
```

**Verbose:** Displays additional information for each translation table entry, including how long ago the entry was created and used.
Observation
What is the translation of the inside local host address?

Step 11: Configuring static mapping
Workstation 10.10.10.10/24 will be designated as the public WWW server. Thus it needs a permanent public IP address. This mapping is defined using a static NAT mapping.

Configure one of the PCs on the LAN with the IP address 10.10.10.10/24 and a default gateway 10.10.10.1. To configure a static IP NAT mapping, use the following command at the privileged EXEC mode prompt:

```
Gateway (Config)# ip nat inside source static 10.10.10.10 199.99.9.33
```

This permanently maps 199.99.9.33 to the inside address 10.10.10.10.

Step 12: Look at the translation table.

```
Gateway (config-if)# show ip nat translations
```

Does the mapping show up in the output of the `show` command?

Step 13: Testing the Configuration
From the 10.10.10.10 workstation, verify it can ping 172.16.1.1
From the ISP router ping the host with the static NAT translation, by typing `PING 10.10.10.10`
From the ISP router, ping 199.99.9.33. If successful, look at the NAT translation on the Gateway router, using the command:

```
Gateway (config-if)# show ip nat translations
```
Command Syntax

**ip nat inside source**

To enable Network Address Translation (NAT) of the inside source address, use the `ip nat inside source` command in global configuration mode. To remove the static translation or remove the dynamic association to a pool, use the `no` form of this command.

```
ip nat inside source {list {access-list-number | access-list-name} | route-map name} {interface type number | pool name} [mapping-id map-name | vrf name] [overload]
```

**ip nat pool**

To define a pool of IP addresses for Network Address Translation (NAT), use the `ip nat pool` command in global configuration mode. To remove one or more addresses from the pool, use the `no` form of this command.

```
ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length}[type rotary]
```

```
o ip nat pool name start-ip end-ip {netmask netmask | prefix-length prefix-length} [type rotary]
```

**Syntax Description**

<table>
<thead>
<tr>
<th><strong>name</strong></th>
<th>Name of the pool.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>start-ip</strong></td>
<td>Starting IP address that defines the range of addresses in the address pool.</td>
</tr>
<tr>
<td><strong>end-ip</strong></td>
<td>Ending IP address that defines the range of addresses in the address pool.</td>
</tr>
<tr>
<td><strong>netmask</strong></td>
<td>Network mask that indicates which address bits belong to the network and subnetwork fields and which bits belong to the host field. Specify the netmask of the network to which the pool addresses belong.</td>
</tr>
<tr>
<td><strong>prefix-length</strong></td>
<td>Number that indicates how many bits of the netmask are ones (how many bits of the address indicate network). Specify the netmask of the network to which the pool addresses belong.</td>
</tr>
<tr>
<td><strong>type rotary</strong></td>
<td>(Optional) Indicates that the range of address in the address pool identify real, inside hosts among which TCP load distribution will occur.</td>
</tr>
</tbody>
</table>