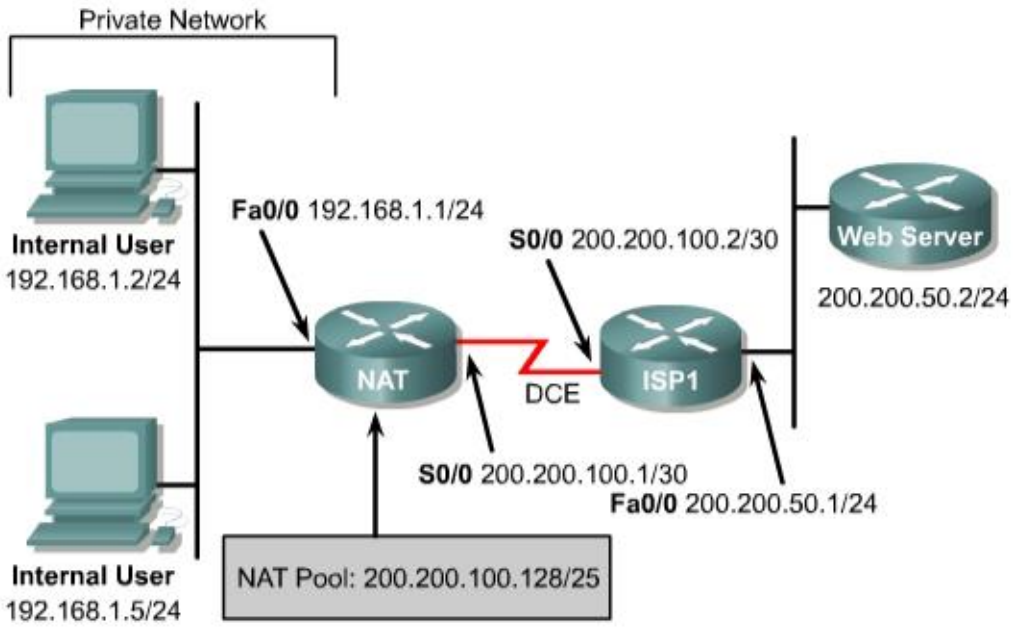
Lab – 4.1

Network Address Translation – Static NAT and Dynamic NAT



Objective

In this lab, static Network Address Translation (NAT) and dynamic NAT are configured.

Scenario

The network needs approximately 100 private IP addresses translated in a one-to-one fashion with a pool of public IP addresses. To do this, network will use NAT translation with a portion of its class C address space allocated by ISP1.

Step 1

Build and configure the network according to the diagram.

Use **`ping`** to test connectivity between the NAT and ISP1 routers, between the workstations and the default gateway, and between WebServer and ISP1.

Step 2

Since no routing protocol will be enabled, configure a default route to the Internet on the NAT router:

```
NAT(config)#ip route 0.0.0.0 0.0.0.0 200.200.100.2
```

ISP1 needs to be able to reach hosts on the 192.168.0/24 network. But these hosts will have their IP addresses translated to public IP addresses in the 200.200.100.128/25 network, so a static route to the 200.200.100.128/25 network is required:

```
ISP1(config)#ip route 200.200.100.128 255.255.255.128 200.200.100.1
```

Step 3

Create a standard Access Control List that defines all Internal Users:

```
NAT(config)#access-list 1 permit 192.168.1.0 0.0.0.255
```

Step 4

In this step, configure private and public address spaces to be used for NAT and configure the translation:

The public address space 200.200.100.128/25 will be used as a pool to provide NAT translation for the private IP addresses. To statically map the Internal User with IP address 192.168.1.2 pictured in the diagram, enter the following command

```
NAT(config)#ip nat inside source static 192.168.1.2 200.200.100.252
```

This static mapping has the advantage of allowing “external” users to always access the host 192.168.1.2 by way of the fixed IP address 200.200.100.252 (in addition to letting the 192.168.1.2 Internal User access the Internet). On the down side, this external accessibility is also viewed as a security vulnerability. To allow the other hosts on the internal (private) network to reach the Internet, translations will need to be made for those hosts as well. A list of static translations could be made one by one, but a simpler alternative is to configure a pool of addresses and let the router make one-to-one dynamic NAT translations for these hosts. For example, to map the non-statically mapped hosts in the 192.168.1.0/24 network to public IP addresses in the range 200.200.100.129 to200.200.100.250, proceed as follows:

```
NAT(config)#ip nat pool public 200.200.100.129 200.200.100.250
netmask 255.255.255.128
NAT(config)#ip nat inside source list 1 pool public
```

This provides a dynamic one-to-one NAT translation between public IP addresses in the “public” pool and private IP addresses specified by access list 1. The Internal Users IP addresses are configured independently of the NAT translation. Dynamic NAT translations are made for any internal hosts for which no static translation has been defined. The configuration above reserves IP addresses 200.200.100.251 to 200.200.100.254 for use in further static NAT mappings. Static translations are often used with an internal server to enable external access to it by way of a fixed external IP.

> **Note:** If there are more than 128 active hosts on the private network, static NAT translation and/or dynamic one-to-one NAT translations will prevent more than 128 hosts from accessing the Internet. For these additional hosts to get on the Internet, “NAT overloading” must be configured (see Lab 2.10.4b).

Step 5

Now, designate the inside NAT interface and the outside NAT interface. In more complex topologies, it is possible to have more than one inside NAT interface.

```
NAT(config)#interface fastethernet 0/0
NAT(config-if)#ip nat inside

NAT(config-if)#interface serial 0/0
NAT(config-if)#ip nat outside
```

There are several **show** commands that can be used to see if NAT is working: **show ip nat translations**, **show ip nat statistics**, and **show ip nat translations verbose.**

From the two Internal User workstations, ping WebServer (200.200.50.2). Then check that WebServer is accessible by connecting from an Internal User workstation using a browser with the WebServer IP address, 200.200.50.2. Issue the three NAT show commands listed above on the NAT router. Sample outputs are shown below.

```
NAT#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 200.200.100.129    192.168.1.5        ---                ---
--- 200.200.100.252    192.168.1.2        ---                ---
```

```
NAT#show ip nat statistics
Total active translations: 2 (1 static, 1 dynamic; 0 extended)
Outside interfaces:
  Serial0/0
Inside interfaces:
  FastEthernet0/0
Hits: 131  Misses: 9
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 2] access-list 1 pool public refcount 1
 pool public: netmask 255.255.255.128
        start 200.200.100.129 end 200.200.100.250
        type generic, total addresses 122, allocated 1 (0%), misses 0
```

```
NAT#show ip nat translations verbose
Pro Inside global      Inside local       Outside local      Outside global
--- 200.200.100.129    192.168.1.5        ---                ---
    create 00:02:55, use 00:02:55, left 23:57:04, Map-Id(In): 2,
    flags:
none, use count: 0
--- 200.200.100.252    192.168.1.2        ---                ---
    create 00:40:36, use 00:02:59,
    flags:
static, use_count: 0
```

Notice that the Internal User with IP address 192.168.1.5 had its address dynamically translated to 200.200.100.129, the first available address in the "public" pool. The command **clear ip nat translation *** can be used to clear all dynamic NAT translations:

```
NAT#clear ip nat translation *
NAT#show ip nat translations
Pro Inside global      Inside local       Outside local      Outside global
--- 200.200.100.252    192.168.1.2        ---                ---
```

Save the configurations for NAT and ISP1.