**Discovery 14: Implement NAT**

Implement NATEnterprise/CCNP/Enterprise\_Core/ENCOR/v1.0/ELT\_VIDEOS/ENCOR10\_11-6\_Implement-NAT\_001.mp43Play Transcript ID4438094template\_version4.1.1Enterprise/CCNP/Enterprise\_Core/ENCOR/v1.0/ELT\_VIDEOS/ENCOR10\_11-6\_Implement-NAT\_001.vtt

**Task 1: Configure Static NAT**

**Activity**

Configuring static NAT is a simple process. You have to define inside and outside interfaces using ip nat inside and ip nat outside interface configuration commands, and specify which inside address should be translated to which outside address using the ip nat inside source static inside\_address outside\_address global configuration command.

Configure static NAT translation between inside local address and an inside global address

router(config)# ip nat inside source static local-ip global-ip

Configure the interface as the inside NAT interface.

router(config-if)# ip nat inside

Configure the interface as the outside NAT interface.

router(config-if)# ip nat outside

In this task, SRV1 with a private IP address of 10.10.2.20/24 will represent a public server in the DMZ. You will use static NAT as a means for SRV1 to be accessible from the Internet.

**Step 1:** While R1 does have access to the public IP address space, systems within the private IP address space of the topology do not. Verify this fact. One at a time, access the consoles of R1 and SRV1 and attempt to ping SRV2 at 203.0.113.30. The pings should be successful from R1, but unsuccessful from SRV1.

On R1, enter the following command:

|  |  |
| --- | --- |
| R1# ping 203.0.113.30    When pinging from R1, the source address is a publicly accessible address of 198.51.100.2.  On SRV1, enter the following command:   |  | | --- | | SRV1# ping 203.0.113.30 | |

Because NAT has not been configured, the Internet router R2 is receiving IP packets from the private IP address of SRV1 (10.10.2.20) and dropping the packets. Routers on the Internet are not aware of the private IP address space within the networks that connect to the Internet.

**Step 2:** Configure R1 interfaces for static NAT. GigabitEthernet0/1 is on the inside, and GigabitEthernet0/3 is on the outside.

|  |
| --- |
| R1# conf t  Enter configuration commands, one per line. End with CNTL/Z.  R1(config)# int g0/1  R1(config-if)# ip nat inside    R1(config-if)# int g0/3  R1(config-if)# ip nat outside  R1(config-if)# exit |

**Step 3:** Add a static NAT configuration entry that translates the SRV1 IP address (10.10.2.20) to 198.51.100.20, then leave configuration mode.

On R1, enter the following command:

|  |
| --- |
| R1(config)# ip nat inside source static 10.10.2.20 198.51.100.20  R1(config)# end  R1# |
|  |

**Step 4:** Display the NAT translation table on R1.

On R1, enter the following command:

R1# show ip nat translations

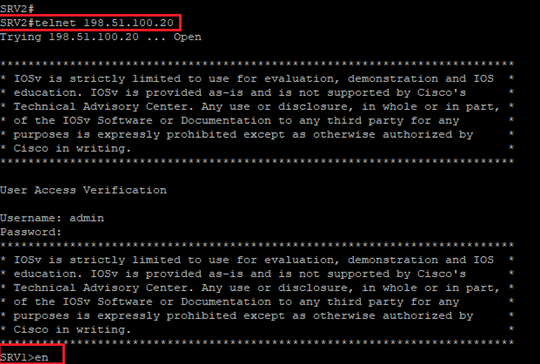


Static translations continuously remain in the translation table, regardless of their use.

**Step 5:** Access the console of SRV2 and establish a Telnet session to SRV1’s inside global address of 198.51.100.20 as if an Internet user was accessing the internal server SRV1 in the DMZ. Use the username of **admin** and password of **root@123**.

On SRV2, enter the following command:

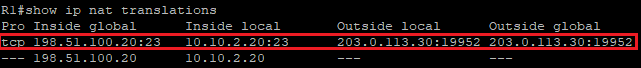
SRV2# telnet 198.51.100.20



**Step 6:** Return to the console of R1 and display the translation table while the session from SRV2 to SRV1 is open.

On R1, enter the following command:

R1# show ip nat translations

****

**Note**

The source port numbers of the outside local and outside global entries in your lab will not match those in this example.

This example shows two entries in the translation table:

* The first entry is an extended entry because it embodies more details than just an IP address that is mapping to an IP address. In this case, it specifies the protocol (TCP) and also the ports in use on both systems. The extended entry is due to the use of the static translation for the Telnet session from SRV1 to SRV2. It details the characteristics of that session.
* The second entry is a simple entry; it maps one IP address to another. The simple entry is the persistent entry that is associated with the configured static translation.

**Step 7:** Access the console of SRV2 and terminate the Telnet session to SRV1.

On SRV2, enter the following command:

SRV1> exit

****

**Task 2: Configure Dynamic NAT**

**Activity**

Dynamic NAT configuration differs from static NAT, but it also has some similarities. Like static NAT, it requires the configuration to identify each interface as an inside or outside interface. However, rather than creating a static map to a single IP address, a pool of inside global addresses is used, and an ACL that identifies which inside local addresses are to be translated. The ACL-to-NAT pool mapping is defined by the ip nat inside source list acl pool pool\_name global configuration command.

Configure the dynamic NAT address pool.

router(config)# ip nat pool pool-name start-ip end-ip {netmask netmask | prefix-length prefix-length}

Configure a static access list to define the addresses to be translated.

router(config)# access-list access-list-number permit source [source-wildcard]

Configure the dynamic NAT translation. The overload keyword enables the use of PAT.

router(config)# ip nat inside source list access-list-number pool pool-name [overload]

Configure the interface as the inside NAT interface.

router(config-if)# ip nat inside

Configure the interface as the outside NAT interface.

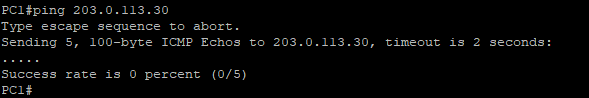
router(config-if)# ip nat outside

In this task, PC1 and PC2 have addresses in the private subnet of 10.10.1.0/24. You will use dynamic NAT as a means for these hosts to communicate with the Internet.

**Step 1:** While R1 does have access to the public IP address space, systems within the private IP address space of the topology do not. Verify this fact. Access the console of PC1 and attempt to ping SRV2 at 203.0.113.30. This process should fail.

On PC1, enter the following command:

PC1# ping 203.0.113.30



Because NAT has not been configured, the Internet router R2 is receiving IP packets from the private IP address of PC1 (10.10.1.10) and dropping the packets. Routers on the Internet are not aware of the private IP address space within the networks that connect to the Internet.

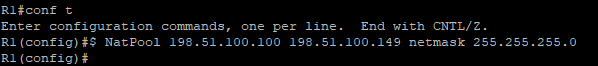
**Step 2:** On R1, define a pool of outside global addresses named "NatPool" by specifying the address range from 198.51.100.100 to 198.51.100.149.

On R1, enter the following command:

R1# conf t

Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# ip nat pool NatPool 198.51.100.100 198.51.100.149 netmask 255.255.255.0

****

**Step 3:** Configure access list number 10 to identify addresses within the 10.10.1.0/24 subnet as addresses eligible to be translated.

On R1, enter the following command:

R1(config)# access-list 10 permit 10.10.1.0 0.0.0.255

****

**Step 4:** Configure the R1 GigabitEthernet0/0 interface as a NAT inside interface.

On R1, enter the following commands:

R1(config)# int g0/0

R1(config-if)# ip nat inside

R1(config-if)# exit

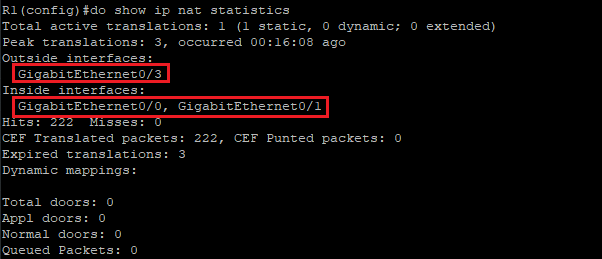
****

**Step 5:** The R1 GigabitEthernet0/3 interface would be required to be configured as a NAT outside interface, but this was already completed in the previous task.

Verify that the R1 GigabitEthernet0/3 interface is still configured as the NAT outside interface by using the command show ip nat statistics.

On R1, enter the following command:

R1(config)# do show ip nat statistics



**Step 6:** Define a dynamic translation rule that specifies access list 10 as the source and that uses addresses from the pool NatPool.

On R1, enter the following commands:

R1(config)# ip nat inside source list 10 pool NatPool

R1(config)# end

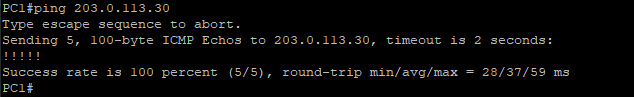
R1#

****

**Step 7:** Verify that there is now bidirectional connectivity between PC1 and SRV2. Access the console of PC1 and send a ping to SRV2.

On PC1, enter the following command:

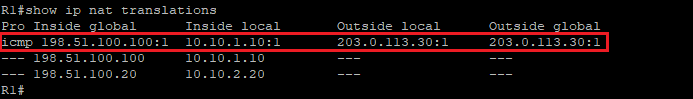
PC1# ping 203.0.113.30



**Step 8:** Access the console of R1 and view the current translation table.

On R1, enter the following command:

R1# show ip nat translations



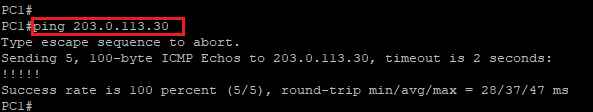
If you proceeded quickly enough, three translations will be in the table.

* The extended translation that is associated with the ICMP session is short-lived and may have timed out. If it did, you can resend the ping from PC1 and display the translation table again. However, if this were a dynamic TCP translation that was assigned from a NAT pool, it would have a 24-hour inactivity timeout.
* There is a simple entry in the table that is associated with the assignment of an address from the pool to PC1.
* The third entry that is translating 10.10.2.20 to 198.51.100.20 is the static entry from the previous task.

**Step 9:** One at a time, access the consoles of PC1 and PC2, and send a ping to SRV2.

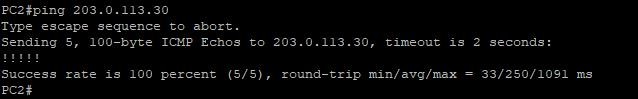
On PC1, enter the following command:

PC1# ping 203.0.113.30



On PC2, enter the following command:

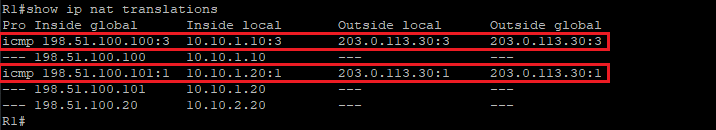
PC2# ping 203.0.113.30



**Step 10:** Return to the console of R1 and view the translation table.

On R1, enter the following command:

R1# show ip nat translations



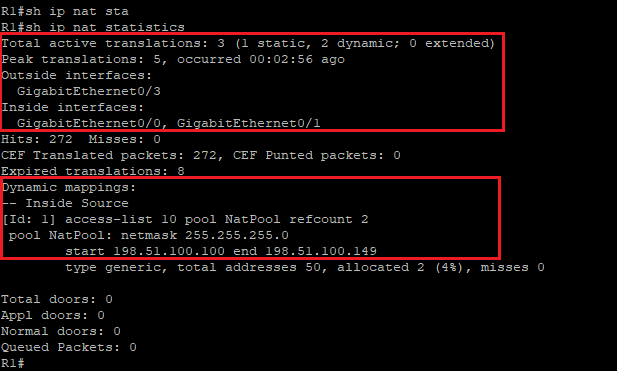
The extended ICMP entries that are associated with the ping activity are short-lived. You can always try to resend the pings and redisplay the translation table.

PC1 (10.10.1.10) and PC2 (10.10.1.20) have been assigned IP addresses from the NAT pool. In this example, the addresses assigned were 198.151.100.100 and 198.151.100.101.

**Step 11:** Display the translation statistics on R1.

On R1, enter the following command:

R1# sh ip nat statistics



The statistics that are displayed in the lab environment will likely differ from the example. But, in any case, statistics include the status such as the current active translation count, historical statistics such as the largest number of translations that are seen on R1, and configuration information such as the details of the NAT pools.

**Step 12:** Return to the console of R1 and clear all dynamic translations from the translation table.

On R1, enter the following command:

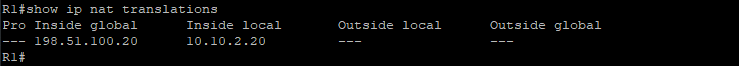
R1# clear ip nat translation \*

****

**Step 13:** Display the translation table, verifying the removal of the dynamic entries.

On R1, enter the following command:

R1# show ip nat translation



The dynamic entries have been removed, but the statically configured entry for SRV1 remains.

**Task 3: Configure PAT**

**Activity**

To configure PAT, identify inside and outside interfaces by using the ip nat inside and ip nat outside interface configuration commands, respectively. An ACL must be configured that will match all inside local addresses that need to be translated, and NAT will need to be configured so that all inside local addresses are translated to the address of the outside interface. This solution is achieved by using the ip nat inside source list acl interface interface overload global configuration command.

Configure a static access list to define the addresses to be translated.

router(config)# access-list access-list-number permit source [source-wildcard]

Configure PAT.

router(config)# ip nat inside source list access-list-number interface interface overload

Configure the interface as the inside NAT interface.

router(config-if)# ip nat inside

Configure the interface as the outside NAT interface.

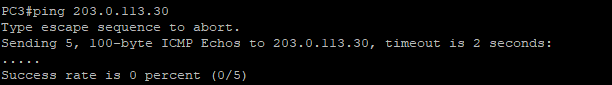
router(config-if)# ip nat outside

In this task, PC3 and PC4 have addresses in the private subnet of 10.10.3.0/24. You will use PAT as a means for these hosts to communicate with the Internet.

**Step 1:** While R1 does have access to the public IP address space, systems within the private IP address space of the topology do not. Verify this fact. Access the console of PC3 and attempt to ping SRV2. This process should fail.

On PC3, enter the following command:

PC3# ping 203.0.113.30



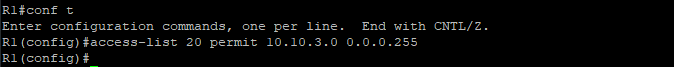
Because NAT has not been configured, the Internet router R2 is receiving IP packets from the private IP address of PC3 (10.10.3.10) and dropping the packets. Routers on the Internet are not aware of the private IP address space within the networks that connect to the Internet.

**Step 2:** Configure access list number 20 to identify addresses within the 10.10.3.0/24 subnet as addresses eligible to be translated.

On R1, enter the following command:

R1# conf t Enter configuration commands, one per line. End with CNTL/Z.

R1(config)# access-list 20 permit 10.10.3.0 0.0.0.255

****

**Step 3:** Configure the R1 GigabitEthernet0/2 interface as a NAT inside interface.

On R1, enter the following commands:

R1(config)# int g0/2

R1(config-if)# ip nat inside

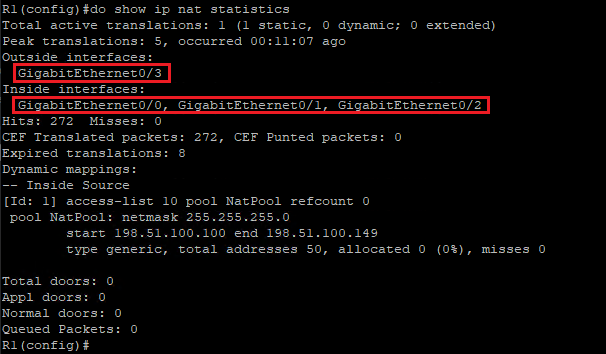
R1(config-if)# exit

****

**Step 4:** Verify that the R1 GigabitEthernet0/3 interface is still configured as the NAT outside interface by using the command, show ip nat statistics.

On R1, enter the following command:

R1(config)# do show ip nat statistics



**Step 5:** Add a NAT statement that enables PAT by translating the addresses that are permitted by access list 20 into the IP address that is assigned to the interface GigabitEthernet0/3.

On R1, enter the following commands:

R1(config)# ip nat inside source list 20 interface g0/3 overload

R1(config)# end

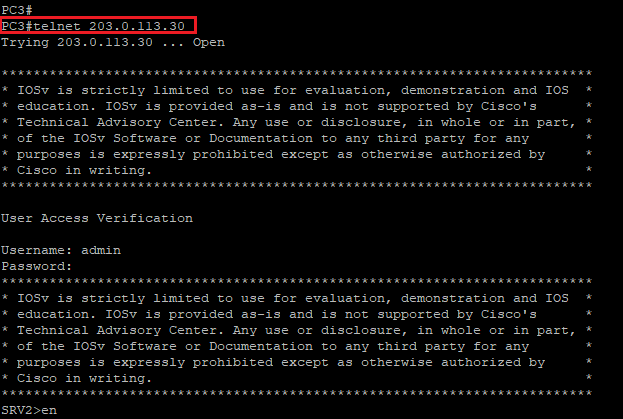
R1#

****

**Step 6:** Verify that there is now bidirectional connectivity between PC3 and SRV2. Access the console of PC3 and telnet to SRV2. Enter the username **admin** with the password **root@123**.

On PC3, enter the following command:

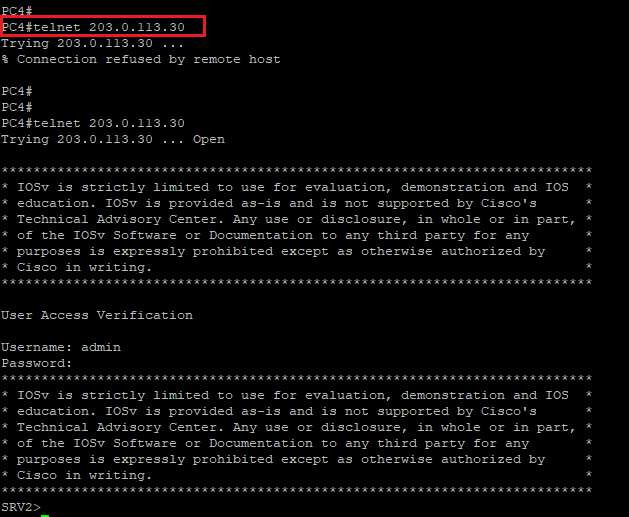
PC3# telnet 203.0.113.30



**Step 7:** Verify that there is now bidirectional connectivity between PC4 and SRV2. Access the console of PC4 and telnet to SRV2. Enter the username admin with the password Cisco123.

On PC4, enter the following command:

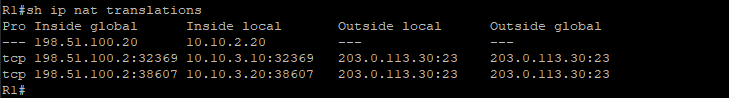
PC4# telnet 203.0.113.30



**Step 8:** Leaving both connections to SRV2 running, access the console of R1. Display the translation table on R1.

On R1, enter the following command:

R1# show ip nat translations



R1 is using the inside source port to uniquely identify the two translation sessions. The source ports are dynamically generated so the ports that are shown in the example will not match those ports that you see in the lab environment.

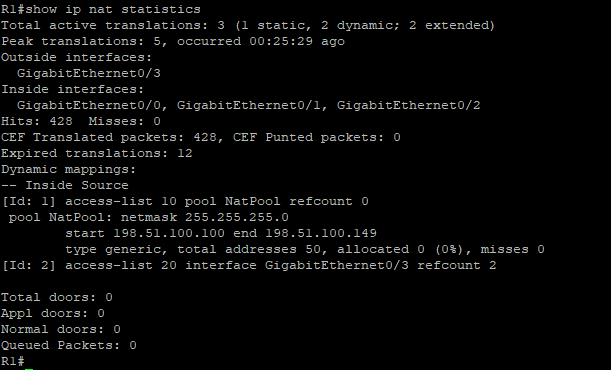
In this example, when R1 receives a packet from SRV2 (203.0.113.30) with a source port of 23 that is destined for 198.51.100.2 and a destination port of 21299, R1 knows to translate the destination address to 10.10.3.10 and forward the packet to PC3.

On the other hand, if the destination port of a similar inbound packet is 34023, R1 will translate the destination address to 10.10.3.20 and forward the packet to PC4.

**Step 9:** Display the translation statistics on R1.

On R1, enter the following command:

R1# show ip nat statistics



The statistics that are displayed in the lab environment will likely differ from the example. But, in any case, statistics include the status such as the current active translation count, historical statistics such as the largest number of translations that are seen on R1, and configuration information such as the details of the NAT pools.

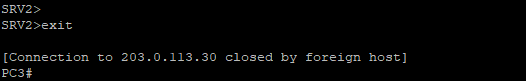
**Step 10:** One at a time, access the consoles of PC3 and PC4. Terminate their Telnet sessions to SRV2.

Terminate the PC3 Telnet session to SRV2:

SRV2> exit

[Connection to 203.0.113.30 closed by foreign host]

PC3#

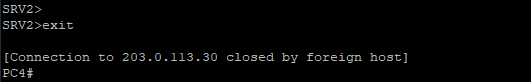


Terminate the PC4 Telnet session to SRV2:

SRV2> exit

[Connection to 203.0.113.30 closed by foreign host]

PC4#



**Step 11:** Return to the console of R1 and clear all dynamic translations from the translation table.

On R1, enter the following command:

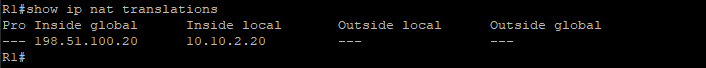
R1# clear ip nat translation \*

****

**Step 12:** Display the translation table, verifying the removal of the dynamic entries.

On R1, enter the following command:

R1# show ip nat translation



The dynamic entries have been removed, but the statically configured entry for SRV1 remains.