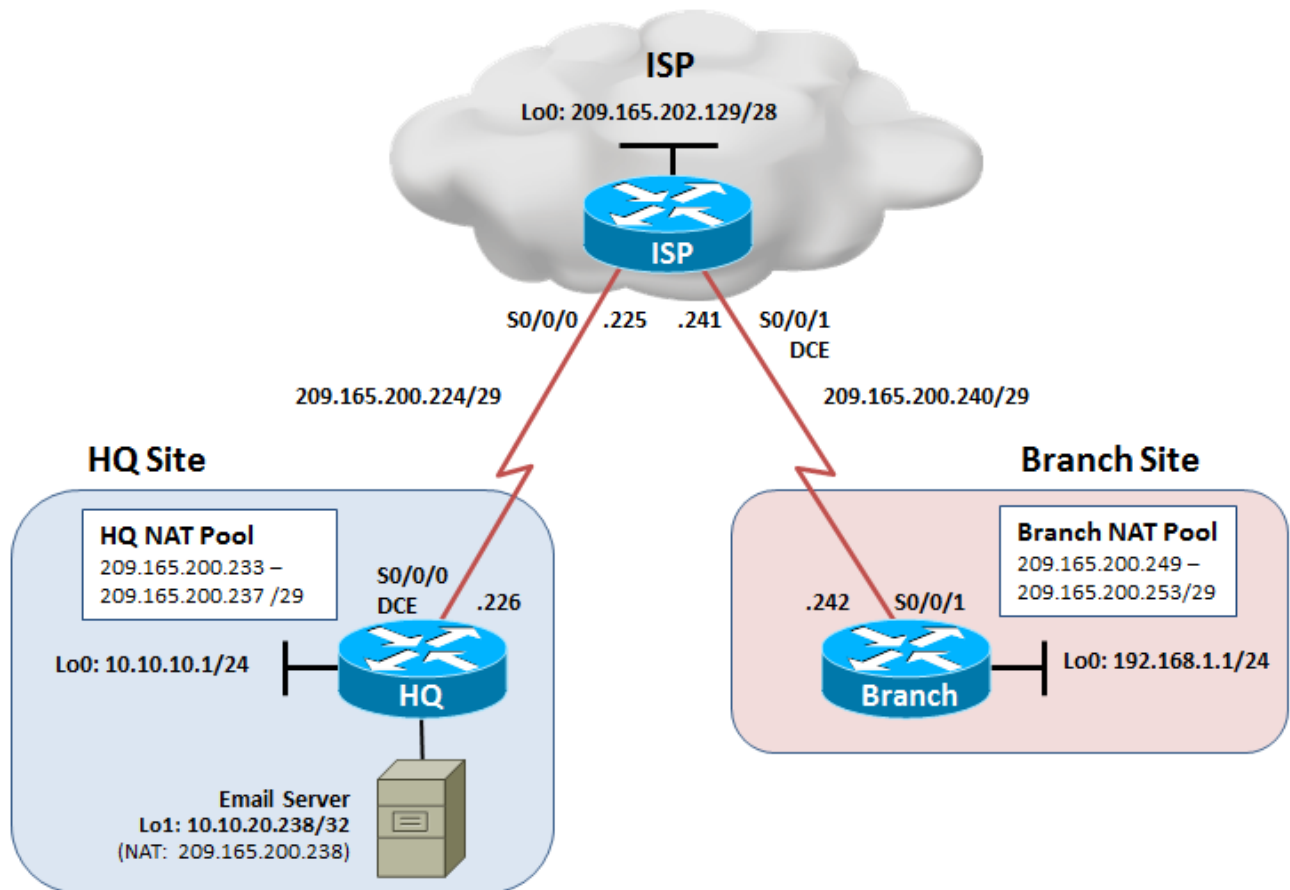


CCNPv7 ROUTE

Chapter 6 Lab 6-1, Configure NAT Services

Instructor Version

Topology



Objectives

- Configure dynamic NAT and static NAT on the HQ router.
- Configure dynamic NAT on the Branch router.
- Verify the configuration and operation using **show** commands.

Background

The HQ and Branch sites must be configured to support NAT. Specifically, the HQ and Branch routers will be configured to provide inside LAN users with outside public addresses using NAT. The HQ router will also provide static NAT to access the Email server from the outside network.

Note: This lab uses Cisco 1941 routers with Cisco IOS Release 15.2 with IP Base. Depending on the router or switch model and Cisco IOS Software version, the commands available and output produced might vary from what is shown in this lab.

Required Resources

- 3 routers (Cisco IOS Release 15.2 or comparable)
- Serial and Ethernet cables

Step 1: Configure loopbacks and assign addresses.

Cable the network as shown in the topology diagram. Erase the startup configuration and reload each router to clear previous configurations. Using the addressing scheme in the diagram, apply the IP addresses to the interfaces on the HQ, ISP, and Branch routers.

You can copy and paste the following configurations into your routers to begin.

Note: Depending on the router model, interfaces might be numbered differently than those listed. You might need to alter the designations accordingly.

HQ (R1)

```
hostname HQ
!
interface Loopback0
  description Headquarters LAN
  ip address 10.10.10.1 255.255.255.0
exit
!
interface Loopback1
  description Simulates the Email Server
  ip address 10.10.20.238 255.255.255.255
exit
!
interface Serial0/0/0
  description Connection to ISP
  ip address 209.165.200.226 255.255.255.248
  clock rate 128000
  no shut
exit
!
end
```

ISP (R2)

```
hostname ISP
!
interface Loopback0
  description Simulating the Internet
  ip address 209.165.202.129 255.255.255.240
exit
```

```

!
interface Serial0/0/0
  description Connection to HQ
  ip address 209.165.200.225 255.255.255.248
  no shut
exit
!
interface Serial0/0/1
  description Connection to Branch
  ip address 209.165.200.241 255.255.255.248
  clock rate 128000
  no shut
exit
!
ip route 209.165.200.232 255.255.255.248 Serial0/0/0
ip route 209.165.200.248 255.255.255.248 Serial0/0/1
!
end

```

Branch (R3)

```

hostname Branch
!
interface Loopback0
  description Branch LAN
  ip address 192.168.1.1 255.255.255.0
exit
!
interface Serial0/0/1
  description Connection to ISP
  ip address 209.165.200.242 255.255.255.248
  no shut
exit
!
end

```

- a. Verify your configuration by using the **show ip interface brief** and the **show interfaces description** command. The output from the Branch router is shown here as an example.

```

Branch# show ip interface brief | include up
Serial0/0/1          209.165.200.242 YES manual up      up
Loopback0           192.168.1.1     YES manual up      up
Branch#
Branch# show interfaces description | include up
Se0/0/1             up              up          Connection to ISP
Lo0                  up              up          Branch LAN
Branch#

```

- b. From the Branch router, run the following Tcl script to verify connectivity.

```

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
} { ping $address }

```

```
Branch# tclsh
```

```

Branch(tcl)# foreach address {
+>209.165.200.241
+>209.165.202.129
+>209.165.200.226
+>} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
Branch(tcl)#

```

Why do the pings to the ISPs loopback and HQ router address fail?

The ping fails because the Branch and HQ routers require a default route to ISP.

Step 2: Configure default static routes on Branch and HQ.

- a. On HQ, configure a default static route to ISP.

```
HQ(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.225
```

- b. On the Branch router, configure a default static route to ISP.

You can copy and paste the following configurations into your routers.

```
Branch(config)# ip route 0.0.0.0 0.0.0.0 209.165.200.241
```

- c. From the Branch router, run the following Tcl script to verify connectivity.

```

foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
+>} { ping $address}

Branch# tclsh
Branch(tcl)# foreach address {
+>209.165.200.241
+>209.165.202.129
+>209.165.200.226
+>} { ping $address }
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms

```

Type escape sequence to abort.
 Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
 !!!!!
 Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
 Branch(tcl)#

Are the pings now successful?

Yes. If not, troubleshoot.

- d. Connectivity from the Branch router to external addresses has been established. But could a Branch LAN user successfully reach those external addresses? To verify, initiate pings sourced from the Branch LAN interface to the ISP interface, the ISPs loopback interface, and the HQ Internet interface. Run the following Tcl script on the Branch router to verify connectivity.

```
foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
} { ping $address source 192.168.1.1}
```

```
Branch# tclsh
Branch(tcl)# foreach address {
+>209.165.200.241
+>209.165.202.129
+>209.165.200.226
+>} { ping $address source 192.168.1.1}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
.....
Success rate is 0 percent (0/5)
Branch(tcl)#
```

Note: You can also specify the router interface designator (for example, S0/0/0, Fa0/0, or Lo1) as the source for the extended ping, as follows:

```
Branch# ping 209.165.200.226 source Lo1
```

Why are the pings unsuccessful?

The pings fail because the source 192.168.1.1 IP address is an internal private address, and the ISP is unaware of this address.

The ISP cannot route back to the internal private address of the Branch LAN.

Step 3: Configure NAT on the HQ router.

The HQ and Branch internal LANs will be translated to global public IP addresses using NAT when exiting the corporate network.

The ISP has allocated the **209.165.200.233 – 209.165.200.238 (209.165.200.232/29)** pool of public addresses to the HQ site.

The HQ site also has an email server that must be accessible to mobile users and Branch office users. Therefore, static NAT must also be configured to use a public address to reach the email server.

- a. On the HQ router, create an extended NAT ACL that matches the 10.10.10.0/24 LAN.

```
HQ(config)# ip access-list extended HQ-NAT-ACL
HQ(config-ext-nacl)# remark Permit Local LAN to use NAT
HQ(config-ext-nacl)# permit ip 10.10.10.0 0.0.0.255 any
HQ(config-ext-nacl)# exit
HQ(config)#
```

- b. The NAT pool must identify addresses 209.165.200.232 /29.

```
HQ(config)# ip nat pool HQ-NAT-POOL 209.165.200.233 209.165.200.237 prefix-
length 29
HQ(config)#
```

- c. The NAT pool and the ACL must be bound together.

```
HQ(config)# ip nat inside source list HQ-NAT-ACL pool HQ-NAT-POOL
HQ(config)#
```

- d. The email server with private IP address 10.10.20.238 will be statically assigned the last public IP address from the NAT pool, 209.165.200.238. Interface loopback 0 on HQ simulates this server.

```
HQ(config)# ip nat inside source static 10.10.20.238 209.165.200.238
HQ(config)#
```

- e. The LAN interface must be identified as an inside NAT interface, and the Internet interface must be identified as an outside NAT interface.

```
HQ(config)# interface Loopback 0
HQ(config-if)# ip nat inside
HQ(config-if)# exit
HQ(config)#
HQ(config)# interface Loopback 1
HQ(config-if)# ip nat inside
HQ(config-if)# exit
HQ(config)#
HQ(config)# interface Serial0/0/0
HQ(config-if)# ip nat outside
HQ(config-if)# exit
HQ(config)#
```

Step 4: Configure NAT on the Branch router.

The ISP has allocated the **209.165.200.249 – 209.165.200.254 (209.165.200.248/29)** pool of public addresses to the Branch site.

- a. On the Branch router, create a standard NAT ACL that identifies the 192.168.1.0/24 LAN.

```
Branch(config)# ip access-list extended BRANCH-NAT-ACL
Branch(config-ext-nacl)# remark Permit Local LAN to use NAT
Branch(config-ext-nacl)# permit ip 192.168.1.0 0.0.0.255 any
Branch(config-ext-nacl)# exit
Branch(config)#
```

- b. The NAT pool must identify addresses 209.165.200.232 /29.

```
Branch(config)# ip nat pool BRANCH-NAT-POOL 209.165.200.249 209.165.200.254
prefix-length 29
Branch(config)#
```

- c. The NAT pool and the ACL must be bound together.

```
Branch(config)# ip nat inside source list BRANCH-NAT-ACL pool BRANCH-NAT-POOL
Branch(config)#
```

- d. The LAN interface must be identified as an inside NAT interface, and the Internet interface must be identified as an outside NAT interface.

```
Branch(config)# interface Loopback 0
Branch(config-if)# ip nat inside
Branch(config-if)# exit
Branch(config)#
Branch(config)# interface Serial0/0/1
Branch(config-if)# ip nat outside
Branch(config-if)# exit
Branch(config)#
```

Step 5: Verify NAT Configuration.

- a. Verify the NAT configuration by using the **show ip nat statistics** and **show ip nat translations** commands.

```
Branch# show ip nat statistics
Total active translations: 0 (0 static, 0 dynamic; 0 extended)
Peak translations: 0
Outside interfaces:
  Serial0/0/1
Inside interfaces:
  Loopback0
Hits: 0 Misses: 0
CEF Translated packets: 0, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list BRANCH-NAT-ACL pool BRANCH-NAT-POOL refcount 0
  pool BRANCH-NAT-POOL: netmask 255.255.255.248
  start 209.165.200.249 end 209.165.200.254
  type generic, total addresses 6, allocated 0 (0%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Branch#
```

As shown above, the pool has been configured and the interfaces assigned. The output of the **show ip nat translations** command confirms that there are currently no active NAT translations:

```
Branch# show ip nat translations
Branch#
```

- b. Initiate NAT traffic by pinging from the Branch LAN to the ISP interface, ISP's loopback, the HQ Internet interface, and this time also include the HQ public email server address. Run the following Tcl script on the Branch router to verify connectivity.

```
foreach address {
209.165.200.241
209.165.202.129
209.165.200.226
209.165.200.238
} { ping $address source 192.168.1.1}
```

```
Branch# tclsh
Branch(tcl)# foreach address {
+>209.165.200.241
+>209.165.202.129
+>209.165.200.226
+>209.165.200.238
+>} { ping $address source 192.168.1.1}
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.241, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.202.129, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 12/13/16 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.226, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 209.165.200.238, timeout is 2 seconds:
Packet sent with a source address of 192.168.1.1
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 28/28/28 ms
Branch(tcl)#
```

All pings should be successful. Troubleshoot if necessary.

- c. Verify that NAT is occurring by using the **show ip nat statistics** and **show ip nat translations** commands.

```
Branch# show ip nat statistics
Total active translations: 5 (0 static, 5 dynamic; 4 extended)
Peak translations: 5, occurred 00:00:13 ago
Outside interfaces:
  Serial0/0/1
Inside interfaces:
```

```
Loopback0
Hits: 40 Misses: 0
CEF Translated packets: 20, CEF Punted packets: 0
Expired translations: 0
Dynamic mappings:
-- Inside Source
[Id: 1] access-list BRANCH-NAT-ACL pool BRANCH-NAT-POOL refcount 5
  pool BRANCH-NAT-POOL: netmask 255.255.255.248
    start 209.165.200.249 end 209.165.200.254
    type generic, total addresses 6, allocated 1 (16%), misses 0

Total doors: 0
Appl doors: 0
Normal doors: 0
Queued Packets: 0
Branch#
Branch# show ip nat translations
Pro Inside global      Inside local          Outside local         Outside global
icmp 209.165.200.249:31 192.168.1.1:31       209.165.200.241:31
209.165.200.241:31
icmp 209.165.200.249:32 192.168.1.1:32       209.165.202.129:32
209.165.202.129:32
icmp 209.165.200.249:33 192.168.1.1:33       209.165.200.226:33
209.165.200.226:33
icmp 209.165.200.249:34 192.168.1.1:34       209.165.200.238:34
209.165.200.238:34
--- 209.165.200.249    192.168.1.1          ---                  ---
Branch#
```

Notice that translations are occurring. The output lists the details of the NAT translations sourced by the 192.168.1.1 Branch LAN IP address, which was translated to public IP address 209.165.200.249.

Device Configurations (Instructor version)

Router HQ (R1)

```
hostname HQ
!
interface Loopback0
  description Headquarters LAN
  ip address 10.10.10.1 255.255.255.0
  ip nat inside
!
interface Serial0/0/0
  description Connection to ISP
  ip address 209.165.200.226 255.255.255.248
  ip nat outside
  clock rate 128000
!
ip nat pool HQ-NAT-POOL 209.165.200.233 209.165.200.237 prefix-length 29
ip nat inside source list HQ-NAT-ACL pool HQ-NAT-POOL
ip nat inside source static 10.10.20.238 209.165.200.238
ip route 0.0.0.0 0.0.0.0 209.165.200.225
!
ip access-list extended HQ-NAT-ACL
  remark Permit Local LAN to use NAT
  permit ip 10.10.10.0 0.0.0.255 any
!
end
```

Router ISP (R2)

```
hostname ISP
!
interface Loopback0
  description Simulating the Internet
  ip address 209.165.202.129 255.255.255.240
!
interface Serial0/0/0
  description Connection to HQ
  ip address 209.165.200.225 255.255.255.248
!
interface Serial0/0/1
  description Connection to Branch
  ip address 209.165.200.241 255.255.255.248
  clock rate 128000
!
ip route 209.165.200.232 255.255.255.248 Serial0/0/0
ip route 209.165.200.248 255.255.255.248 Serial0/0/1
!
end
```

Router Branch (R3)

```
hostname Branch
!
interface Loopback0
  description Branch LAN
  ip address 192.168.1.1 255.255.255.0
```

```
ip nat inside
!
interface Serial0/0/1
description Connection to ISP
ip address 209.165.200.242 255.255.255.248
ip nat outside
!
ip nat pool BRANCH-NAT-POOL 209.165.200.249 209.165.200.254 prefix-length 29
ip nat inside source list BRANCH-NAT-ACL pool BRANCH-NAT-POOL
!
ip route 0.0.0.0 0.0.0.0 209.165.200.241
!
ip access-list standard BRANCH-NAT-ACL
remark Permit Local LAN to use NAT
permit 192.168.1.0 0.0.0.255
!
end
```