2.2.4 Configuration Reference

Configuration on R1

```
#
 sysname R1
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.1 255.255.255.0
#
return
```

Configuration on R2

```
#
 sysname R2
#
aaa
 uthentication-scheme datacom
authorization-scheme datacom
 domain datacom
  authentication-scheme datacom
  authorization-scheme datacom
 local-user hcia@datacom password irreversible-cipher
%^%#.}hB'1"=&=:FWx!Ust(3s^_<.[Z}kEc/>==P56gUVU*cE^|]5@|8/O5FC$9A%^%#
 local-user hcia@datacom privilege level 3
 local-user hcia@datacom service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 10.0.12.2 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
 authentication-mode aaa
 user privilege level 15
#
return
```

2.2.5 Quiz

The details are not provided here.

2.3 Lab 3: NAT Configuration

2.3.1 Introduction

2.3.1.1 About This Lab

Network Address Translation (NAT) translates the IP address in an IP packet header to another IP address. As a transitional plan, NAT enables address reuse to alleviate the IPv4 address shortage. In addition to solving the problem of IP address shortage, NAT provides the following advantages:

- Protects private networks against external attacks.
- Enables and controls the communication between private and public networks.

  In this lab activity, you will configure NAT to understand its principle.

2.3.1.2 Objectives

Upon completion of this task, you will be able to:

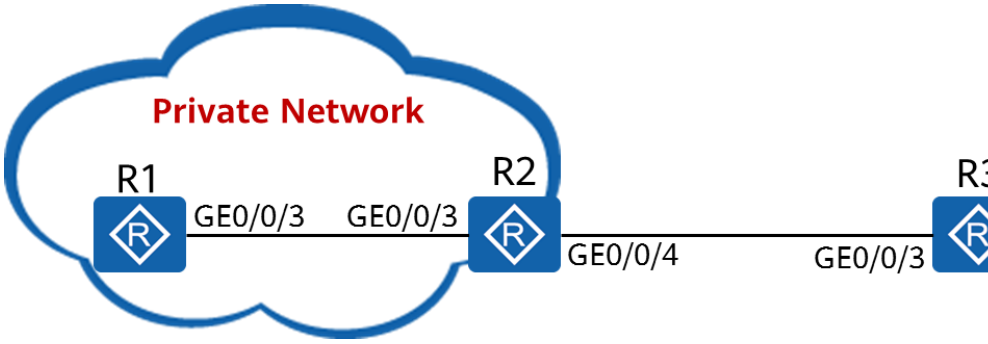
- Learn how to configure dynamic NAT
- Learn how to configure Easy IP
- Learn how to configure NAT server

2.3.1.3 Networking Topology

Due to the shortage of IPv4 addresses, enterprises usually use private IPv4 addresses. However, enterprise network users often need to access the public network and provide services for external users. In this case, you need to configure NAT to meet these requirements.

1. The network between R1 and R2 is an intranet and uses private IPv4 addresses.
2. R1 functions as the client, and R2 functions as the gateway of R1 and the egress router connected to the public network.
3. R3 simulates the public network.

Figure 2-1 Lab topology for NAT configuration



2.3.2 Lab Configuration

2.3.2.1 Configuration Roadmap

1. Configure dynamic NAT.
2. Configure Easy IP.
3. Configure NAT server.

2.3.2.2 Configuration Procedure

Step 1 Complete basic configurations.

Configure IP addresses and routes.

```
[R1]interface GigabitEthernet 0/0/3
[R1-GigabitEthernet0/0/3]ip address 192.168.1.1 24
[R1-GigabitEthernet0/0/3]quit
[R1]ip route-static 0.0.0.0 0 192.168.1.254
```

```
[R2]interface GigabitEthernet 0/0/3
[R2-GigabitEthernet0/0/3]ip address 192.168.1.254 24
[R2-GigabitEthernet0/0/3]quit
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]ip address 1.2.3.4 24
[R2-GigabitEthernet0/0/4]quit
```

```
[R2]ip route-static 0.0.0.0 0 1.2.3.254
```

```
[R3]interface GigabitEthernet 0/0/3
[R3-GigabitEthernet0/0/3]ip address 1.2.3.254 24
```

Configure the Telnet function on R1 and R3 for subsequent verification.

```
[R1]user-interface vty 0 4
[R1-ui-vty0-4]authentication-mode aaa
[R1-ui-vty0-4]quit
[R1]aaa
[R1-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R1-aaa]local-user test service-type telnet
[R1-aaa]local-user test privilege level 15
```

```
[R3]user-interface vty 0 4
[R3-ui-vty0-4]authentication-mode aaa
[R3-ui-vty0-4]quit
[R3]aaa
[R3-aaa]local-user test password irreversible-cipher Huawei@123
Info: Add a new user.
[R3-aaa]local-user test service-type telnet
[R3-aaa]local-user test privilege level 15
[R3-aaa]quit
```

Test connectivity.

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Request time out
    Request time out
    Request time out
    Request time out
    Request time out

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    0 packet(s) received
100.00% packet loss
```

```
[R2]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=255 time=40 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=255 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=255 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 20/24/40 ms
```

R1 cannot communicate with R3 because no route to 192.168.1.0/24 is configured on R3.

Moreover, routes to private networks cannot be configured on R3.

Step 2 The enterprise obtains the public IP addresses ranging from 1.2.3.10 to 1.2.3.20 and needs the dynamic NAT function.

Configure a NAT address pool.

```
[R2]nat address-group 1 1.2.3.10 1.2.3.20
```

The **nat address-group** command configures a NAT address pool. In this example, 1 indicates the number of the address pool. The address pool must be a set of consecutive IP addresses. When internal data packets reach the edge of the private network, the private source IP addresses will be translated into public IP addresses.

Configure an ACL.

```
[R2]acl 2000
[R2-acl-basic-2000]rule 5 permit source any
```

Configure dynamic NAT on GigabitEthernet0/0/4 of R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]nat outbound 2000 address-group 1
```

The **nat outbound** command associates an ACL with an NAT address pool. The IP addresses of packets matching the ACL will be translated into an address in the address pool. If the address pool has sufficient addresses, you can add the **no-pat** argument to enable one-to-one address translation. In this case, only the IP addresses of data packets are translated, and the ports are not translated.

Test connectivity.

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=60 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=20 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=20 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
round-trip min/avg/max = 20/32/60 ms

# Telnet R3 from R1 to simulate TCP traffic.
<R1>telnet 1.2.3.254
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.254 ...
  Connected to 1.2.3.254 ...

Login authentication


Username:test
Password:
<R3>
```

Display the NAT session table on R2.

```
[R2]display nat session all
  NAT Session Table Information:
     Protocol                : TCP(6)
     SrcAddr  Port Vpn       : 192.168.1.1        62185      //Source IP address and source port before NAT
     DestAddr Port Vpn       : 1.2.3.254          23
     NAT-Info
     New SrcAddr             : 1.2.3.11           //Source IP address after NAT
     New SrcPort             : 49149              //Source port after NAT
     New DestAddr            : ----
     New DestPort            : ----

  Total : 1
```

Although R3 does not have a route to R1, R3 sends the data to the translated source address 1.2.3.11. After receiving the data, R2 translates the source address to the address of R1 based

on the data in the NAT session table and forwards the data. Therefore, R1 can **initiate** access to R3.

Step 3 If the IP address of GigabitEthernet0/0/4 on R2 is dynamically assigned (e.g. through DHCP or PPPoE dialup), you need to configure Easy IP.

Delete the configuration in the previous step.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4]undo nat outbound 2000 address-group 1
```

Configure Easy IP.

```
[R2-GigabitEthernet0/0/1]nat outbound 2000
```

Test connectivity.

```
[R1]ping 1.2.3.254
  PING 1.2.3.254: 56  data bytes, press CTRL_C to break
    Reply from 1.2.3.254: bytes=56 Sequence=1 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=2 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=3 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=4 ttl=254 time=30 ms
    Reply from 1.2.3.254: bytes=56 Sequence=5 ttl=254 time=30 ms

  --- 1.2.3.254 ping statistics ---
    5 packet(s) transmitted
    5 packet(s) received
    0.00% packet loss
    round-trip min/avg/max = 30/30/30 ms
```

Telnet R3 from R1 to simulate TCP traffic.

```
[R2]display nat session all
 NAT Session Table Information:
     Protocol          : TCP(6)
       SrcAddr  Port Vpn      : 192.168.1.1     58546          //Source IP address and source port before NAT
        DestAddr Port Vpn     : 1.2.3.4     23
        NAT-Info
        New SrcAddr           : 1.2.3.4    //Source IP address after NAT, that is, the address of GigabitEthernet 0/0/4 on R2
    New SrcPort               : 49089            //Source port after NAT
        New DestAddr          : ----
        New DestPort                    : ----

  Total : 1
```

Step 4 R3 needs to provide network services (telnet in this example) for users on the public network. Because R3 does not have a public IP address, you need to configure NAT server on the outbound interface of R2.

Configure NAT server on R2.

```
[R2]interface GigabitEthernet 0/0/4
[R2-GigabitEthernet0/0/4] nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
```

The **nat server** command defines a mapping table of internal servers so that external users can access internal servers through address and port translation. You can configure an internal server so that users on an external network can **initiate** access to the internal server. When a host on an external network sends a connection request to the public address (global-address) of the internal NAT server, the NAT server translates the destination address of the request into a private address (inside-address) and forwards the request to the server on the private network.

Telnet R1 from R3.

```
<R3>telnet 1.2.3.4 2323
  Press CTRL_] to quit telnet mode
  Trying 1.2.3.4 ...
```

```
 Connected to 1.2.3.4 ...

Login authentication


Username:test
Password:
<R1>
```

Display the NAT session table on R2.

```
[R2]display nat session all
        Protocol               : TCP(6)
    SrcAddr  Port Vpn          : 1.2.3.254     61359
    DestAddr Port Vpn          : 1.2.3.4     2323          //Destination IP address and port before NAT
    NAT-Info
    New SrcAddr                          : ----
    New SrcPort                : ----
        New DestAddr           : 192.168.1.1         //Destination IP address after NAT, that is, the IP address of R1
    New DestPort               : 23              //Destination port after NAT

 Total : 1
```

----End

2.3.3 Verification

The details are not provided here.

2.3.4 Configuration Reference

Configuration on R1

```
#
 sysname R1
#
aaa
local-user test password irreversible-cipher
%^%#y'BJ=em]VY(E%IH!+,f~[|n*'L`HU#H=vlVzMJR'^+^U3qWRm%&:Kd't7oI$%^%#
 local-user test privilege level 3
 local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.1 255.255.255.0
#
 telnet server enable
#
ip route-static 0.0.0.0 0.0.0.0 192.168.1.254
#
user-interface vty 0 4
 authentication-mode aaa
#
return
```

Configuration on R2

```
#
 sysname R2
#
acl number 2000
 rule 5 permit
#
 nat address-group 1 1.2.3.10 1.2.3.20
#
interface GigabitEthernet0/0/3
 ip address 192.168.1.254 255.255.255.0
#
interface GigabitEthernet0/0/4
```

```
 ip address 1.2.3.4 255.255.255.0
 nat server protocol tcp global current-interface 2323 inside 192.168.1.1 telnet
 nat outbound 2000
#
return
```

Configuration on R3

```
#
 sysname R3
#
aaa
local-user test password irreversible-cipher %^%#s<LQ(8-ZC6FNGG1#)n=.GgU|@)n`Z'n%$43+2>7,I>#XBkfcu(}-
3y+o:`UD%^%#
 local-user test privilege level 15
 local-user test service-type telnet
#
interface GigabitEthernet0/0/3
 ip address 1.2.3.254 255.255.255.0
#
 telnet server enable
#
user-interface vty 0 4
authentication-mode aaa
#
return
```

2.3.5 Quiz

1. When configuring NAT Server, should the destination ports before translation be the same as those after translation?