**NAT Configuration**

Student Version



Huawei Technologies Co., Ltd.

|  |
| --- |
| **Copyright © Huawei Technologies Co., Ltd. 2020. All rights reserved.**  No part of this document may be reproduced or transmitted in any form or by any means without prior written consent of Huawei Technologies Co., Ltd.  **Trademarks and Permissions**  HW_POS_RBG_Vertical-150ppi.png and other Huawei trademarks are trademarks of Huawei Technologies Co., Ltd.  All other trademarks and trade names mentioned in this document are the property of their respective holders.  **Notice**  The purchased products, services and features are stipulated by the contract made between Huawei and the customer. All or part of the products, services and features described in this document may not be within the purchase scope or the usage scope. Unless otherwise specified in the contract, all statements, information, and recommendations in this document are provided "AS IS" without warranties, guarantees or representations of any kind, either express or implied.  The information in this document is subject to change without notice. Every effort has been made in the preparation of this document to ensure accuracy of the contents, but all statements, information, and recommendations in this document do not constitute a warranty of any kind, express or implied. |

|  |  |
| --- | --- |
| Huawei Technologies Co., Ltd. | |
| Address: | Huawei Industrial Base  Bantian, Longgang  Shenzhen 518129  People's Republic of China |
| Website: | <https://e.huawei.com/> |

**Huawei Certification System**

Huawei Certification follows the "platform + ecosystem" development strategy, which is a new collaborative architecture of ICT infrastructure based on "Cloud-Pipe-Terminal". Huawei has set up a complete certification system consisting of three categories: ICT infrastructure certification, platform and service certification, and ICT vertical certification. It is the only certification system that covers all ICT technical fields in the industry. Huawei offers three levels of certification: Huawei Certified ICT Associate (HCIA), Huawei Certified ICT Professional (HCIP), and Huawei Certified ICT Expert (HCIE). Huawei Certification covers all ICT fields and adapts to the industry trend of ICT convergence. With its leading talent development system and certification standards, it is committed to fostering new ICT talent in the digital era, and building a sound ICT talent ecosystem.

Huawei Certified ICT Associate-Datacom (HCIA-Datacom) is designed for Huawei's frontline engineers and anyone who want to understand Huawei's datacom products and technologies. The HCIA-Datacom certification covers routing and switching principles, basic WLAN principles, network security basics, network management and O&M basics, SDN and programmability and automation basics.

The Huawei certification system introduces the industry, fosters innovation, and imparts cutting-edge datacom knowledge.



# NAT Configuration

## Background

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.

## Objectives

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

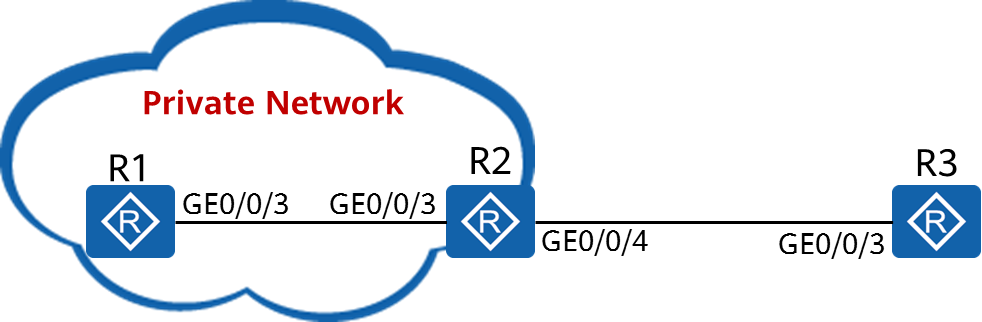
Learn how to configure dynamic NAT

Learn how to configure Easy IP

Learn how to configure NAT server

## Topology

Lab 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.

The network between R1 and R2 is an intranet and uses private IPv4 addresses.

R1 functions as the client, and R2 functions as the gateway of R1 and the egress router connected to the public network.

R3 simulates the public network.

## Implementation

### Roadmap

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

### Procedure

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.

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]

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]

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.

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]

# Configure Easy IP.

[R2-GigabitEthernet0/0/4]

# 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

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]

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**

* 1. **Verification**

The details are not provided here.