**Using Dynamic NAT for Internet Access**

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.



# Using Dynamic NAT for Internet Access

## Background

The company Jan16 has deployed a switch to build a LAN for its several PCs, as well as an egress router to enable Internet access. To ensure security of the internal network and enable the PCs using private IP addresses to access the Internet, dynamic NAT needs to be configured on the egress router to translate PCs' private IP addresses into public IP addresses. Figure 1-1 shows the network topology. The specific requirements are as follows:

The internal network segment is 192.168.1.0/24, and the egress network segment is 16.16.16.0/24.

Public IP addresses 16.16.16.1 to 16.16.16.5 have been obtained for NAT translation on the egress router.

The IP addresses and interfaces of the PCs and egress router are shown in the following topology.

## Objectives

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

Learn how to manually configure dynamic NAT

Learn how to configure ACL to limit source addresses of NAT

## Topology

Lab topology



Public IP addresses 16.16.16.1 to 16.16.16.5 are used as post-NAT addresses. You need to configure these public IP addresses in a NAT address pool on the egress router, create an ACL to match packets with PCs' private IP addresses, and apply NAT on G0/0/1 of the egress router. To enable connectivity with the Internet, configure a routing protocol on the egress router according to the ISP network environment.

The IP address planning and interface planning can be referred in the appendix.

## Implementation

### Roadmap

1. Configure interfaces on the egress router.
2. Configure dynamic NAT.
3. Configure an IP address for each PC.

### Procedure

Configure interfaces on the egress router.

#Configure IP addresses for interfaces on the egress router.

[Huawei]system-view

[Huawei]sysname R1

[R1]int G0/0/0

[R1-GigabitEthernet0/0/0]ip add 192.168.10.254 24

[R1]int G0/0/1

[R1-GigabitEthernet0/0/1]ip add 16.16.16.16 24

Configure dynamic NAT.

#Run the **nat address-group** command on R1 to create a NAT address pool that contains public IP addresses 16.16.16.1 to 16.16.16.5.

[R1]

#Create basic ACL 2000.

[R1]acl 2000

[R1-acl-basic-2000]

#Run the **nat outbound** command on G0/0/1 of R1 to associate ACL 2000 with the NAT address pool. In this way, source addresses specified in ACL 2000 can be translated into public addresses in the NAT address pool.

[R1-acl-basic-2000]int G0/0/1

[R1-GigabitEthernet0/0/1]

Configure an IP address for each PC.

Configure the IP addresses of PCs referred by the appendix.

* 1. **Verification**

The details are not provided here.

Check outbound NAT information.

#Run the display nat outbound command on R1 to view outbound NAT information.

<R1>display nat outbound

NAT Outbound Information:

--------------------------------------------------------------------------

Interface Acl Address-group/IP/Interface Type

--------------------------------------------------------------------------

GigabitEthernet0/0/1 2000 1 no-pat

--------------------------------------------------------------------------

Total : 1

Test the connectivity with the Internet.

#Test the connectivity between PC1 and the Internet, and obtain packet information on G0/0/1 of R1.

PC>ping 16.16.16.15

Ping 16.16.16.15: 32 data bytes, Press Ctrl\_C to break

From 16.16.16.15: bytes=32 seq=1 ttl=127 time=31 ms

From 16.16.16.15: bytes=32 seq=2 ttl=127 time=31 ms

From 16.16.16.15: bytes=32 seq=3 ttl=127 time=31 ms

From 16.16.16.15: bytes=32 seq=4 ttl=127 time=32 ms

From 16.16.16.15: bytes=32 seq=5 ttl=127 time=31 ms

--- 16.16.16.15 ping statistics ---

5 packet(s) transmitted

5 packet(s) received

0.00% packet loss

round-trip min/avg/max = 31/31/32 ms

Check NAT session information.

#Run the **display nat session** command on R1 to view NAT session information.

<R1>display nat session all

NAT Session Table Information:

Protocol : ICMP(1)

SrcAddr Vpn : 192.168.10.1

DestAddr Vpn : 16.16.16.15

Type Code IcmpId : 0 8 33944

NAT-Info

New SrcAddr : 16.16.16.1

New DestAddr : ----

New IcmpId : ----

Protocol : ICMP(1)

SrcAddr Vpn : 192.168.10.1

DestAddr Vpn : 16.16.16.15

Type Code IcmpId : 0 8 33946

NAT-Info

New SrcAddr : 16.16.16.2

New DestAddr : ----

New IcmpId : ----

Protocol : ICMP(1)

SrcAddr Vpn : 192.168.10.1

DestAddr Vpn : 16.16.16.15

Type Code IcmpId : 0 8 33947

The command output shows that R1 has translated the source IP address 192.168.10.1 of the received packets into 16.16.16.1, enabling PC1 to access the Internet.

----E**nd**

* 1. **Appendix**

IP address planning

| **Device** | **Interface** | **IP Address** |
| --- | --- | --- |
| R1 | G0/0/0 | 192.168.1.254/24 |
| R1 | G0/0/1 | 16.16.16.16/24 |
| PC1 | E0/0/1 | 192.168.10.1/24 |
| PC2 | E0/0/1 | 192.168.10.2/24 |
| PC3 | E0/0/1 | 192.168.10.3/24 |
| PC4 | E0/0/1 | 16.16.16.15/24 |

Interface planning

| **Local Device** | **Local Interface** | **Peer Device** | **Peer Interface** |
| --- | --- | --- | --- |
| R1 | G0/0/0 | SW1 | G0/0/1 |
| R1 | G0/0/1 | SW2 | G0/0/1 |