Network Address Translation



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.



Contents

[1 Network Address Translation 1](#_Toc60149257)

[1.1 Foreword 1](#_Toc60149258)

[1.2 Objectives 1](#_Toc60149259)

[1.3 NAT Overview 2](#_Toc60149260)

[1.3.1 Motivation Behind NAT 2](#_Toc60149261)

[1.3.2 Private IP Addresses 2](#_Toc60149262)

[1.3.3 NAT Implementation 3](#_Toc60149263)

[1.4 Static NAT 3](#_Toc60149264)

[1.4.2 Static NAT Example 4](#_Toc60149265)

[1.4.3 Configuring Static NAT 4](#_Toc60149266)

[1.4.4 Example for Configuring Static NAT 5](#_Toc60149267)

[1.5 Dynamic NAT 6](#_Toc60149268)

[1.5.1 Dynamic NAT Implementation 6](#_Toc60149269)

[1.5.2 Dynamic NAT Example 6](#_Toc60149270)

[1.5.3 Configuring Dynamic NAT 7](#_Toc60149271)

[1.5.4 Example for Configuring Dynamic NAT 8](#_Toc60149272)

[1.6 NAPT and Easy IP 9](#_Toc60149273)

[1.6.1 NAPT Implementation 9](#_Toc60149274)

[1.6.2 NAPT Example 9](#_Toc60149275)

[1.6.3 Example for Configuring NAPT 10](#_Toc60149276)

[1.6.4 Easy IP 11](#_Toc60149277)

[1.6.5 Example for Configuring Easy IP 11](#_Toc60149278)

[1.7 NAT Server 12](#_Toc60149279)

[1.7.1 NAT Server 12](#_Toc60149280)

[1.7.2 NAT Server Example 13](#_Toc60149281)

[1.7.3 Example for Configuring NAT Server 13](#_Toc60149282)

[1.8 Summary 14](#_Toc60149283)

[1.9 Quiz 15](#_Toc60149284)

# Network Address Translation

## Foreword

User management is one of the most basic security management requirements for   
With the development of the Internet and the increase of network applications, limited public IPv4 addresses have become the bottleneck of network development. To solve this problem, Network Address Translation (NAT) was introduced.

NAT enables hosts on an internal network to access an external network. It not only helps alleviate IPv4 address shortage but also improves the security of the internal network as NAT prevents devices on the external network from directly communicating with hosts on the internal network that uses private addresses.

This course describes the motivation behind NAT, and implementations and application scenarios of different types of NAT.

## Objectives

On completion of this course, you will be able to:

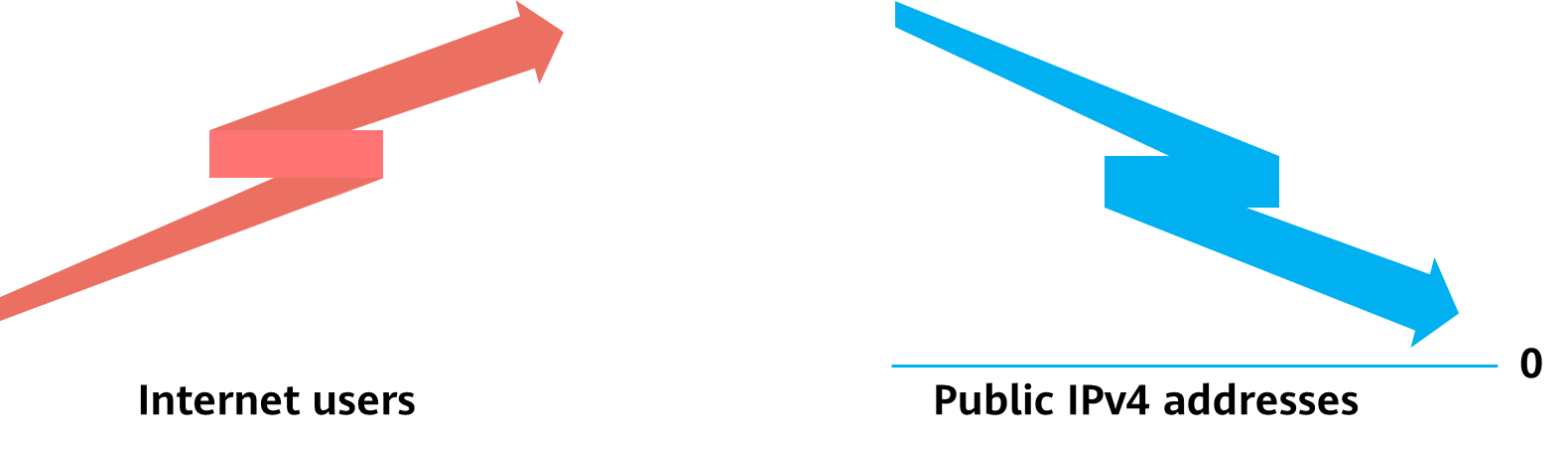
Understand the motivation behind NAT.

Master NAT classification and implementations.

Master NAT selection in different scenarios.

## NAT Overview

### Motivation Behind NAT



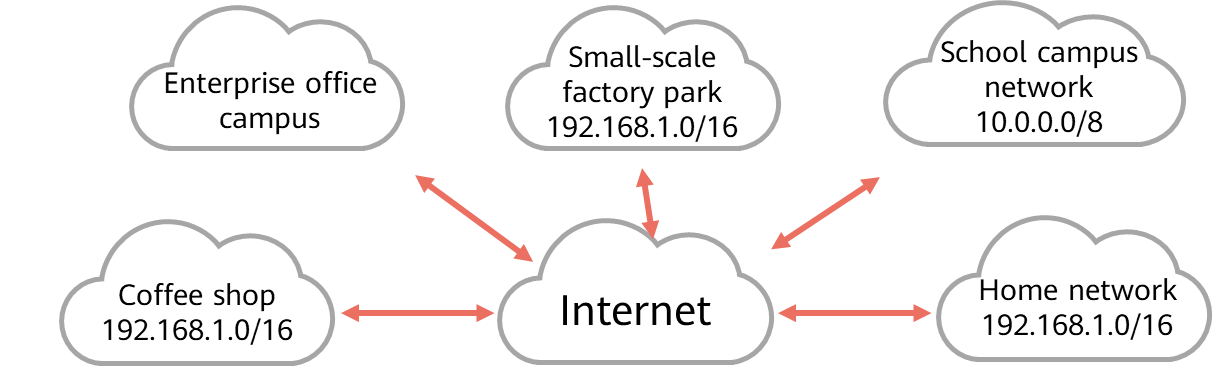
Motivation Behind NAT

As the number of Internet users increases, public IPv4 addresses become scarcer.

What's worse, uneven allocation of these addresses has resulted in a severe shortage of available public IPv4 addresses in some areas.

To overcome public IPv4 address shortage, it is necessary to use transition technologies.

### Private IP Addresses



Private IP Addresses

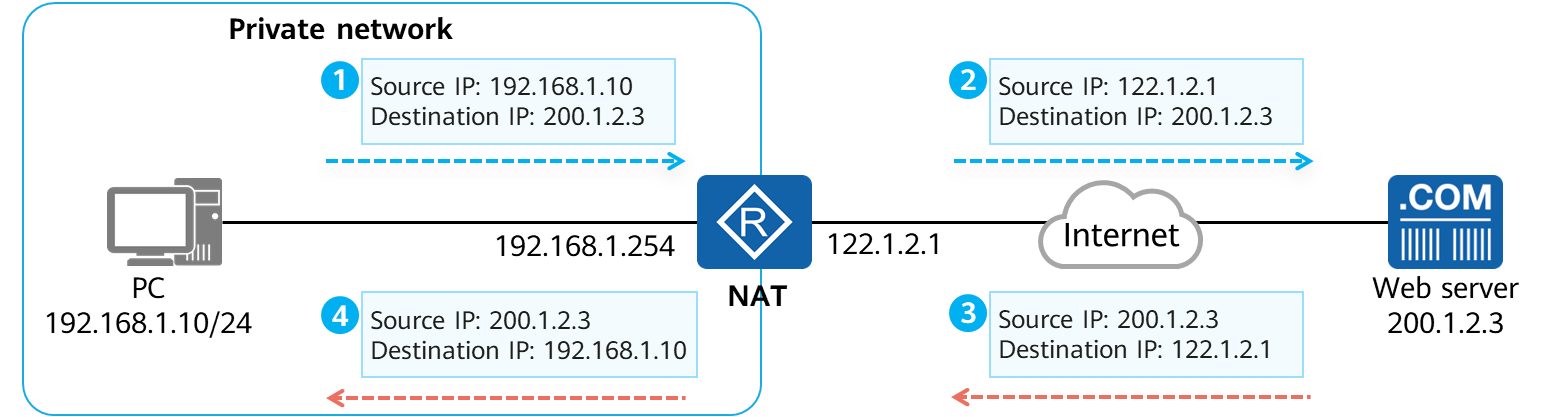
Public IP addresses: managed and allocated by a dedicated organization and can be used for direct communication on the Internet

Private IP addresses: can be used by organizations or individuals randomly on internal networks, but cannot be used for direct communication on the Internet

The following Class A, B, and C addresses are reserved as private IP addresses:

* Class A: 10.0.0.0–10.255.255.255
* Class B: 172.16.0.0–172.31.255.255
* Class C: 192.168.0.0–192.168.255.255

### NAT Implementation



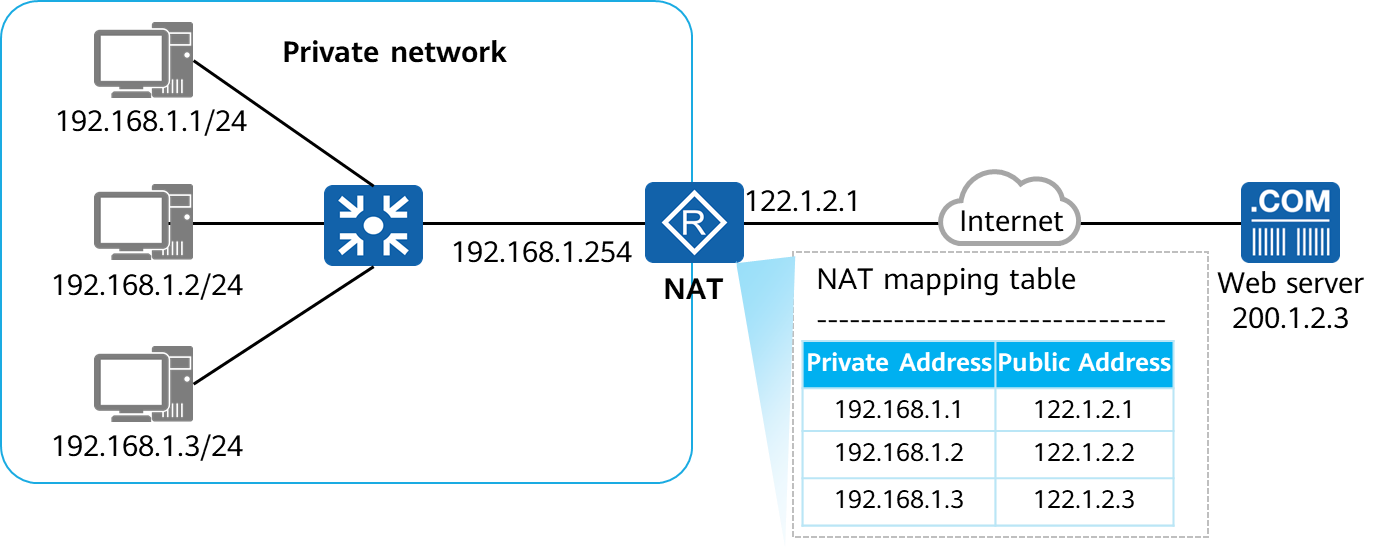
NAT Implementation

NAT: translates IP addresses in IP data packets. It is widely used on live networks and is usually deployed on network egress devices, such as routers or firewalls.

Typical NAT application scenario: Private addresses are used on private networks (enterprises or homes), and NAT is deployed on egress devices. For traffic from an internal network to an external network, NAT translates the source addresses of the data packets into specific public addresses. For traffic from an external network to an internal network, NAT translates the destination address of the data packets.

NAT+private addresses effectively conserve public IPv4 addresses.

## Static NAT

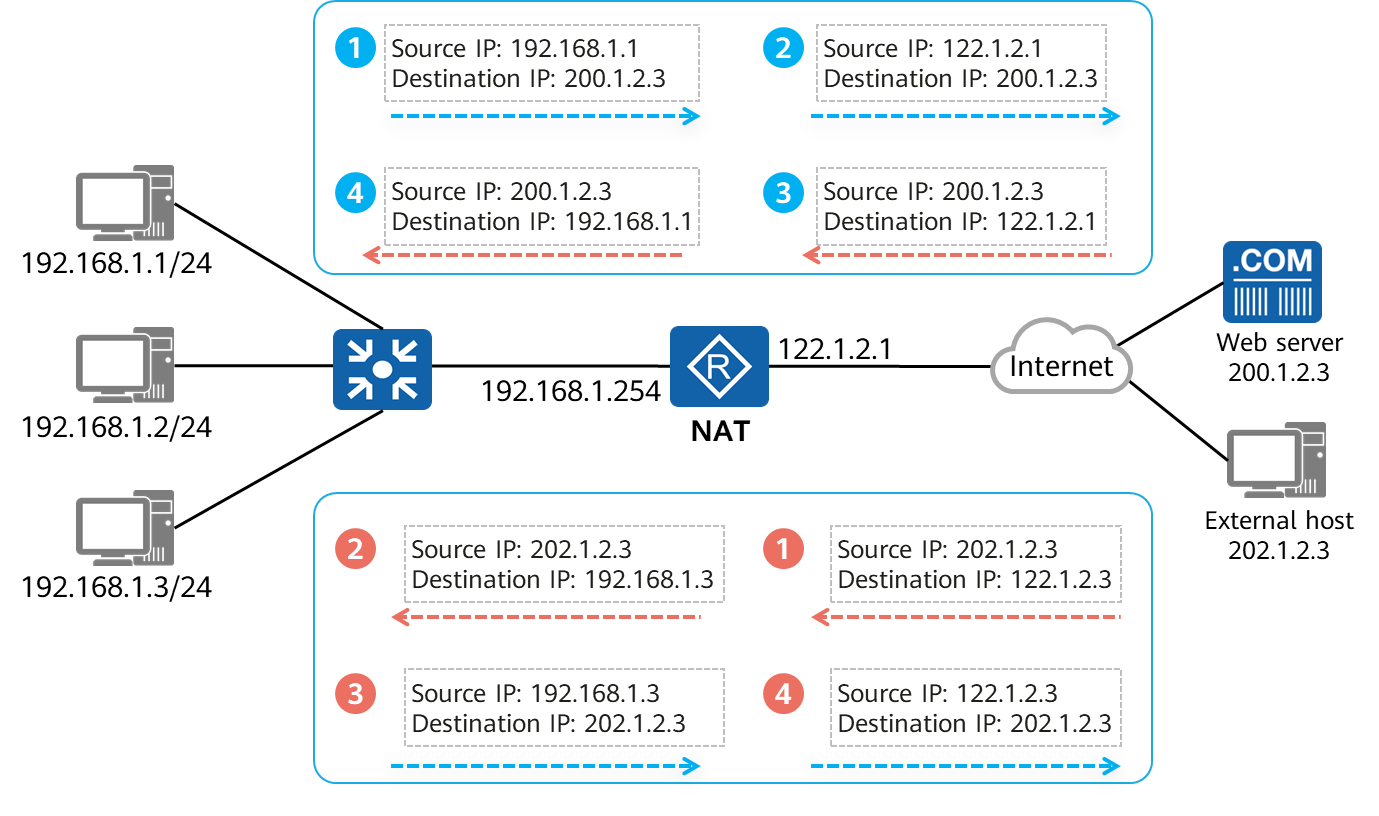


Static NAT

Static NAT: A private IP address is mapped to a fixed public IP address.

Bidirectional access: When an internal host with a private IP address accesses the Internet, the egress NAT device translates the private IP address into a public IP address. Similarly, when an external network device sends packets to access an internal network, the NAT device translates the public address (destination address) carried in the packets into a private address.

### Static NAT Example



Static NAT Example

Outbound process:

* The source address 192.168.1.1 is translated into 122.1.2.1 for Internet access.
* The destination IP address 122.1.2.1 of the packet returned from the Internet is translated into 192.168.1.1

Inbound process:

* When the external host sends a packet to proactively access 122.1.2.3, the destination address of the packet is translated into 192.168.1.3 by the egress device through NAT.
* The source IP address of the packet sent from 192.168.1.3 is translated into 122.1.2.3 by NAT when the packet passes through the egress device.

### Configuring Static NAT

* Method 1: Configure static NAT in the interface view.

[Huawei-GigabitEthernet0/0/0] **nat static global** *{global-address}* **inside** *{host-address }*

**global** *{ global-address}* is used to configure an external public IP address, and **inside** *{host-address }* is used to configure an internal private IP address.

* Method 2: Configure static NAT in the system view.

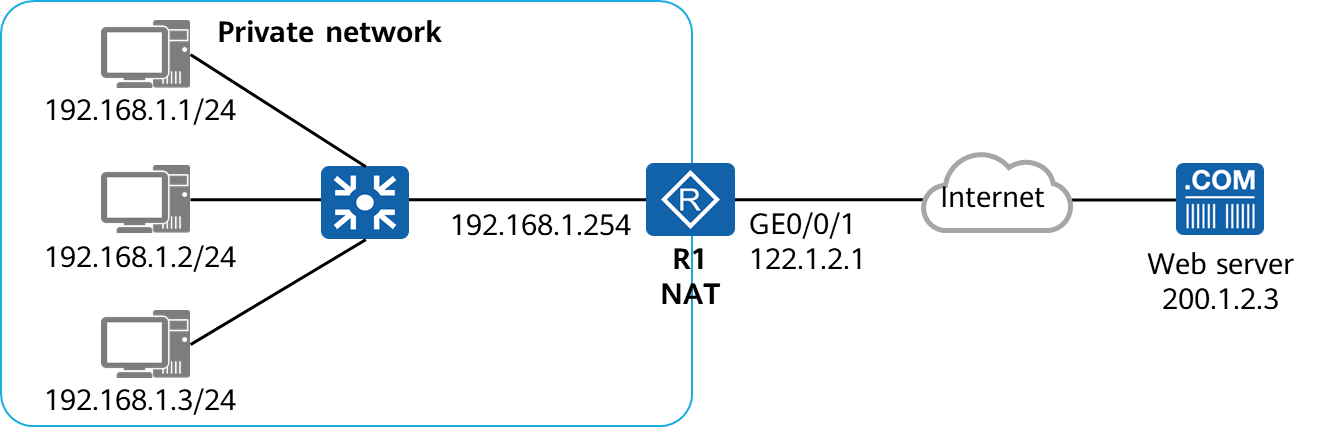
[Huawei] **nat static global** *{ global-address}* **inside** *{host-address }*

The command format in the system view is the same as that in the interface view. After this configuration, enable static NAT on a specific interface.

[Huawei-GigabitEthernet0/0/0] **nat static enable**

This command enables static NAT on the interface.

### Example for Configuring Static NAT



Example for Configuring Static NAT

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24

[R1-GigabitEthernet0/0/1]nat static global 122.1.2.1 inside 192.168.1.1

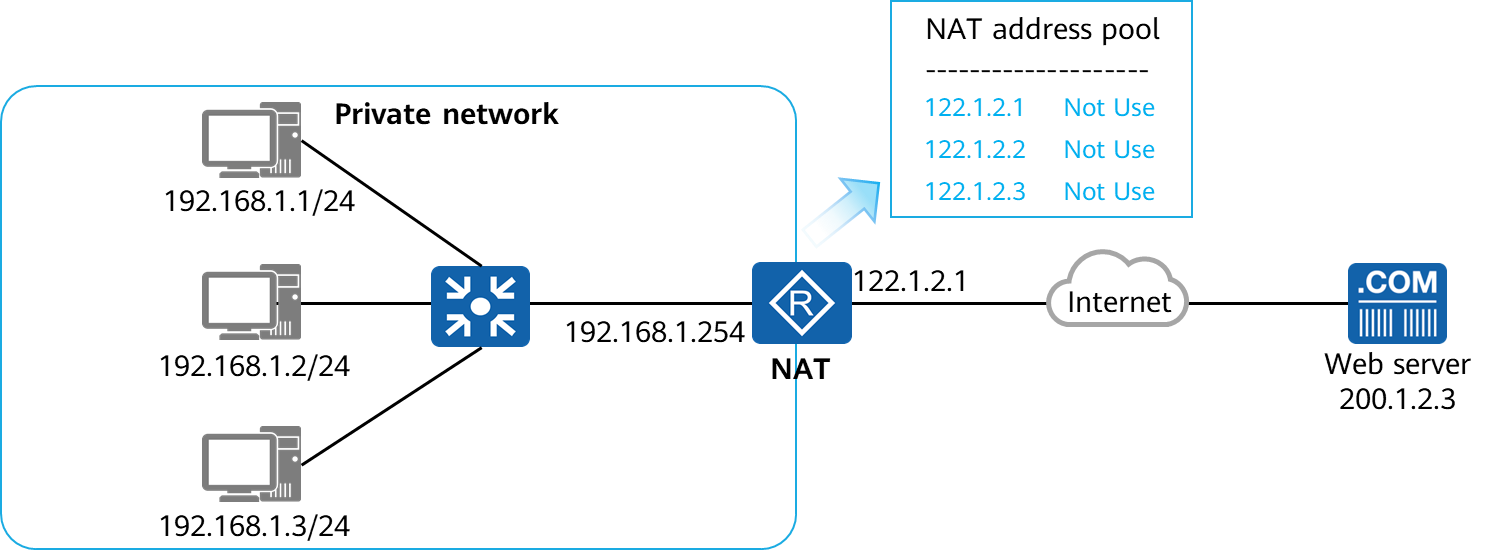
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.2 inside 192.168.1.2

[R1-GigabitEthernet0/0/1]nat static global 122.1.2.3 inside 192.168.1.3

Configure static NAT on R1 to map private addresses of internal hosts to public addresses in one-to-one mode.

## Dynamic NAT

### Dynamic NAT Implementation

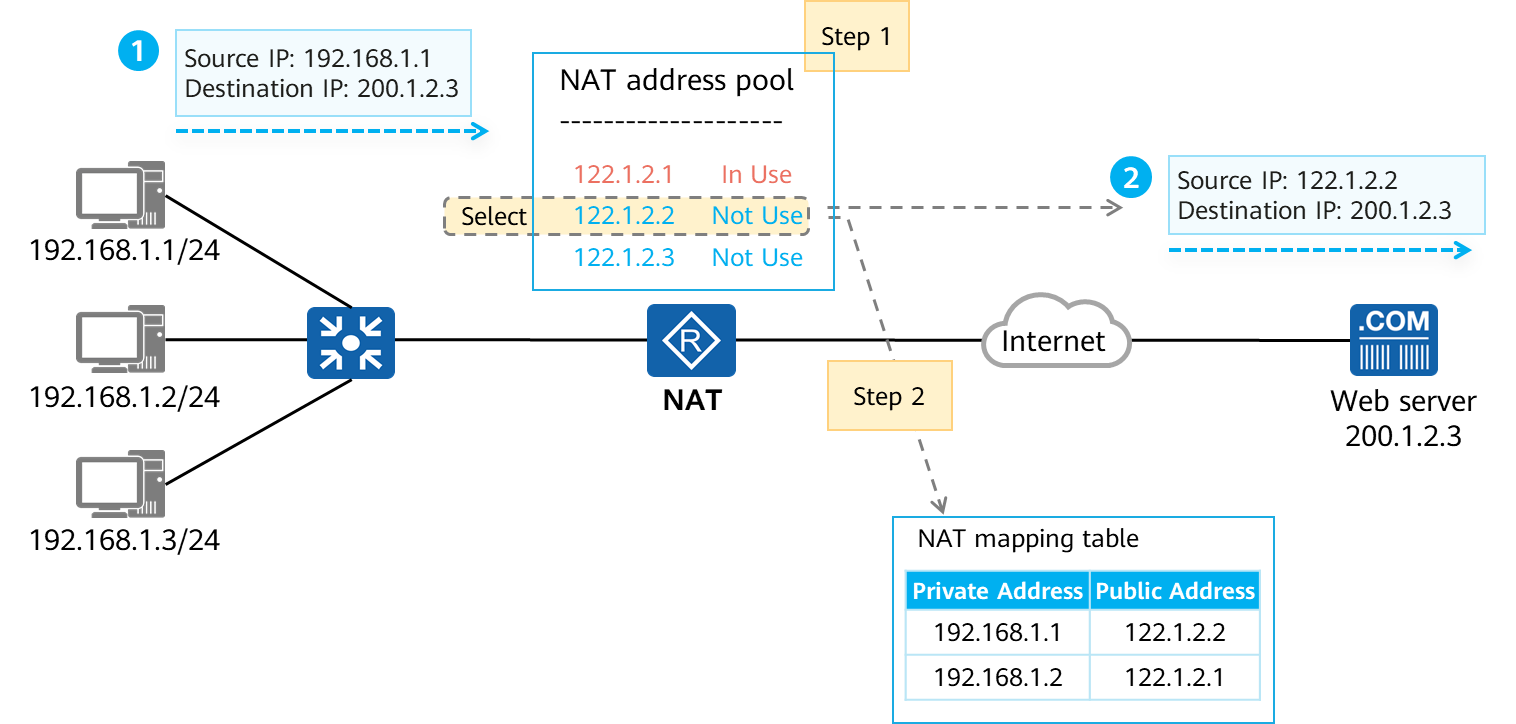


Dynamic NAT Implementation

Dynamic NAT: A private IP address is mapped to a public IP address from a NAT address pool containing a group of public IP addresses. Static NAT strictly maps addresses in one-to-one mode. As a result, even if an internal host is offline for a long time or does not send data, the public address is still occupied by the host.

Dynamic NAT prevents such address wastes. When an internal host accesses an external network, an available IP address in a NAT address pool is temporarily assigned to the host and marked as In Use. When the host no longer accesses the external network, the assigned IP address is reclaimed and marked as Not Use.

### Dynamic NAT Example



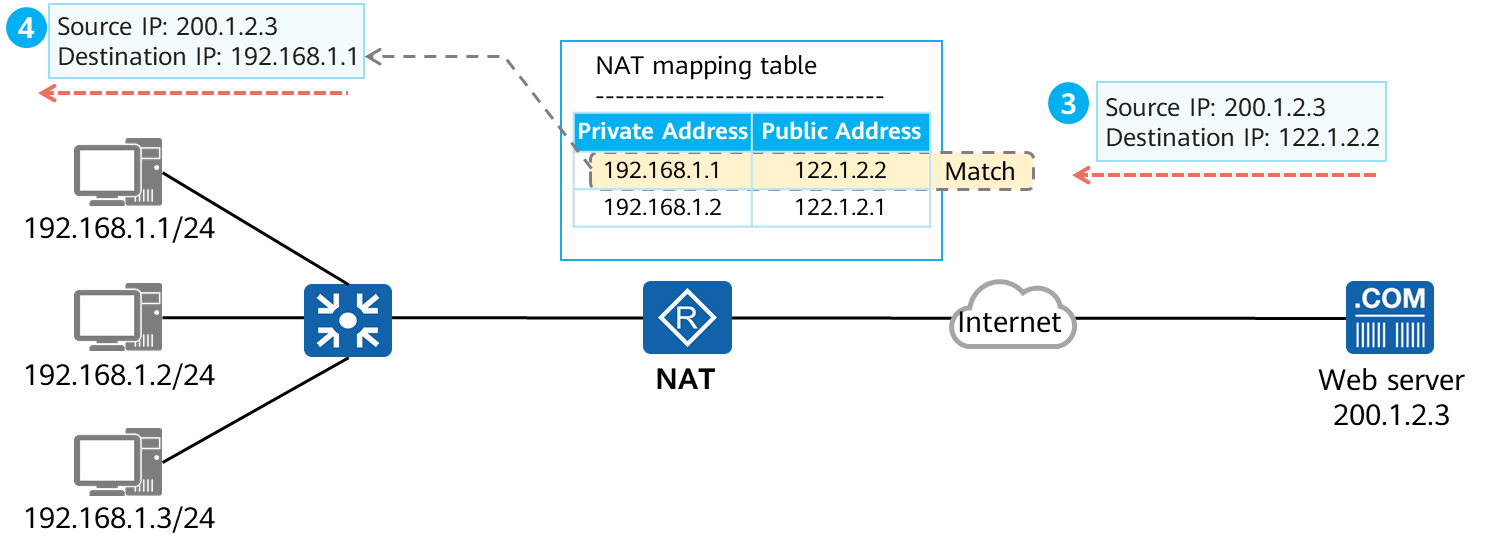
Dynamic NAT Example (1)

Step 1:

Selects an unused address in the address pool as the post-translated address and marks the address as **In Use**.

Step 2

Generates a temporary NAT mapping table.



Dynamic NAT Example (2)

When the responding packet arrive the NAT device：

The NAT device searches the NAT mapping table for the desired private IP address based on the public IP address and translates the destination IP address of the IP data packet into the private address.

### Configuring Dynamic NAT

* Create an address pool.

[Huawei] **nat address-group** *group-index start-address end-address*

Configure a public address range. group-index specifies the address pool ID, and start-address and end-address specify the start and end addresses of the address pool, respectively.

* Configure an ACL rule for NAT.

[Huawei] **acl** number

[Huawei-acl-basic-number ] **rule permit source** *source-address source-wildcard*

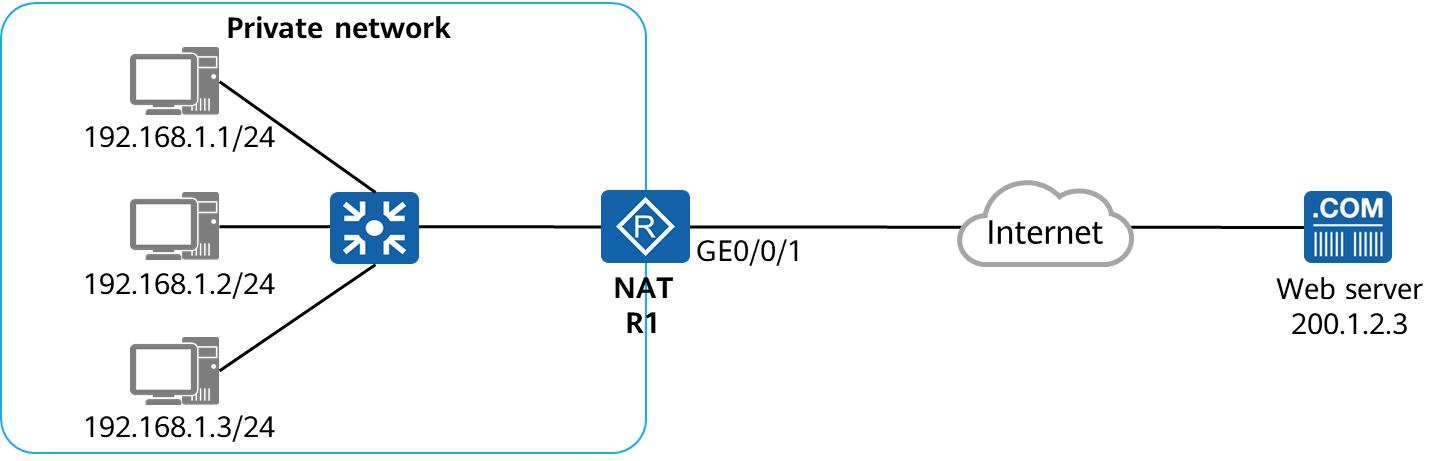
Configure a basic ACL to match the source address range that requires dynamic NAT.

* Configure outbound NAT with the address pool in the interface view.

[Huawei-GigabitEthernet0/0/0] **nat outbound** *acl-number* **address-group** *group-index* [ **no-pat** ]

Associate the ACL rule with the address pool for dynamic NAT on the interface. The no-pat parameter specifies that port translation is not performed.

### Example for Configuring Dynamic NAT



Example for Configuring Dynamic NAT

[R1]nat address-group 1 122.1.2.1 122.1.2.3

[R1]acl 2000

[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255

[R1-acl-basic-2000]quit

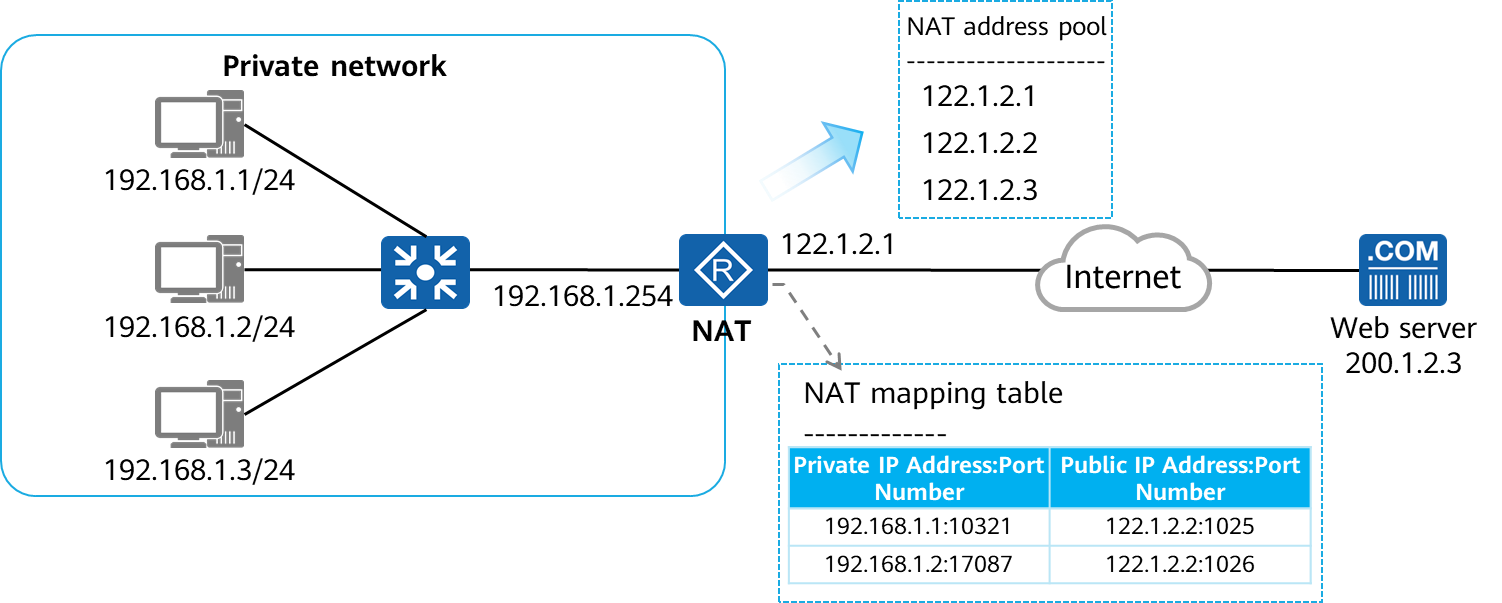
[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1 no-pat

Configure dynamic NAT on R1 to dynamically map private addresses of internal hosts to public addresses.

## NAPT and Easy IP

### NAPT Implementation

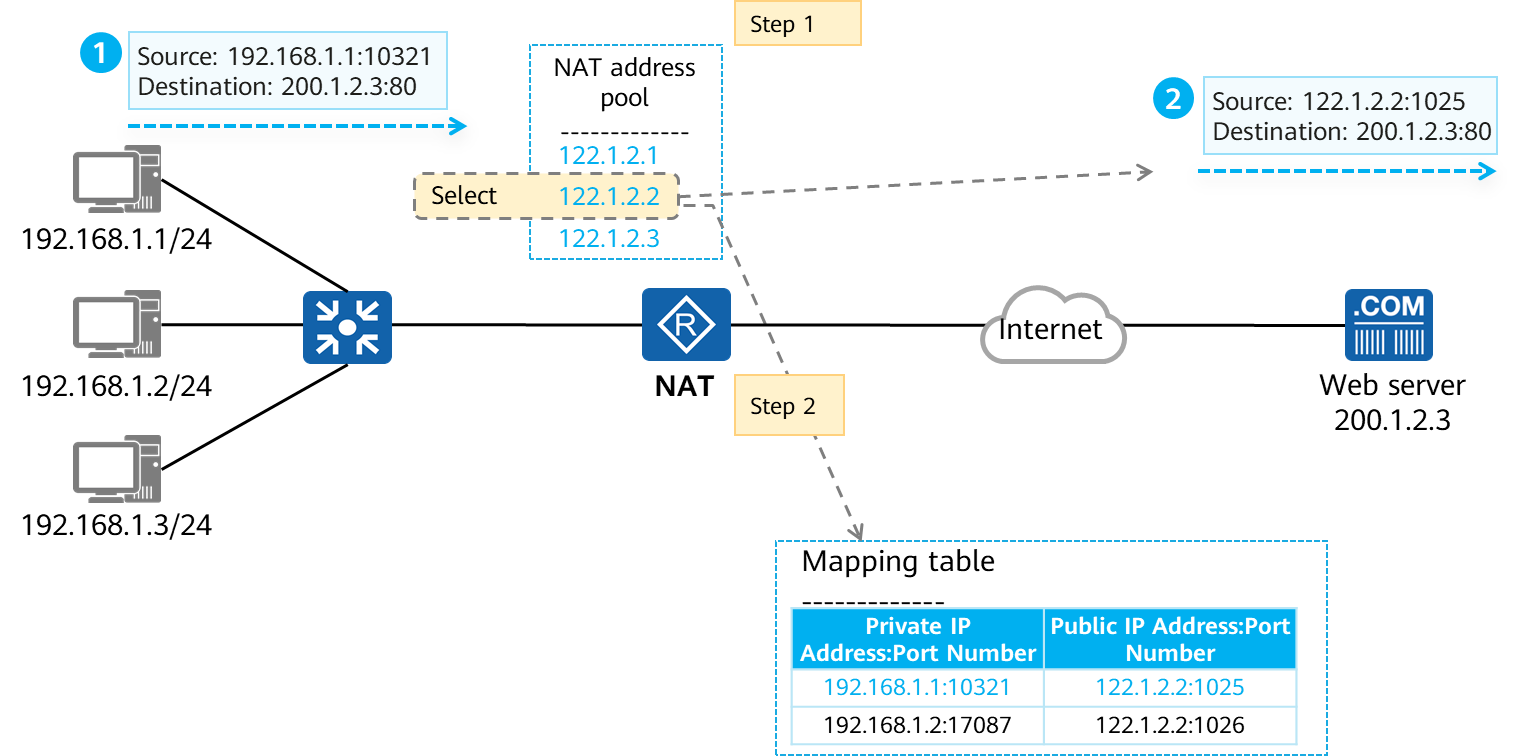


NAPT Implementation

Dynamic NAT does not translate port numbers. It belongs to No-Port Address Translation (No-PAT). In this mode, the mapping between public and private addresses is still 1:1, which cannot improve public address utilization.

Network Address and Port Translation (NAPT): translates both IP addresses and port numbers from multiple internal hosts to one public IP address in an address pool. In this way, 1:n mapping between public and private addresses is implemented, which effectively improves public address utilization.

### NAPT Example



NAPT Example (1)

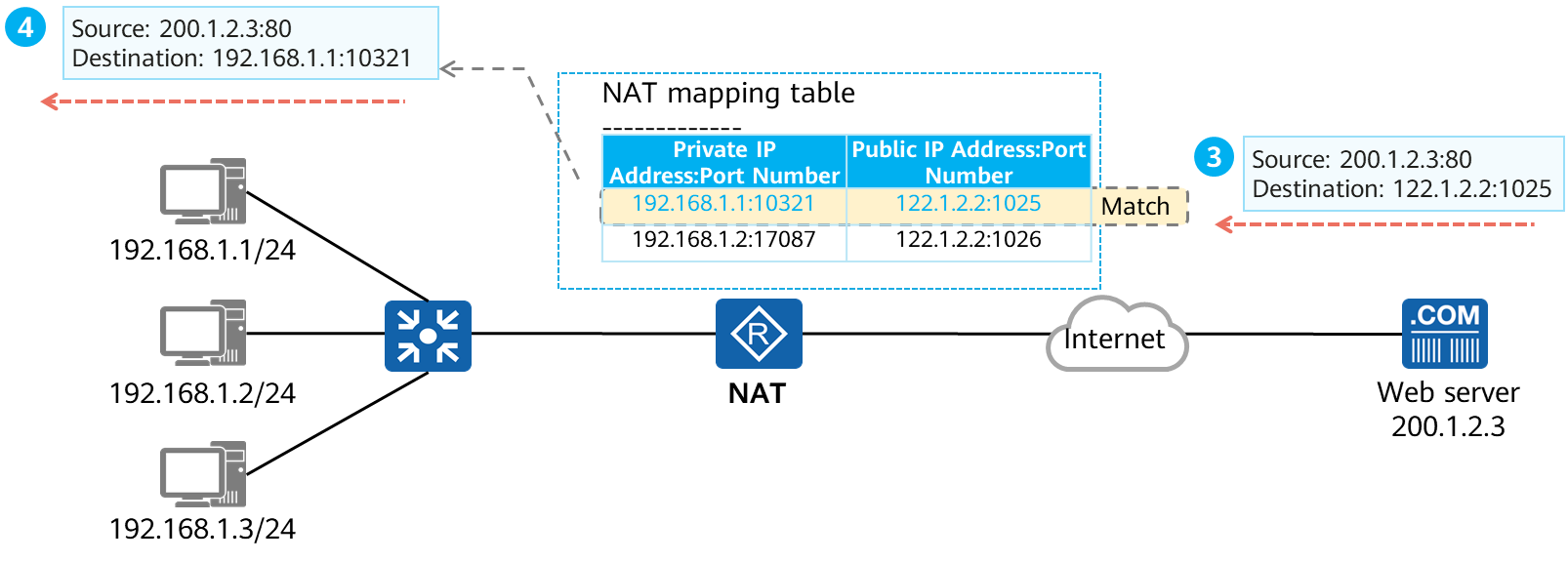
Step 1

Selects an address from the address pool and translates both the source IP address and port number.

Step 2

Generates a temporary NAT mapping table, which records:

[Source IP address:port number before translation], [IP address:port number after translation].

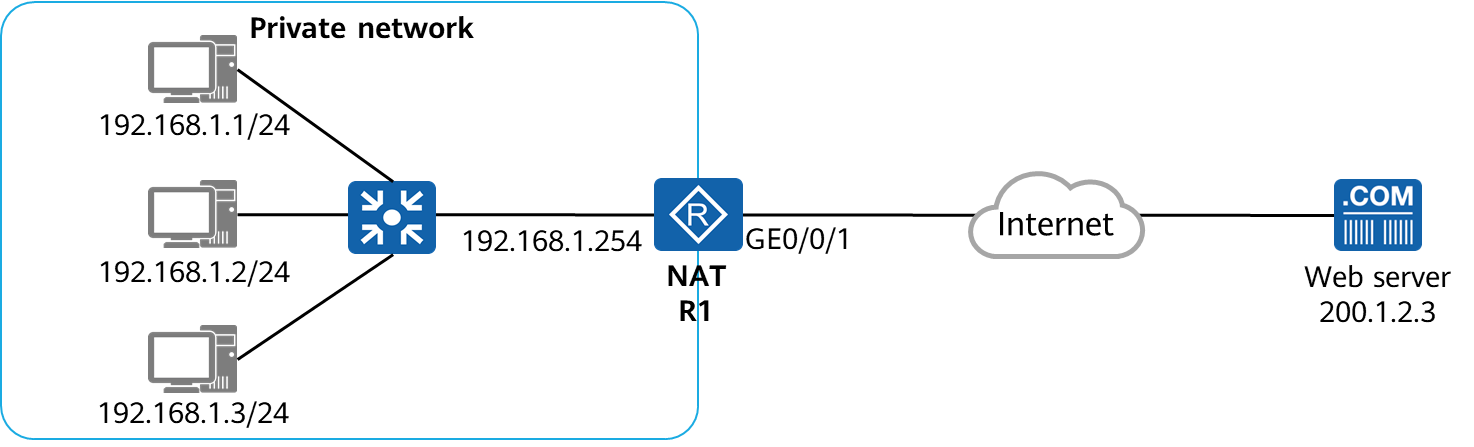


NAPT Example (2)

When the responding packet arrive the NAT device：

Searches the NAT mapping table for the desired private IP address and port number based on the public IP address and port number, and translates the destination IP address and port number of the IP data packet.

### Example for Configuring NAPT



Example for Configuring NAPT

[R1]nat address-group 1 122.1.2.1 122.1.2.1

[R1]acl 2000

[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255

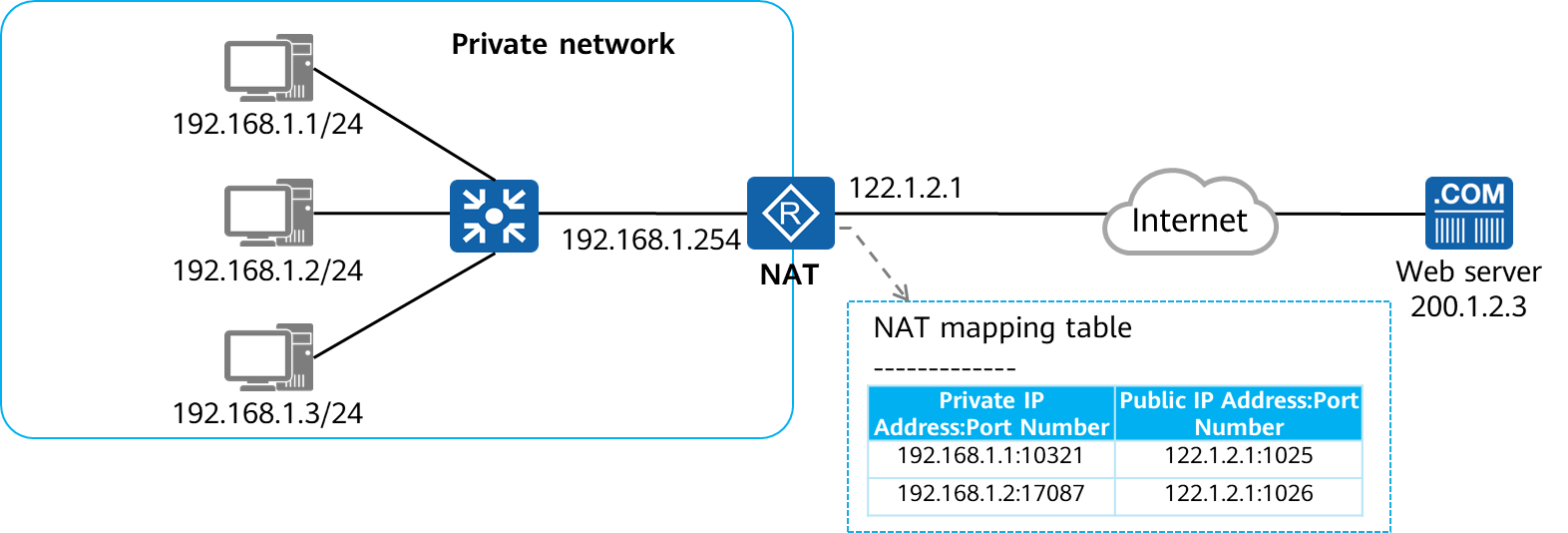
[R1-acl-basic-2000]quit

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1

Configure NAPT on R1 to allow all hosts with private IP addresses on the internal network to access the public network through 122.1.2.1.

### Easy IP

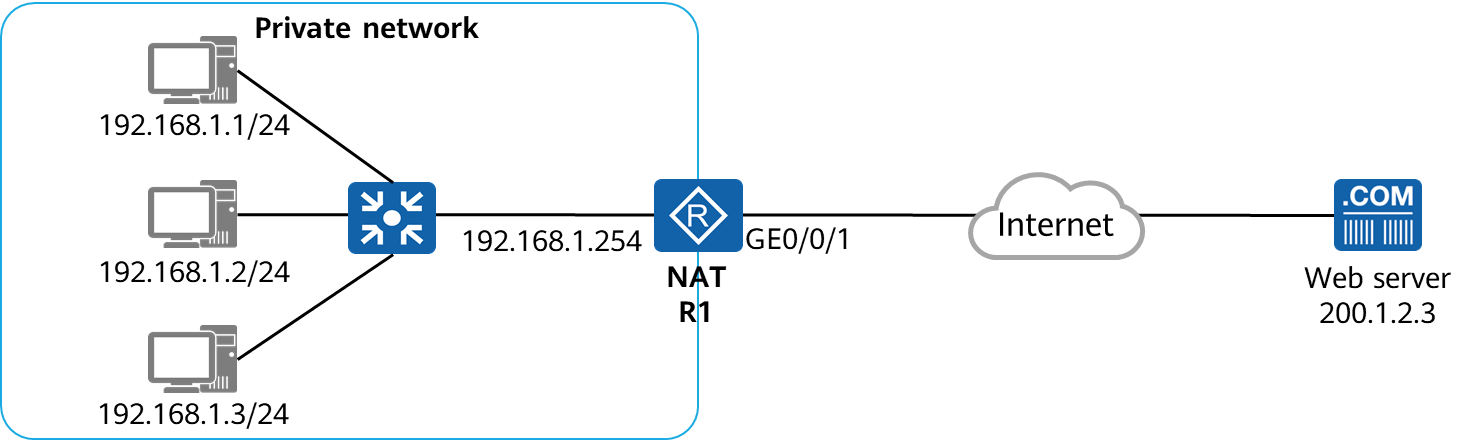


Easy IP

Easy IP: translates both IP addresses and transport-layer port numbers. The implementation of Easy IP is the same as that of NAPT. The difference is that Easy IP does not involve address pools. It uses an interface address as a public address for NAT.

Easy IP applies to scenarios where public IP addresses are not fixed, such as scenarios where public IP addresses are dynamically obtained by egress devices on private networks through DHCP or PPPoE dialup.

### Example for Configuring Easy IP



Example for Configuring Easy IP

[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255

[R1-acl-basic-2000]quit

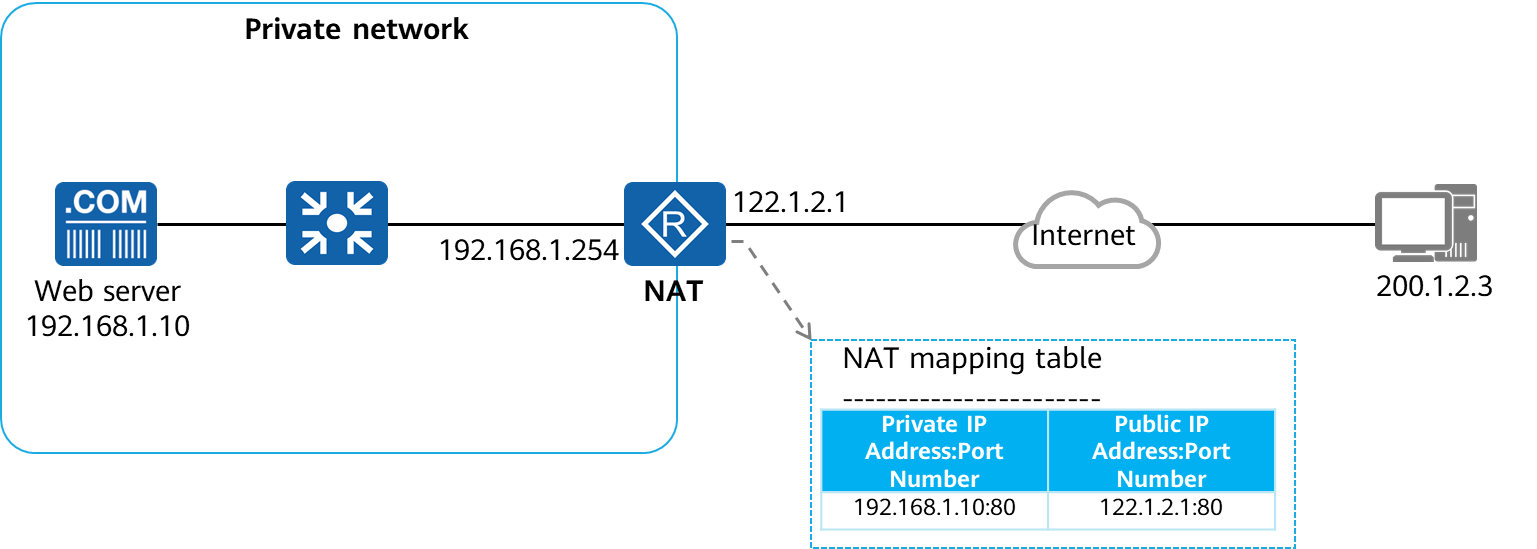
[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]nat outbound 2000

Configure Easy IP on R1 to allow all hosts with private IP addresses on the internal network to access the public network through 122.1.2.1.

## NAT Server

### NAT Server

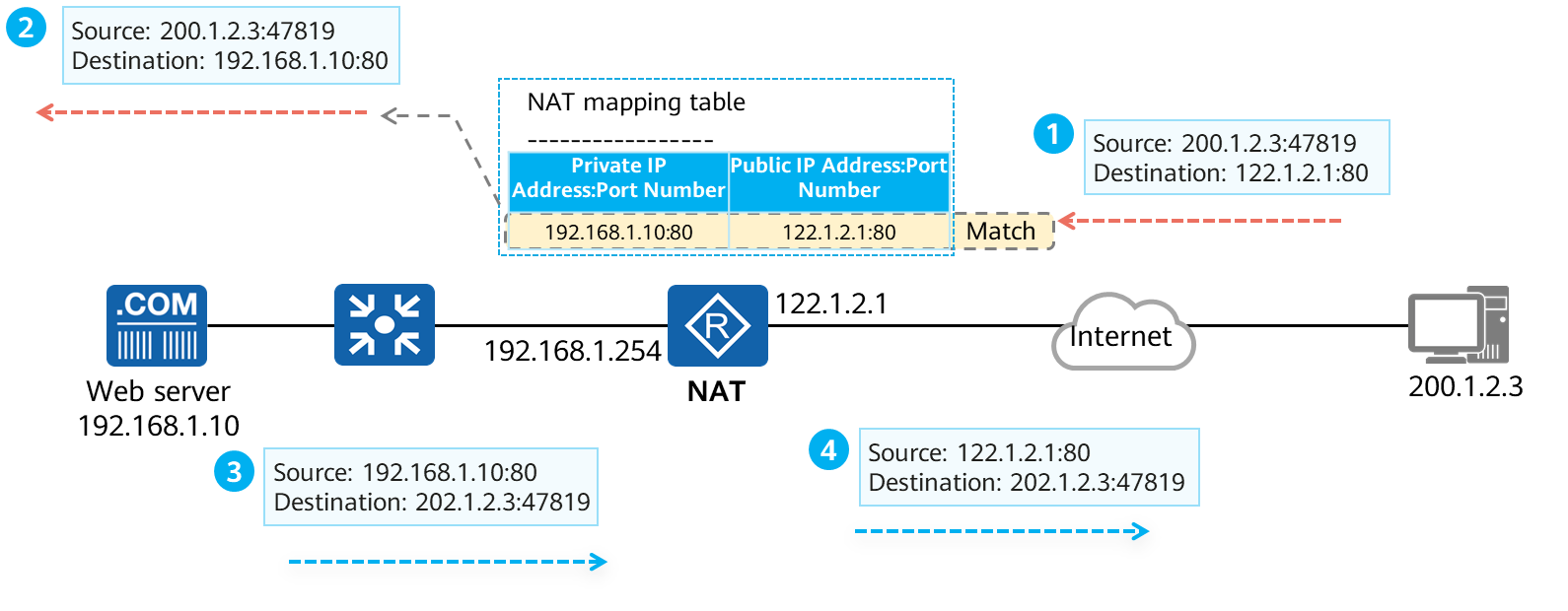


NAT Server

NAT Server: maps an internal server to a public network through a one-to-one mapping between a [public IP address:port number] and a [private IP address:port number]. This function is used when the internal server needs to provide services for the public network.

An external host proactively accesses the [public IP address:port number] to communicate with the internal server.

### NAT Server Example



NAT Server Example

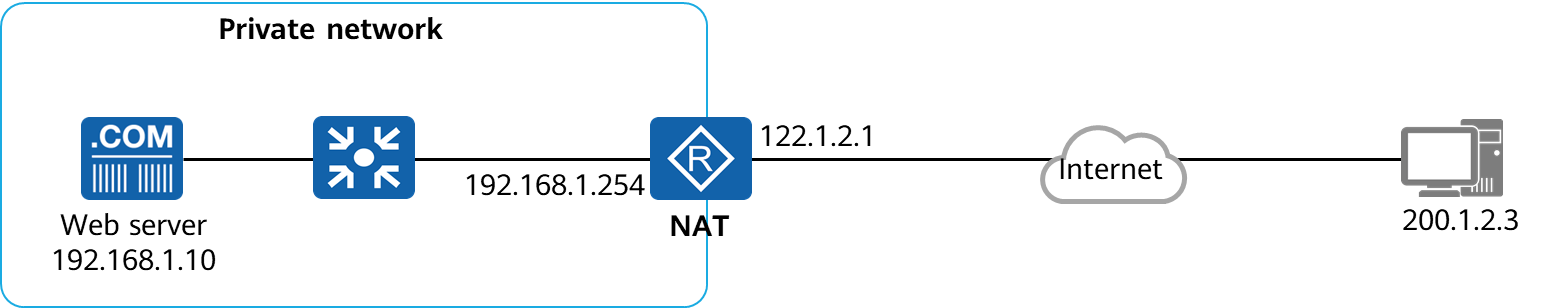
Outbound packet process：

NAT device searches the NAT mapping table for the desired private address:port number based on the public address:port number, and translates the destination address:port number of the IP data packet to the private address:port number.

Inbound packet process：

Reversely translates the source IP address:port number based on the NAT mapping table.

### Example for Configuring NAT Server



Example for Configuring NAT Server

[R1]interface GigabitEthernet0/0/1

[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24

[R1-GigabitEthernet0/0/1]nat server protocol tcp global current-interface www inside 192.168.1.10 8080

Configure NAT Server on R1 to map the internal server's IP address 192.168.1.10 and port number 8080 to the public IP address 122.1.2.1 and port number 80.

## Summary

Using private addresses on private networks and using NAT at the network egress effectively reduce the number of required public IPv4 addresses. NAT effectively alleviates the shortage of public IPv4 addresses.

Dynamic NAT, NAPT, and Easy IP provide source address translation for private network hosts to access the public network.

NAT Server enables internal servers to provide services for public networks.

Static NAT provides one-to-one mapping and supports bidirectional communication.

## Quiz

1. (Single) What is the function of NAT? ( )
2. Save public IP addresses.
3. Improves the routing and forwarding performance.
4. Enhances data transmission security.
5. Prevent computers from being attacked.
6. (Multiple) Which NAT can be used when an enterprise intranet needs to proactively access an external network? ( )
7. Static NAT
8. Dynamic NAT NO-PAT
9. Dynamic NAT NAPT
10. NAT Server
11. (Multiple) Which NAT can be used when an enterprise external network needs to proactively access the internal network? ( )
12. Static NAT
13. Dynamic NAT NO-PAT
14. Dynamic NAT NAPT
15. NAT Server
16. (True or False) Easy IP is a special NAPT, which translates port numbers. ( )
17. True
18. False
19. (True or False) NAPT and NAT Server cannot be deployed on the same device. ( )
20. True
21. False
22. What types of NAT can enable external devices to proactively access an internal server?
23. What are the advantages of NAPT over No-PAT?