Fondamenti di Internet

Network Address Translation

Prof. Gianluca Reali

Foreword

- 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

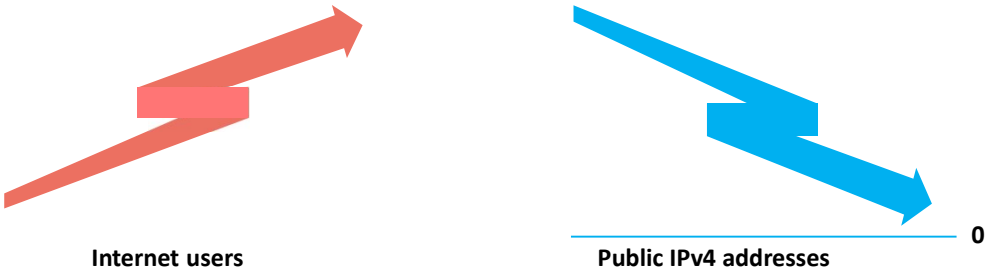
- On completion of this course, you will be able to:
  - Understand the motivation behind NAT.
  - Master NAT classification and implementations.
  - Master NAT selection in different scenarios.

Contents

1. **NAT Overview**
2. Static NAT
3. Dynamic NAT
4. NAPT and Easy IP
5. NAT Server

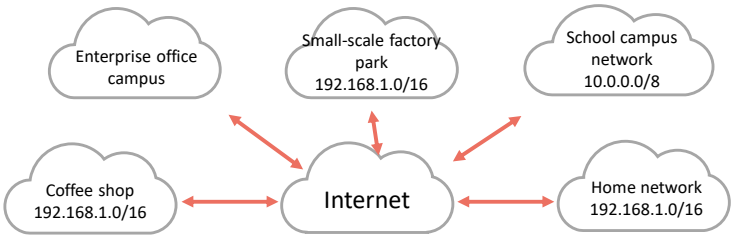
Motivation Behind NAT

- 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.



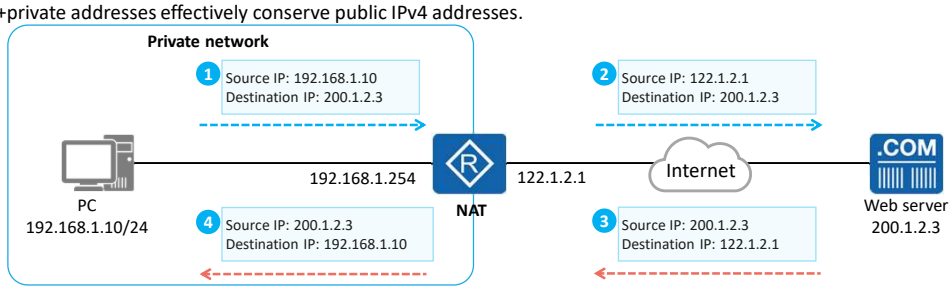
Private IP Addresses

- 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: 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.



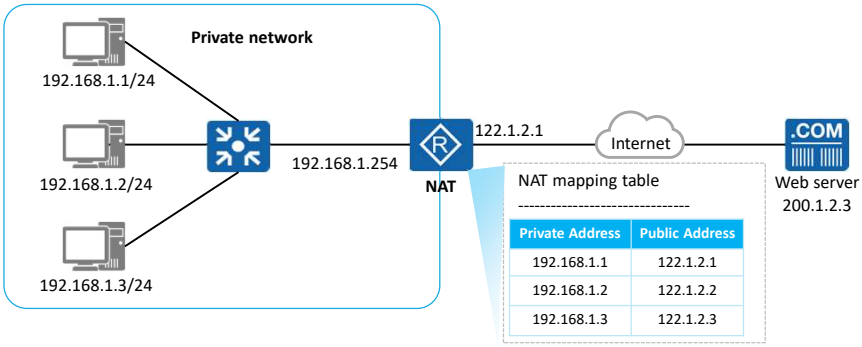
- Because packets with private IP addresses cannot be routed and forwarded on the Internet, IP packets destined for the Internet cannot reach the egress device of the private network due to lack of routes.
- If a host that uses a private IP address needs to access the Internet, NAT must be configured on the network egress device to translate the private source address in the IP data packet into a public source address.

Contents

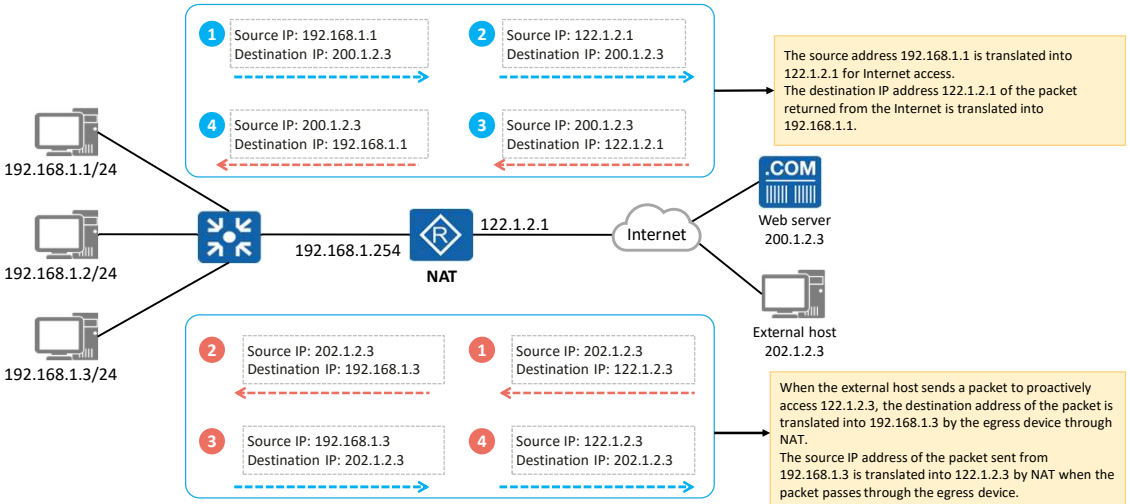
1. NAT Overview
2. **Static NAT**
3. Dynamic NAT
4. NAPT and Easy IP
5. NAT Server

Static NAT Implementation

- 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



Configuring Static NAT

1. 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.

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

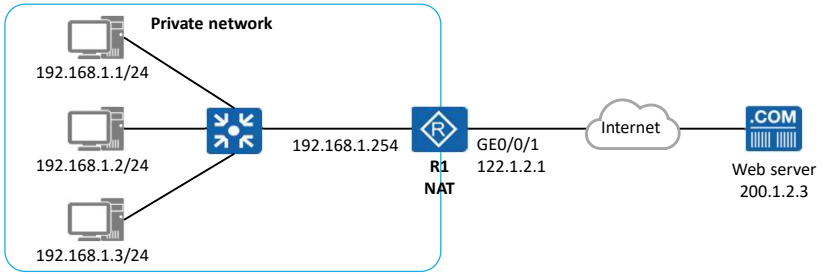
   [Huawei] **nat static global** *{ global-address}* **inside** *{host-address }*

   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



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

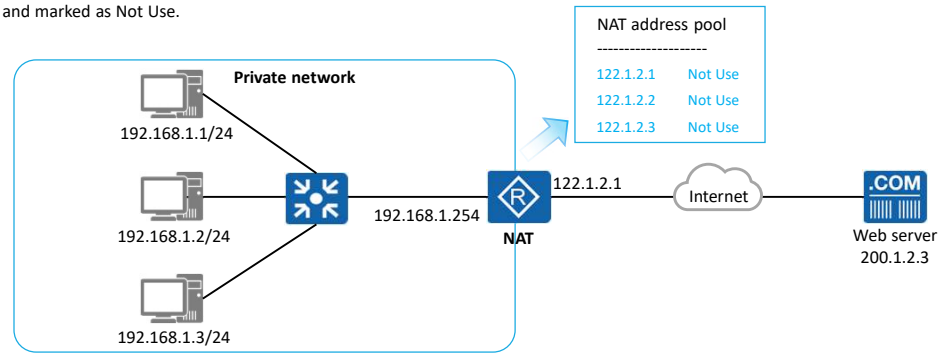
```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.1 inside 192.168.1.1
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.2 inside 192.168.1.2
[R1-GigabitEthernet0/0/1]nat static global 122.1.2.3 inside 192.168.1.3
```

Contents

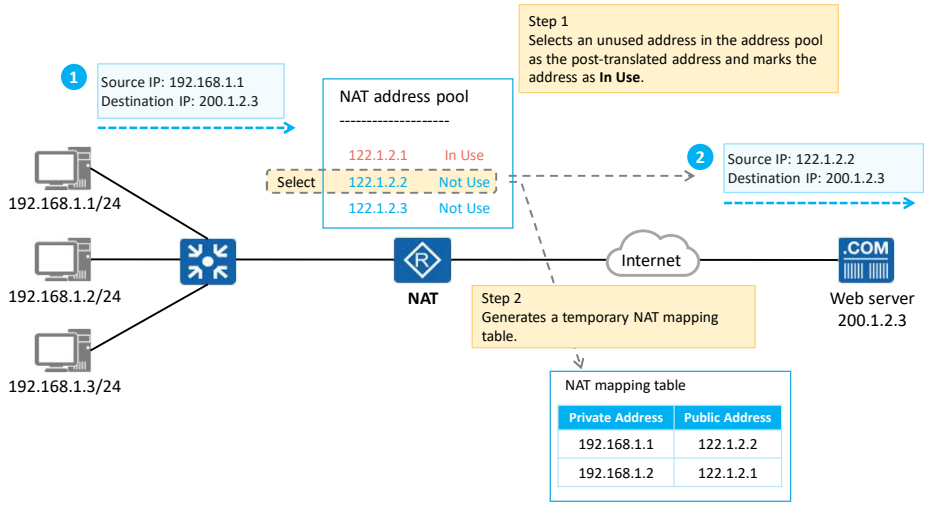
1. NAT Overview
2. Static NAT
3. **Dynamic NAT**
4. NAPT and Easy IP
5. NAT Server

Dynamic NAT Implementation

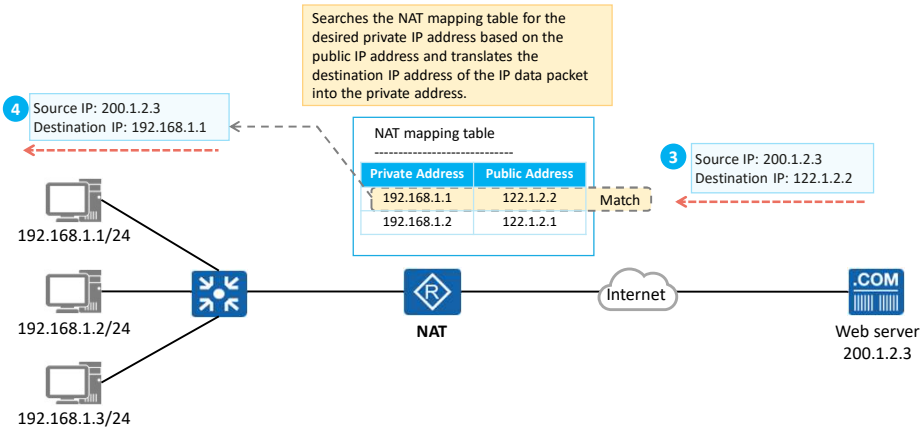
- Dynamic NAT: A private IP address is mapped to a public IP address from a NAT address pool containing a group of public IP addresses. Static NAT strictly maps addresses in one-to-one mode. As a result, even if an internal host is offline for a long time or does not send data, the public address is 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 (1)



Dynamic NAT Example (2)



Configuring Dynamic NAT

1. 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.

2. Configure an ACL rule for NAT.

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

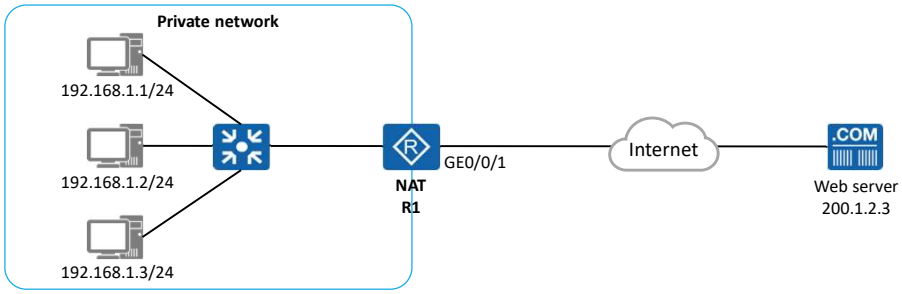
   Configure a basic ACL to match the source address range that requires dynamic NAT.

3. 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



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

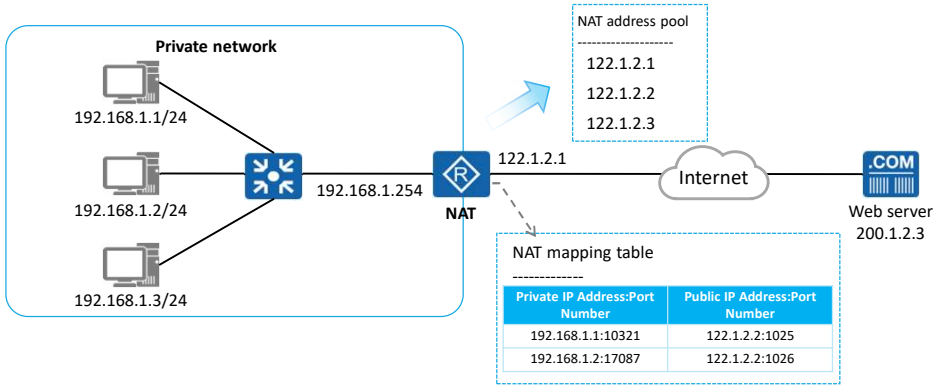
```
[R1]nat address-group 1 122.1.2.1 122.1.2.3
[R1]acl 2000
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000 address-group 1 no-pat
```

Contents

1. NAT Overview
2. Static NAT
3. Dynamic NAT
4. **NAPT and Easy IP**
5. NAT Server

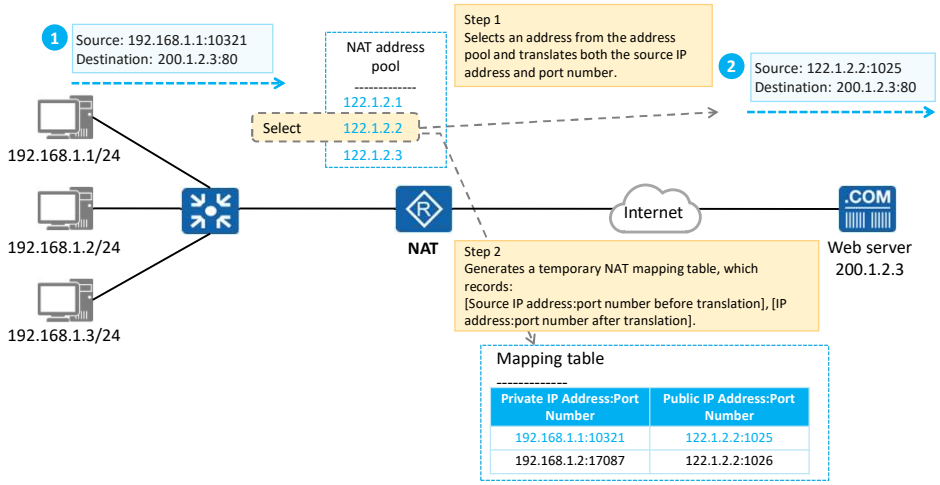
NAPT Implementation

- 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.



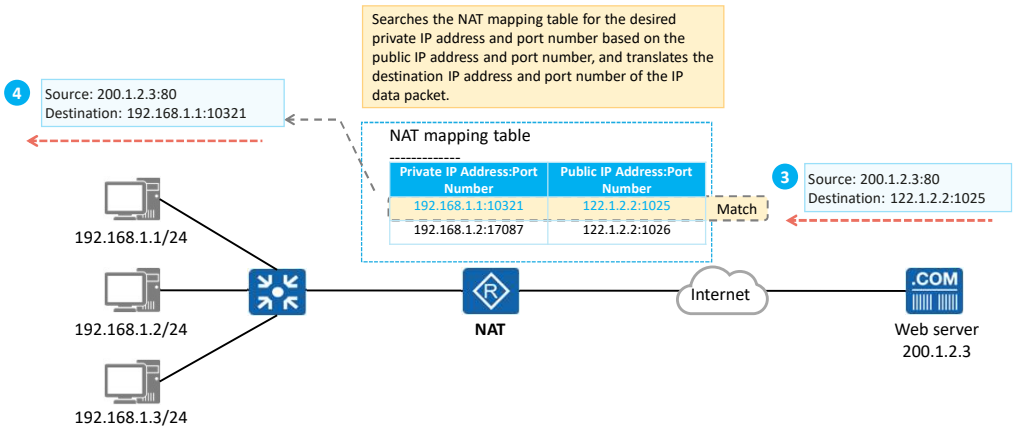
- NAPT enables a public IP address to map multiple private IP addresses through ports. In this mode, both IP addresses and transport-layer ports are translated so that different private addresses with different source port numbers are mapped to the same public address with different source port numbers.

NAPT Example (1)

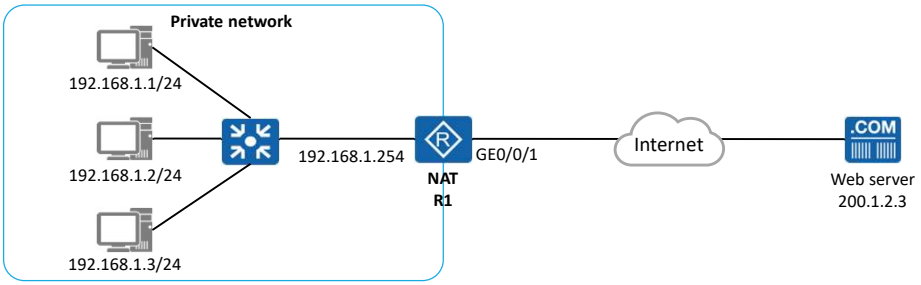


Private IP Address:Port Number	Public IP Address:Port Number
192.168.1.1:10321	122.1.2.2:1025
192.168.1.2:17087	122.1.2.2:1026

NAPT Example (2)



Example for Configuring NAPT

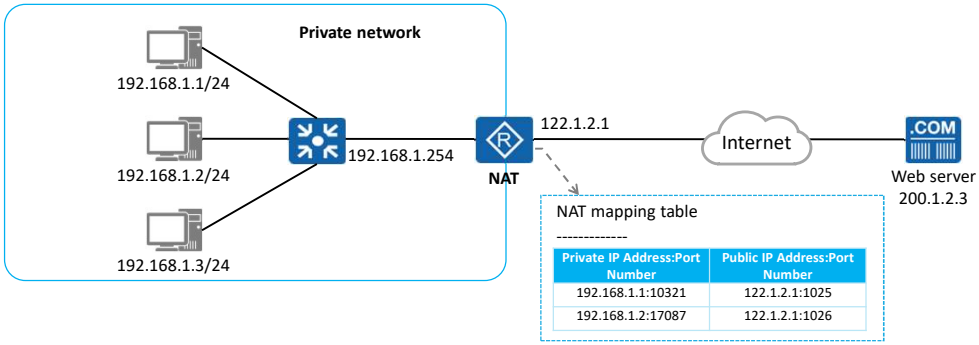


- Configure NAPT on R1 to allow all hosts with private IP addresses on the internal network to access the public network through 122.1.2.1.

```
[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
```

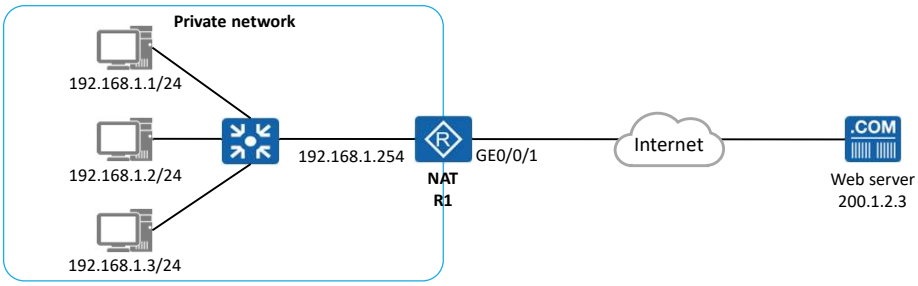
Easy IP

- 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.



- DHCP: Dynamic Host Configuration Protocol
- PPPoE: Point-to-Point Protocol over Ethernet

Example for Configuring Easy IP



- 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.

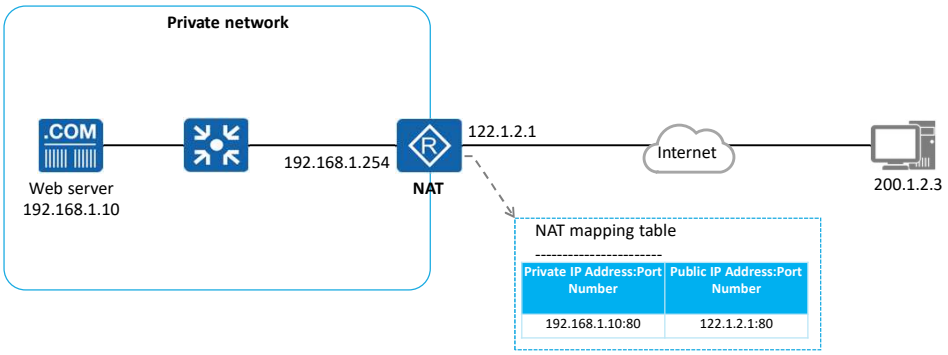
```
[R1-acl-basic-2000]rule 5 permit source 192.168.1.0 0.0.0.255
[R1-acl-basic-2000]quit
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]nat outbound 2000
```

Contents

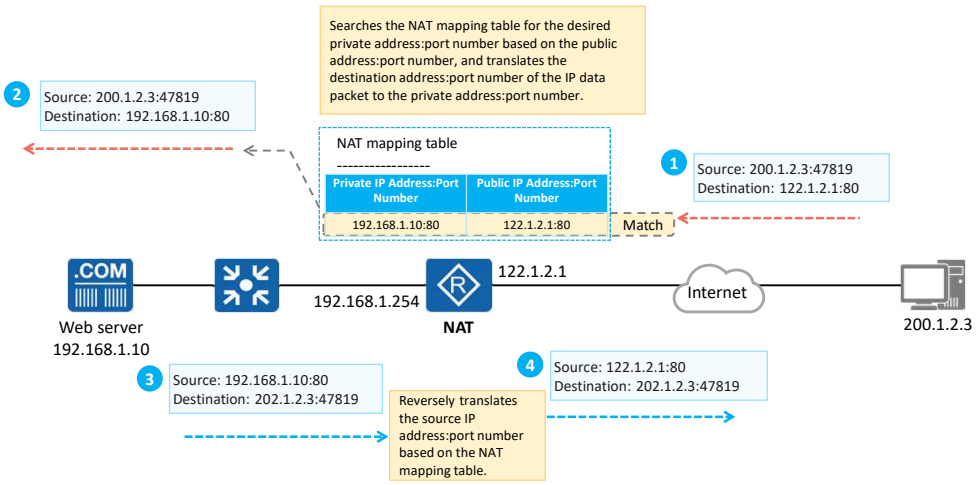
1. NAT Overview
2. Static NAT
3. Dynamic NAT
4. NAPT and Easy IP
5. **NAT Server**

NAT Server

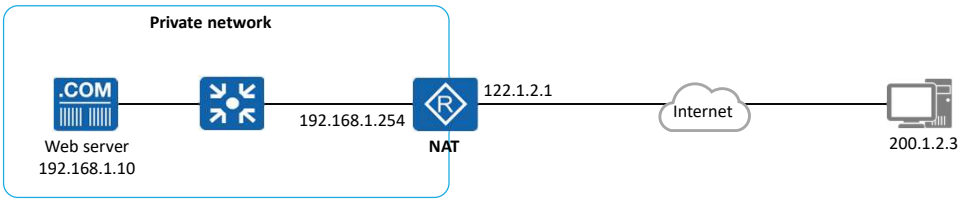
- NAT Server: maps an internal server to a public network through a one-to-one mapping between a [**public IP address:port number**] and a [**private IP address:port number**]. This function is used when the internal server needs to provide services for the public network.
- An external host proactively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



NAT Server Example



Example for Configuring NAT Server

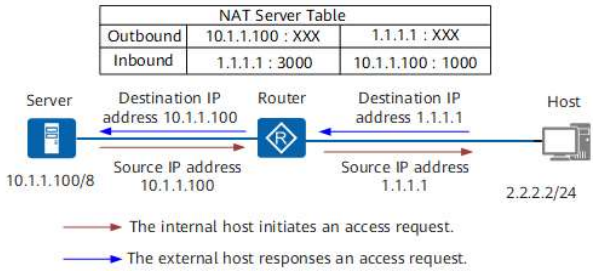


- Configure NAT Server on R1 to map the internal server's IP address 192.168.1.10 and port number 80 to the public IP address 122.1.2.1 and port number 8080.

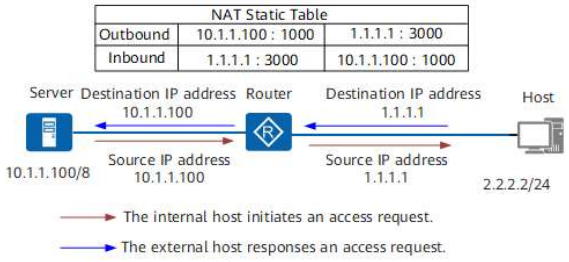
```
[R1]interface GigabitEthernet0/0/1
[R1-GigabitEthernet0/0/1]ip address 122.1.2.1 24
[R1-GigabitEthernet0/0/1]nat server protocol tcp global 122.1.2.1 www inside 192.168.1.10 8080
```

Difference between NAT Static and NAT Server

For the access **from the public network to the private network**, the NAT server and NAT static modes are the same. For the access **from the private network to the public network**, the NAT server mode translates only the IP address, while the NAT static mode translates both the IP address and port.



For the access from the private network to the public network, the When the NAT server proactively accesses the Internet, NAT server mode translates only the IP address, regardless of the port number.



For the access from the private network to the public network, the NAT static mode translates both IP address and port.

The enterprise requires that **private users** can access the **public server** and **public users** can access the **private server**.

If both the NAT server and Easy IP functions are configured on the router, since the NAT server mode translates only the IP address for the access from the private network to the public network, flow tables may fail to be established. In this case, you are advised to change NAT server to NAT static.