# Лабораторная работа Настройка NAT

### Общая информация

#### О лабораторной работе

Преобразование сетевых адресов (Network Address Translation, NAT) — механизм, позволяющий преобразовать IP-адрес в заголовке IP-пакета в другой IP-адрес. В качестве плана транзитной сети NAT позволяет повторно использовать адреса, чтобы решить проблему нехватки IPv4-адресов. Помимо этого, NAT дает следующие преимущества:

* Обеспечивает защиту частных сетей от внешних атак.
* Обеспечивает и контролирует связь между частными и общедоступными сетями.

С помощью данной лабораторной работы вы научитесь настраивать механизм NAT и поймете принцип его работы.

#### Цели

Лабораторная работа помогает получить практические навыки по изучению следующих тем:

* Настройка динамического NAT
* Настройка Easy IP
* Настройка NAT-сервера

#### Топология сети

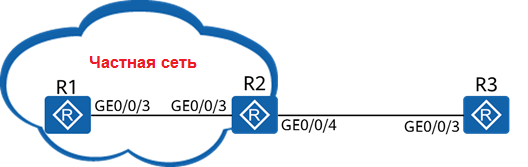
Для решения проблемы нехватки адресов IPv4 предприятия, как правило, используют частные адреса IPv4. Однако корпоративная сеть должна предоставлять доступ сотрудникам к общедоступной сети и услуги внешним пользователям. В этом случае необходимо настроить NAT в соответствии с приведенными выше требованиями.

Сеть между маршрутизаторами R1 и R2 является интрасетью и использует частные адреса IPv4.

R1 выполняет функции клиента, а R2 является шлюзом для R1 и граничным маршрутизатором, подключенным к общедоступной сети.

R3 имитирует общедоступную сеть.

Топология сети для конфигурирования NAT, используемая в данной лабораторной работе



### Лабораторная работа

#### План работы

Настройка динамического NAT.

Настройка Easy IP.

Настройка сервера NAT.

#### Процедура конфигурирования

Настройте основные параметры.

# Настройте IP-адреса и маршруты.

[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

# Настройте функцию Telnet на маршрутизаторах R1 и R3 для последующей проверки.

[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

# Проверьте возможность установления связи.

[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

У маршрутизатора R1 нет связи с R3, потому что на R3 не настроен маршрут к адресу 192.168.1.0/24.

Более того, на R3 нельзя настраивать маршруты в частные сети.

Предприятие получает общедоступные IP-адреса в диапазоне от 1.2.3.10 до 1.2.3.20, поэтому ему требуется функция динамического NAT.

# Настройте пул адресов NAT.

[R2]nat address-group 1 1.2.3.10 1.2.3.20

С помощью команды **nat address-group** можно настроить пул адресов NAT. В данном примере пул адресов имеет номер 1. Пул адресов должен быть набором последовательных IP-адресов. При достижении внутренними пакетами данных границы частной сети частные IP-адреса источников будут преобразовываться в общедоступные IP-адреса.

# Настройте ACL.

[R2]acl 2000

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

# Настройте динамический NAT на GigabitEthernet0/0/4 маршрутизатора R2.

[R2]interface GigabitEthernet 0/0/4

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

Команда **nat outbound** позволяет установить привязку ACL к пулу адресов NAT.   
IP-адреса пакетов, соответствующих списку ACL, будут преобразовываться в адреса из пула адресов. Если в пуле достаточно адресов, можно добавить аргумент **no-pat**, чтобы включить однозначное преобразование адресов. В этом случае будут преобразовываться только IP-адреса пакетов данных, а порты преобразовываться не будут.

# Проверьте возможность установления связи.

[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

# Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

<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>

# Выведите на экран таблицу сеансов NAT на R2.

[R2]display nat session all

NAT Session Table Information:

Protocol : TCP(6)

SrcAddr Port Vpn : 192.168.1.1 62185 *//IP-адрес и порт источника перед преобразованием NAT*

DestAddr Port Vpn : 1.2.3.254 23

NAT-Info

New SrcAddr : 1.2.3.11 *//IP-адрес источника после преобразования NAT*

New SrcPort : 49149 *//Порт источника после преобразования NAT*

New DestAddr : ----

New DestPort : ----

Total : 1

Несмотря на то, что R3 не имеет маршрута к R1, он передает данные на преобразованный адрес источника 1.2.3.11. После получения данных R2 преобразует адрес источника в адрес R1 на основе данных в таблице сеансов NAT и передает данные. Таким образом, R1 может инициировать доступ к R3.

Если IP-адрес GigabitEthernet0/0/4 на R2 назначается динамически (например, через DHCP или PPPoE), необходимо настроить Easy IP.

# Удалите конфигурацию, созданную на предыдущем шаге.

[R2]interface GigabitEthernet 0/0/4

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

# Настройте Easy IP.

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

# Проверьте возможность установления связи.

[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

# Выполните вход с R1 на R3 через Telnet, чтобы смоделировать трафик TCP.

[R2]display nat session all

NAT Session Table Information:

Protocol : TCP(6)

SrcAddr Port Vpn : 192.168.1.1 58546 *//IP-адрес и порт источника перед преобразованием NAT*

DestAddr Port Vpn : 1.2.3.4 23

NAT-Info

New SrcAddr : 1.2.3.4 //*IP-адрес источника после преобразования NAT, то есть, адрес GigabitEthernet 0/0/4 на R2*

New SrcPort : 49089 *//Порт источника после преобразования NAT*

New DestAddr : ----

New DestPort : ----

Total : 1

R3 должен предоставлять сетевые услуги (в данном примере telnet) для пользователей в общедоступной сети. Поскольку R3 не имеет общедоступного   
IP-адреса, необходимо настроить сервер NAT на исходящем интерфейсе R2.

# Настройте сервер NAT на 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

Команда **nat server** позволяет определить таблицу сопоставления внутренних серверов, чтобы внешние пользователи могли получать доступ к внутренним серверам через преобразование адресов и портов. Можно настроить внутренний сервер так, чтобы пользователи внешней сети могли инициировать доступ к внутреннему серверу. Когда хост во внешней сети отправляет запрос на соединение на общедоступный адрес (глобальный адрес) внутреннего сервера NAT, сервер NAT преобразует адрес назначения, содержащийся в запросе, в частный адрес (внутренний адрес) и пересылает запрос на сервер в частной сети.

# Выполните вход с R3 на R1 через Telnet.

<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>

# Выведите на экран таблицу сеансов NAT на 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 *//IP-адрес и порт назначения перед преобразованием NAT*

NAT-Info

New SrcAddr : ----

New SrcPort : ----

New DestAddr : 192.168.1.1 *//IP-адрес назначения после преобразования NAT, то есть, IP-адрес маршрутизатора R1*

New DestPort : 23 *//Порт назначения после преобразования NAT*

Total : 1

----Конец

### Проверка

Подробности данной операции здесь не приводятся.

### Справочные конфигурации

Конфигурация на 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

Конфигурация на 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

Конфигурация на 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

### Вопросы

После настройки сервера NAT должны ли порты назначения до преобразования соответствовать портам назначения после преобразования?