

Лабораторная работа № 12

Настройка NAT

Хватов Максим Григорьевич

Содержание

1	Цель работы	4
2	Задание	5
3	Выполнение лабораторной работы	6
4	Выводы	13
5	Контрольные вопросы	14

Список иллюстраций

3.1	Первоначальная настройка маршрутизатора provider-gw-1	6
3.2	Первоначальная настройка коммутатора provider-sw-1	6
3.3	Настройка интерфейсов маршрутизатора provider-gw-1	7
3.4	Настройка интерфейсов коммутатора provider-sw-1	7
3.5	Настройка интерфейсов коммутатора provider-sw-1	8
3.6	Настройка интерфейсов маршрутизатора msk-donskaya-gw-1 . . .	8
3.7	Проверка доступности маршрутизатора	9
3.8	Настройка роута по умолчанию	9
3.9	Попытка пропинговать 198.51.100.1	9
3.10	Настройка пула адресов	10
3.11	Настройка PAT	10
3.12	Пинг	10
3.13	Пинг	11
3.14	Пинг	11
3.15	www.yandex.ru	11
3.16	198.51.100.2	12

1 Цель работы

Приобрести практические навыки по настройке доступа локальной сети к внешней сети посредством NAT.

2 Задание

1. Сделать первоначальную настройку маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера: задать имя, настроить доступ по паролю и т.п.
2. Настроить интерфейсы маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера.
3. Настроить интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера.
4. Настроить на маршрутизаторе сети «Донская» NAT с правилами.
5. Настроить доступ из внешней сети в локальную сеть организации.
6. Проверить работоспособность заданных настроек.
7. При выполнении работы необходимо учитывать соглашение об именовании.

3 Выполнение лабораторной работы

Проведем первоначальную настройку маршрутизатора provider-gw-1 (рис. 3.1).
Зададим имя, настроим доступ по паролю.

```
provider-mgkhvatov-gw-1>enable
provider-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
provider-mgkhvatov-gw-1(config)#line vty 0 4
provider-mgkhvatov-gw-1(config-line)#password cisco
provider-mgkhvatov-gw-1(config-line)#login
provider-mgkhvatov-gw-1(config-line)#exit
provider-mgkhvatov-gw-1(config)#line console 0
provider-mgkhvatov-gw-1(config-line)#password cisco
provider-mgkhvatov-gw-1(config-line)#login
provider-mgkhvatov-gw-1(config-line)#exit
provider-mgkhvatov-gw-1(config)#enable secret cisco
provider-mgkhvatov-gw-1(config)#service password-encryption
provider-mgkhvatov-gw-1(config)#username admin privilege 1 secret cisco
provider-mgkhvatov-gw-1(config)#^Z
provider-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]
```

Рис. 3.1: Первоначальная настройка маршрутизатора provider-gw-1

Проведем первоначальную настройку коммутатора provider-sw-1 (рис. 3.2).
Зададим имя, настроим доступ по паролю.

```
provider-mgkhvatov-gw-1(config)#interface f0/0
provider-mgkhvatov-gw-1(config-if)#no shutdown

provider-mgkhvatov-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0, changed state to up

provider-mgkhvatov-gw-1(config-if)#exit
provider-mgkhvatov-gw-1(config)#interface f0/0.4
provider-mgkhvatov-gw-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/0.4, changed state to up

provider-mgkhvatov-gw-1(config-subif)#encapsulation dot1Q 4
provider-mgkhvatov-gw-1(config-subif)#ip address 190.51.100.1 255.255.255.240
provider-mgkhvatov-gw-1(config-subif)#descriprion msk-donskaya-mgkhvatov
^
% Invalid input detected at '^' marker.

provider-mgkhvatov-gw-1(config-subif)#description msk-donskaya-mgkhvatov
provider-mgkhvatov-gw-1(config-subif)#exit
```

Рис. 3.2: Первоначальная настройка коммутатора provider-sw-1

Проведем настройку интерфейсов маршрутизатора provider-gw-1 (рис. 3.3). Поднимем интерфейс f0/0, создадим интерфейс f0/0.4 для 4 vlan и зададим ip-адрес, поднимем интерфейс f0/1.

```

provider-mgkhvatov-gw-1(config)#interface f0/1
provider-mgkhvatov-gw-1(config-if)#no shutdown
^
% Invalid input detected at '^' marker.

provider-mgkhvatov-gw-1(config-if)#no shutdown

provider-mgkhvatov-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

provider-mgkhvatov-gw-1(config-if)#ip address 192.0.2.1 255.255.255.0
provider-mgkhvatov-gw-1(config-if)#description internet
provider-mgkhvatov-gw-1(config-if)#exit
provider-mgkhvatov-gw-1(config)#exit
provider-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.3: Настройка интерфейсов маршрутизатора provider-gw-1

Проведем настройку интерфейсов коммутатора provider-sw-1 (рис. 3.5). Сделаем порты f0/1 и f0/2 транковыми, зададим 4 vlan с именем nat.

```

provider-mgkhvatov-sw-1>en
provider-mgkhvatov-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
provider-mgkhvatov-sw-1(config)#line vty 0 4
provider-mgkhvatov-sw-1(config-line)#password cisco
provider-mgkhvatov-sw-1(config-line)#login
provider-mgkhvatov-sw-1(config-line)#exit
provider-mgkhvatov-sw-1(config)#line console 0
provider-mgkhvatov-sw-1(config-line)#password cisco
provider-mgkhvatov-sw-1(config-line)#login
provider-mgkhvatov-sw-1(config-line)#exit
provider-mgkhvatov-sw-1(config)#enable secret cisco
provider-mgkhvatov-sw-1(config)#service password-encryption
provider-mgkhvatov-sw-1(config)#username admin privilege 1 secret cisco
provider-mgkhvatov-sw-1(config)#^Z
provider-mgkhvatov-sw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-mgkhvatov-sw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.4: Настройка интерфейсов коммутатора provider-sw-1

```

provider-mgkhvatov-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
provider-mgkhvatov-sw-1(config)#interface f0/1
^
% Invalid input detected at '^' marker.

provider-mgkhvatov-sw-1(config)#interface f0/1
provider-mgkhvatov-sw-1(config-if)#switchport mode trunk

provider-mgkhvatov-sw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

provider-mgkhvatov-sw-1(config-if)#interface f0/2
provider-mgkhvatov-sw-1(config-if)#switchport mode trunk

provider-mgkhvatov-sw-1(config-if)#
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to down

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/2, changed state to up

provider-mgkhvatov-sw-1(config-if)#^Z
provider-mgkhvatov-sw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-mgkhvatov-sw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.5: Настройка интерфейсов коммутатора provider-sw-1

Проведем настройку интерфейсов маршрутизатора msk-donskaya-gw-1. Поднимем интерфейс f0/1, создадим интерфейс f0/1.4 для 4 vlan и зададим ip-адрес.

```

msk-donskaya-mgkhvatov-gw-1>en
Password:
msk-donskaya-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#interface f0/1
msk-donskaya-mgkhvatov-gw-1(config-if)#no shutdown

msk-donskaya-mgkhvatov-gw-1(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1, changed state to up

msk-donskaya-mgkhvatov-gw-1(config-if)#^Z
msk-donskaya-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#interface f0/1.4
msk-donskaya-mgkhvatov-gw-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.4, changed state to up

msk-donskaya-mgkhvatov-gw-1(config-subif)#encapsulation dot1Q 4
msk-donskaya-mgkhvatov-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-mgkhvatov-gw-1(config-subif)#description internet
msk-donskaya-mgkhvatov-gw-1(config-subif)#^Z
msk-donskaya-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.6: Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

Пропингую адрес 192.0.2.1. Пинг проходит успешно


```
Cisco Packet Tracer SERVER Command Line 1.0
C:\>ping 192.0.2.1

Pinging 192.0.2.1 with 32 bytes of data:

Reply from 192.0.2.1: bytes=32 time<1ms TTL=255
Reply from 192.0.2.1: bytes=32 time<1ms TTL=255
Reply from 192.0.2.1: bytes=32 time<1ms TTL=255
Reply from 192.0.2.1: bytes=32 time<1ms TTL=255

Ping statistics for 192.0.2.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

Рис. 3.7: Проверка доступности маршрутизатора

Назначу роут по умолчанию для gw-1.

```
msk-donskaya-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1
msk-donskaya-mgkhvatov-gw-1(config)#^Z
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]
```

Рис. 3.8: Настройка роута по умолчанию

Попытка пропинговать устройство 198.51.100.1 оказывается неудачной и для этого я разорвал связь, и тогда все заработало.

```
msk-donskaya-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#ip nat pool main-pool 198.51.100.2 198.51.100.14 netmask 255.255.255.240
msk-donskaya-mgkhvatov-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark dk
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark departments
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.14 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#^Z
msk-donskaya-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-mgkhvatov-gw-1#
```

Рис. 3.9: Попытка пропинговать 198.51.100.1

```

msk-donskaya-mgkhvatov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#ip nat pool main-pool 198.51.100.2 198.51.100.14 netmask 255.255.255.240
msk-donskaya-mgkhvatov-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark dk
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark departments
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.14 eq 80
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-mgkhvatov-gw-1(config-ext-nacl)#Z
msk-donskaya-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-mgkhvatov-gw-1#

```

Рис. 3.10: Настройка пула адресов

Настроим Port Address Translation (PAT) на субинтерфейсах маршрутизатора с территории Донская (рис. 3.11).

```

msk-donskaya-mgkhvatov-gw-1#cont t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80 198.51.100.2 80
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 80 198.51.100.3 20
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 198.51.100.2 20
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 198.51.100.3 21
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 198.51.100.3 20
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25 198.51.100.4 25
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.0.4 110 198.51.100.4 110
msk-donskaya-mgkhvatov-gw-1(config)#ip nat inside source static tcp 10.128.6.200 3389 198.51.100.10 3389
msk-donskaya-mgkhvatov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-mgkhvatov-gw-1#wr mem
Building configuration...
[OK]

```

Рис. 3.11: Настройка PAT

Добавил ноутбук laptop-ext в схему в область internet. Проверка доступности к маршрутизаторам от ноутбука админ. Все доступны.

```

C:\>ping 198.51.100.1

Pinging 198.51.100.1 with 32 bytes of data:

Reply from 198.51.100.1: bytes=32 time=14ms TTL=254
Reply from 198.51.100.1: bytes=32 time<1ms TTL=254
Reply from 198.51.100.1: bytes=32 time<1ms TTL=254

Ping statistics for 198.51.100.1:
    Packets: Sent = 3, Received = 3, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 14ms, Average = 4ms

```

Рис. 3.12: Пинг

```

C:\>ping 198.51.100.2

Pinging 198.51.100.2 with 32 bytes of data:

Reply from 198.51.100.2: bytes=32 time=1ms TTL=255
Reply from 198.51.100.2: bytes=32 time<1ms TTL=255
Reply from 198.51.100.2: bytes=32 time<1ms TTL=255
Reply from 198.51.100.2: bytes=32 time<1ms TTL=255

Ping statistics for 198.51.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

```

Рис. 3.13: Пинг

```

C:\>ping 192.0.2.11

Pinging 192.0.2.11 with 32 bytes of data:

Request timed out.
Reply from 192.0.2.11: bytes=32 time<1ms TTL=126
Reply from 192.0.2.11: bytes=32 time<1ms TTL=126
Reply from 192.0.2.11: bytes=32 time=4ms TTL=126

Ping statistics for 192.0.2.11:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 4ms, Average = 1ms

```

Рис. 3.14: Пинг

Проверил возможность выхода в интрнет после всех настроек

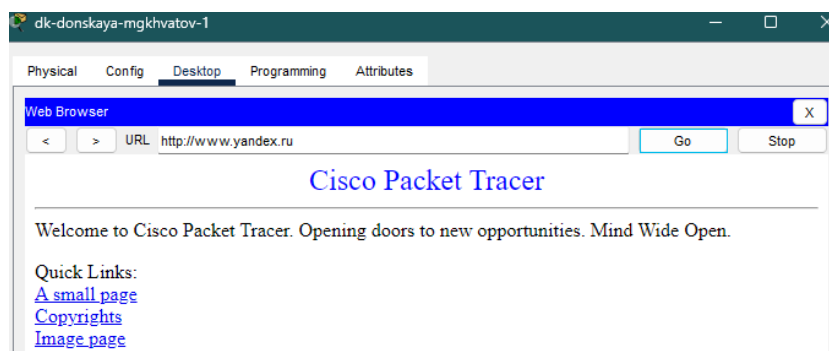


Рис. 3.15: www.yandex.ru

Страница отобразилась. Также проверил через браузер на устройстве laptop-ext доступ к адресу 198.51.100.2, он оказался доступен тоже.

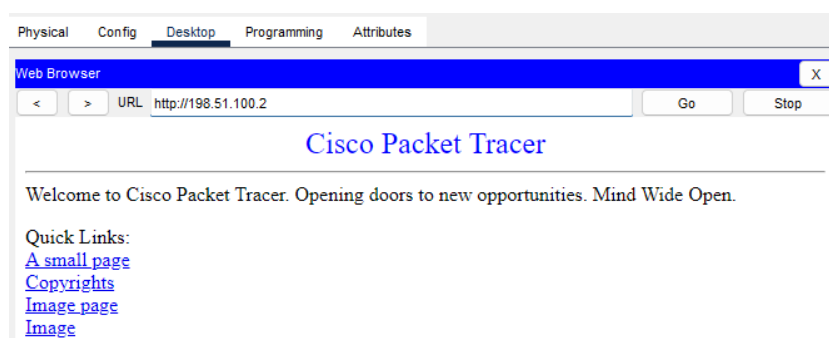


Рис. 3.16: 198.51.100.2

4 Выводы

В результате выполнения данной лабораторной работы я приобрел практические навыки по настройке доступа локальной сети к внешней сети посредством NAT.

5 Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)?

Идея NAT заключается в том, чтобы осуществлять перевод частного локального IP-адреса в общедоступный глобальный IP-адрес и наоборот. Это необходимо для обеспечения доступа к Интернету локальным узлам, использующим частные адреса.

Наличие NAT в сети организации позволяет экономить публичные IP-адреса и повышать безопасность защитой внутренних устройств от прямого доступа извне.

2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?

Как правило, граничный маршрутизатор настроен для NAT, то есть маршрутизатор, который имеет один интерфейс в локальной (внутренней, inside) сети и один интерфейс в глобальной (внешней, outside) сети. Когда пакет проходит за пределы локальной (inside) сети, NAT преобразует локальный (частный, private) IP-адрес в глобальный (публичный, public) IP-адрес. Когда пакет входит в локальную сеть, глобальный (public) IP-адрес преобразуется в локальный (private) IP-адрес. Граничный маршрутизатор выступает в роли шлюза между внутренней корпоративной сетью и внешней сетью, например, Интернетом.

3. Можно ли применить Cisco IOS NAT к субинтерфейсам?

Да. Преобразования NAT источника или назначения могут применяться к любому интерфейсу или подинтерфейсу с IP-адресом (включая интерфейсы программы набора номера).

4. Что такое пулы IP NAT?

Пул NAT — это набор из одного или нескольких общедоступных IPv4-адресов, которые используются в маршрутизаторе NAT.

При отправке трафика устройством из внутренней сети во внешнюю сеть маршрутизатор преобразует его внутренний IPv4-адрес в один из адресов, входящих в состав пула.

В результате действия такого механизма весь исходящий из сети трафик внешние устройства «видят» с общедоступным адресом IPv4, который можно назвать NAT IP-адресом.

5. Что такое статические преобразования NAT?

Статическое преобразование сетевых адресов (NAT) выполняет взаимно однозначное преобразование внутренних IP-адресов во внешние. Это позволяет преобразовать IP-адрес внутренней сети во внешний IP-адрес. Статический NAT позволяет устанавливать соединения как внутренним, так и внешним системам, например, хостам Internet.