

Отчёт по лабораторной работе №12

Настройка NAT

Козлов Всеволод Павлович НФИбд-02-22

Содержание

1	Цель работы	5
2	Задание	6
3	Выполнение лабораторной работы	7
4	Выводы	15
5	Контрольные вопросы	16
6	Список литературы	18

Список иллюстраций

3.1	Первоначальная настройка маршрутизатора provider-gw-1	7
3.2	Настройка интерфейсов маршрутизатора provider-gw-1	8
3.3	Первоначальная настройка коммутатора provider-sw-1	8
3.4	Настройка интерфейсов коммутатора provider-sw-1	9
3.5	Настройка интерфейсов маршрутизатора msk-donskaya-gw-1	9
3.6	Пул адресов для NAT	10
3.7	Настройка списка доступа для NAT	10
3.8	Настройка сетей	10
3.9	Настройка NAT	11
3.10	Проверка доступности маршрутизаторов	11
3.11	Проверка доступности www.yandex.ru	12
3.12	Настройка доступа из Интернета (WWW-сервер, Файловый сервер)	12
3.13	Настройка доступа из Интернета (WWW-сервер, Файловый сервер)	12
3.14	Добавление ноутбука к internet	13
3.15	Проверка доступа по ftp	13
3.16	Проверка доступа к веб-серверу	14

Список таблиц

1 Цель работы

Приобретение практических навыков 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, указанными в разделе 12.2.
5. Настроить доступ из внешней сети в локальную сеть организации, как указано в разделе 12.2.
6. Проверить работоспособность заданных настроек.
7. При выполнении работы необходимо учитывать соглашение об именовании.

3 Выполнение лабораторной работы

Провел первоначальную настройку маршрутизатора provider-gw-1 (рис. 3.1)

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

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

Провел настройку маршрутизатора provider-gw-1 (рис. 3.2)

```

%SYS-5-CONFIG_I: Configured from console by console
provider-vpkozlov-gw-1(config)#interface f0/0
provider-vpkozlov-gw-1(config-if)#no shutdown

provider-vpkozlov-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-vpkozlov-gw-1(config-if)#exit
provider-vpkozlov-gw-1(config)#exit
provider-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
provider-vpkozlov-gw-1(config)#interface f0/0.4
provider-vpkozlov-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-vpkozlov-gw-1(config-subif)#encapsulation dot1Q 4
provider-vpkozlov-gw-1(config-subif)#ip address 190.51.100.1 255.255.255.240
provider-vpkozlov-gw-1(config-subif)#description mask-donskaya
provider-vpkozlov-gw-1(config-subif)#exit
provider-vpkozlov-gw-1(config)#interface f0/1
provider-vpkozlov-gw-1(config-if)#no shutdown

provider-vpkozlov-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-vpkozlov-gw-1(config-if)#ip address 192.0.2.1 255.255.255.0
provider-vpkozlov-gw-1(config-if)#description internet
provider-vpkozlov-gw-1(config-if)#exit
provider-vpkozlov-gw-1(config)#exit
provider-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]

```

Рис. 3.2: Настройка интерфейсов маршрутизатора provider-gw-1

Провел первоначальную настройку коммутатора provider-sw-1 (рис. 3.3)

```

provider-sw-1#configure terminal
provider-sw-1(config)#line vty 0 4
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit
provider-sw-1(config)#line console 0
provider-sw-1(config-line)#password cisco
provider-sw-1(config-line)#login
provider-sw-1(config-line)#exit
% Invalid input detected at '^' marker.
provider-sw-1(config-line)#exit
provider-sw-1(config)#enable secret cisco
provider-sw-1(config)#service password-encryption
% Invalid input detected at '^' marker.
provider-sw-1(config)#service password-encryption
provider-sw-1(config)#username admin privilege 15 secret cisco
provider-sw-1(config)#

```

Рис. 3.3: Первоначальная настройка коммутатора provider-sw-1

Провел настройку интерфейсов коммутатора provider-sw-1 (рис. 3.4)


```

Enter configuration commands, one per line. End with CNTL/Z.
provider-vpkozlov-sw-1(config)#interface f0/1
provider-vpkozlov-sw-1(config-if)#switchport mode trunk

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

provider-vpkozlov-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-vpkozlov-sw-1(config-if)#exit
provider-vpkozlov-sw-1(config)#exit
provider-vpkozlov-sw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
provider-vpkozlov-sw-1#vlan 4
^
% Invalid input detected at '^' marker.

provider-vpkozlov-sw-1#en
provider-vpkozlov-sw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
provider-vpkozlov-sw-1(config)#vlan 4
provider-vpkozlov-sw-1(config-vlan)#name nat
provider-vpkozlov-sw-1(config-vlan)#exit
provider-vpkozlov-sw-1(config)#interface vlan4
provider-vpkozlov-sw-1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

provider-vpkozlov-sw-1(config-if)#no shutdown
provider-vpkozlov-sw-1(config-if)#exit
provider-vpkozlov-sw-1(config)#exit

```

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

Настройка интерфейсов маршрутизатора msk-donskaya-gw-1 (рис. 3.5)

```

msk-donskaya-vpkozlov-gw-1(config)#
msk-donskaya-vpkozlov-gw-1(config)#interface f0/1
msk-donskaya-vpkozlov-gw-1(config-if)#no shutdown
msk-donskaya-vpkozlov-gw-1(config-if)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/1.4
msk-donskaya-vpkozlov-gw-1(config-subif)#encapsulation dot1q 4
msk-donskaya-vpkozlov-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-vpkozlov-gw-1(config-subif)#description internet
msk-donskaya-vpkozlov-gw-1(config-subif)#
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#en
msk-donskaya-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkozlov-gw-1(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#

```

Рис. 3.5: Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

Настроил пул адресов для NAT (рис. 3.6)

```

msk-donskaya-vpkoszlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkoszlov-gw-1(config)#ip nat pool main pool 198.51.100.2
^
% Invalid input detected at '^' marker.
msk-donskaya-vpkoszlov-gw-1(config)#ip nat pool main-pool 198.51.100.2 198.51.100.14 netmask
255.255.255.240
msk-donskaya-vpkoszlov-gw-1(config)#

```

Copy Paste

Рис. 3.6: Пул адресов для NAT

Настройка списка доступа для NAT (рис. 3.7)

```

msk-donskaya-vpkoszlov-gw-1(config)#ip access list extended natinet
^
% Invalid input detected at '^' marker.
msk-donskaya-vpkoszlov-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#

```

Рис. 3.7: Настройка списка доступа для NAT

Настроил сеть дисплейных классов, кафедр и тп (рис. 3.8)

```

msk-donskaya-vpkoszlov-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#remark dk
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq
80
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq
80
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#remark departments
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.13 eq
80
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#remark adm
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq
80
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#remark admin
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-vpkoszlov-gw-1(config-ext-nacl)#exit
msk-donskaya-vpkoszlov-gw-1(config)#exit
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkoszlov-gw-1#

```

Copy Paste

Рис. 3.8: Настройка сетей

Настройка NAT (рис. 3.9)

```
msk-donskaya-vpkozlov-gw-1#
msk-donskaya-vpkozlov-gw-1#
msk-donskaya-vpkozlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkozlov-gw-1(config)#ip nat inside source list nat-inet pool main-pool overload
msk-donskaya-vpkozlov-gw-1(config)#int f0/0.3
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat inside
msk-donskaya-vpkozlov-gw-1(config-subif)#interface f0/0.101
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat inside
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/0.102
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat inside
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/0.103
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat inside
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/0.104
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat inside
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#interface f0/1.4
msk-donskaya-vpkozlov-gw-1(config-subif)#ip nat outside
msk-donskaya-vpkozlov-gw-1(config-subif)#exit
msk-donskaya-vpkozlov-gw-1(config)#exit
msk-donskaya-vpkozlov-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write memory
Building configuration...
[OK]
msk-donskaya-vpkozlov-gw-1#
```

Рис. 3.9: Настройка NAT

Проверка доступности маршрутизаторов (рис. 3.10)

```
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<1ms TTL=254
Reply from 198.51.100.1: bytes=32 time<1ms TTL=254
Request timed out.
Reply from 198.51.100.1: bytes=32 time=1ms TTL=254

Ping statistics for 198.51.100.1:
    Packets: Sent = 4, Received = 3, Lost = 1 (25% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 1ms, Average = 0ms

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:
```

Рис. 3.10: Проверка доступности маршрутизаторов

Проверка доступности www.yandex.ru (рис. 3.11)

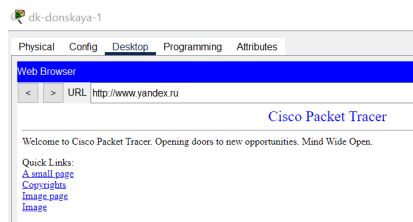


Рис. 3.11: Проверка доступности www.yandex.ru

Настройка доступа из Интернета (WWW-сервер, Файловый сервер) (рис. 3.12)

```
msk-donskaya-vpkorlov-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80 198.51.100.2 80
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 198.51.100.3 20
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 198.51.100.3 21
msk-donskaya-vpkorlov-gw-1(config)#
```

Рис. 3.12: Настройка доступа из Интернета (WWW-сервер, Файловый сервер)

Настройка доступа из Интернета (Почтовый сервер, Доступ по RDP) (рис. 3.13)

```
msk-donskaya-vpkorlov-gw-1#conf t
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25 198.51.100.4 25
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.0.4 110 198.51.100.4 110
msk-donskaya-vpkorlov-gw-1(config)#ip nat inside source static tcp 10.128.6.200 3389 198.51.100.10 3389
msk-donskaya-vpkorlov-gw-1(config)#
```

Рис. 3.13: Настройка доступа из Интернета (WWW-сервер, Файловый сервер)

Добавил ноутбук к internet (рис. 3.14)

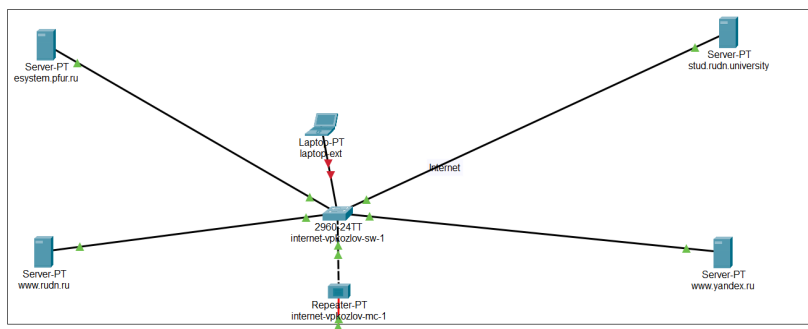


Рис. 3.14: Добавление ноутбука к internet

Проверка доступа по ftp (рис. 3.15)

```
C:\>ftp 198.51.100.3
Trying to connect...198.51.100.3
Connected to 198.51.100.3
220- Welcome to FT Ftp server
Username:cisco
331- Username ok, need password
Password:
230- Logged in
(passive mode On)
ftp>
```

Рис. 3.15: Проверка доступа по ftp

Проверка доступа к веб-серверу (рис. 3.16)

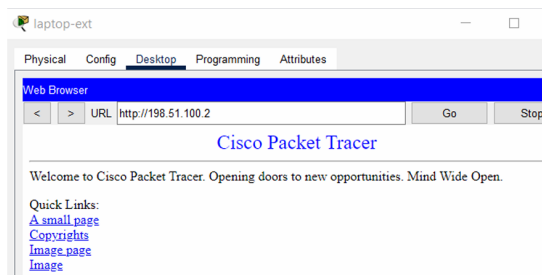


Рис. 3.16: Проверка доступа к веб-серверу

4 Выводы

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.

6 Список литературы

1. 802.1D-2004 - IEEE Standard for Local and Metropolitan Area Networks. Media Access Control (MAC) Bridges : тех. отч. / IEEE. — 2004. — С. 1—
2. — DOI: 10.1109/IEEESTD.2004.94569. — URL: <http://ieeexplore.ieee.org/servlet/opac?punumb>
3. 802.1Q - Virtual LANs. — URL: <http://www.ieee802.org/1/pages/802.1Q.html>.
4. A J. Packet Tracer Network Simulator. — Packt Publishing, 2014. — ISBN 9781782170426. — URL: https://books.google.com/books?id=eVOcAgAAQBAJ&dq=cisco+packet+tracer&hl=es&source=gbs_navlinks_
- s.
4. Cotton M., Vegoda L. Special Use IPv4 Addresses : RFC / RFC Editor. — 01.2010. — С. 1—11. — № 5735. — DOI: 10.17487/rfc5735. — URL: <https://www.rfc-editor.org/info/rfc5735>.
5. Droms R. Dynamic Host Configuration Protocol : RFC / RFC Editor. — 03.1997. — С. 1—45. — № 2136. — DOI: 10.17487/rfc2131. — URL: <https://www.ietf.org/rfc/rfc2131.txt%20https://www.rfc-editor.org/info/rfc2131>.
6. McPherson D., Dykes B. VLAN Aggregation for Efficient IP Address Allocation, RFC 3069. — 2001. — URL: <http://www.ietf.org/rfc/rfc3069.txt>.
7. Moy J. OSPF Version 2 : RFC / RFC Editor. — 1998. — С. 244. — DOI: 10.17487/rfc2328. — URL: <https://www.rfc-editor.org/info/rfc2328>.
8. NAT Order of Operation. — URL: <https://www.cisco.com/c/en/us/support/docs/ip/network-address-translation-nat/6209-5.html>.
9. NAT: вопросы и ответы / Сайт поддержки продуктов и технологий компании

Cisco. — URL: [https://www.cisco.com/cisco/web/support/ RU/9/92/92029_nat-faq.html](https://www.cisco.com/cisco/web/support/RU/9/92/92029_nat-faq.html).

10. Neumann J. C. Cisco Routers for the Small Business A Practical Guide for IT Professionals. — Apress, 2009.