

Лабораторная работа №12

Настройка NAT

Шуваев Сергей Александрович

Содержание

| | | |
|----------|---------------------------------------|-----------|
| 1 | Цель работы | 4 |
| 2 | Задание | 5 |
| 3 | Выполнение лабораторной работы | 6 |
| 4 | Выводы | 16 |
| 5 | Контрольные вопросы | 17 |

Список иллюстраций

| | | |
|------|---|----|
| 3.1 | Первоначальная настройка маршрутизатора provider-gw-1 | 6 |
| 3.2 | Первоначальная настройка коммутатора provider-sw-1 | 7 |
| 3.3 | Настройка интерфейсов маршрутизатора provider-gw-1 | 8 |
| 3.4 | Настройка интерфейсов коммутатора provider-sw-1 | 9 |
| 3.5 | Настройка интерфейсов маршрутизатора msk-donskaya-gw-1 | 10 |
| 3.6 | Проверка доступности маршрутизатора | 10 |
| 3.7 | Настройка пула адресов для NAT | 10 |
| 3.8 | Настройка списка доступа для NAT | 11 |
| 3.9 | Настройка NAT | 11 |
| 3.10 | Проверка доступности маршрутизаторов | 12 |
| 3.11 | Настройка доступа из Интернета | 12 |
| 3.12 | Добавление ноутбука на территорию Интернет | 13 |
| 3.13 | Проверка доступа из Интернета по ftp | 13 |
| 3.14 | Проверка доступа из Интернета к web-серверу | 14 |
| 3.15 | Доступ dep-donskaya-1 к 192.0.2.13 | 14 |
| 3.16 | Доступ dk-donskaya-1 к www.yandex.ru | 15 |
| 3.17 | Доступ dk-donskaya-1 к stud.rudn.university | 15 |
| 3.18 | Доступ adm-donskaya-1 к www.rudn.ru | 15 |

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.

```
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write m
Building configuration...
[OK]
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#line console 0
Router(config-line)#password cisco
Router(config-line)#login
Router(config-line)#exit
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write n
      ^
% Invalid input detected at '^' marker.

Router#write m
Building configuration...
[OK]
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#enable secret cisco
Router(config)#service password encryption
      ^
% Invalid input detected at '^' marker.

Router(config)#service password-encryption
Router(config)#username admin privilege 1 secret cisco
Router(config)#exit
Router#
%SYS-5-CONFIG_I: Configured from console by console
write m
Building configuration...
[OK]
Router#
```

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.

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

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.

```

Router#
Router#en
Router#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Router(config)#interface f0/0
Router(config-if)#no shutdown

Router(config-if)#
%LINK-5-CHANGED: Interface FastEthernet0/0, changed state to up
exit
Router(config)#interface f0/0.4
Router(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/0.4, changed state to up
encapsulation dot1Q 4
Router(config-subif)#encapsulation dot1Q 4
Router(config-subif)#ip address 198.51.100.1 255.255.255.240
Router(config-subif)#description msk-donskaya
Router(config-subif)#exit
Router(config)#interface f0/1
Router(config-if)#no shutdown

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

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

```

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

Проведем настройку интерфейсов коммутатора provider-sw-1 (рис. 3.4). Сделаем порты f0/1 и f0/2 транковыми, зададим 4 vlan с именем nat.


```

Building configuration...
[OK]
Switch#en
Switch#conf t
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)#interface f0/1
Switch(config-if)#switchport mode trunk

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

%LINK-5-CHANGED: Interface FastEthernet0/1, changed state to

Switch(config-if)#exit
Switch(config)#interface f0/2
Switch(config-if)#switchport mode trunk
Switch(config-if)#exit
Switch(config)#vlan 4
Switch(config-vlan)#name nat
Switch(config-vlan)#exit
Switch(config)#interface vlan4
Switch(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

%LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan4, changed state to up

Switch(config-if)#no shutdown
Switch(config-if)#exit
Switch(config)#exit
Switch#
%SYS-5-CONFIG_I: Configured from console by console
write m
Building configuration...
[OK]
Switch#

```

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

Проведем настройку интерфейсов маршрутизатора msk-donskaya-gw-1 (рис. 3.5). Поднимем интерфейс f0/1, создадим интерфейс f0/1.4 для 4 vlan и зададим ip-адрес.

```

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

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

msk-donskaya-shuvayev-gw-1(config-if)#exit
msk-donskaya-shuvayev-gw-1(config)#interface f0/1.4
msk-donskaya-shuvayev-gw-1(config-subif)#
%LINK-5-CHANGED: Interface FastEthernet0/1.4, changed state to up

msk-donskaya-shuvayev-gw-1(config-subif)#encapsulation dot1Q 4
msk-donskaya-shuvayev-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-shuvayev-gw-1(config-subif)#description internet
msk-donskaya-shuvayev-gw-1(config-subif)#exit
msk-donskaya-shuvayev-gw-1(config)#exit
msk-donskaya-shuvayev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write m
Building configuration...
[OK]
msk-donskaya-shuvayev-gw-1#en
msk-donskaya-shuvayev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-shuvayev-gw-1(config)#ip route 0.0.0.0 0.0.0.0 198.51.100.1
msk-donskaya-shuvayev-gw-1(config)#exit
msk-donskaya-shuvayev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console
write m
Building configuration...
[OK]
msk-donskaya-shuvayev-gw-1#

```

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

Проверим доступ с маршрутизатора на Донской к маршрутизатору провайдера (рис. 3.6).

```

msk-donskaya-shuvayev-gw-1>ping 198.51.100.1

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 198.51.100.1, timeout is 2 seconds:
!!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 0/2/13 ms

msk-donskaya-shuvayev-gw-1>

```

Рис. 3.6: Проверка доступности маршрутизатора

Настроим пул адресов 198.51.100.2 – 198.51.100.14 для NAT (рис. 3.7).

```

msk-donskaya-shuvayev-gw-1(config)#ip nat pool main-pool 198.51.100.2 198.51.100.14 netmask
255.255.255.240
msk-donskaya-shuvayev-gw-1(config)#

```

Рис. 3.7: Настройка пула адресов для NAT

Теперь настроим список доступа к nat на всех подсетях для пользователей(рис. 3.9).

```

msk-donskaya-shuvayev-gw-1#en
msk-donskaya-shuvayev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-shuvayev-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#remark dk
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#remark adm
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq 80
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#remark admin
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-shuvayev-gw-1(config-ext-nacl)#

```

Рис. 3.8: Настройка списка доступа для NAT

Настроим Port Address Translation (PAT) на субинтерфейсах маршрутизатора с территории Донская (рис. 3.9).

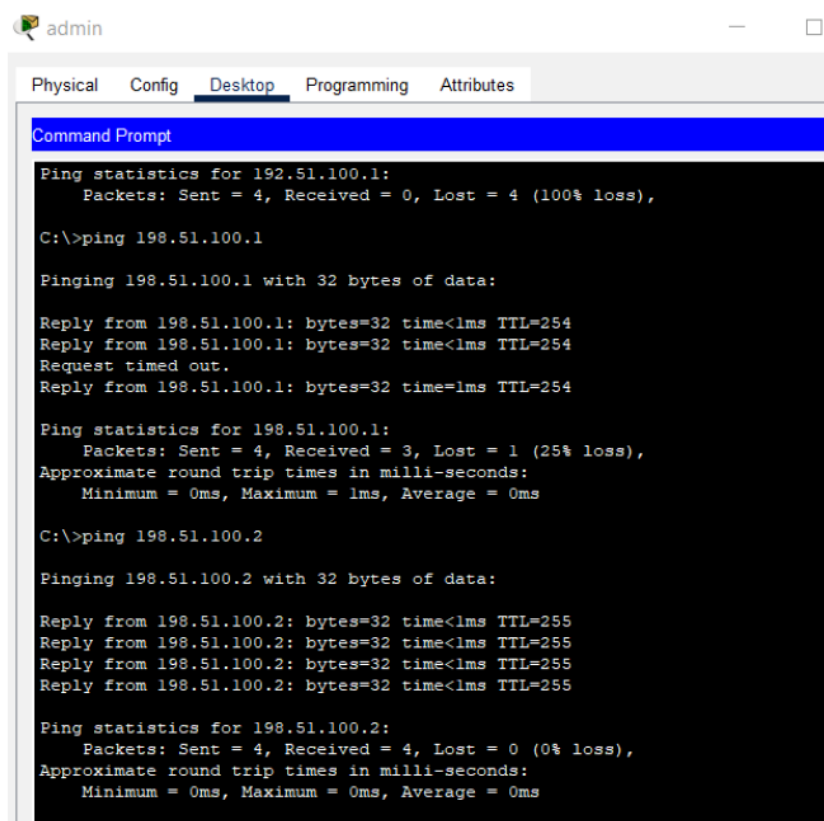
```

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

```

Рис. 3.9: Настройка NAT

Проверка доступности к маршрутизаторам от ноутбука админ (рис. 3.9).



```
admin
Physical Config Desktop Programming Attributes
Command Prompt
Ping statistics for 192.51.100.1:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

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<lms TTL=254
Reply from 198.51.100.1: bytes=32 time<lms TTL=254
Request timed out.
Reply from 198.51.100.1: bytes=32 time=lms 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 = lms, 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<lms TTL=255
Reply from 198.51.100.2: bytes=32 time<lms TTL=255
Reply from 198.51.100.2: bytes=32 time<lms TTL=255
Reply from 198.51.100.2: bytes=32 time<lms 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 = 0ms, Average = 0ms
```

Рис. 3.10: Проверка доступности маршрутизаторов

Настроим доступа из Интернета (рис. 3.11).

```
msk-donskaya-shuvayev-gw-1>en
Password:
msk-donskaya-shuvayev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-shuvayev-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 198.51.100.3 20
msk-donskaya-shuvayev-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 198.51.100.3 21
msk-donskaya-shuvayev-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25 198.51.100.4 25
msk-donskaya-shuvayev-gw-1(config)#ip nat inside source static tcp 10.128.0.4 110 198.51.100.4 110
msk-donskaya-shuvayev-gw-1(config)#ip nat inside source static tcp 10.128.6.200 3389 198.51.100.10
3389
msk-donskaya-shuvayev-gw-1(config)#
```

Рис. 3.11: Настройка доступа из Интернета

Добавим ноутбук на территории Интернета (рис. 3.12).

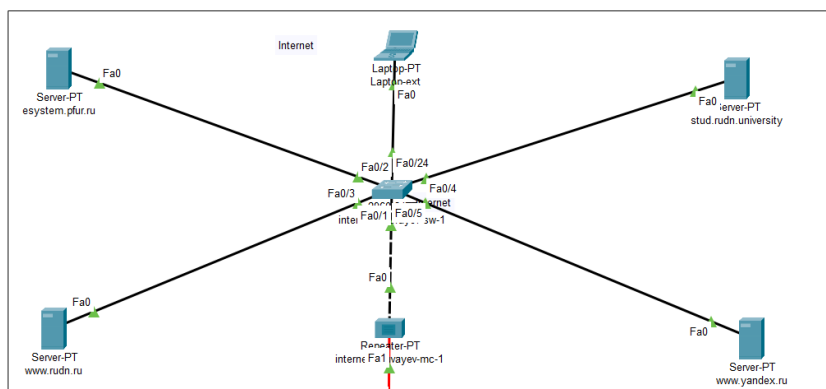


Рис. 3.12: Добавление ноутбука на территорию Интернет

Проверим работоспособность соединения из сети Интернет в сеть Донской к web-серверу и файловому серверу по ftp (рис. 3.13, 3.14).

```

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<lms TTL=255
Reply from 192.0.2.1: bytes=32 time<lms TTL=255
Reply from 192.0.2.1: bytes=32 time<lms TTL=255
Reply from 192.0.2.1: bytes=32 time<lms 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

C:\>ftp 10.128.0.3
Trying to connect...10.128.0.3

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

```

Рис. 3.13: Проверка доступа из Интернета по ftp

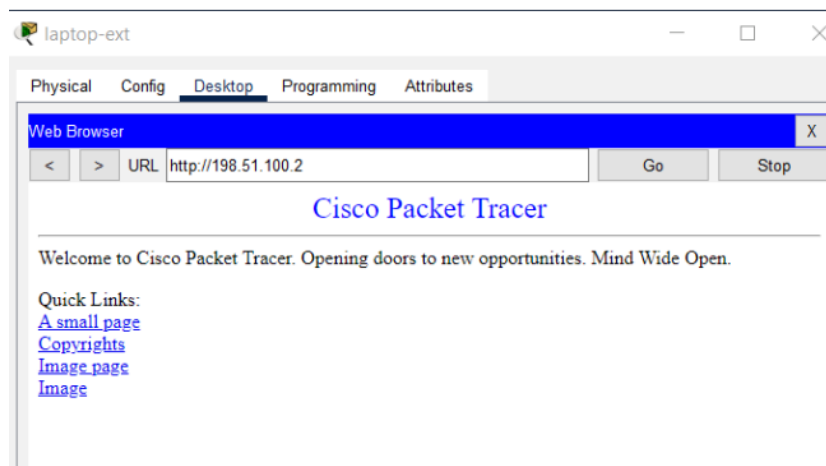


Рис. 3.14: Проверка доступа из Интернета к web-серверу

Проверим доступ к необходимым интернет-ресурсам конечных устройств сети. Убедимся, что устройствам доступны и недоступны заданные нами сайты(рис. 3.15 - 3.18).

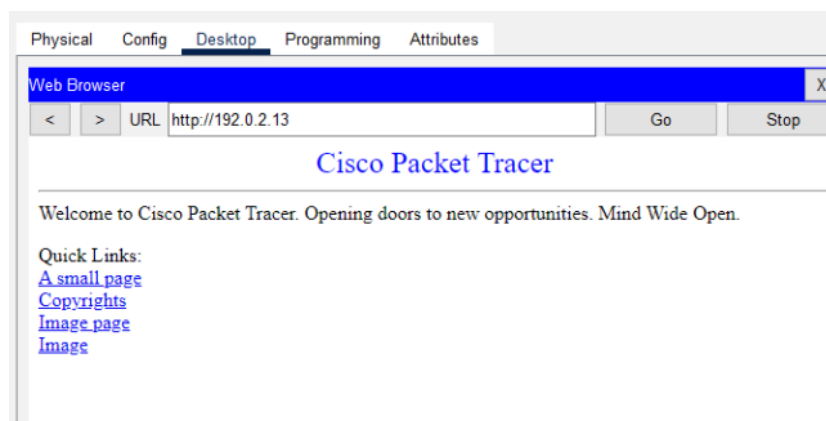


Рис. 3.15: Доступ der-donskaya-1 к 192.0.2.13

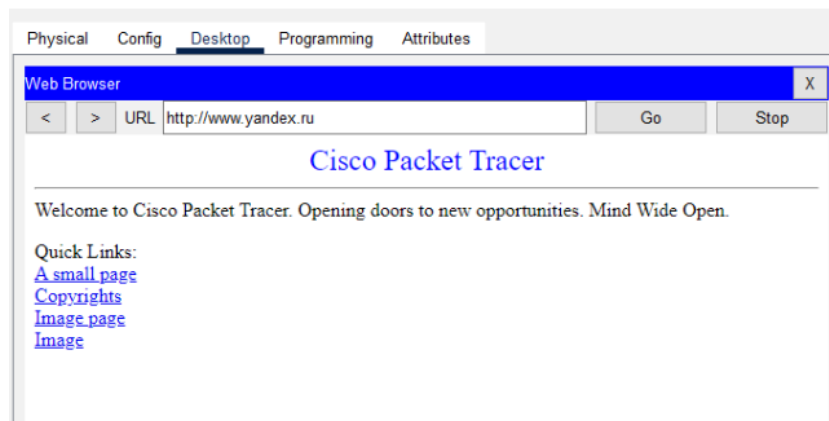


Рис. 3.16: Доступ dk-donskaya-1 к www.yandex.ru

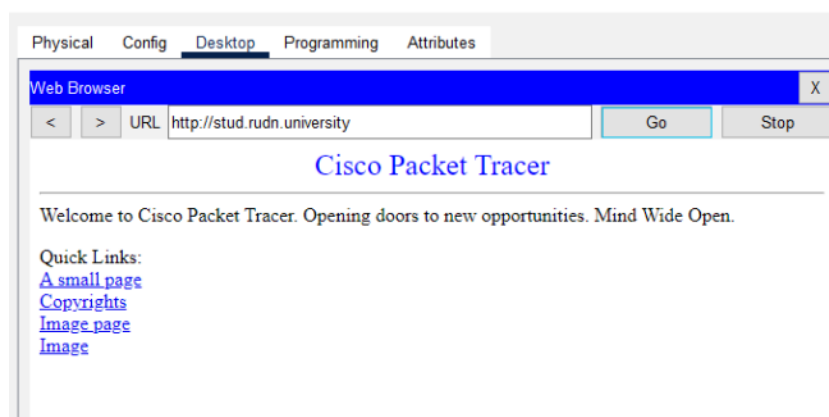


Рис. 3.17: Доступ dk-donskaya-1 к stud.rudn.university

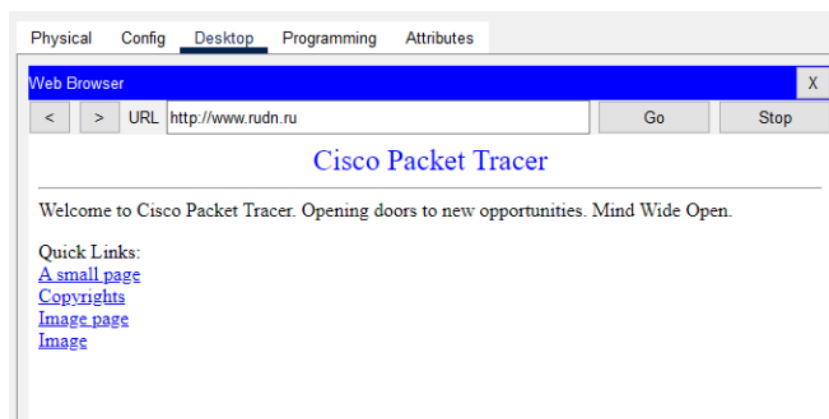


Рис. 3.18: Доступ adm-donskaya-1 к www.rudn.ru

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.