Лабораторная работа 12

Настройка NAT

Ланцова Яна Игоревна

Содержание

Список иллюстраций

Список таблиц

1 Цель работы

Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT.

2 Задание

Требуется подключить локальную сеть организации к сети Интернет с учётом ограничений, накладываемых на определённые подсети локальной сети:

1) сеть управления устройствами не должна иметь доступ в Интернет;
2) оконечные устройства сети дисплейных классов должны иметь доступ только к сайтам, необходимым для учёбы (в данном случае к www.yandex.ru, stud.rudn.university);
3) пользователям из сети кафедр разрешено работать только с образовательными сайтами (в данном случае это esystem.pfur.ru);
4) пользователям сети администрации разрешено работать только с сайтом университета www.rudn.ru;
5) в сети для других пользователей компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи – не должны выходить в Интернет;
6) ограничения для серверов:

   - WEB-сервер должен быть доступен по порту 80;
   - почтовый сервер должен быть доступен по портам 25 и 110;
   - файловый сервер должен быть доступен извне по портам протокола FTP;

7) компьютер администратора должен быть доступен из внешней сети по протоколу удалённого рабочего стола (Remote Desktop Protocol, RDP).

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.

3 Выполнение лабораторной работы

Проведем первоначальную настройку маршрутизатора provider-yalantsova-gw-1: зададим имя, настроим доступ по паролю к виртуальным терминалам(рис. 3.1).

```
provider-yalantsova-gw-1>enable
provider-yalantsova-gw-1#configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
provider-yalantsova-gw-1(config)#line vty 0 4
provider-yalantsova-gw-1(config-line)#password cisco
provider-yalantsova-gw-1(config-line)#login
provider-yalantsova-gw-1(config-line)#exit
provider-yalantsova-gw-1(config)#line console 0
provider-yalantsova-gw-1(config-line)#password cisco
provider-yalantsova-gw-1(config-line)#login
provider-yalantsova-gw-1(config-line)#exit
provider-yalantsova-gw-1(config)#enable secret cisco
provider-yalantsova-gw-1(config)#service password encryption
                                               ^
% Invalid input detected at '^' marker.

provider-yalantsova-gw-1(config)#service password-encryption
provider-yalantsova-gw-1(config)#username admin privilege 1 secret cisco
```

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

Затем сделаем то же самое для коммутатора provider-yalantsova-sw-1(рис. 3.2):

```
provider-yalantsova-sw-1>enable
provider-yalantsova-sw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
provider-yalantsova-sw-1(config)#line vty 0 4
provider-yalantsova-sw-1(config-line)#password cisco
provider-yalantsova-sw-1(config-line)#login
provider-yalantsova-sw-1(config-line)#exit
provider-yalantsova-sw-1(config)#line console 0
provider-yalantsova-sw-1(config-line)#password cisco
provider-yalantsova-sw-1(config-line)#login
provider-yalantsova-sw-1(config-line)#exit
provider-yalantsova-sw-1(config)#enable secret cisco
provider-yalantsova-sw-1(config)#service password-encryption
provider-yalantsova-sw-1(config)#username admin privilege 1 secret cisco
```

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

Настроим интерфейсы маршрутизатора provider-yalantsova-gw-1: поднимем интерфейс f0/0, создадим интерфейс f0/0.4 для 4 vlan и зададим ip-адрес, поднимем интерфейс f0/1 для доступа в интернет(рис. 3.3).

```
provider-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
provider-yalantsova-gw-1(config)#interface f0/0
provider-yalantsova-gw-1(config-if)#no shutdown

provider-yalantsova-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-yalantsova-gw-1(config-if)#exit
provider-yalantsova-gw-1(config)#interface f0/0.4
provider-yalantsova-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-yalantsova-gw-1(config-subif)#encapsulation dot1Q 4
provider-yalantsova-gw-1(config-subif)#ip address 198.51.100.1 255.255.255.240
provider-yalantsova-gw-1(config-subif)#description mks-donskaya
provider-yalantsova-gw-1(config-subif)#exit
provider-yalantsova-gw-1(config)#interface f0/1
provider-yalantsova-gw-1(config-if)#no shutdown

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

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

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

Настроим интерфейсы коммутатора provider-yalantsova-sw-1: сделаем транковыми порты f0/1 и f0/2, зададим 4 vlan с именем nat(рис. 3.4).

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

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

provider-yalantsova-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-yalantsova-sw-1(config-if)#exit
provider-yalantsova-sw-1(config)#vlan 4
provider-yalantsova-sw-1(config-vlan)#name nat
provider-yalantsova-sw-1(config-vlan)#exit
provider-yalantsova-sw-1(config)#interface vlan4
provider-yalantsova-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-yalantsova-sw-1(config-if)#no shutdown
provider-yalantsova-sw-1(config-if)#exit
provider-yalantsova-sw-1(config)#exit
provider-yalantsova-sw-1#
%SYS-5-CONFIG_I: Configured from console by console

provider-yalantsova-sw-1#wr mem
Building configuration...
```

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

Настроим интерфейсы маршрутизатора msk-donskaya-yalantsova-gw-1: поднимем интерфейс f0/1, создадим интерфейс f0/1.4 для 4 vlan и зададим

ip-адрес(рис. 3.5).

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

msk-donskaya-yalantsova-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-yalantsova-gw-1(config-if)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/1.4
msk-donskaya-yalantsova-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-yalantsova-gw-1(config-subif)#encapsulation dot1Q 4
msk-donskaya-yalantsova-gw-1(config-subif)#ip address 198.51.100.2 255.255.255.240
msk-donskaya-yalantsova-gw-1(config-subif)#description internet
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#exit
msk-donskaya-yalantsova-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

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

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

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

```
msk-donskaya-yalantsova-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 80 percent (4/5), round-trip min/avg/max = 0/0/1 ms

msk-donskaya-yalantsova-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 = 0/0/1 ms
```

Рис. 3.6: Проверка связи между маршрутизаторами

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

```
msk-donskaya-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-yalantsova-gw-1(config)#ip nat pool main-pool 198.51.100.2 198.51.100.14 netmask 255.255.255.240
msk-donskaya-yalantsova-gw-1(config)#
```

Рис. 3.7: Настройка пула адресов для NAT

Теперь настроим список доступа к nat на всех подсетях для пользователей(рис. 3.8).

```
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark dk
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark departments
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.13 eq 80
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark adm
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq 80
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#remark admin
msk-donskaya-yalantsova-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
```

Рис. 3.8: Оборудование в здании сети модельного Интернета

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

```
msk-donskaya-yalantsova-gw-1#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source list nat-inet pool main-pool overload
msk-donskaya-yalantsova-gw-1(config)#int f0/0.3
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat inside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.101
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat inside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.102
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat inside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.103
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat inside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/0.104
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat inside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
msk-donskaya-yalantsova-gw-1(config)#interface f0/1.4
msk-donskaya-yalantsova-gw-1(config-subif)#ip nat outside
msk-donskaya-yalantsova-gw-1(config-subif)#exit
```

Рис. 3.9: Настройка PAT

Настроим доступа из Интернета. Для этого добавим компьютер на территории Интернета(рис. 3.10).

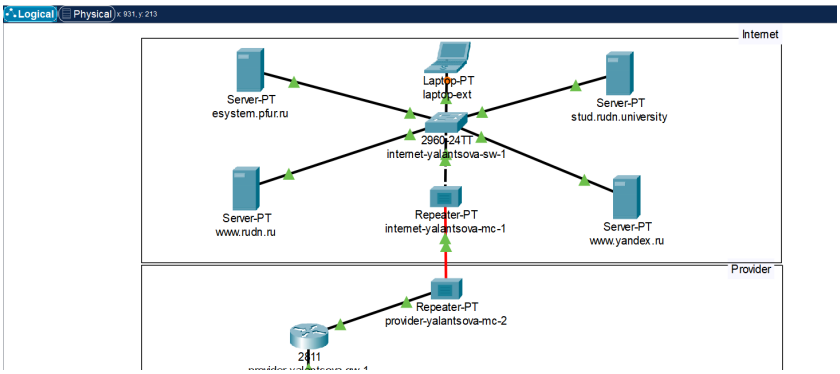

Рис. 3.10: Схема сети Интернет с ноутбуком

Затем свяжем ip-адреса серверов с территории Донская с ip-адресами серверов в Интернете(рис. 3.11).

```
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80 198.51.100.2 8
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20
% Incomplete command.
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 198.51.100.3 20
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 198.51.100.3 21
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25
% Incomplete command.
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.4 25 198.51.100.4 25
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.0.4 110 198.51.100.4 110
msk-donskaya-yalantsova-gw-1(config)#ip nat inside source static tcp 10.128.6.200 3389 198.51.100.10 3389
```

Рис. 3.11: Настройка доступа из Интернета

Проверим доступ к необходимым интернет-ресурсам конечных устройств сети. Убедимся, что устройствам доступны и недоступны заданные нами сайты(рис. 3.12 - 3.15).

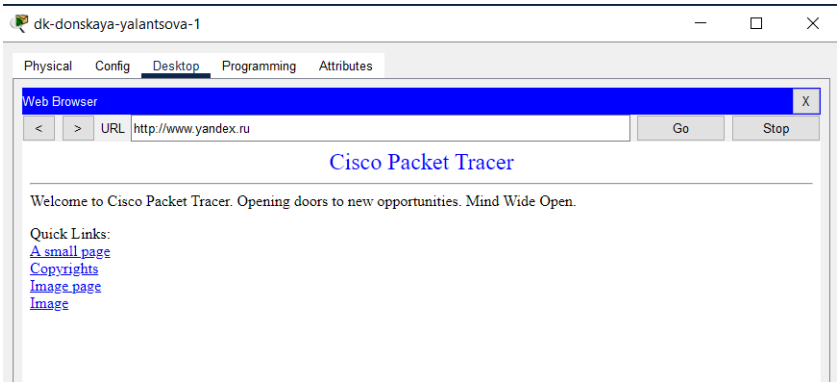

Рис. 3.12: Доступ dk-donskaya-1 к www.yandex.ru

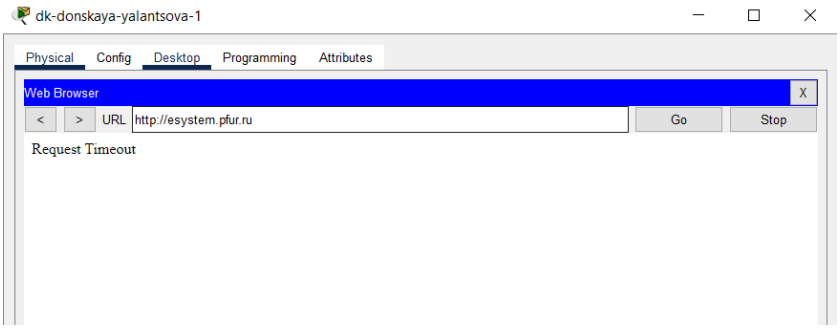

Рис. 3.13: Доступ dk-donskaya-1 к esystem.pfur.ru

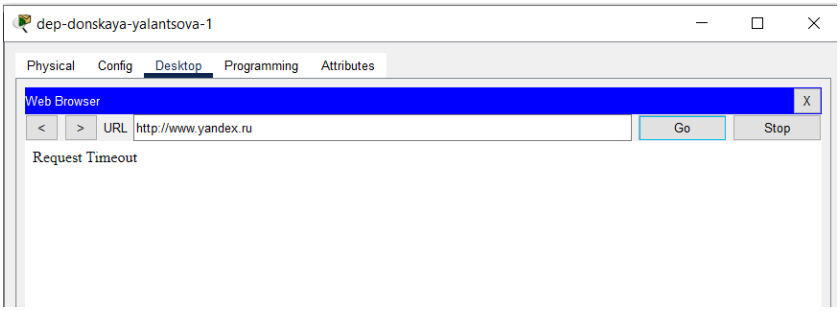

Рис. 3.14: Доступ dep-donskaya-1 к www.yandex.ru

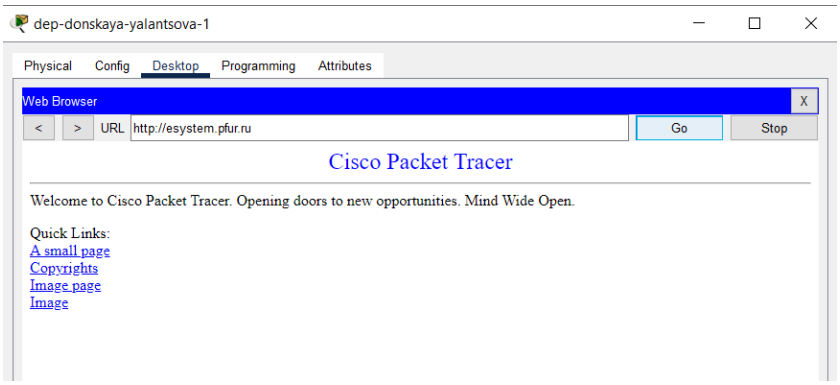

Рис. 3.15: Доступ dep-donskaya-1 к esystem.pfur.ru

Также проверим работоспособность соединения из сети Интернет в сеть Донской к web-серверу и файловому серверу по ftp(рис. 3.16, 3.17):

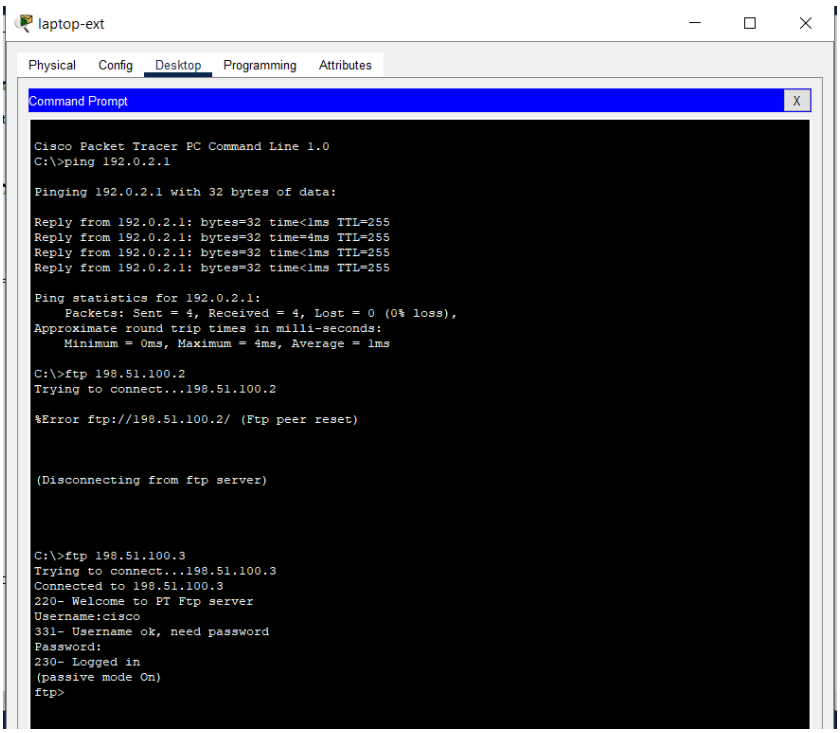

Рис. 3.16: Проверка доступа из Интернета по ftp

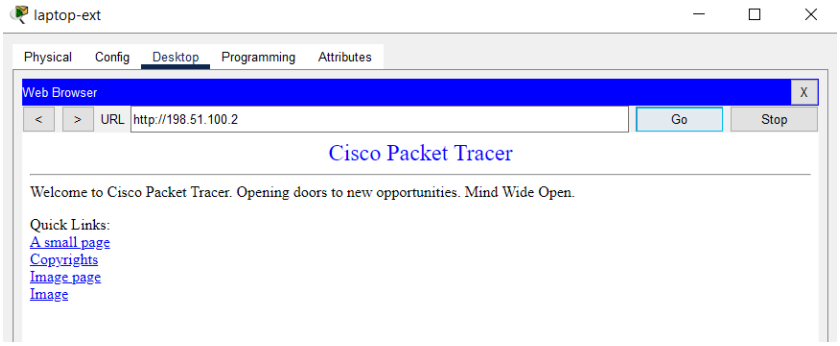

Рис. 3.17: Проверка доступа из Интернета к web-серверу

4 Выводы

В результате выполнения лабораторной были приобретены 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)?
2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?
3. Можно ли применить Cisco IOS NAT к субинтерфейсам?
4. Что такое пулы IP NAT?
5. Что такое статические преобразования NAT?
6. Основной принцип работы NAT (Network Address Translation) заключается в том, что он позволяет скрывать внутренние IP-адреса устройств в локальной сети за одним или несколькими публичными IP-адресами, которые используются для общения с внешними сетями, такими как Интернет. Наличие NAT в сети организации позволяет экономить публичные IP-адреса и повышать безопасность защитой внутренних устройств от прямого доступа извне.
7. Для настройки NAT на оборудовании (например, маршрутизаторе или межсетевом экране) необходимо определить правила преобразования адресов. Настройка NAT позволяет установить соответствие между внутренними и внешними IP-адресами, а также определить, какие порты и протоколы будут использоваться для коммуникации между внутренней и внешней сетями.

8. Да, Cisco IOS NAT можно применить к субинтерфейсам. Субинтерфейсы позволяют разделять один физический интерфейс на несколько логических интерфейсов, каждый из которых может иметь свои собственные настройки NAT.

9. Пулы IP NAT представляют собой диапазон публичных IP-адресов, которые используются для преобразования внутренних адресов при прохождении трафика через устройство NAT. Пулы IP NAT могут быть динамическими (когда каждое внутреннее устройство получает временный доступ к одному из публичных адресов из пула) или статическими (когда определенное внутреннее устройство всегда связано с определенным публичным адресом).

10. Статические преобразования NAT (Static NAT) — это метод, при котором определенный внутренний IP-адрес связывается с определенным публичным IP-адресом, и все запросы к этому внутреннему адресу направляются на соответствующий публичный адрес. Это позволяет установить постоянное соответствие между внутренним и внешним адресами для конкретных устройств в сети.