

РОССИЙСКИЙ УНИВЕРСИТЕТ ДРУЖБЫ НАРОДОВ

Факультет физико-математических и естественных наук

Кафедра прикладной информатики и теории вероятностей

ОТЧЕТ

ПО ЛАБОРАТОРНОЙ РАБОТЕ № 12

дисциплина: Администрирование локальных сетей

Студент: Каримов Зуфар

Группа: НПИ-01-18

Москва 2021

Оглавление

| | |
|-----------------------------------|----|
| 1. Цель работы..... | 3 |
| 2. Постановка задачи..... | 4 |
| 3. Порядок выполнения работы..... | 5 |
| 4. Выводы | 21 |
| 5. Контрольные вопросы..... | 22 |

Цель работы

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

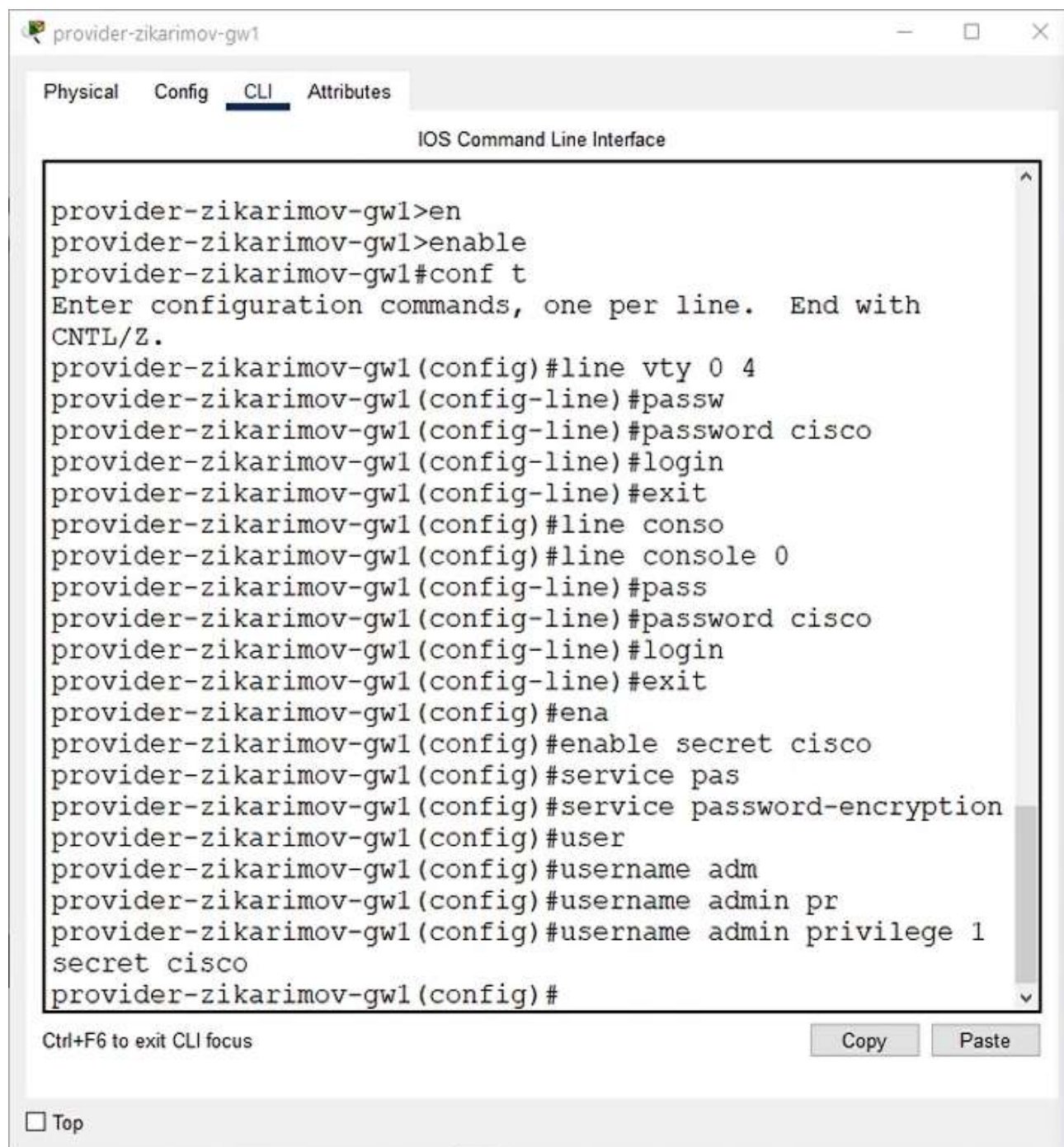
Постановка задачи

Требуется подключить локальную сеть организации к сети Интернет (распределение внешних ip-адресов дано в табл. 12.1) с учётом ограничений, накладываемых на определённые подсети локальной сети (VLAN подсетей даны в табл. 12.2):

- 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).

Последовательность выполнения работы

12.4.1. Первоначальная настройка маршрутизатора provider-gw-1



```
provider-zikarimov-gw1>en
provider-zikarimov-gw1>enable
provider-zikarimov-gw1#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
provider-zikarimov-gw1(config)#line vty 0 4
provider-zikarimov-gw1(config-line)#passw
provider-zikarimov-gw1(config-line)#password cisco
provider-zikarimov-gw1(config-line)#login
provider-zikarimov-gw1(config-line)#exit
provider-zikarimov-gw1(config)#line conso
provider-zikarimov-gw1(config)#line console 0
provider-zikarimov-gw1(config-line)#pass
provider-zikarimov-gw1(config-line)#password cisco
provider-zikarimov-gw1(config-line)#login
provider-zikarimov-gw1(config-line)#exit
provider-zikarimov-gw1(config)#ena
provider-zikarimov-gw1(config)#enable secret cisco
provider-zikarimov-gw1(config)#service pas
provider-zikarimov-gw1(config)#service password-encryption
provider-zikarimov-gw1(config)#user
provider-zikarimov-gw1(config)#username adm
provider-zikarimov-gw1(config)#username admin pr
provider-zikarimov-gw1(config)#username admin privilege 1
secret cisco
provider-zikarimov-gw1(config)#
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

12.4.2. Первоначальная настройка коммутатора provider-sw-1

```
provider-zikarimov-sw1(config)#line vty 0 4
provider-zikarimov-sw1(config-line)#pas
provider-zikarimov-sw1(config-line)#password cisco
provider-zikarimov-sw1(config-line)#log
provider-zikarimov-sw1(config-line)#login
provider-zikarimov-sw1(config-line)#exit
provider-zikarimov-sw1(config)#line console 0
provider-zikarimov-sw1(config-line)#password cisco
provider-zikarimov-sw1(config-line)#login
provider-zikarimov-sw1(config-line)#exit
provider-zikarimov-sw1(config)#enable secret cisco
provider-zikarimov-sw1(config)#service pas
provider-zikarimov-sw1(config)#service password-encryption
provider-zikarimov-sw1(config)#user
provider-zikarimov-sw1(config)#username admin pr
provider-zikarimov-sw1(config)#username admin privilege 1
secret cisco
provider-zikarimov-sw1(config)#^Z
```

12.4.3. Настройка интерфейсов маршрутизатора provider-gw-1

```
provider-zikarimov-gw1(config)#inte
provider-zikarimov-gw1(config)#interface f0/0
provider-zikarimov-gw1(config-if)#no sh
provider-zikarimov-gw1(config-if)#no shutdown

provider-zikarimov-gw1(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-zikarimov-gw1(config)#interface f0/0.4
provider-zikarimov-gw1(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-zikarimov-gw1(config-subif)#enc
provider-zikarimov-gw1(config-subif)#encapsulation dot1Q 4
provider-zikarimov-gw1(config-subif)#ip address
provider-zikarimov-gw1(config-subif)#ip address
198.51.100.1 255.255.255.240
provider-zikarimov-gw1(config-subif)#des
provider-zikarimov-gw1(config-subif)#description msk-
konkova
provider-zikarimov-gw1(config-subif)#exit
```

```
provider-zikarimov-gw1(config)#interface f0/1
provider-zikarimov-gw1(config-if)#no sh
provider-zikarimov-gw1(config-if)#no shutdown

provider-zikarimov-gw1(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-zikarimov-gw1(config-if)#ip ad
provider-zikarimov-gw1(config-if)#ip address 192.0.2.1
255.255.255.0
provider-zikarimov-gw1(config-if)#des
provider-zikarimov-gw1(config-if)#description internet
provider-zikarimov-gw1(config-if)#exit
```

12.4.4. Настройка интерфейсов коммутатора provider-sw-1

provider-zikarimov-sw1

Physical Config CLI Attributes

IOS Command Line Interface

```
provider-zikarimov-sw1(config)#int
provider-zikarimov-sw1(config)#interface f0/1
provider-zikarimov-sw1(config-if)#sw
provider-zikarimov-sw1(config-if)#switchport mode tr
provider-zikarimov-sw1(config-if)#switchport mode trunk

provider-zikarimov-sw1(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-zikarimov-sw1(config-if)#exit
provider-zikarimov-sw1(config)#int
provider-zikarimov-sw1(config)#interface f0/2
provider-zikarimov-sw1(config-if)#sw
provider-zikarimov-sw1(config-if)#switchport mode tr
provider-zikarimov-sw1(config-if)#switchport mode trunk

provider-zikarimov-sw1(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
e
```

Ctrl+F6 to exit CLI focus

Copy Paste

☐ Top

```
provider-zikarimov-sw1(config)#vlan 4
provider-zikarimov-sw1(config-vlan)#name nat
provider-zikarimov-sw1(config-vlan)#exit
provider-zikarimov-sw1(config)#int
provider-zikarimov-sw1(config)#interface vlan4
provider-zikarimov-sw1(config-if)#
%LINK-5-CHANGED: Interface Vlan4, changed state to up

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


12.4.5. Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

```
msk-konkova-zikarimov-gw1(config)#in
msk-konkova-zikarimov-gw1(config)#interface f0/1
msk-konkova-zikarimov-gw1(config-if)#no sh

msk-konkova-zikarimov-gw1(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-konkova-zikarimov-gw1(config-if)#exit
msk-konkova-zikarimov-gw1(config)#inter
msk-konkova-zikarimov-gw1(config)#interface f0/1.4

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

msk-konkova-zikarimov-gw1(config-subif)#en
msk-konkova-zikarimov-gw1(config-subif)#encapsulation
dot1Q 4
msk-konkova-zikarimov-gw1(config-subif)#ip ad
msk-konkova-zikarimov-gw1(config-subif)#ip address
198.51.100.2 255.255.255.240
msk-konkova-zikarimov-gw1(config-subif)#des
msk-konkova-zikarimov-gw1(config-subif)#description
internet
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#exit
```

```
msk-konkova-zikarimov-gw1(config)#ip route 0.0.0.0 0.0.0.0
198.51.100.1
msk-konkova-zikarimov-gw1(config)#exit
```

12.4.6. Настройка пула адресов для NAT

```
msk-konkova-zikarimov-gw1#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
msk-konkova-zikarimov-gw1(config)#ip nat pool main-pool
198.51.100.2 198.51.100.14 netmask 255.255.255.240
msk-konkova-zikarimov-gw1(config)#^Z
```

12.4.7. Настройка списка доступа для NAT

```
msk-konkova-zikarimov-gw1#conf t
Enter configuration commands, one per line. End with
CNTL/Z.
msk-konkova-zikarimov-gw1(config)#ip ac
msk-konkova-zikarimov-gw1(config)#ip access-list ex
msk-konkova-zikarimov-gw1(config)#ip access-list extended
nat-inet
msk-konkova-zikarimov-gw1(config-ext-nacl)#^Z
```

12.4.7.1. Сеть дисплейных классов

12.4.7.2. Сеть кафедр

12.4.7.3. Сеть администрации

12.4.7.4. Доступ для компьютера администратора

```
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark dk
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark adm
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
10.128.5.0 0.0.0.255 host 192.0.2.14 eq 80
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark
departments
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit tcp
10.128.4.0 0.0.0.255 host 192.0.2.13 eq 80
msk-konkova-zikarimov-gw1(config-ext-nacl)#remark admin
msk-konkova-zikarimov-gw1(config-ext-nacl)#permit ip host
10.128.6.200 any
```

12.4.8. Настройка NAT

```
msk-konkova-zikarimov-gw1#conf t
Enter configuration commands, one per line.  End with
CNTL/Z.
msk-konkova-zikarimov-gw1(config)#ip nat ins
msk-konkova-zikarimov-gw1(config)#ip nat inside source
list nat-inet pool main-pool overload
msk-konkova-zikarimov-gw1(config)#int f0/0.3
msk-konkova-zikarimov-gw1(config-subif)#ip nat inside
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#int f0/0.101
msk-konkova-zikarimov-gw1(config-subif)#ip nat inside
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#int f0/0.102
msk-konkova-zikarimov-gw1(config-subif)#ip nat inside
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#int f0/0.103
msk-konkova-zikarimov-gw1(config-subif)#ip nat inside
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#int f0/0.104
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#int f0/1.4
msk-konkova-zikarimov-gw1(config-subif)#ip nat outside
msk-konkova-zikarimov-gw1(config-subif)#exit
msk-konkova-zikarimov-gw1(config)#
```

Здесь я забыл для FastEthernet0/0.104 задать команду ip nat inside. Поэтому я самостоятельно отдельно от скринкаста сделал и выложил ниже скриншот.

```
ip nat inside
!
interface FastEthernet0/0.103
description adm
encapsulation dot1Q 103
ip address 10.128.5.1 255.255.255.0
ip nat inside
!
interface FastEthernet0/0.104
description other
encapsulation dot1Q 104
ip address 10.128.6.1 255.255.255.0
ip access-group other-in in
ip nat inside
!
interface FastEthernet0/1
no ip address
duplex auto
speed auto
!
interface FastEthernet0/1.4
description internet
encapsulation dot1Q 4
ip address 198.51.100.2 255.255.255.240
ip nat outside
!
interface Vlan1
--More--
```

Ctrl+F6 to exit CLI focus

☐ Top

12.4.9. Настройка доступа из Интернета

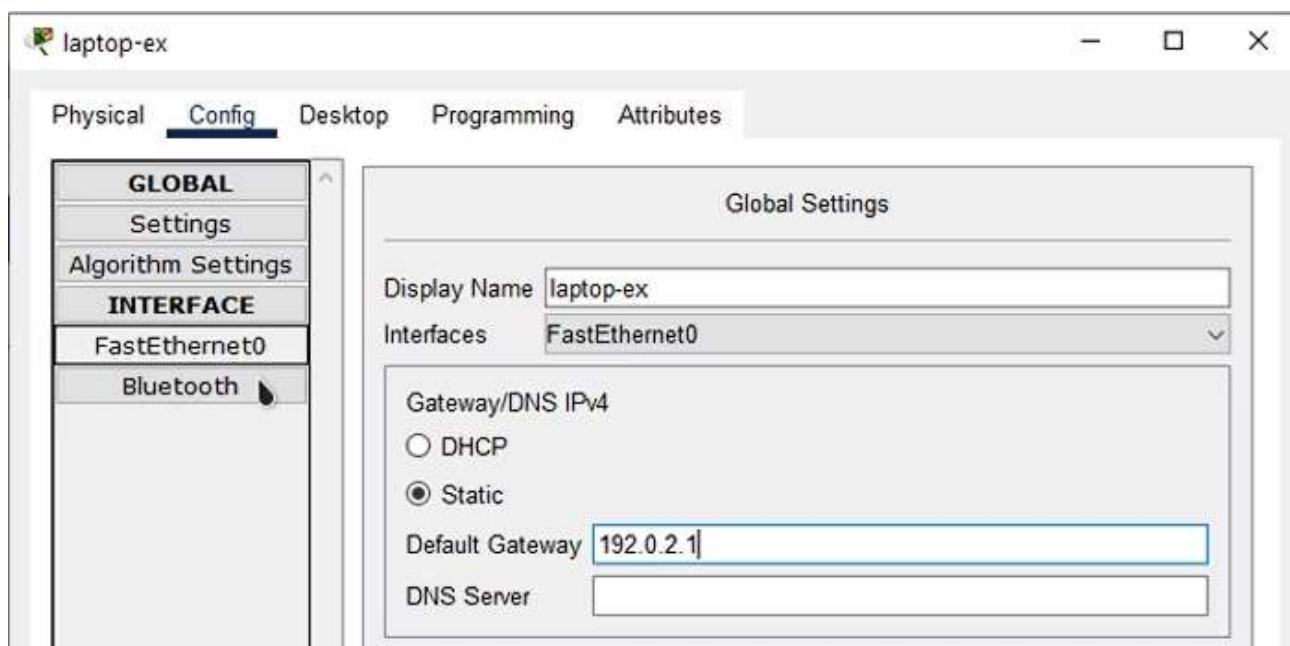
12.4.9.1. WWW-сервер

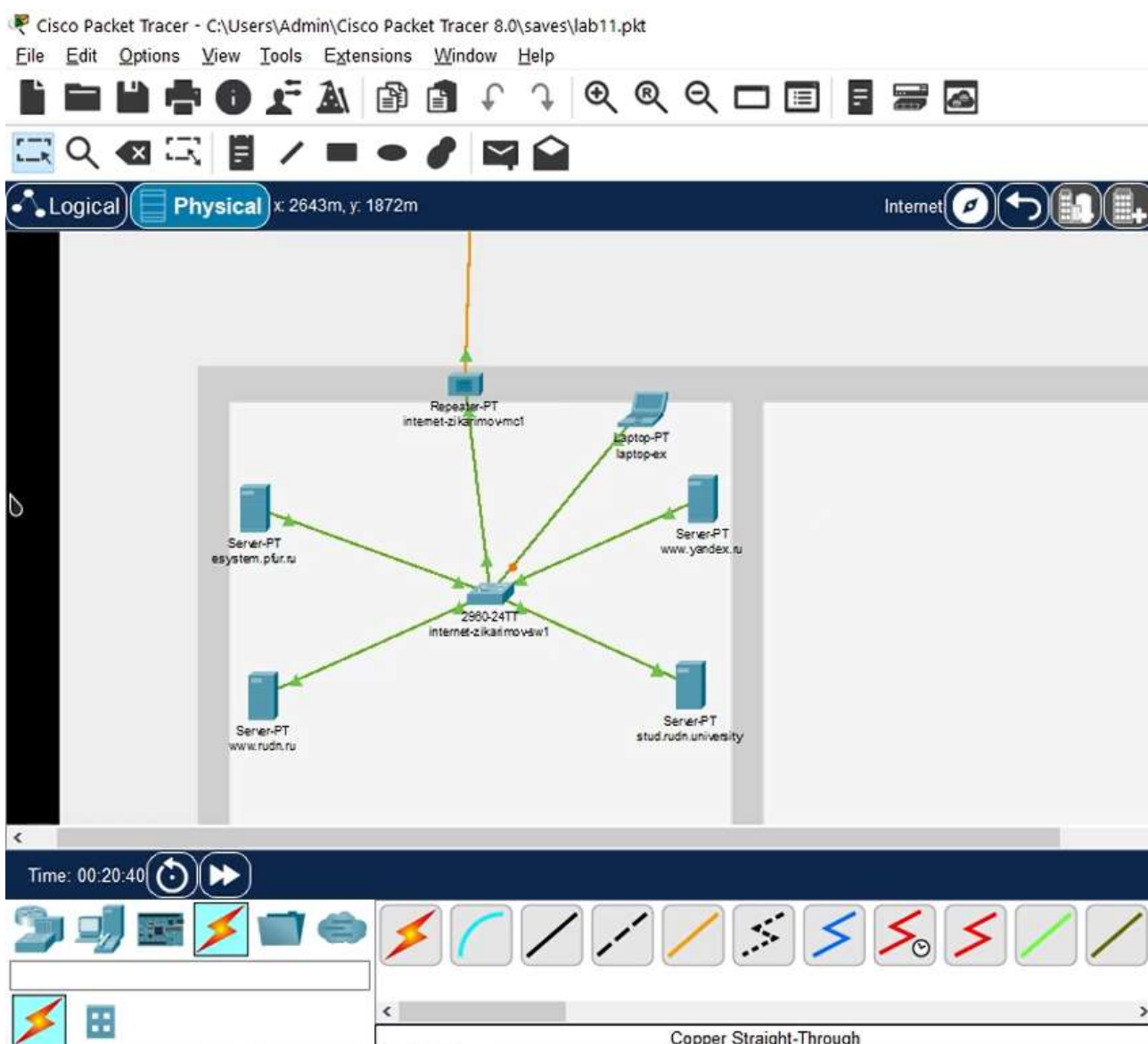
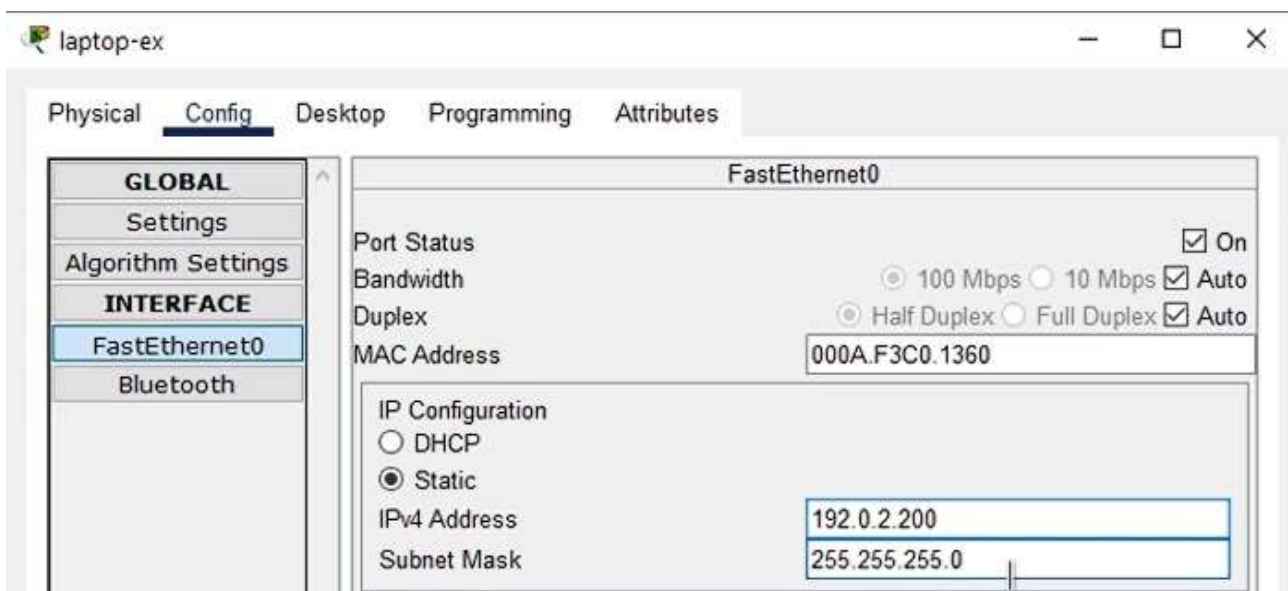
12.4.9.2. Файловый сервер

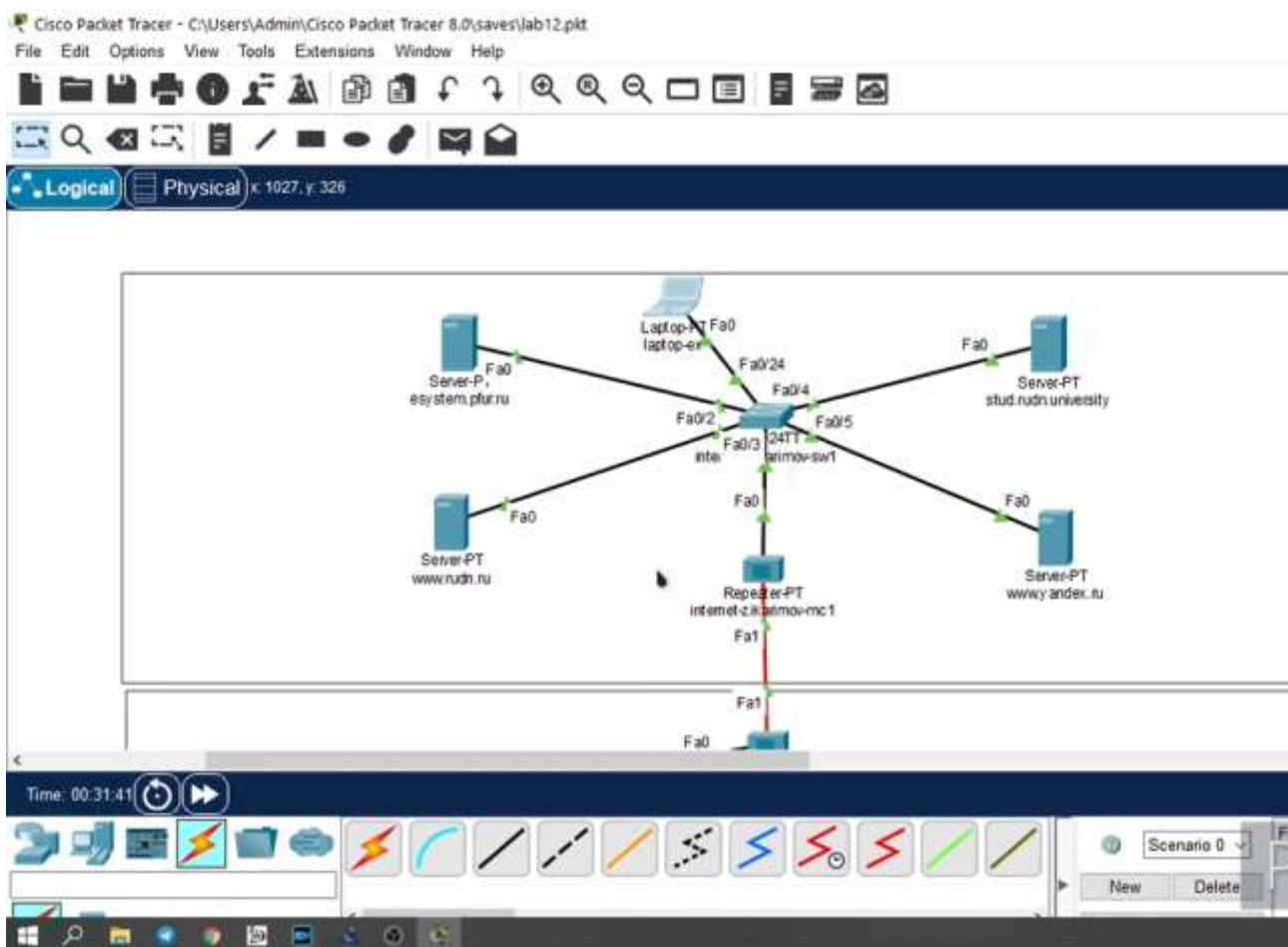
12.4.9.3. Почтовый сервер


```
msk-konkova-zikarimov-gw1(config)#ip nat inside source
static tcp 10.128.0.2 80 198.51.100.2 80
msk-konkova-zikarimov-gw1(config)#ip nat inside source
static tcp 10.128.0.3 20 198.51.100.3 20
msk-konkova-zikarimov-gw1(config)#ip nat inside source
static tcp 10.128.0.3 21 198.51.100.3 21
msk-konkova-zikarimov-gw1(config)#ip nat inside source
static tcp 10.128.0.4 25 198.51.100.4 25
msk-konkova-zikarimov-gw1(config)#ip nat inside source
static tcp 10.128.0.4 110 198.51.100.4 110
msk-konkova-zikarimov-gw1(config)#exit
msk-konkova-zikarimov-gw1#
%SYS-5-CONFIG_I: Configured from console by console
wr m
Building configuration...
[OK]
msk-konkova-zikarimov-gw1#
```

12.4.9.4. Доступ по RDP





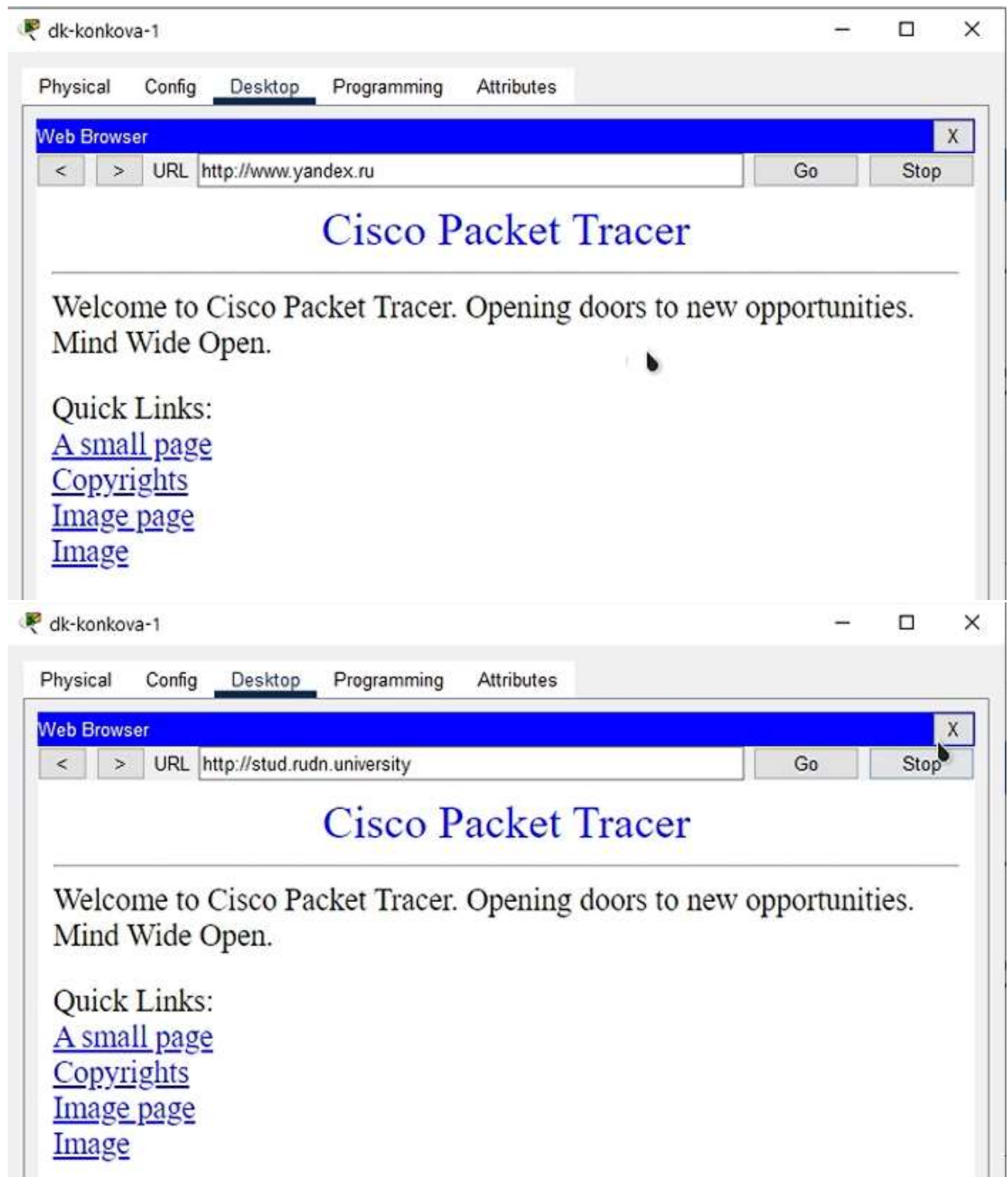


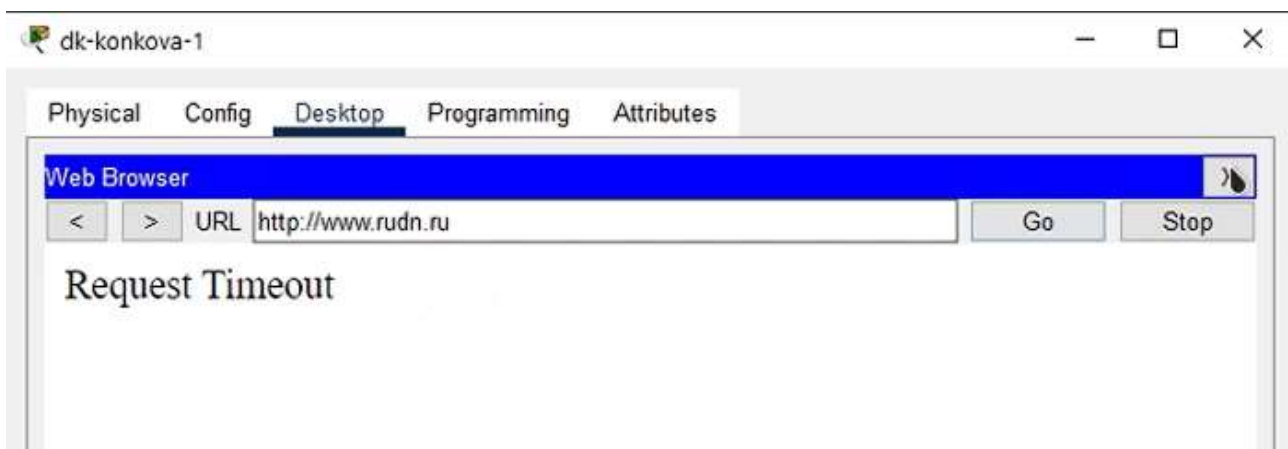
Я добавил laptop-ex в Internet и соединил с коммутатором. Также в физической рабочей области я перенес laptop-ex в Internet. И задал для данного устройства шлюз по умолчанию, ip-address и сетевую маску.

В L1 добавил laptop-ex.

Проверить работоспособность заданных настроек.

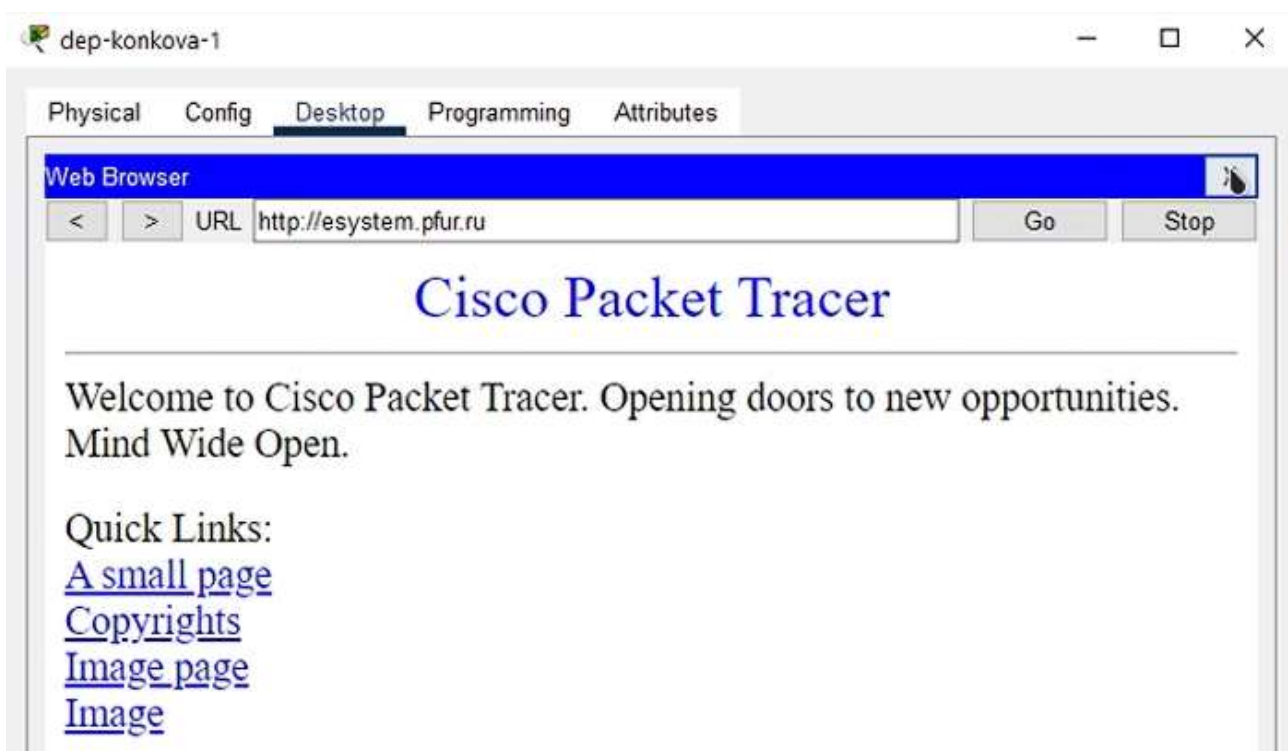
Хосты из сети дисплейных классов имеют доступ только к сайтам, необходимым для учёбы (www.yandex.ru (192.0.2.11), stud.rudn.university (192.0.2.12)).





Можно увидеть, что дисплейный класс не может получить доступ к другому сайту.

Сеть кафедр работает только с образовательными сайтами (esystem.pfur.ru (192.0.2.13)).



Сеть администрации имеет возможность работать только с сайтом университета (www.rudn.ru (192.0.2.14)).



Проверка WWW-сервер и Файловый сервер.

```
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=254
Reply from 198.51.100.2: bytes=32 time=11ms TTL=254
Reply from 198.51.100.2: bytes=32 time=12ms TTL=254
Reply from 198.51.100.2: bytes=32 time<1ms TTL=254

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 = 12ms, Average = 5ms

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>
```

Почтовый сервер

```
C:\>ftp 198.51.100.4  
Trying to connect...198.51.100.4
```

```
C:\>telnet 198.51.100.4 25  
Trying 198.51.100.4 ...Open  
C:\>telnet 198.51.100.4 110  
Trying 198.51.100.4 ...Open  
C:\>|
```

Выводы

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

Контрольные вопросы

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

NAT позволяет одному устройству (маршрутизатору) действовать, как агент между интернетом (или публичной сетью) и локальной сетью (или частной сетью). Таким образом, требуется только один уникальный IP-адрес для представления всей группы компьютеров чему-либо вне их сети.

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

Для настройки традиционного NAT необходимо создать хотя бы один интерфейс на маршрутизаторе (NAT снаружи) и другой интерфейс на маршрутизаторе (NAT внутри). Кроме того, необходимо настроить набор правил для преобразования IP-адресов в заголовках пакетов (и полезных нагрузок, если это необходимо). Для конфигурации виртуального интерфейса NAT (NVI) необходим, по крайней мере, один интерфейс, настроенный с помощью NAT enable совместно с тем же набором правил.

3. Можно ли применить Cisco IOS NAT к субинтерфейсам?

Можно: исходные/конечные преобразования NAT могут быть применены к любому интерфейсу или подинтерфейсам, имеющим IP-адрес (включая интерфейсы номеронабирателя). NAT не может быть настроен с помощью беспроводного виртуального интерфейса. Беспроводной виртуальный интерфейс не существует во время записи в NVRAM. То есть, после перезагрузки маршрутизатор теряет конфигурацию NAT на беспроводном виртуальном интерфейсе.

4. Что такое пулы IP NAT?

Пулы IP-адресов NAT- это диапазон IP- адресов, выделяемых для трансляции NAT по мере необходимости.

Определить пул которые будут использоваться для перевода, используя команду `ip nat pool [имя начальный_ip конечный_ip]`. Этот пул адресов обычно представляет собой группу публичных общедоступных адресов. Адреса определяются указанием начального IP-адреса и конечного IP-адреса пула. Ключевые слова `netmask` или `prefix-length` указывают маску.

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. Этот тип преобразования особенно рекомендуется применять для организации общего доступа к системе, находящейся во внутренней сети. Для этого нужно создать правило NAT для преобразования

фактического адреса системы во внешний адрес. Этот адрес будет доступен внешним пользователям. В этом случае никто не сможет получить информацию о внутренней сети для последующих атак извне.

Особенности статического NAT:

- Это взаимно однозначное преобразование.
- Его можно инициировать как из внешней, так и из внутренней сети.
- Целевой адрес для преобразования может быть любым адресом.
- Целевой адрес для преобразования не может применяться в качестве интерфейса IP.
- Нельзя применять NAT для преобразования портов.