

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: Шагабаев Д.А.

Группа: НПИбд-02-18

Студенческий билет №1032183650

Преподаватель: Королькова А.В.

МОСКВА

2021 г.

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).

Задание:

1. Сделать первоначальную настройку маршрутизатора `provider-dashagabaev-gw-1` и коммутатора `provider-dashagabaev-sw-1` провайдера: задать имя, настроить доступ по паролю и т.п. (см. разделы 12.4.1, 12.4.2).
2. Настроить интерфейсы маршрутизатора `provider-dashagabaev-gw-1` и коммутатора `provider-sw-1` провайдера: (см. разделы 12.4.3, 12.4.4).
3. Настроить интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера (см. раздел 12.4.5).
4. Настроить на маршрутизаторе сети «Донская» NAT с правилами, указанными в разделе 12.2 (см. разделы 12.4.6–12.4.8).

5. Настроить доступ из внешней сети в локальную сеть организации, как указано в разделе 12.2 (см. раздел 12.4.9).
6. Проверить работоспособность заданных настроек.
7. При выполнении работы необходимо учитывать соглашение об именовании (см. раздел 2.5).

Порядок выполнения работы:

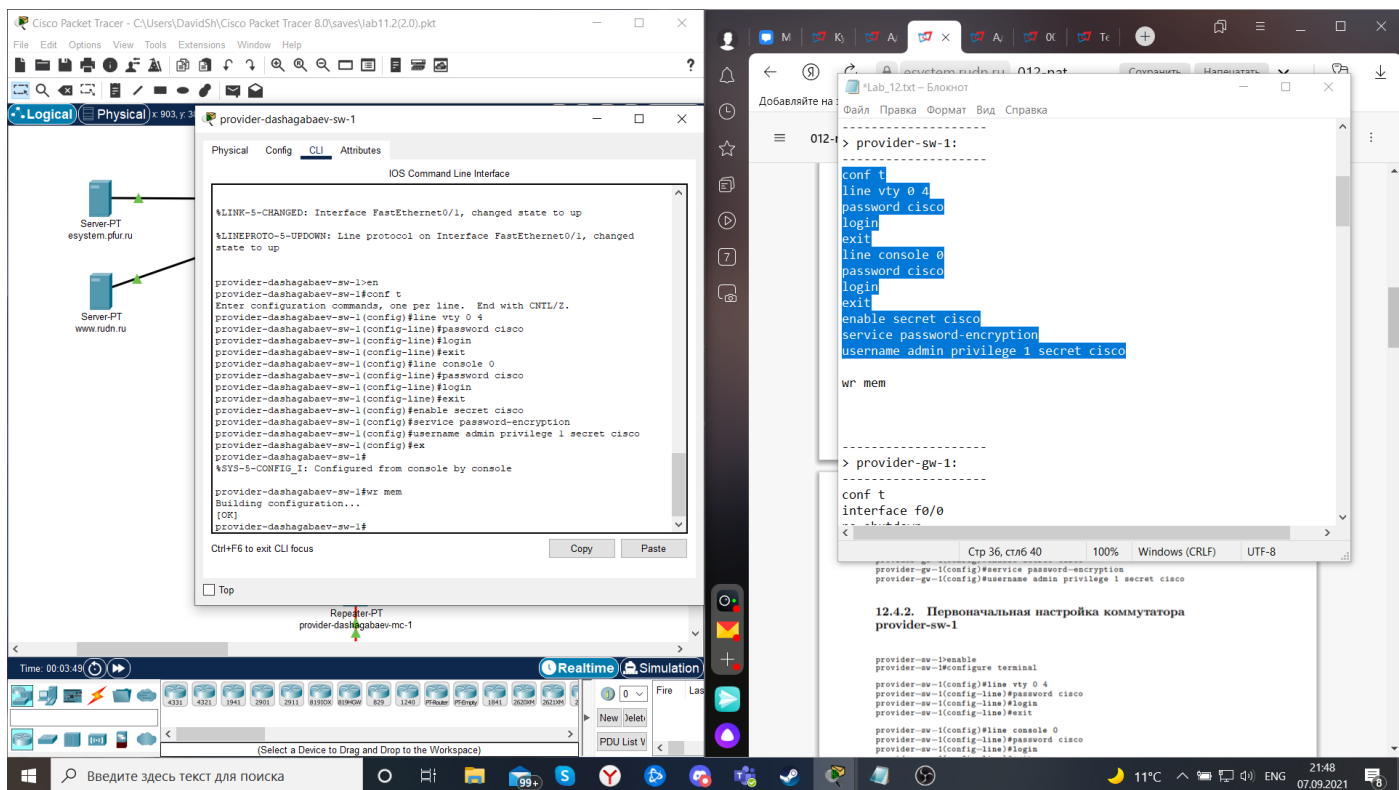
1. Первоначальная настройка маршрутизатора provider-dashagabaev-gw-1

The screenshot shows the Cisco Packet Tracer interface with the CLI window for provider-dashagabaev-gw-1. The configuration commands entered are:

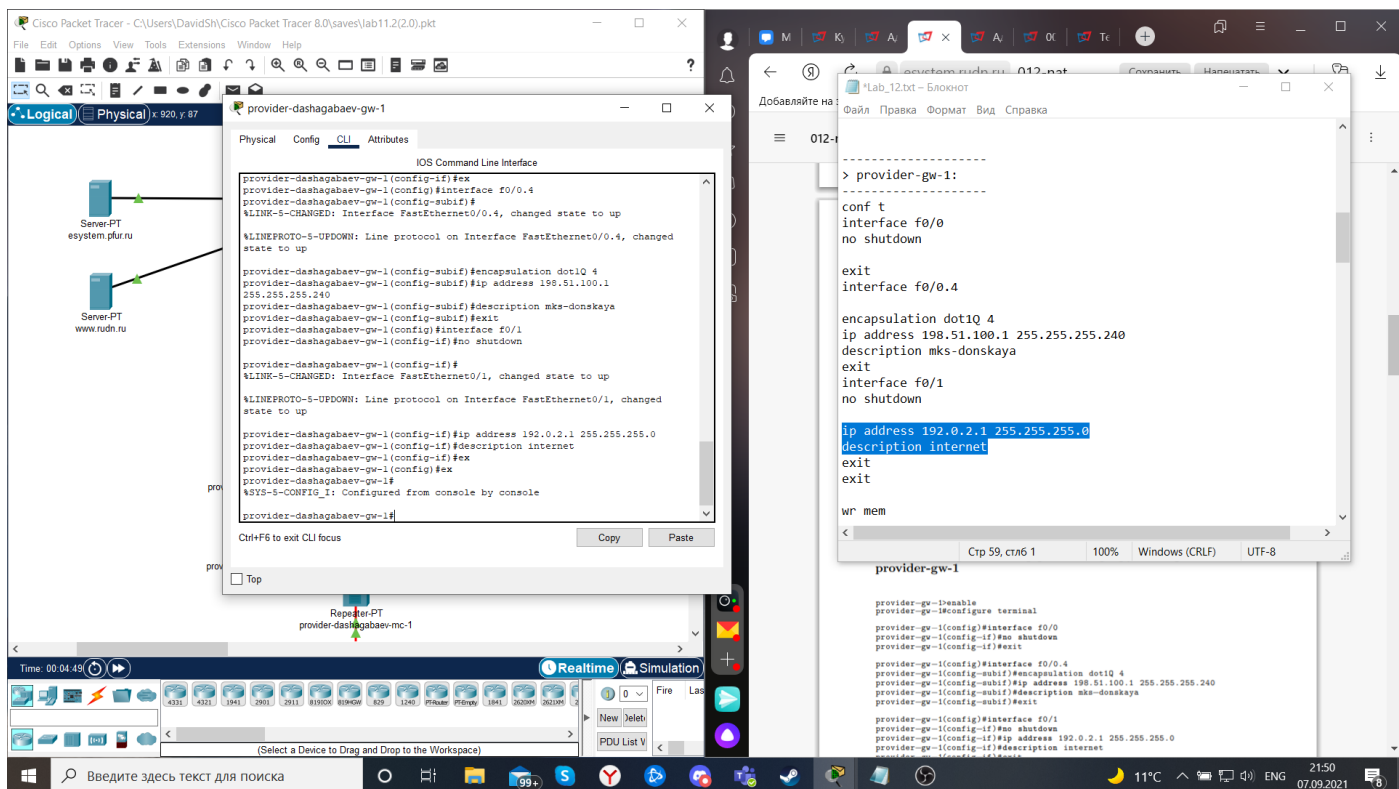
```
provider-dashagabaev-gw-1>enable
provider-dashagabaev-gw-1#configure terminal
provider-dashagabaev-gw-1(config)#line vty 0 4
provider-dashagabaev-gw-1(config-line)#password cisco
provider-dashagabaev-gw-1(config-line)#login
provider-dashagabaev-gw-1(config-line)#exit
provider-dashagabaev-gw-1(config)#line console 0
provider-dashagabaev-gw-1(config-line)#password cisco
provider-dashagabaev-gw-1(config-line)#login
provider-dashagabaev-gw-1(config-line)#exit
provider-dashagabaev-gw-1(config)#enable secret cisco
provider-dashagabaev-gw-1(config)#service password-encryption
provider-dashagabaev-gw-1(config)#username admin privilege 1 secret cisco
provider-dashagabaev-gw-1(config)#exit
provider-dashagabaev-gw-1#show startup-config
%SYS-5-CONFIG_I: Configured from console by console
provider-dashagabaev-gw-1#write mem
Building configuration...
[OK]
provider-dashagabaev-gw-1#
```

The configuration is saved to the startup configuration. The background shows a web browser with a document titled '012-nat.pdf' and a text editor with a configuration script for provider-gw-1 and provider-sw-1.

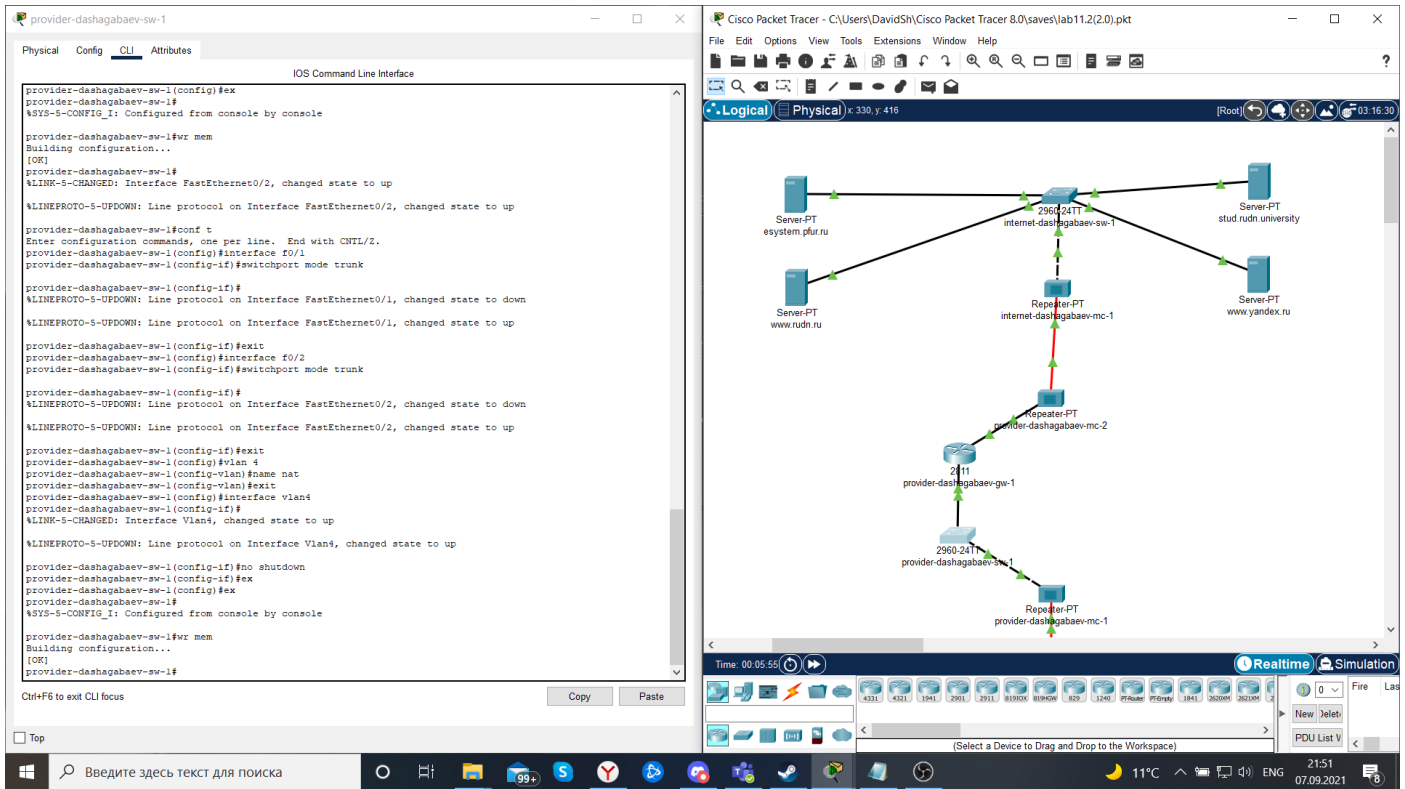
2. Первоначальная настройка коммутатора provider-dashagabaev-sw-1



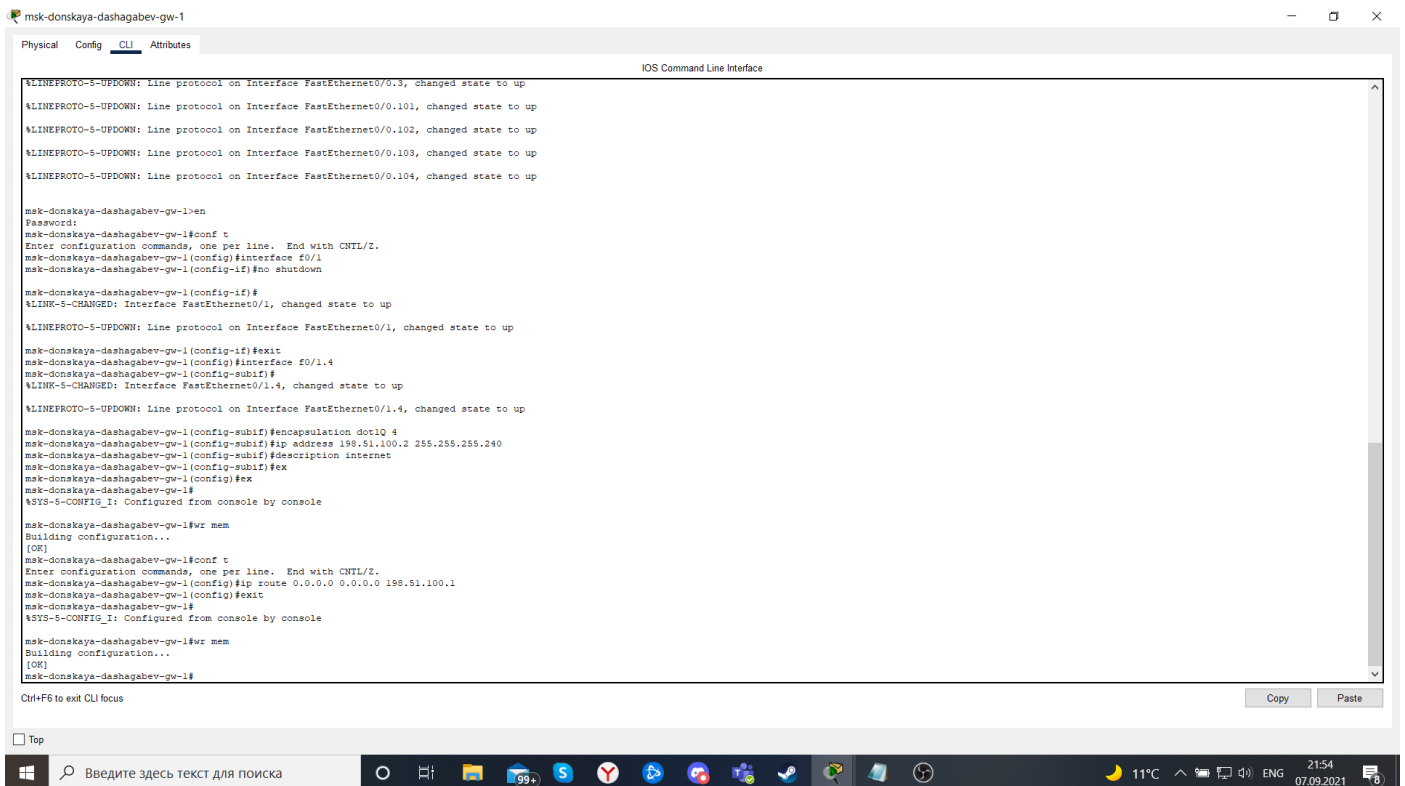
3. Настройка интерфейсов маршрутизатора provider-dashagabaev-gw-1

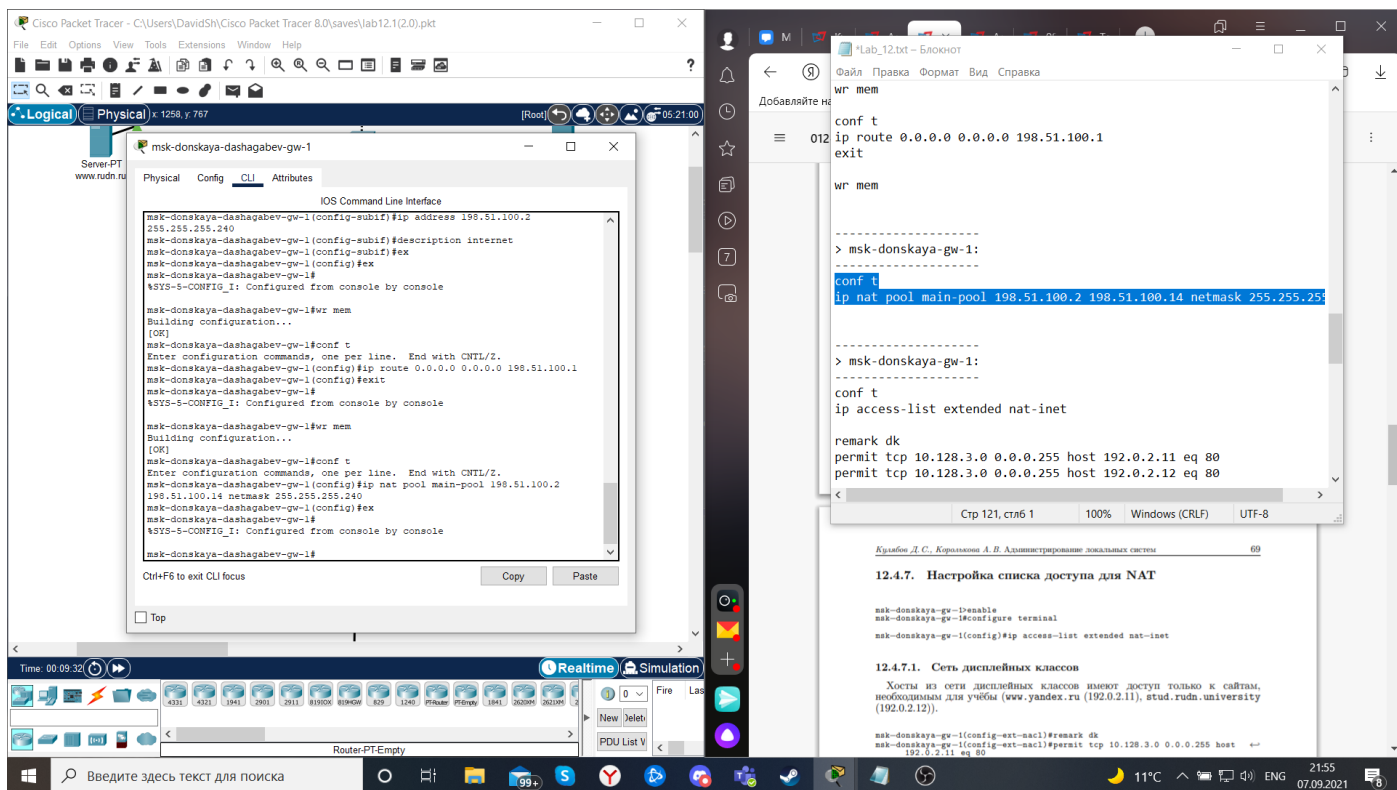


4. Настройка интерфейсов коммутатора provider-dashagabaev-sw-1

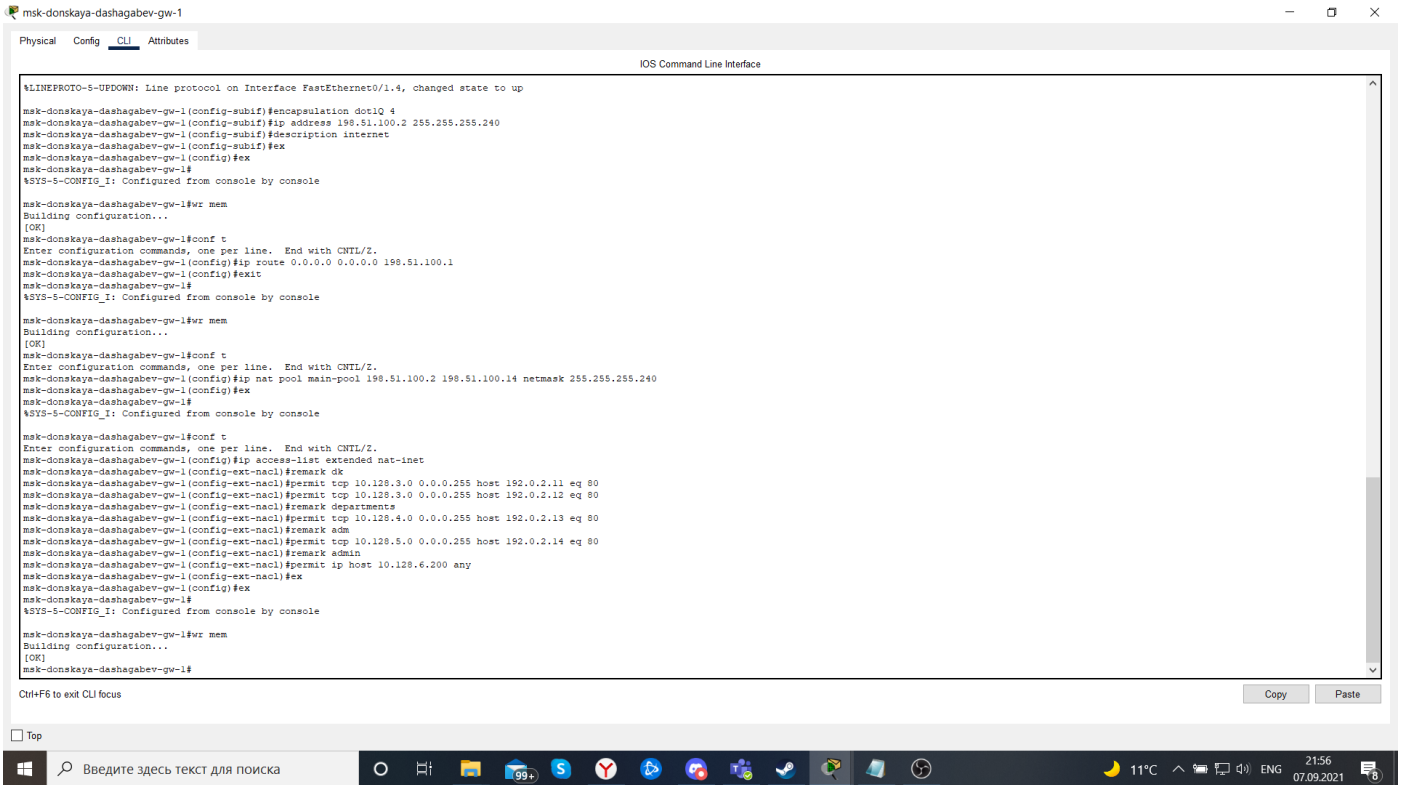


5. Настройка интерфейсов маршрутизатора msk-donskaya-dashagabaev-gw-1





6. Настройка пула адресов для NAT



7. Настройка списка доступа для NAT

Сеть дисплейных классов

Сеть кафедр

Сеть администрации

Доступ для компьютера администратора

msk-donskaya-dashagabev-gw-1

Physical Config CLI Attributes

IOS Command Line Interface

```
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/1.4, changed state to up
msk-donskaya-dashagabev-gw-1(config-subif)#noospaulation dot1q 4
msk-donskaya-dashagabev-gw-1(config-subif)#ip address 190.51.100.2 255.255.255.240
msk-donskaya-dashagabev-gw-1(config-subif)#description internet
msk-donskaya-dashagabev-gw-1(config-subif)#ex
msk-donskaya-dashagabev-gw-1(config)#ex
msk-donskaya-dashagabev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dashagabev-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-dashagabev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dashagabev-gw-1(config)#ip route 0.0.0.0 0.0.0.0 190.51.100.1
msk-donskaya-dashagabev-gw-1(config)#exit
msk-donskaya-dashagabev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dashagabev-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-dashagabev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dashagabev-gw-1(config)#ip nat pool main-pool 190.51.100.2 190.51.100.14 netmask 255.255.255.240
msk-donskaya-dashagabev-gw-1(config)#ex
msk-donskaya-dashagabev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

msk-donskaya-dashagabev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dashagabev-gw-1(config)#ip access-list extended nat-inet
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#remark dk
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq 80
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq 80
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#remark departments
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.13 eq 80
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#remark adm
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq 80
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#remark admin
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#permit ip host 10.128.6.200 any
msk-donskaya-dashagabev-gw-1(config-ext-nacl)#ex
msk-donskaya-dashagabev-gw-1(config)#ex
msk-donskaya-dashagabev-gw-1#
%SYS-5-CONFIG_I: Configured from console by console

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

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Введите здесь текст для поиска

99+

11°C

ENG

21:56

07.09.2021

msk-donskaya-dashagabev-gw-1

Physical Config CLI Attributes

IOS Command Line Interface

```
ip access-list extended servers-out
remark web
permit icmp any any
permit tcp any host 10.128.0.2 eq www
permit tcp host 10.128.6.200 host 10.128.0.2 range 20 ftp
permit tcp host 10.128.6.200 host 10.128.0.2 eq telnet
remark file
permit tcp 10.128.0.0 0.0.255.255 host 10.128.0.3 eq 445
permit tcp any host 10.128.0.3 range 20 ftp
remark mail
permit tcp any host 10.128.0.4 eq smtp
permit tcp any host 10.128.0.4 eq pop3
remark dns
permit udp 10.128.0.0 0.0.255.255 host 10.128.0.5 eq domain
permit tcp host 10.128.6.201 host 10.128.0.2 range 20 ftp
permit tcp host 10.128.6.201 host 10.128.0.2 eq telnet
ip access-list extended other-in
remark admin
permit ip host 10.128.6.200 any
permit ip host 10.128.6.201 any
ip access-list extended management-out
remark admin
permit ip host 10.128.6.200 10.128.1.0 0.0.0.255
permit ip host 10.128.6.201 10.128.1.0 0.0.0.255
ip access-list extended nat-inet
remark dk
permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.11 eq www
permit tcp 10.128.3.0 0.0.0.255 host 192.0.2.12 eq www
remark departments
permit tcp 10.128.4.0 0.0.0.255 host 192.0.2.13 eq www
remark adm
permit tcp 10.128.5.0 0.0.0.255 host 192.0.2.14 eq www
remark admin
permit ip host 10.128.6.200 any
,
,
,
,
line con 0
,
line aux 0
,
line vty 0 4
password 7 0822455D0A16
login
transport input ssh
,
,
,
```

Ctrl+F6 to exit CLI focus

Copy Paste

Top

Введите здесь текст для поиска

99+

11°C

ENG

21:57

07.09.2021

8. Настройка NAT:

The screenshot displays the Cisco Packet Tracer interface with a router configuration window open. The configuration commands for NAT are as follows:

```
msk-donskaya-dashagabev-gw-1#conf t
msk-donskaya-dashagabev-gw-1(config)#ip nat inside source list nat-inet pool main-pool overload
msk-donskaya-dashagabev-gw-1(config)#int f0/0.3
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat inside
msk-donskaya-dashagabev-gw-1(config-subif)#interface f0/0.101
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat inside
msk-donskaya-dashagabev-gw-1(config-subif)#exit
msk-donskaya-dashagabev-gw-1(config)#interface f0/0.102
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat inside
msk-donskaya-dashagabev-gw-1(config-subif)#exit
msk-donskaya-dashagabev-gw-1(config)#interface f0/0.103
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat inside
msk-donskaya-dashagabev-gw-1(config-subif)#exit
msk-donskaya-dashagabev-gw-1(config)#interface f0/0.104
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat inside
msk-donskaya-dashagabev-gw-1(config-subif)#exit
msk-donskaya-dashagabev-gw-1(config)#interface f0/1.4
msk-donskaya-dashagabev-gw-1(config-subif)#ip nat outside
msk-donskaya-dashagabev-gw-1(config-subif)#exit
msk-donskaya-dashagabev-gw-1(config)#ex
msk-donskaya-dashagabev-gw-1#
```

Below the configuration window, a text file named "Lab_12.txt" is open, showing the same configuration commands. The file also includes a section titled "12.4.9. Настройка доступа из Интернета" and "12.4.9.1. WWW-сервер" with static NAT configurations for specific IP addresses.

```
conf t
ip nat inside source list nat-inet pool main-pool overload

int f0/0.3
ip nat inside
interface f0/0.101
ip nat inside
exit
interface f0/0.102
ip nat inside
exit
interface f0/0.103
ip nat inside
exit
interface f0/0.104
ip nat inside
exit
interface f0/1.4
ip nat outside
exit

wr mem
```

The text file also contains the following static NAT configurations:

```
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.2 80 <--> 198.51.100.2 80

12.4.9.2. Файловый сервер

msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 20 <--> 198.51.100.3 20
msk-donskaya-gw-1(config)#ip nat inside source static tcp 10.128.0.3 21 <--> 198.51.100.3 21
```

-
- The screenshot displays a Cisco Packet Tracer simulation environment. The main window shows a network diagram with a router labeled 'msk-donskaya-dashagabev-gw-1'. The router's configuration is shown in the 'CLI' tab, displaying the following commands:
- ```
msk-donskaya-dashagabev-gw-1 (config)#interface f0/1.4
msk-donskaya-dashagabev-gw-1 (config-subif)#ip nat outside
msk-donskaya-dashagabev-gw-1 (config-subif)#exit
msk-donskaya-dashagabev-gw-1 (config)#
msk-donskaya-dashagabev-gw-1#
SYS-S-CONFIG_1: Configured from console by console

msk-donskaya-dashagabev-gw-1#wr mem
Building configuration...
[OK]
msk-donskaya-dashagabev-gw-1#ip nat inside source static top 10.128.0.2 80
198.51.100.2 80
^
Invalid input detected at '^' marker.

msk-donskaya-dashagabev-gw-1#conf t
Enter configuration commands, one per line. End with CNTL/Z.
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.0.2 80 198.51.100.2 80
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.0.3 20 198.51.100.3 20
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.0.3 21 198.51.100.3 21
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.0.4 25 198.51.100.4 25
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.0.4 110 198.51.100.4 110
msk-donskaya-dashagabev-gw-1 (config)#ip nat inside source static top
10.128.6.200 3389 198.51.100.10 3389
msk-donskaya-dashagabev-gw-1 (config)#
```
- A second terminal window, titled 'lab\_12.txt - Блокнот', shows the configuration being applied to the router:
- ```
> msk-donskaya-gw-1:
-----
ip nat inside source static tcp 10.128.0.2 80 198.51.100.2 80

ip nat inside source static tcp 10.128.0.3 20 198.51.100.3 20
ip nat inside source static tcp 10.128.0.3 21 198.51.100.3 21

ip nat inside source static tcp 10.128.0.4 25 198.51.100.4 25
ip nat inside source static tcp 10.128.0.4 110 198.51.100.4 110

ip nat inside source static tcp 10.128.6.200 3389 198.51.100.10 3389
```
- The bottom of the screenshot shows the 'Realtime' and 'Simulation' tabs, indicating the simulation is running. The status bar at the bottom shows the time as 00:13:00 and the simulation is in the 'Running' state.

Проверяем наши настройки:

1. Проверка доступа www.yandex.ru с msk-donskaya-dashagabaev-sw-1.
Сеть управления устройствами не имеет доступа в Интернет.

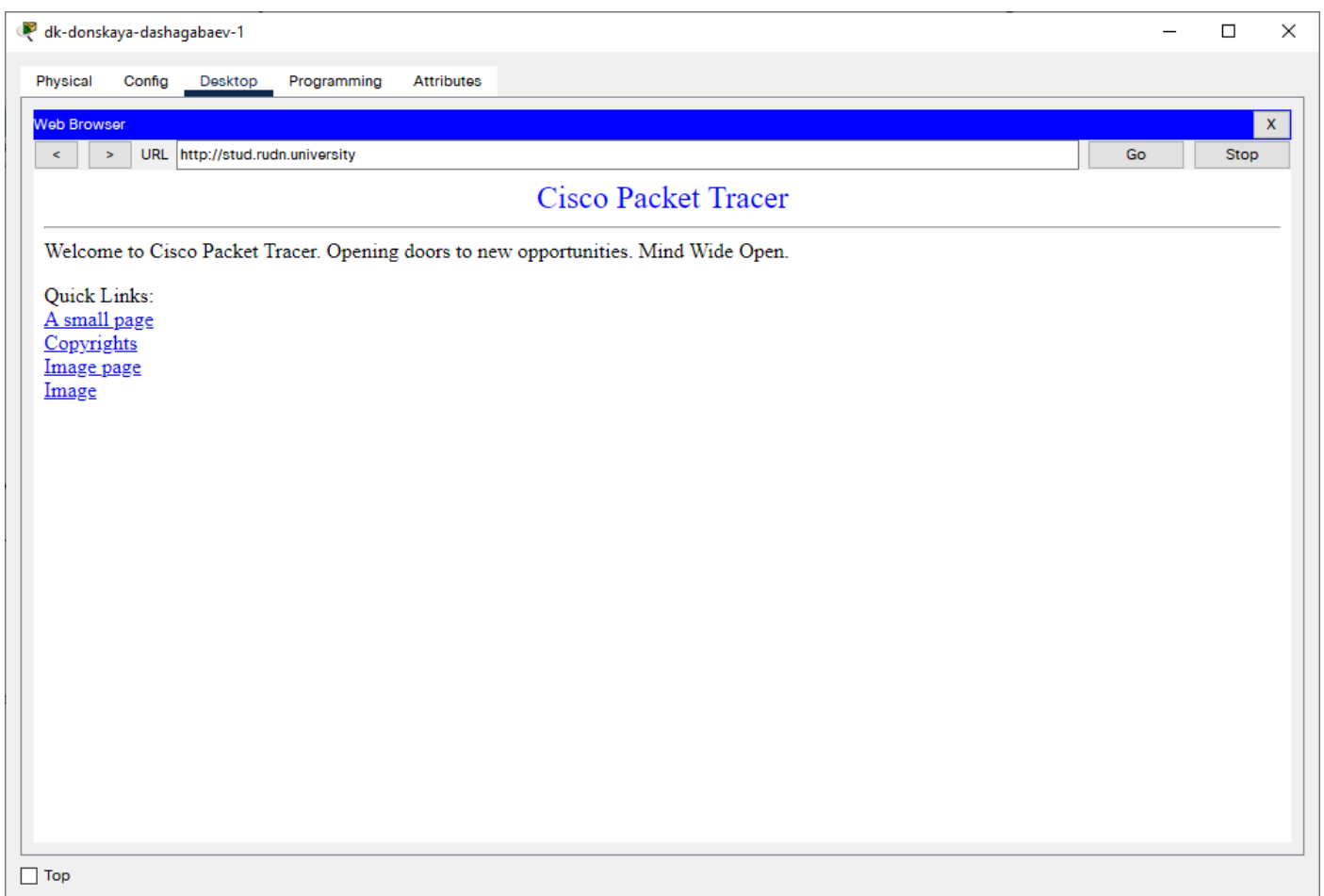
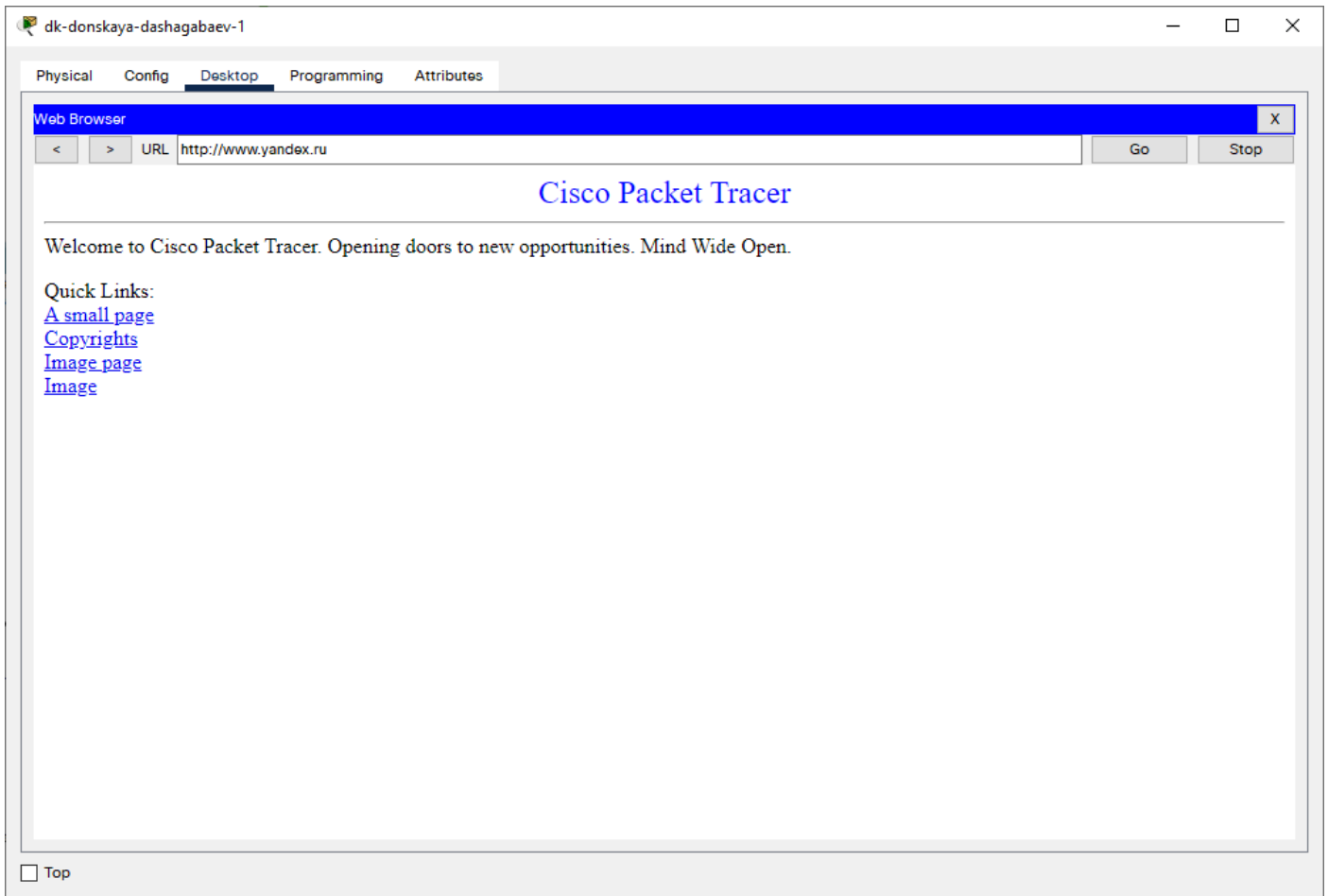
The screenshot displays the Cisco Packet Tracer interface. The main workspace shows a network topology with several devices: a switch (msk-pavlovskaya-dashagabaev-sw-1), a router (msk-pavlovskaya-dashagabaev-r-1), and a laptop (Laptop-PT admin). The switch is connected to the router, which is connected to the laptop. The switch is also connected to a server (Server-PT web) and a PC (PC-PT dk-pavlovskaya-dashagabaev-1). The router is connected to a PC (PC-PT dk-donskaya-dashagabaev-1) and a server (Server-PT mail). The laptop is connected to a server (Server-PT dns).

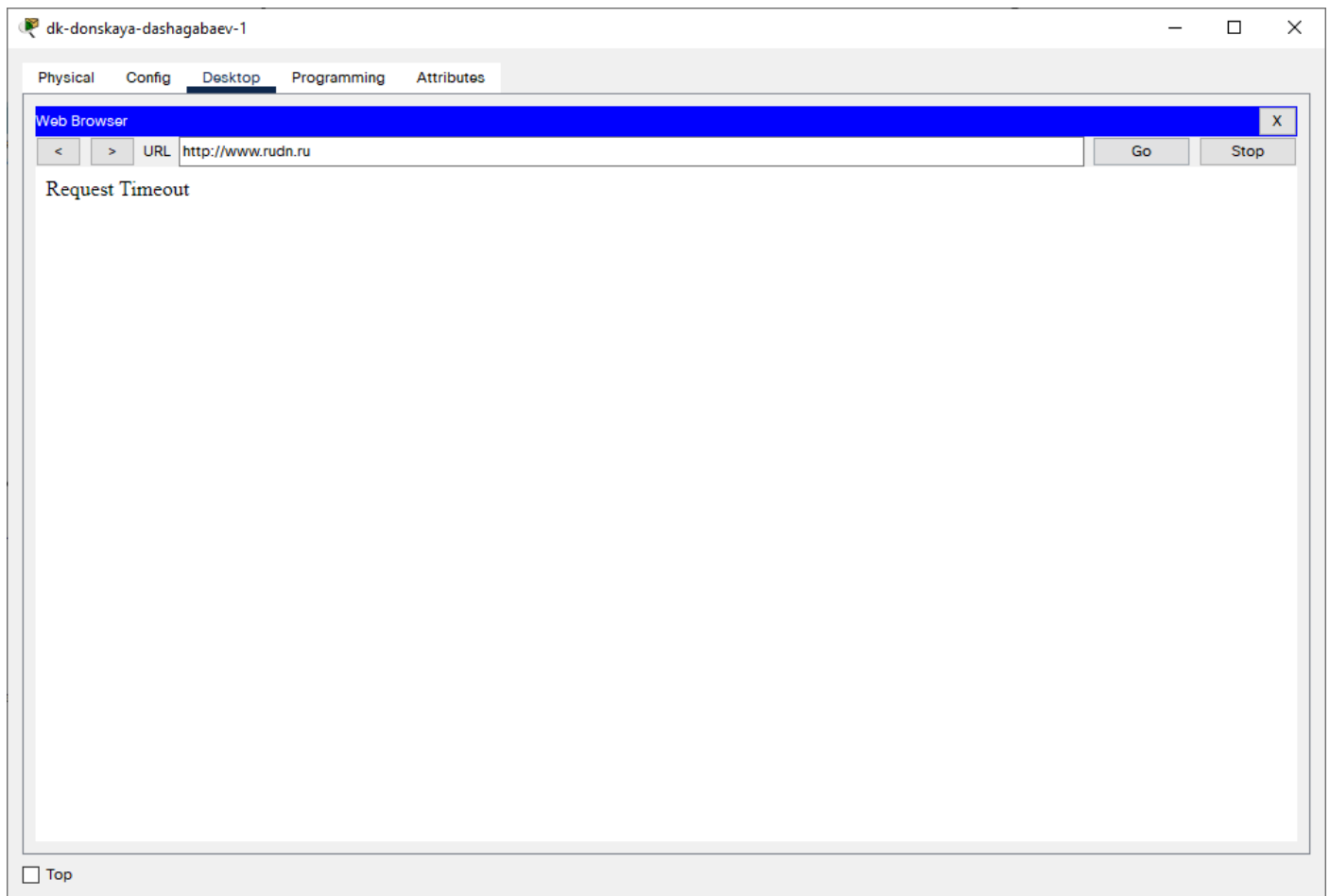
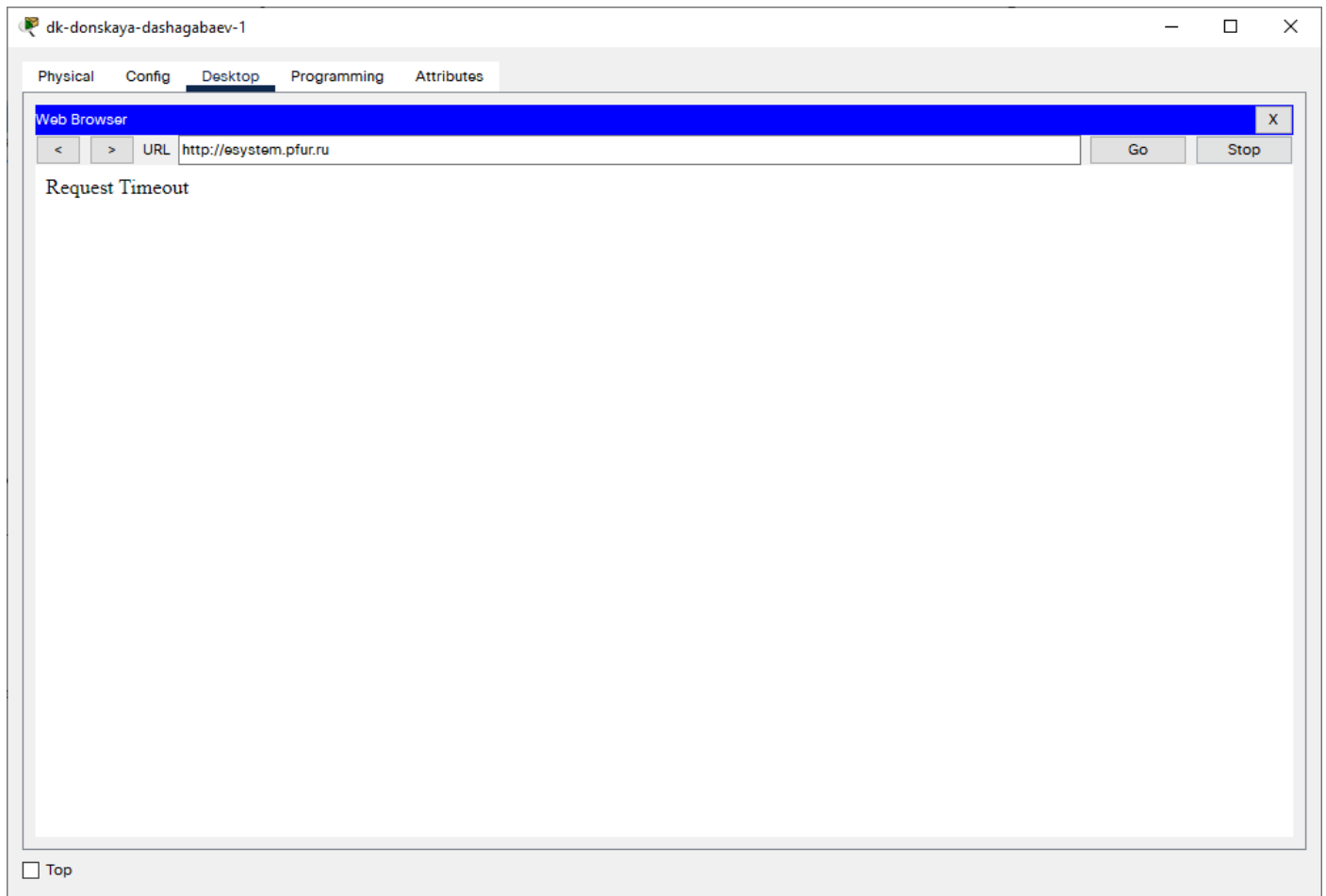
A terminal window for the switch msk-donskaya-dashagabaev-sw-1 is open, showing the following output:

```
IOS Command Line Interface
%LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0/2, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/20, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/21, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up
%LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet0/22, changed state to up
%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

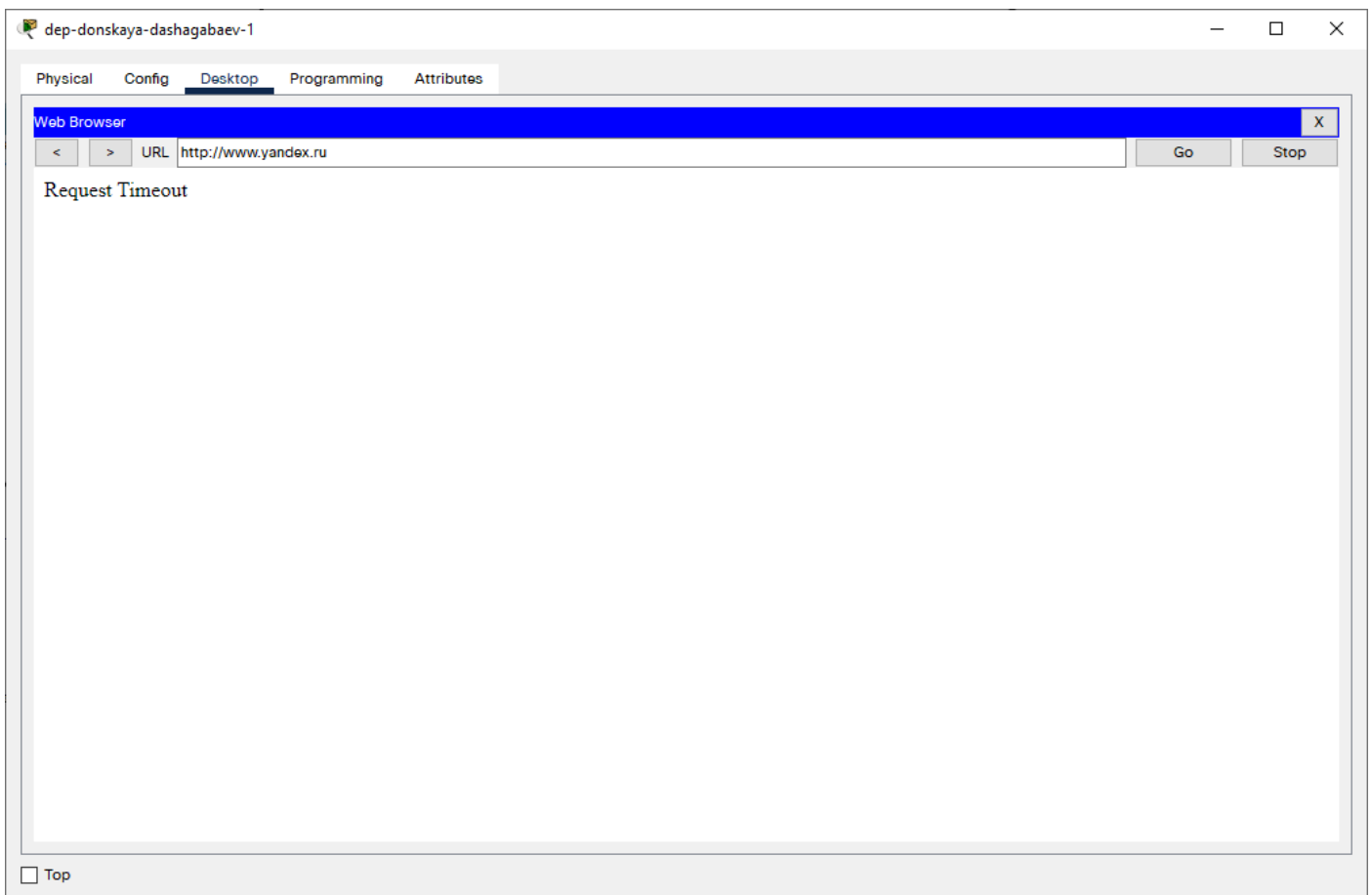
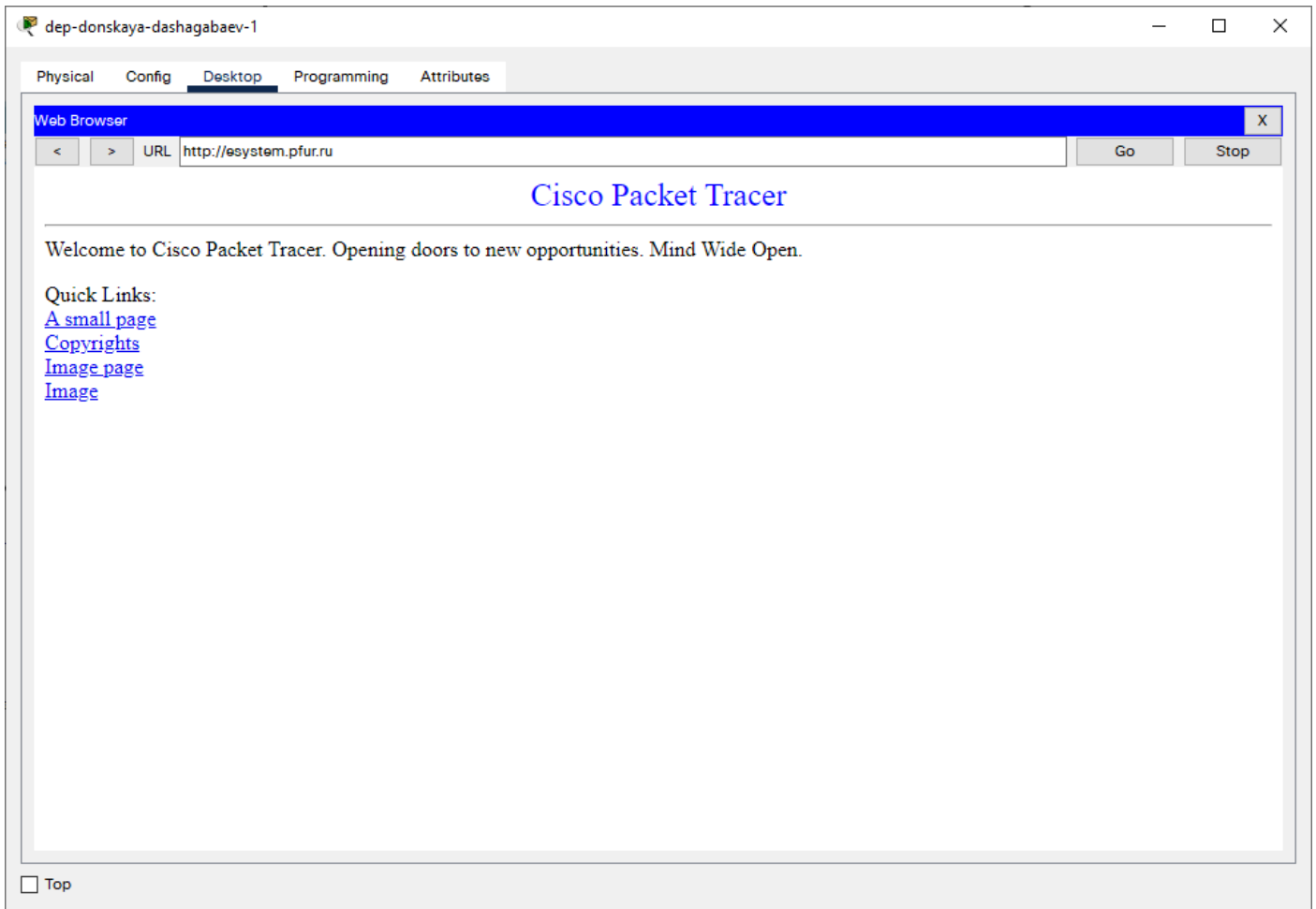
User Access Verification
Password:
msk-donskaya-dashagabaev-sw-1#
msk-donskaya-dashagabaev-sw-1#ping 192.0.2.11
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.0.2.11, timeout is 2 seconds:
.....
Success rate is 0 percent (0/5)
msk-donskaya-dashagabaev-sw-1#
```

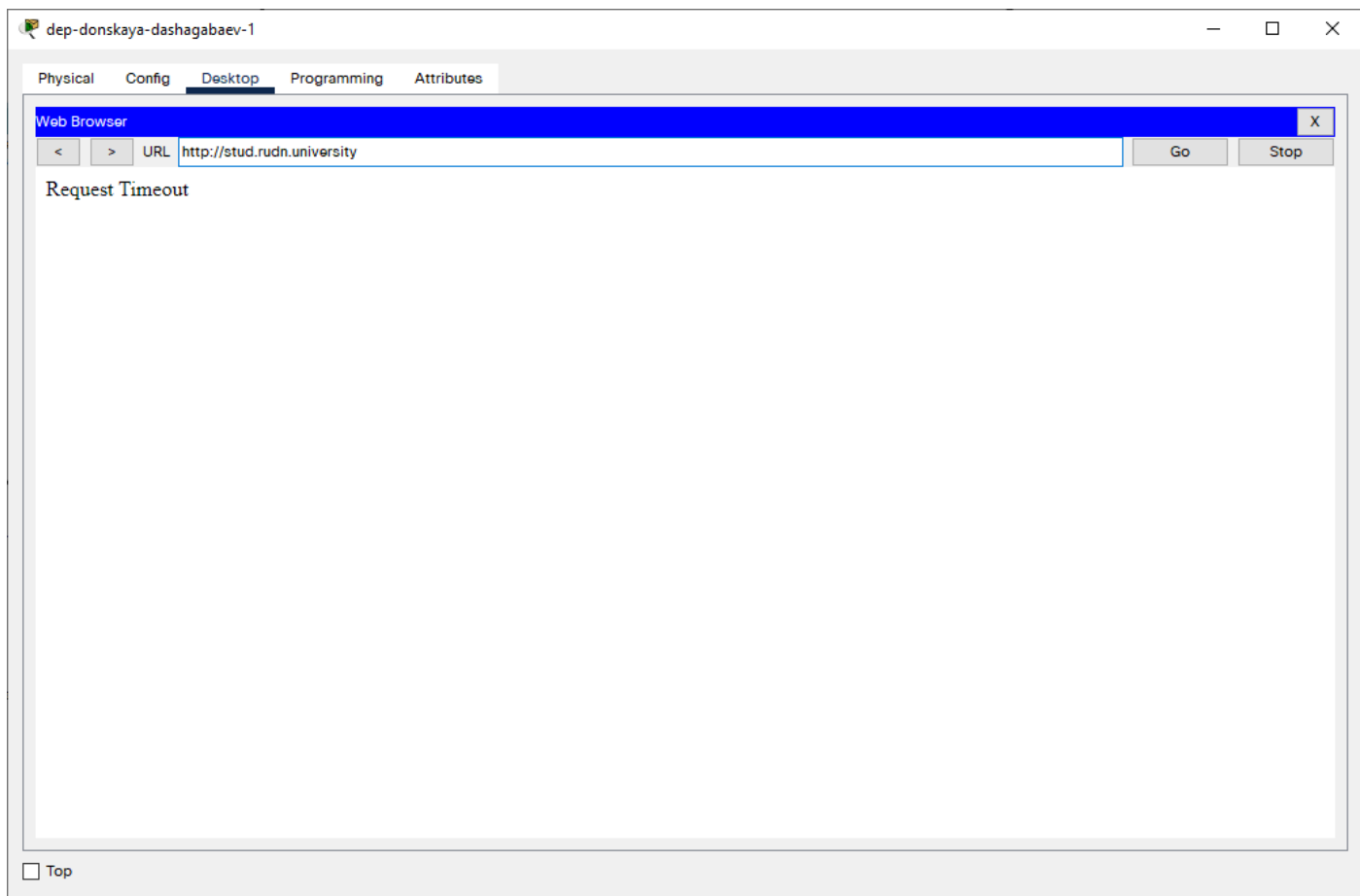
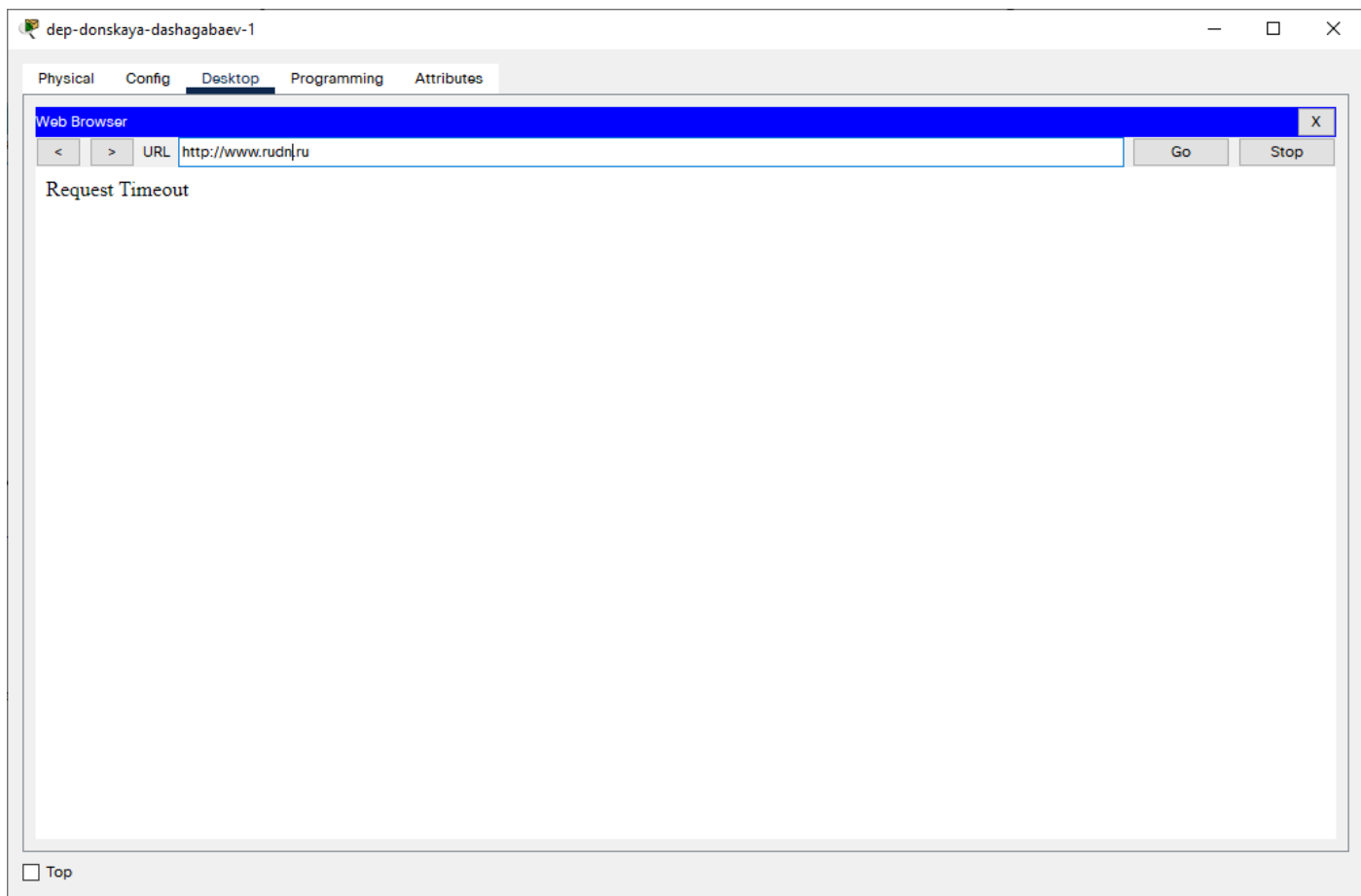
2. Оконечные устройства сети дисплейных классов должны иметь доступ только к определённым сайтам: к www.yandex.ru и stud.rudn.university.



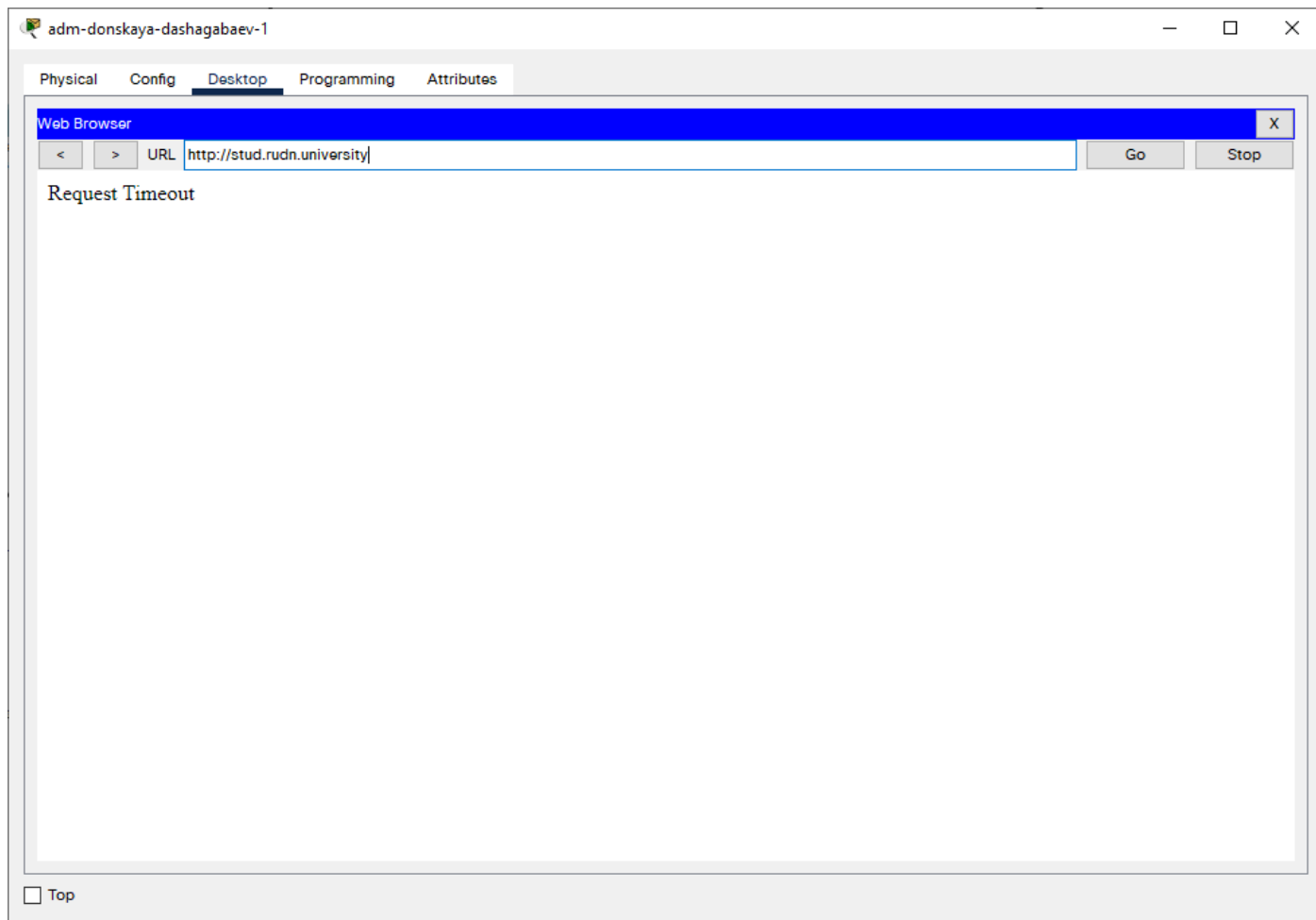


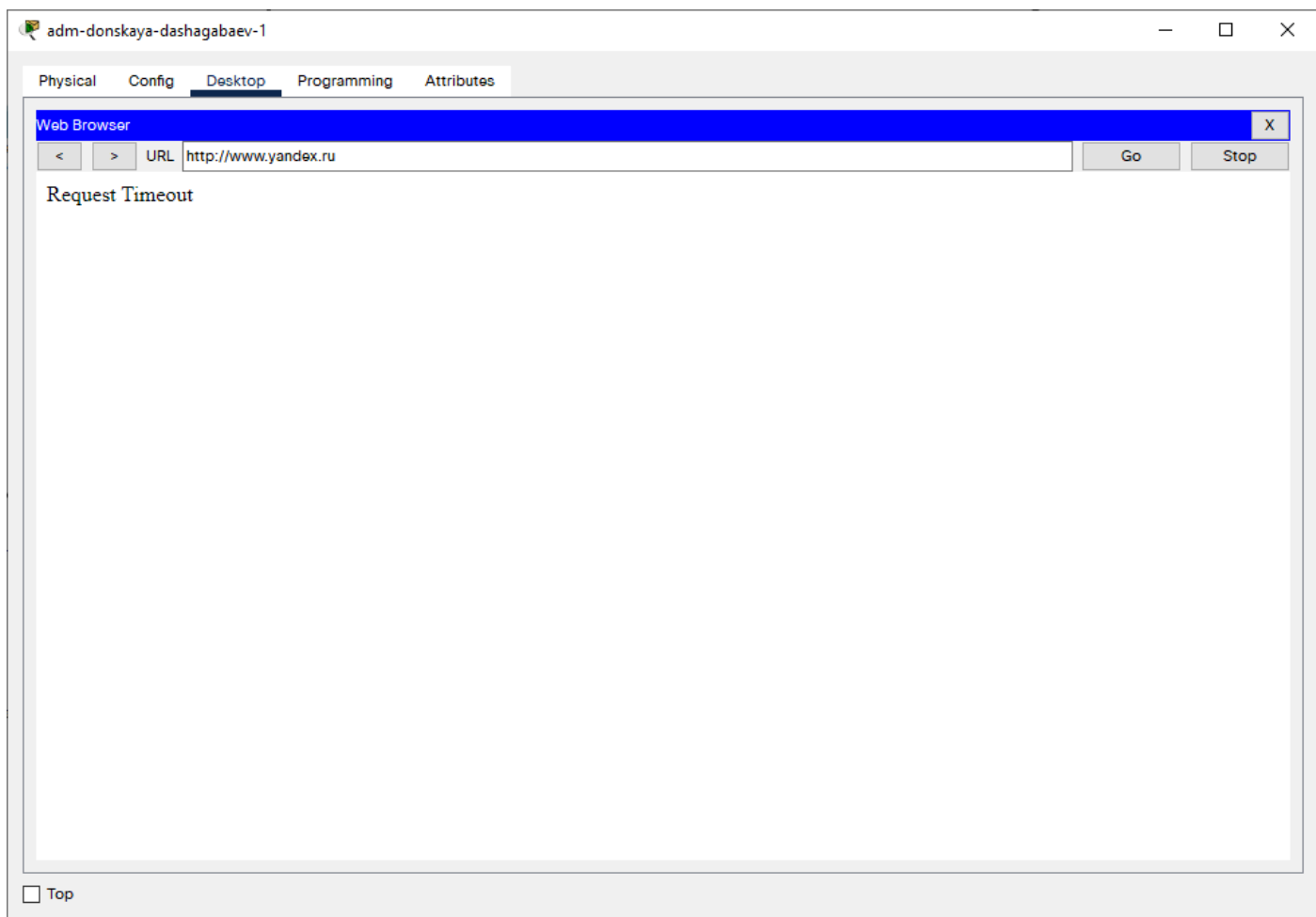
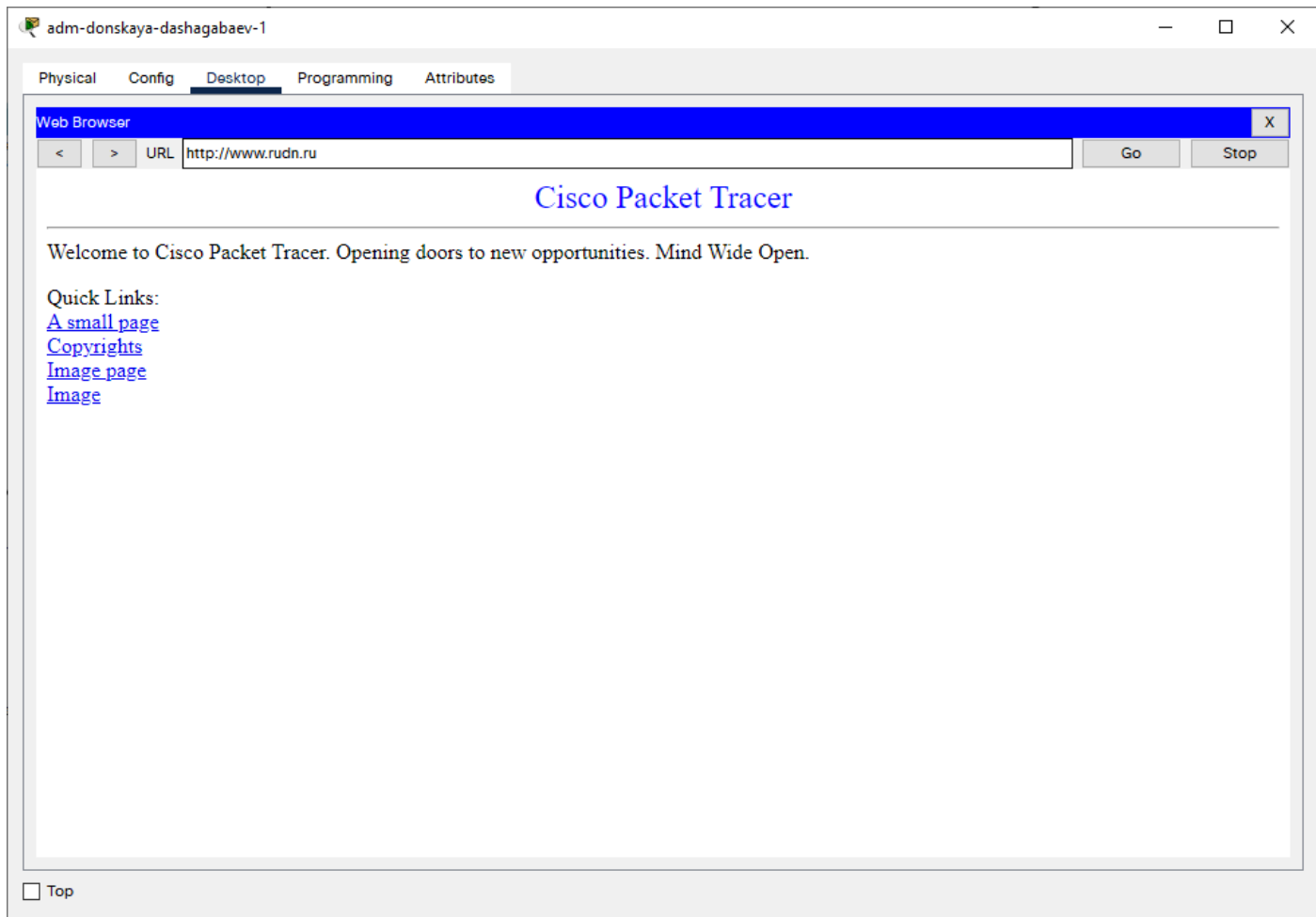
3. Оконечные устройства сети кафедр должны иметь доступ только к сайту esystem.pfur.ru.





4. Оконечные устройства сети администрации должны иметь доступ только к сайту www.rudn.ru.





Physical Config **Desktop** Programming Attributes

Web Browser

X

< > URL

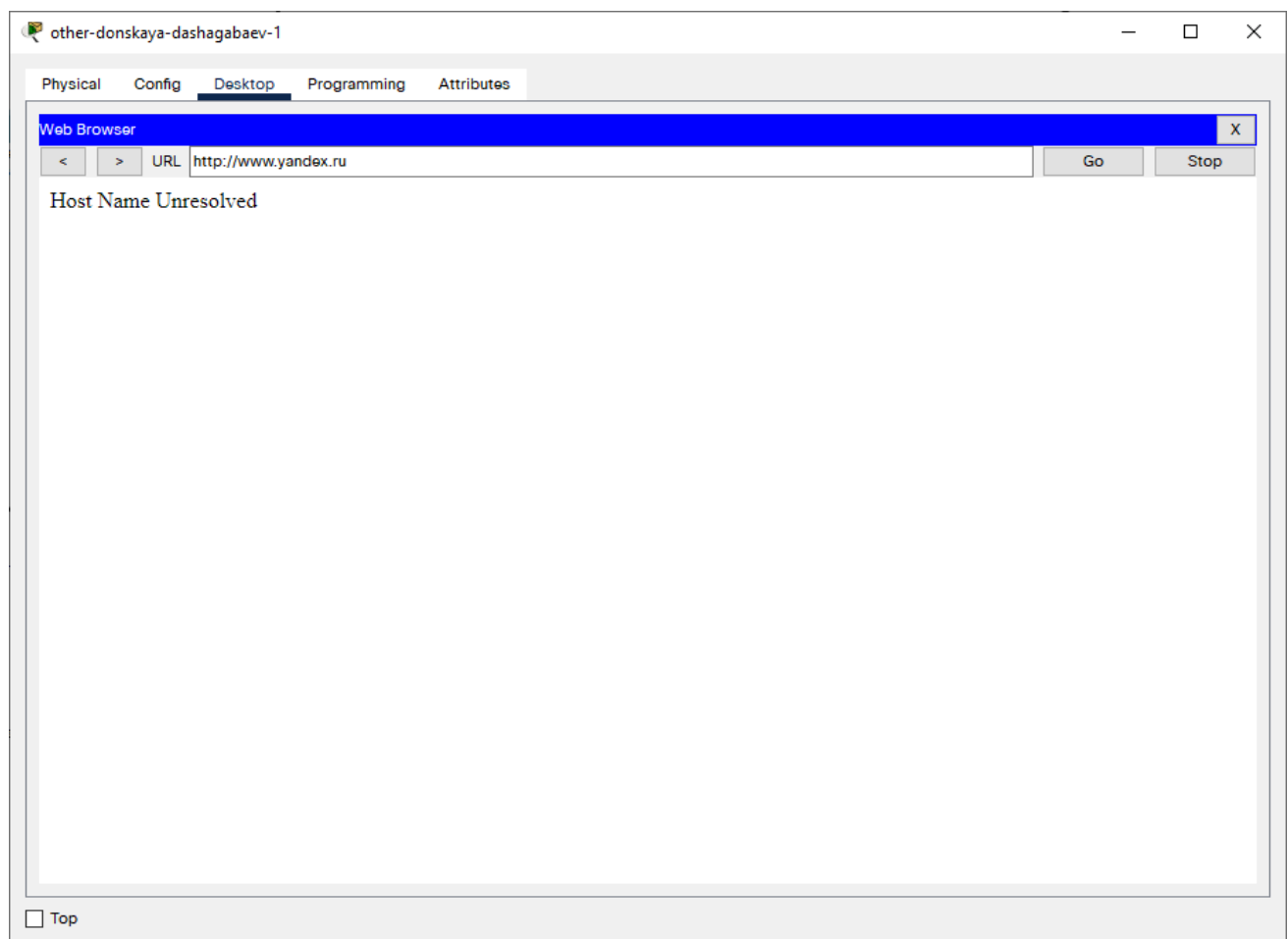
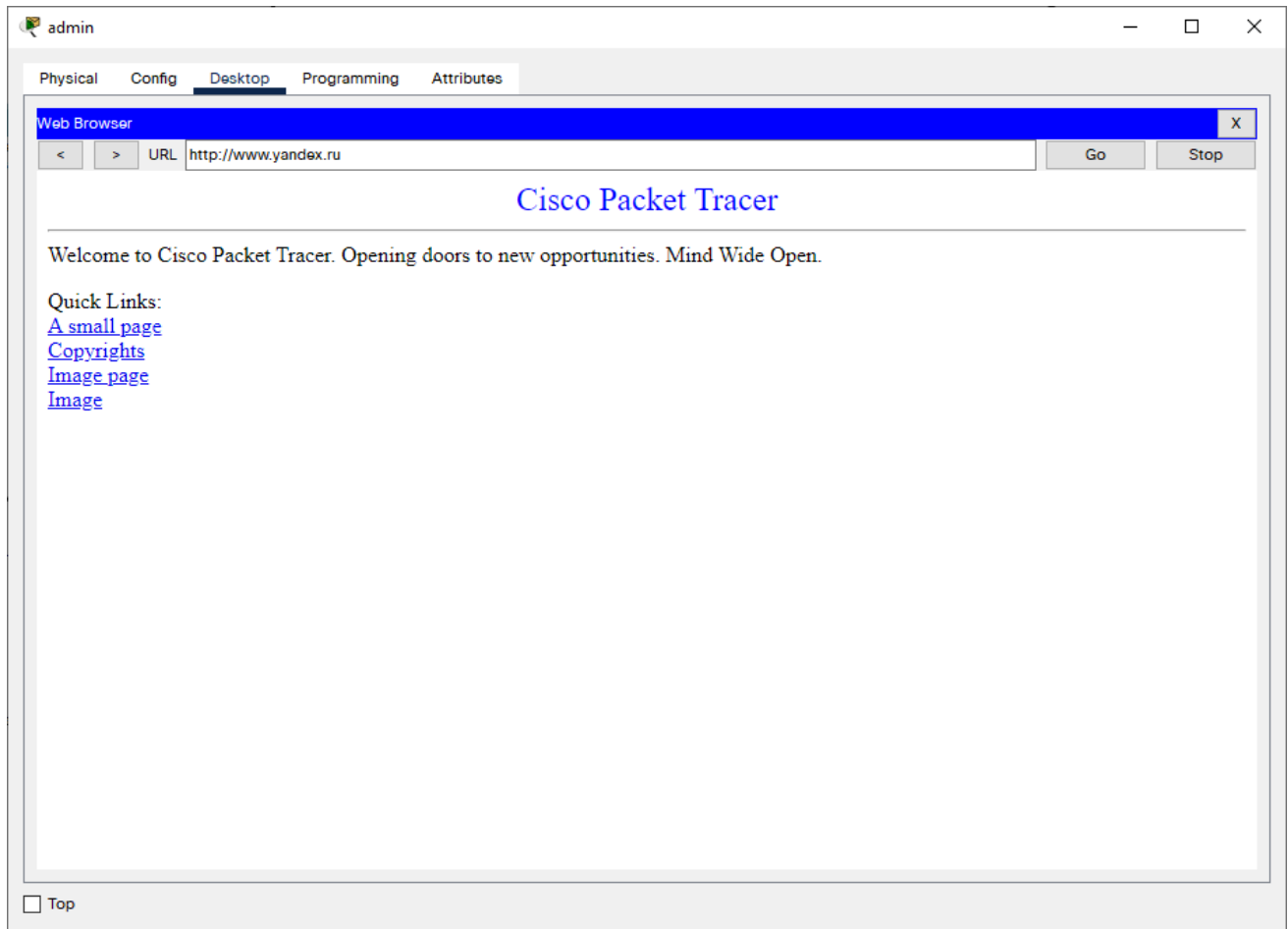
Go

Stop

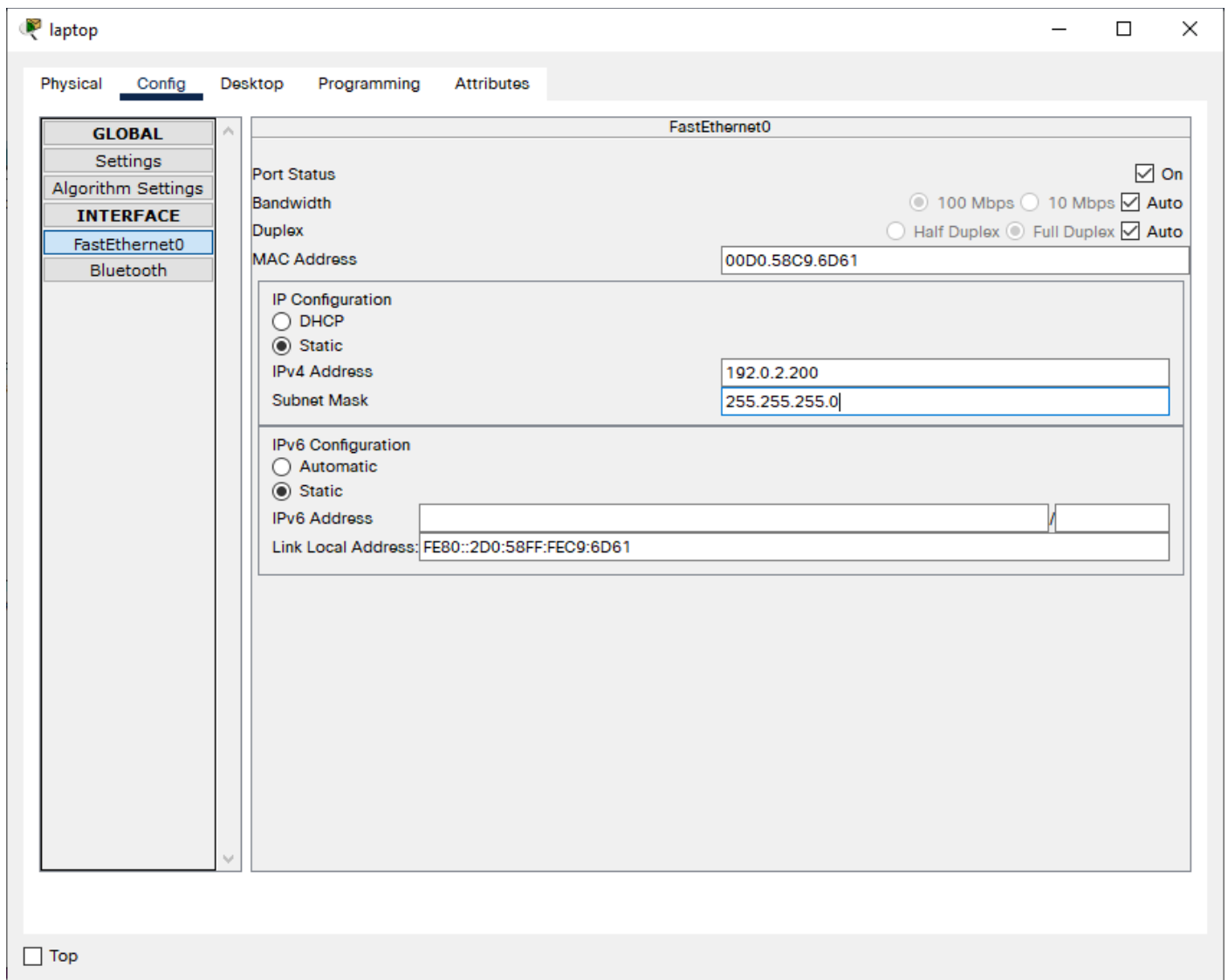
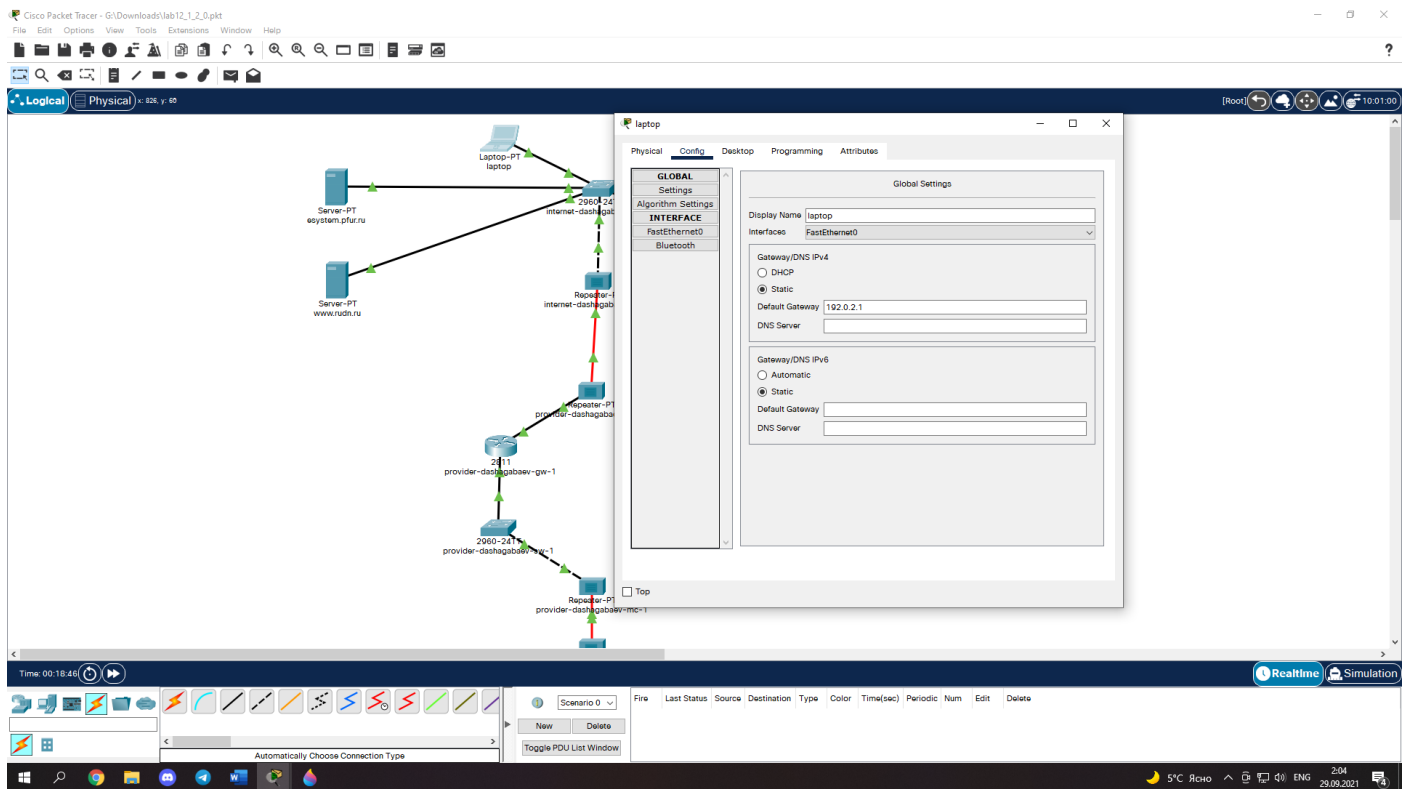
Request Timeout

☐ Top

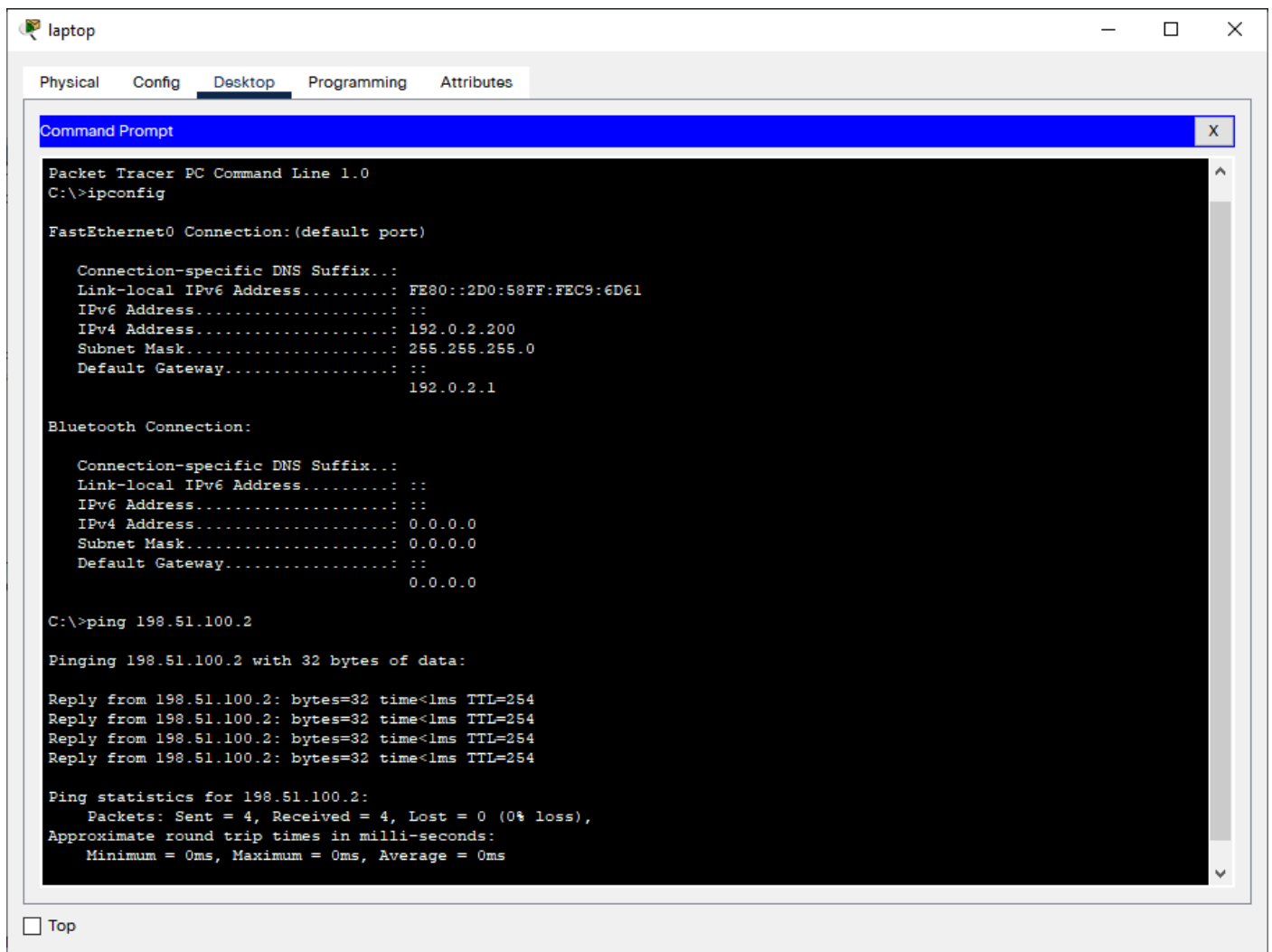
5. Компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи не должны выходить в Интернет.



6. Добавим устройство laptop для проверки конфигурации.



WEB сервер доступен по порту 80:



The screenshot shows a Packet Tracer laptop interface with a 'Command Prompt' window open. The window title is 'Command Prompt' with a close button (X). The interface has tabs for 'Physical', 'Config', 'Desktop', 'Programming', and 'Attributes', with 'Desktop' selected. The Command Prompt text is as follows:

```
Packet Tracer PC Command Line 1.0
C:\>ipconfig

FastEthernet0 Connection:(default port)

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: FE80::2D0:58FF:FEC9:6D61
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 192.0.2.200
    Subnet Mask . . . . .: 255.255.255.0
    Default Gateway . . . . .: ::
                                192.0.2.1

Bluetooth Connection:

    Connection-specific DNS Suffix...:
    Link-local IPv6 Address . . . . .: ::
    IPv6 Address . . . . .: ::
    IPv4 Address . . . . .: 0.0.0.0
    Subnet Mask . . . . .: 0.0.0.0
    Default Gateway . . . . .: ::
                                0.0.0.0

C:\>ping 198.51.100.2

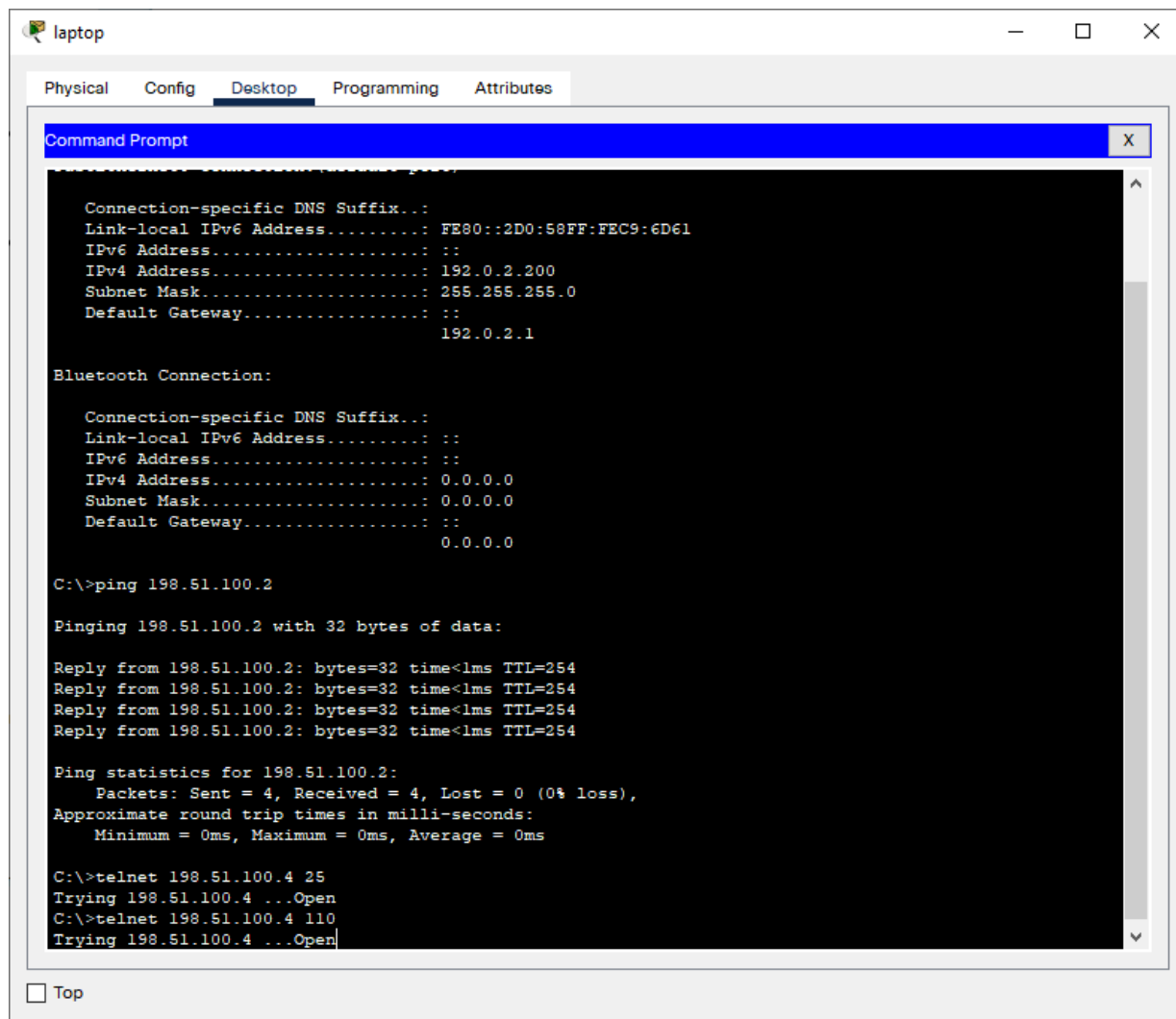
Pinging 198.51.100.2 with 32 bytes of data:

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

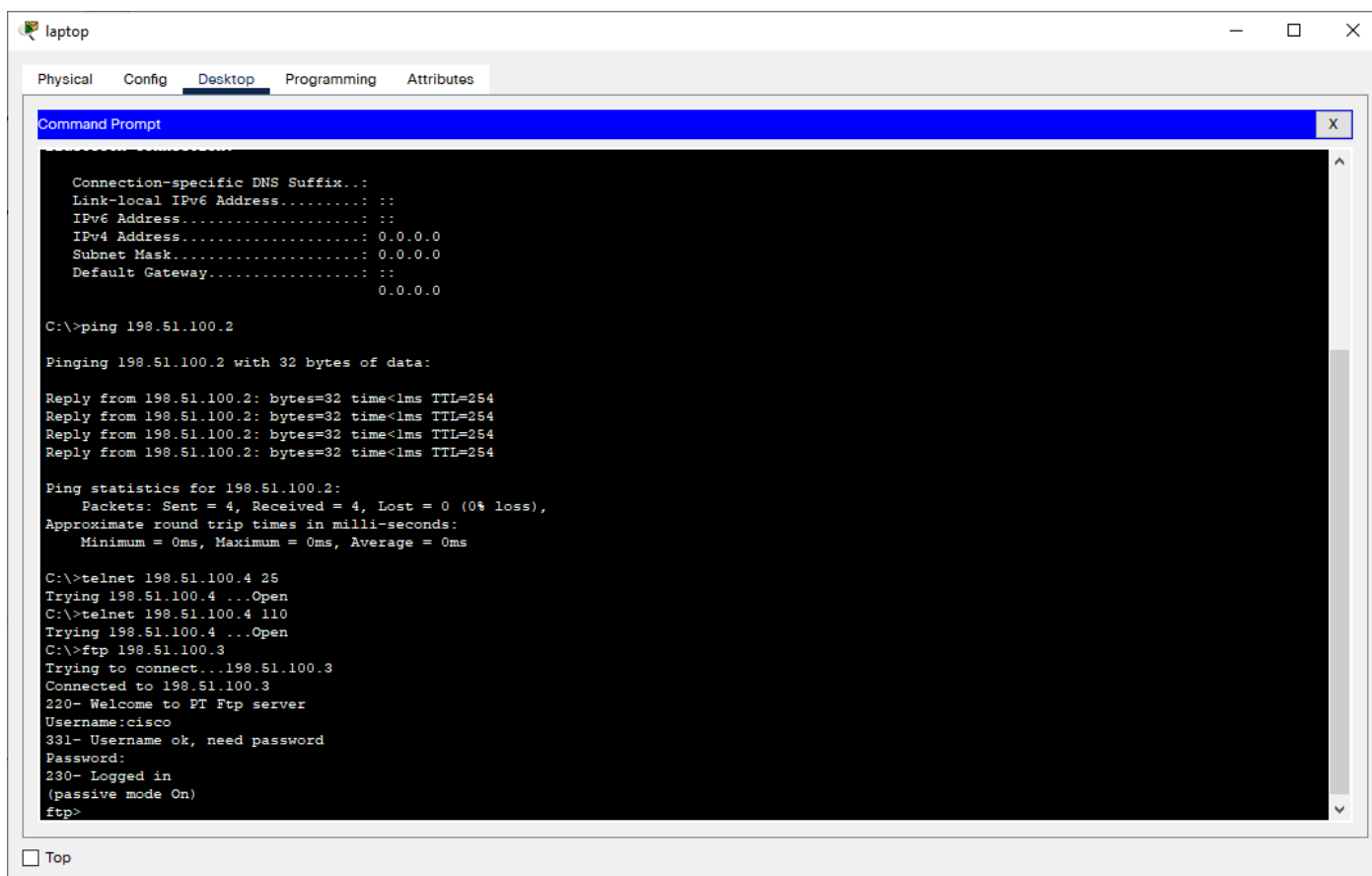
Ping statistics for 198.51.100.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
    Approximate round trip times in milli-seconds:
        Minimum = 0ms, Maximum = 0ms, Average = 0ms
```

At the bottom left of the Command Prompt window, there is a checkbox labeled 'Top' which is currently unchecked.

Почтовый сервер доступен по портам 25 и 110:



Файловый сервер доступен по портам протокола FTP:



Вывод:

Мы приобрели 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.