**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 (cм. 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).

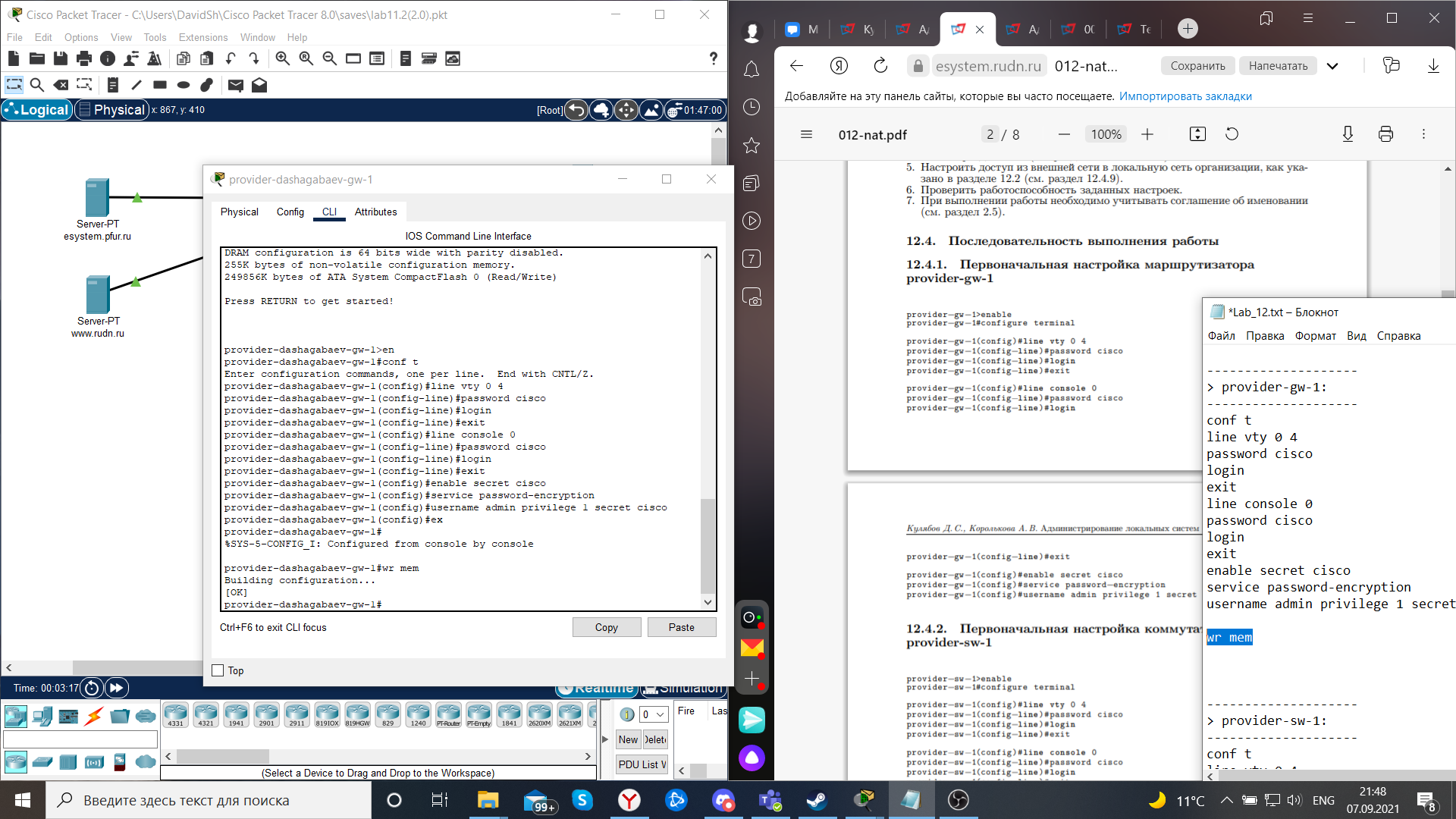
6. Проверить работоспособность заданных настроек.

7. При выполнении работы необходимо учитывать соглашение об именовании

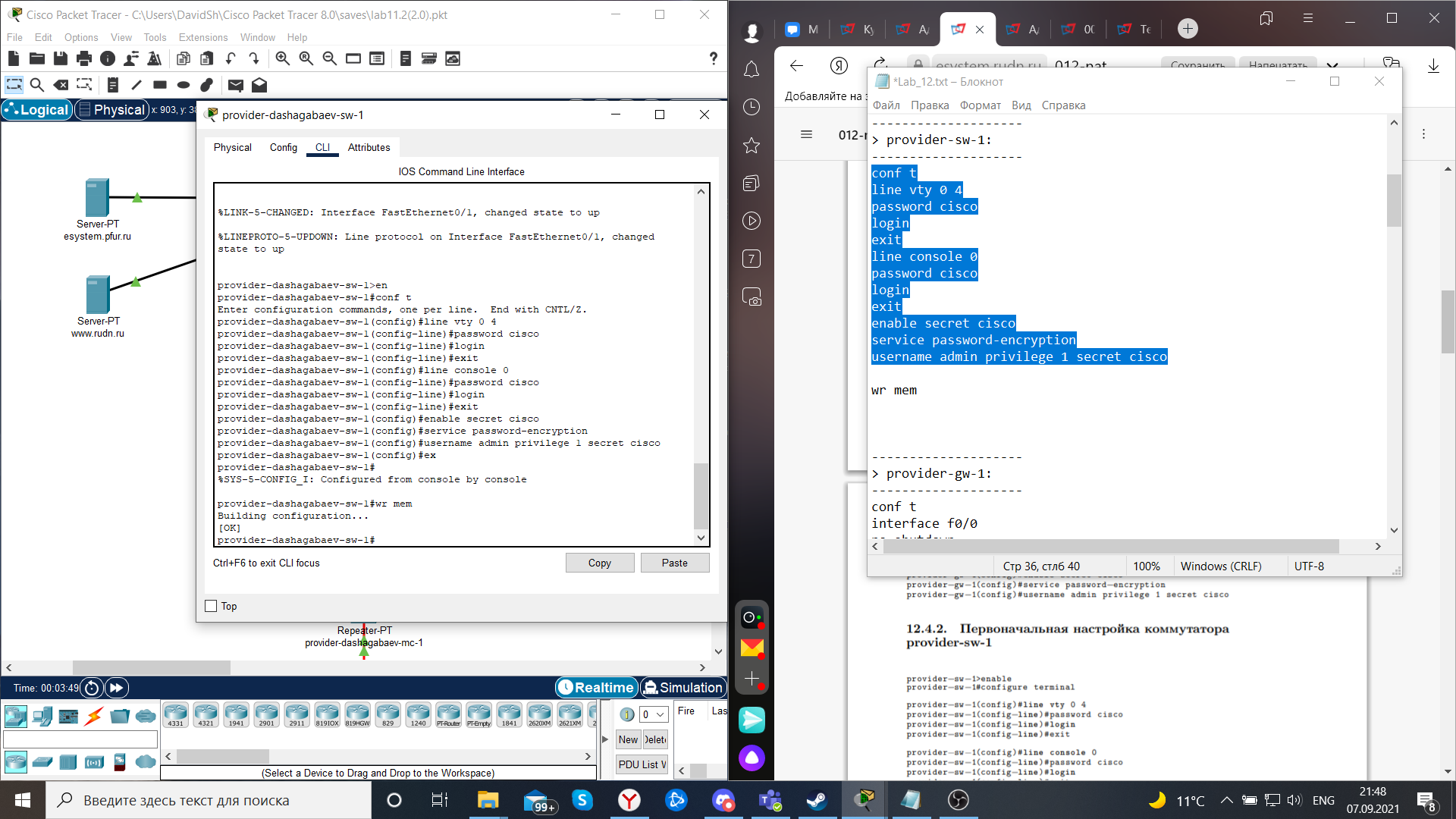
(см. раздел 2.5).

# Порядок выполнения работы:

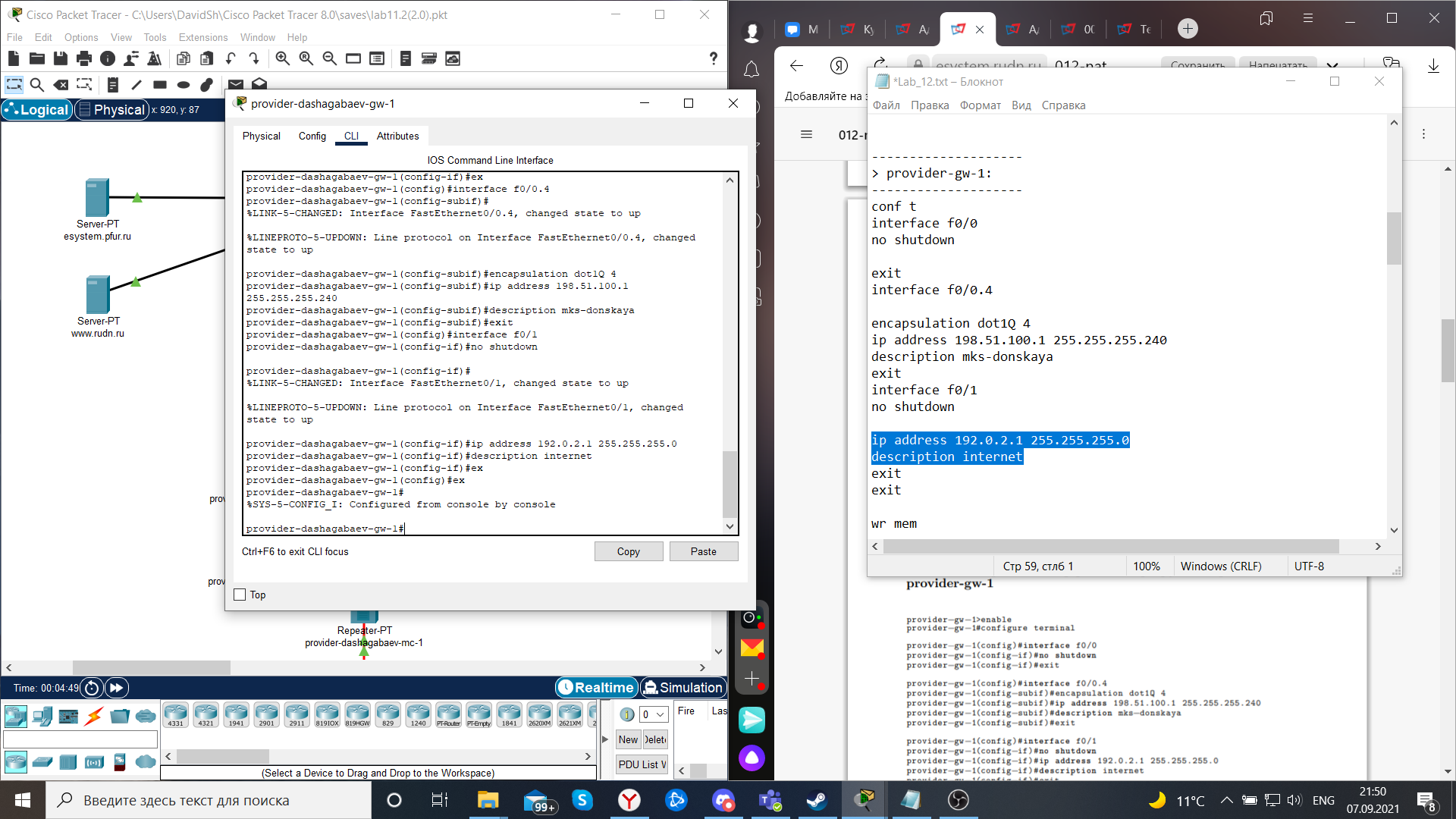
1. Первоначальная настройка маршрутизатора provider-dashagabaev-gw-1



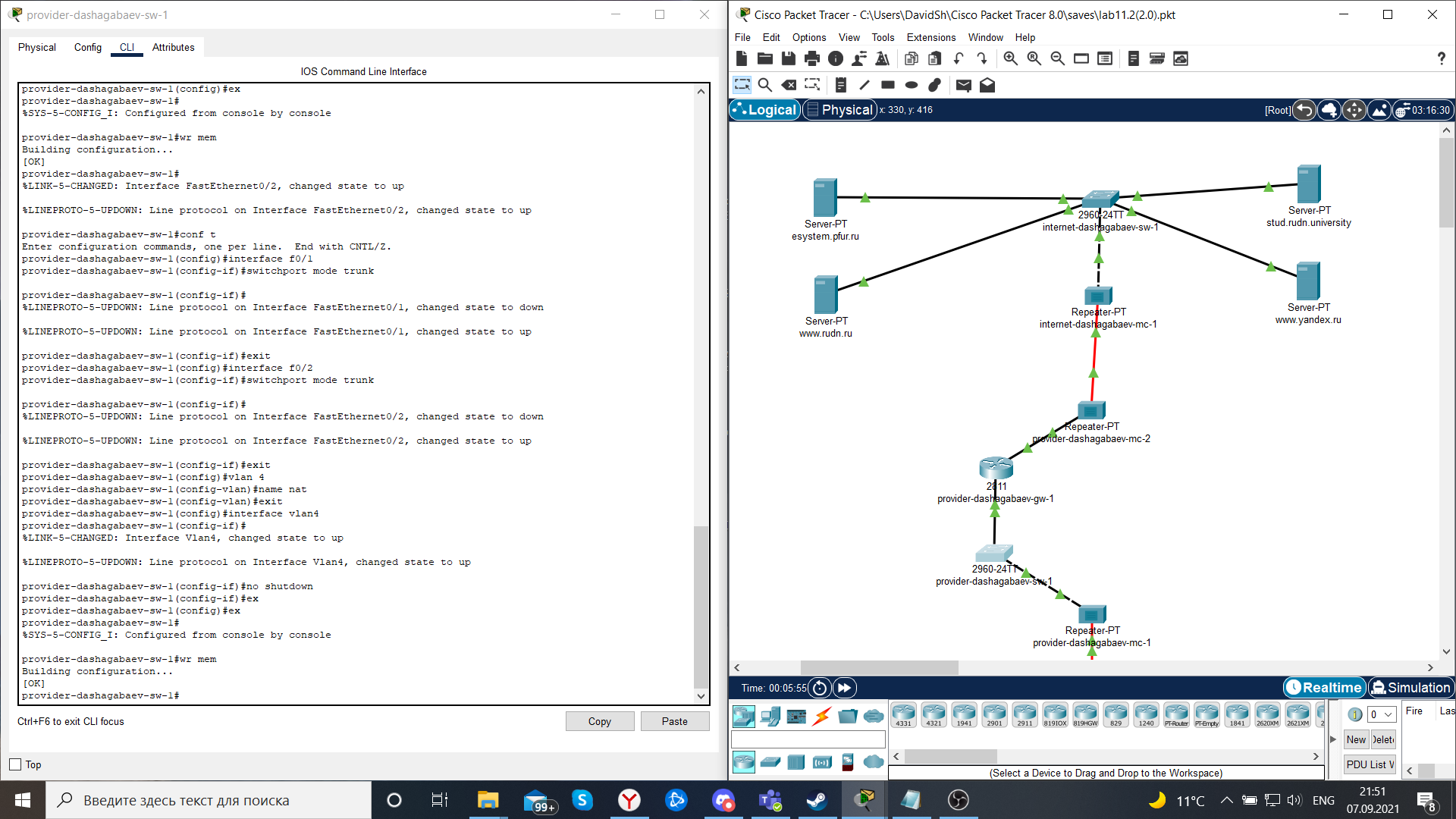
1. Первоначальная настройка коммутатора provider-dashagabaev-sw-1



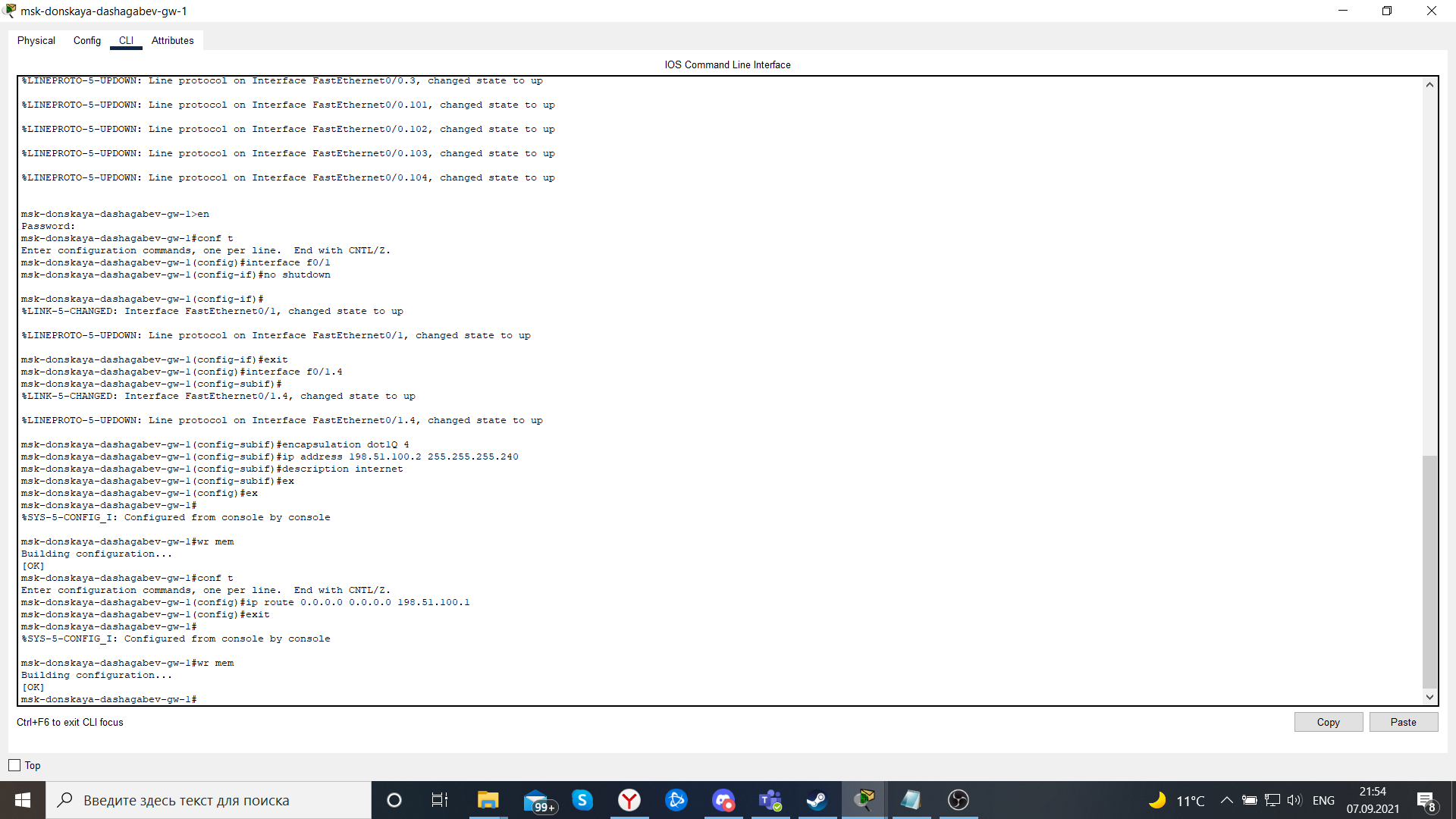
1. Настройка интерфейсов маршрутизатора provider-dashagabaev-gw-1

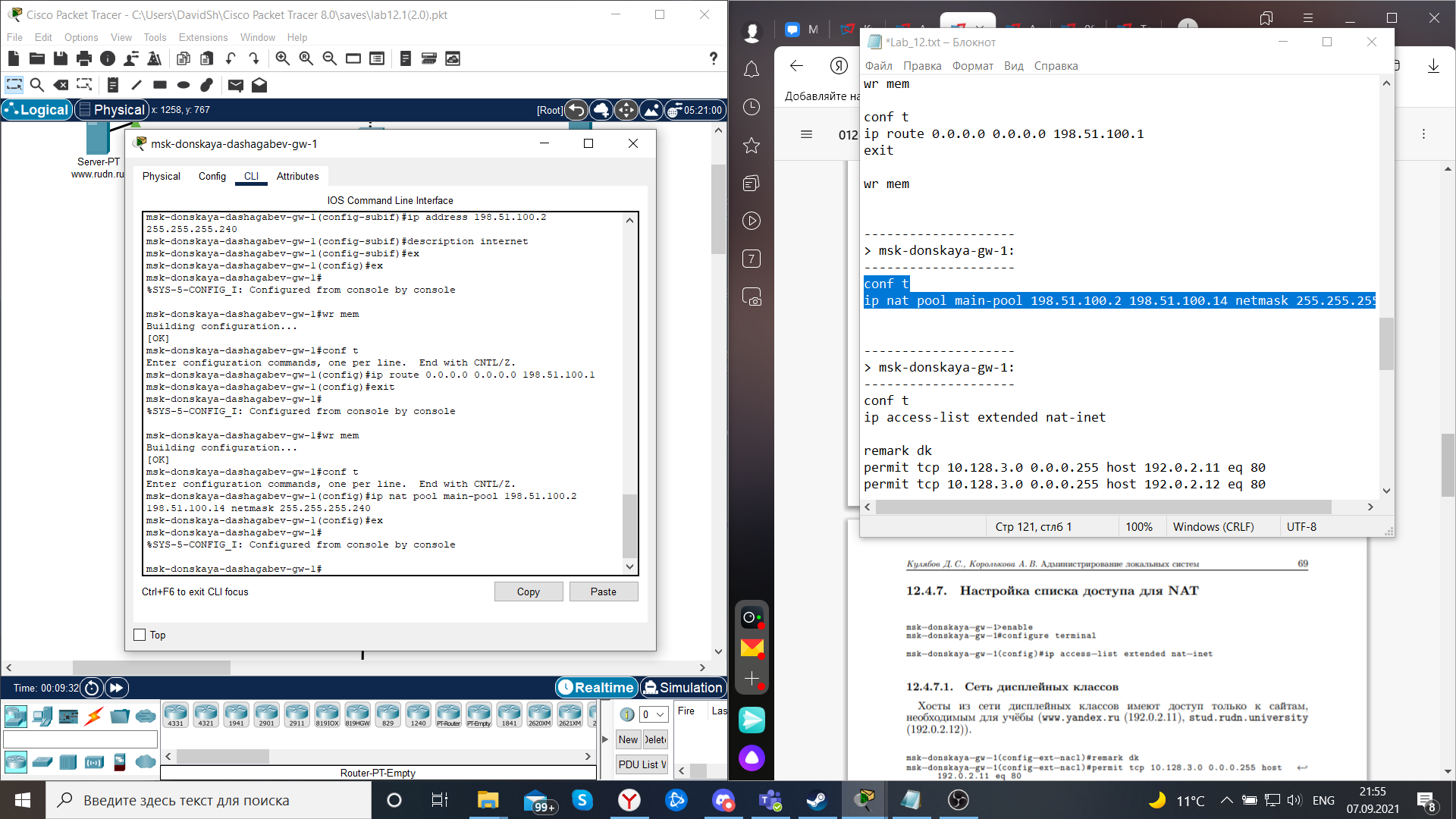


1. Настройка интерфейсов коммутатора provider-dashagabaev-sw-1

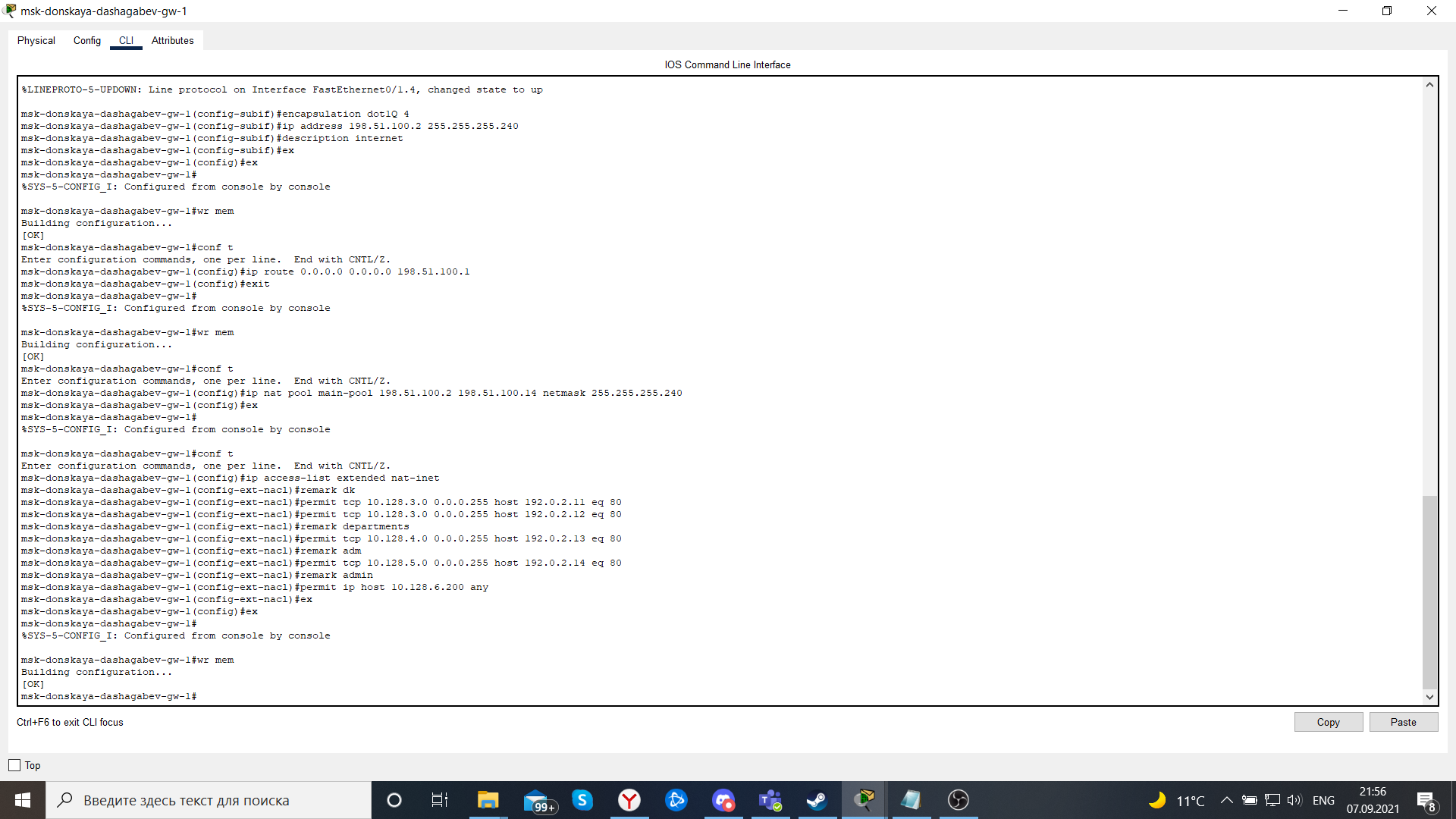


1. Настройка интерфейсов маршрутизатора msk-donskaya-dashagabaev-gw-1





1. Настройка пула адресов для NAT



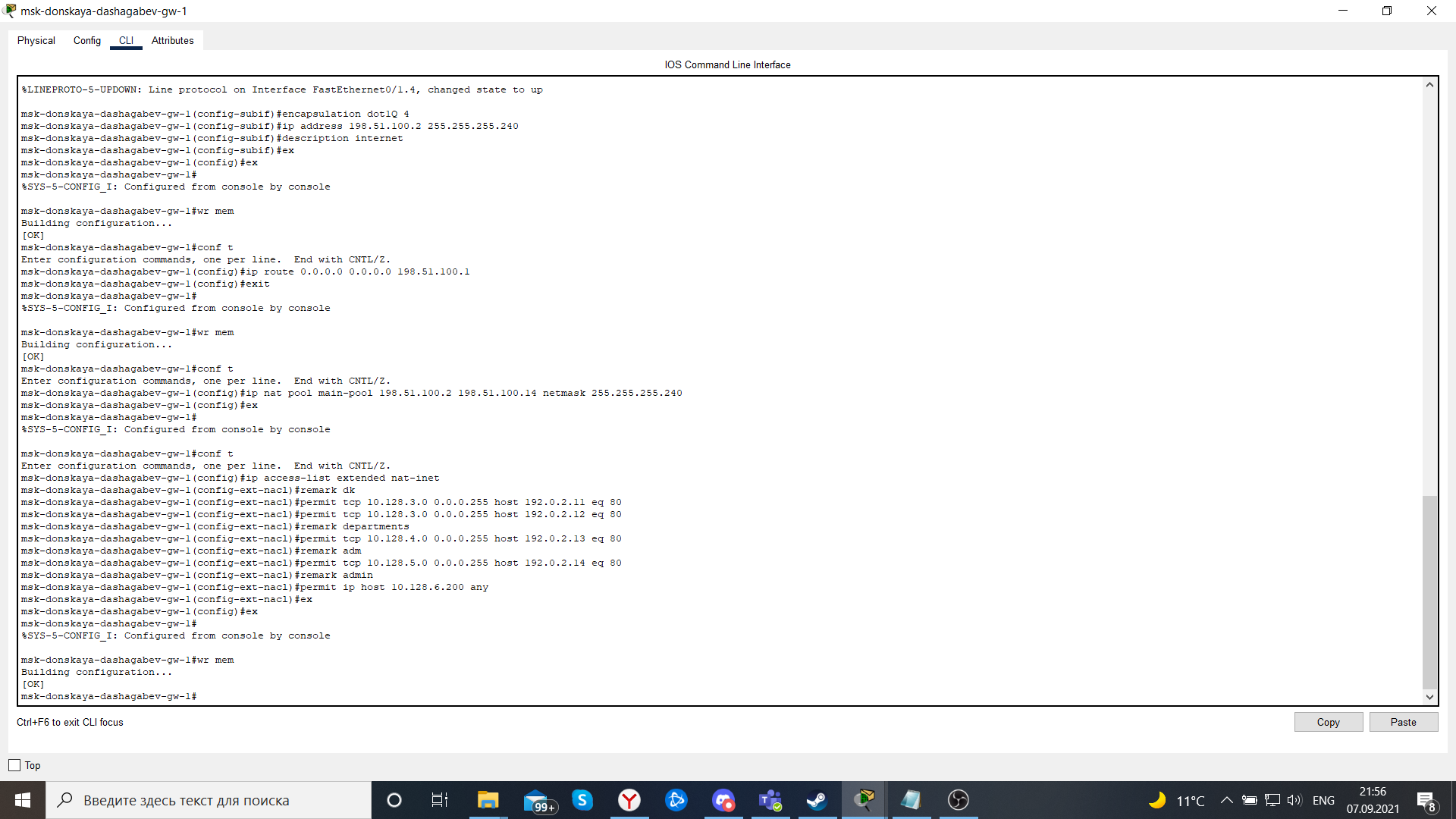
1. Настройка списка доступа для NAT

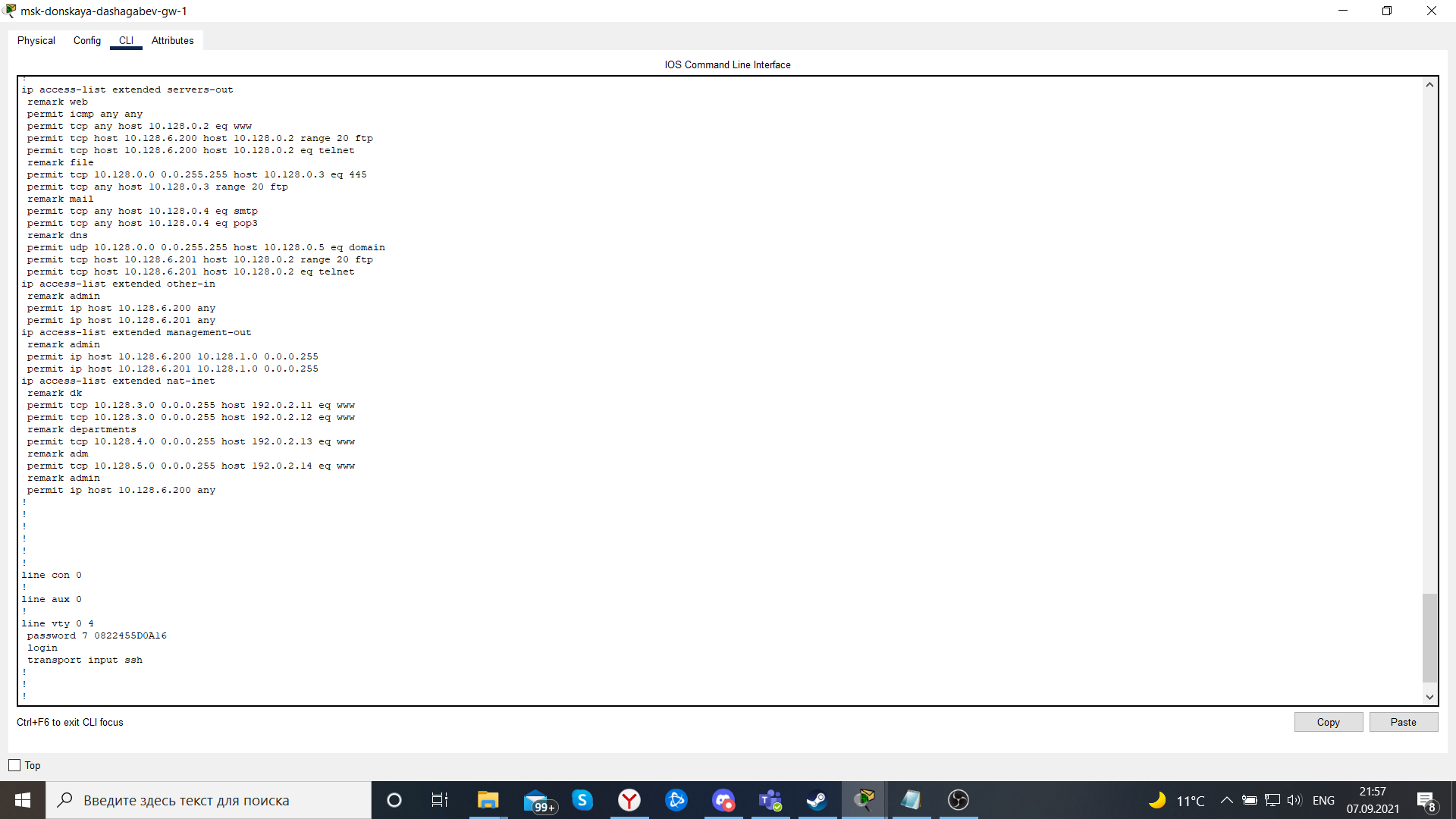
Сеть дисплейных классов

Сеть кафедр

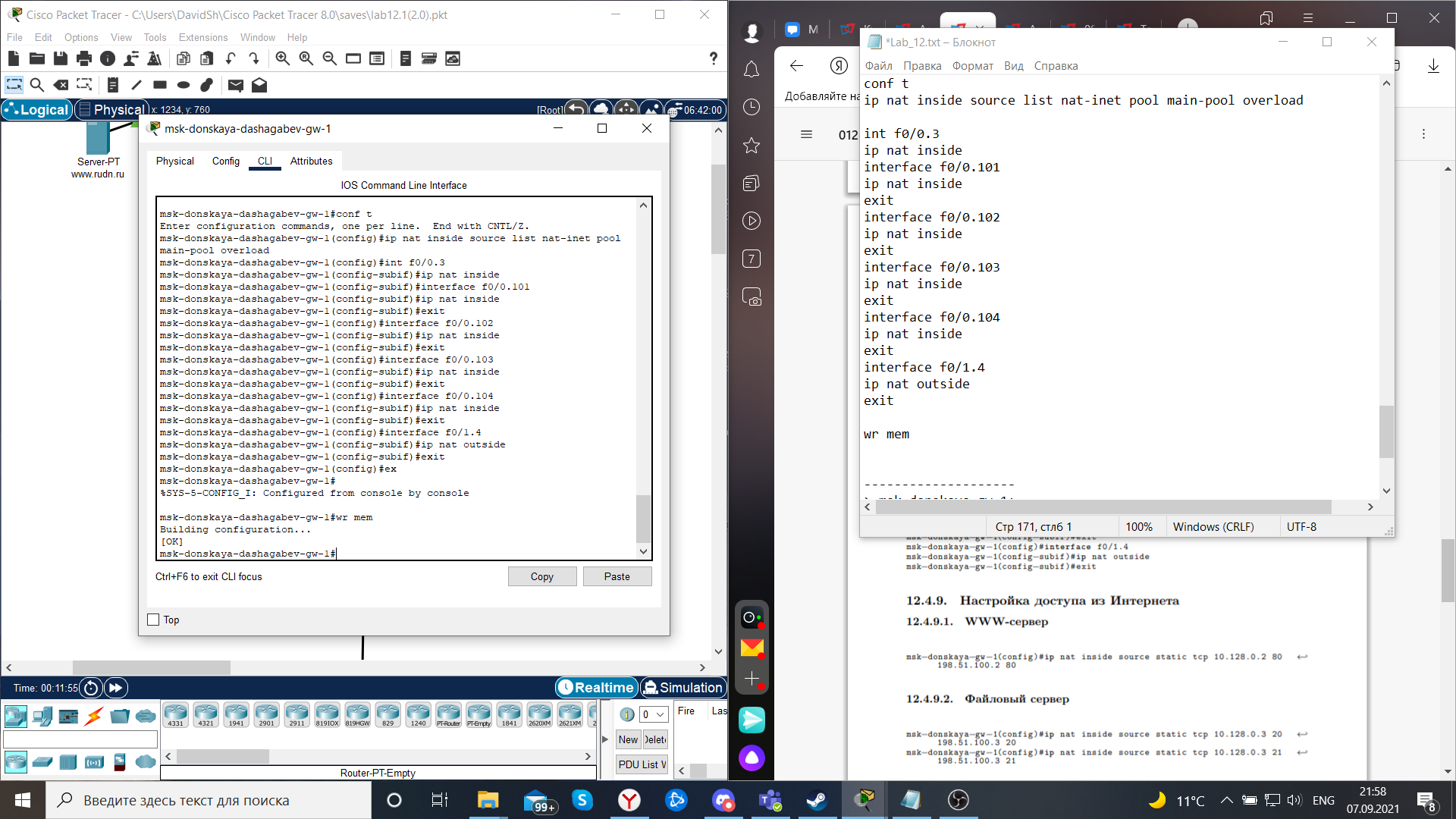
Сеть администрации

Доступ для компьютера администратора

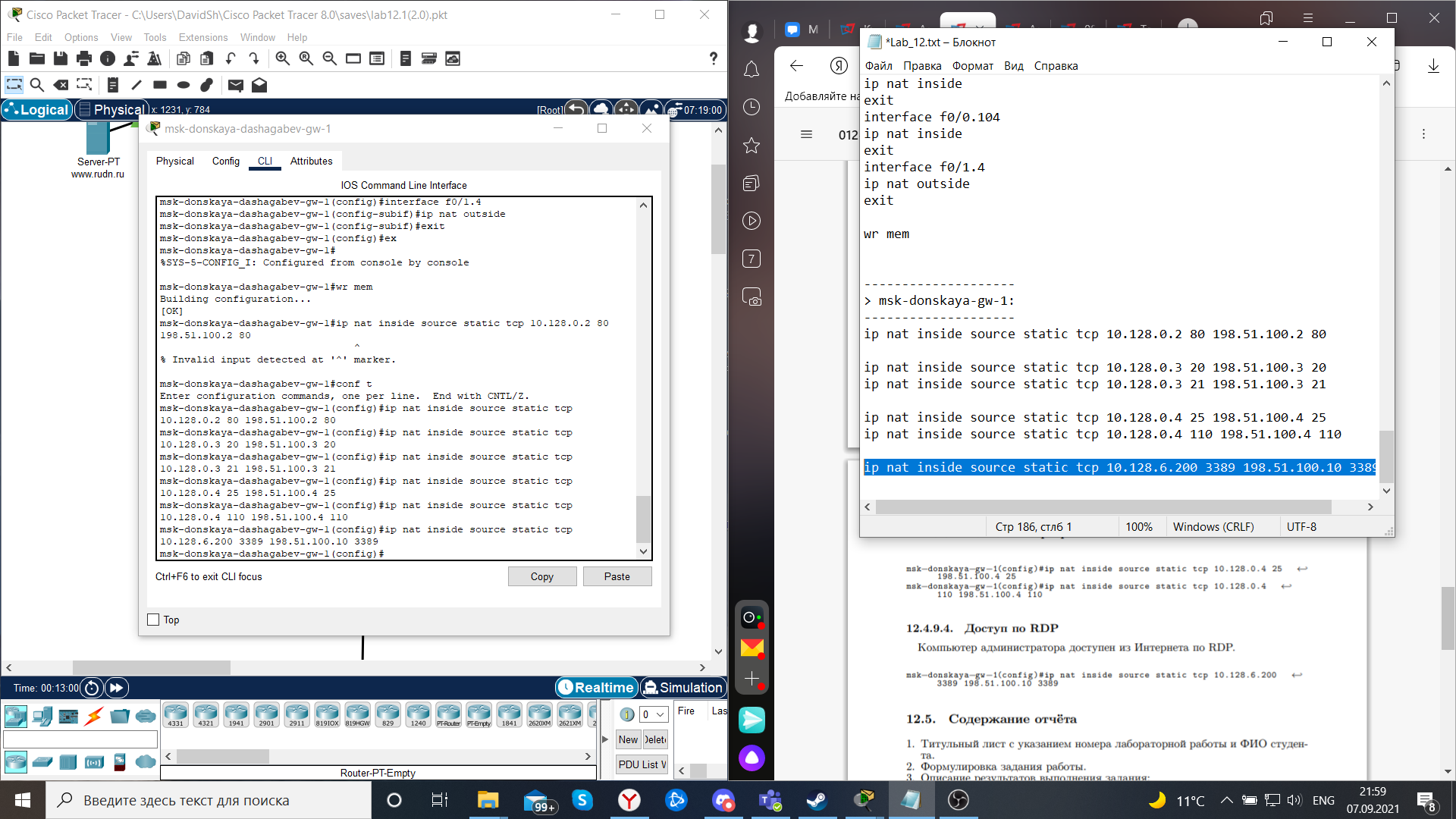




1. Настройка NAT:



1. Настройка доступа из Интернета
2. WWW-сервер
3. Файловый сервер
4. Почтовый сервер
5. Доступ по RDP



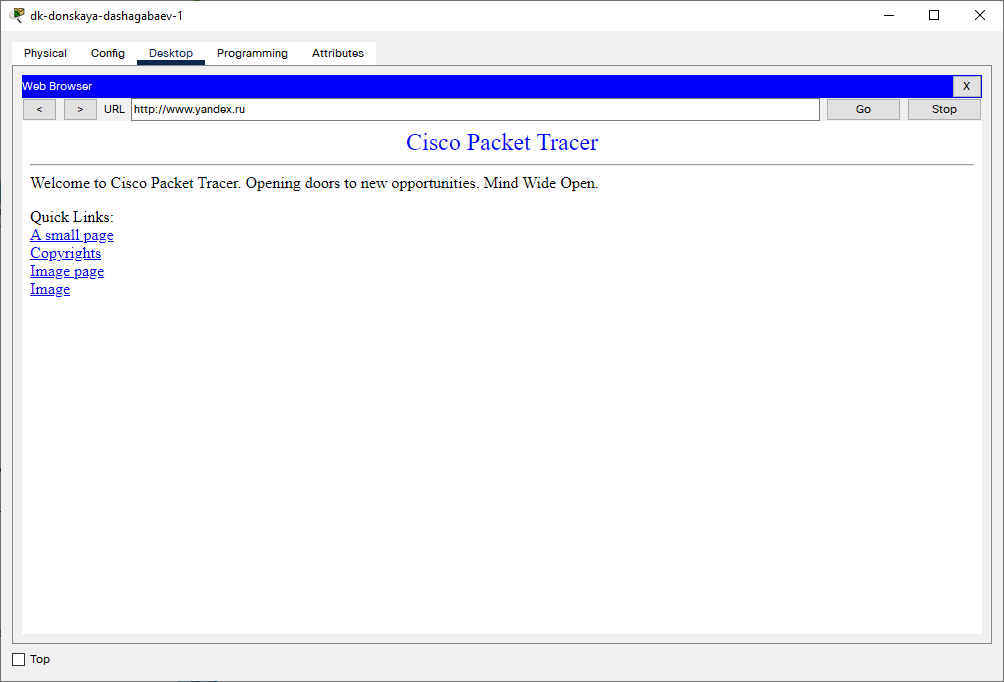
**Проверяем наши настройки:**

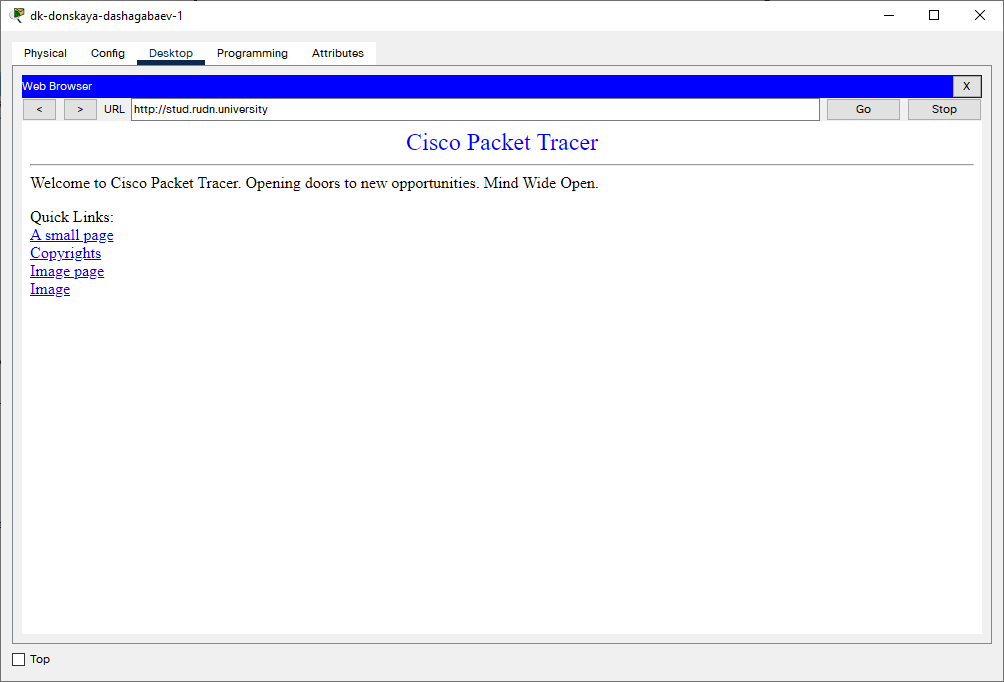
1. Проверка доступа www.yandex.ru c msk-donskaya-dashagabaev-sw-1.

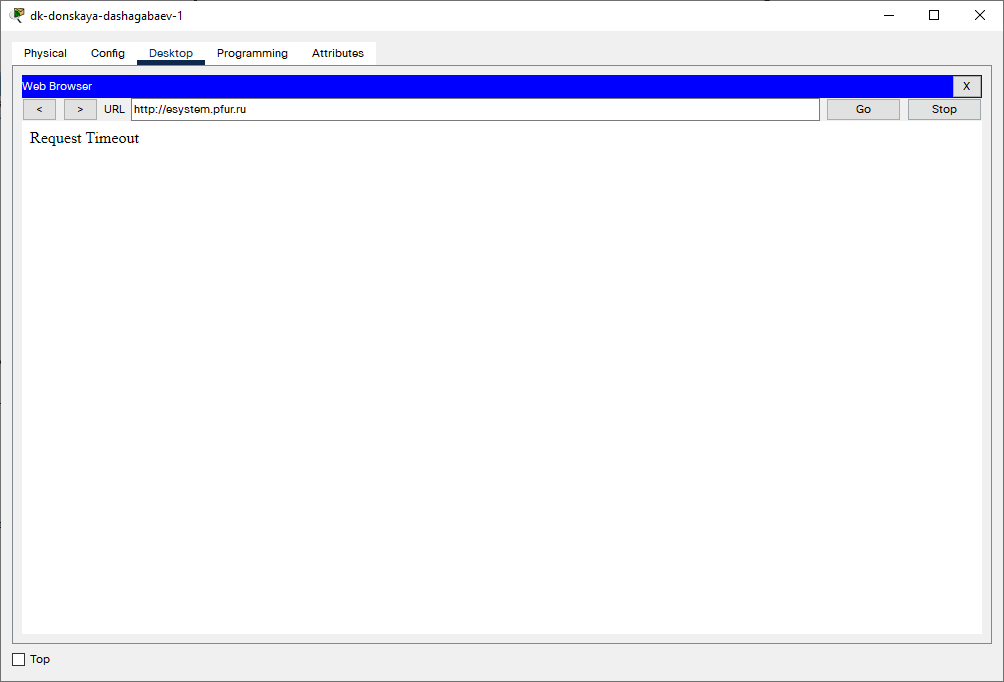
Cеть управления устройствами не имеет доступа в Интернет.



2. Оконечные устройства сети дисплейных классов должны иметь доступ только к определённым сайтам: к [www.yandex.ru](http://www.yandex.ru) и stud.rudn.university.

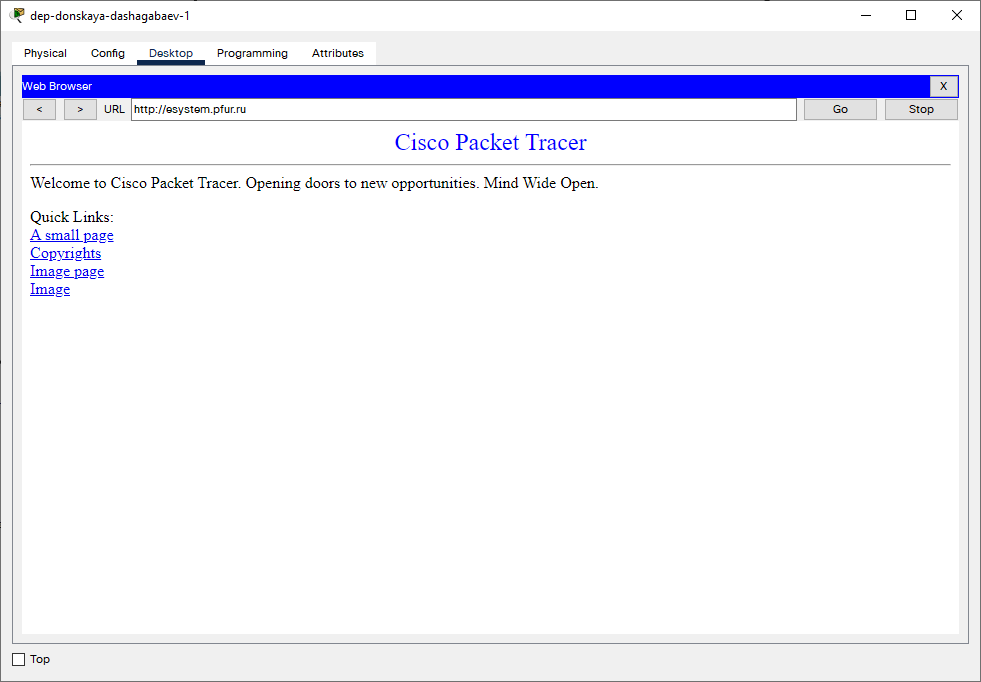


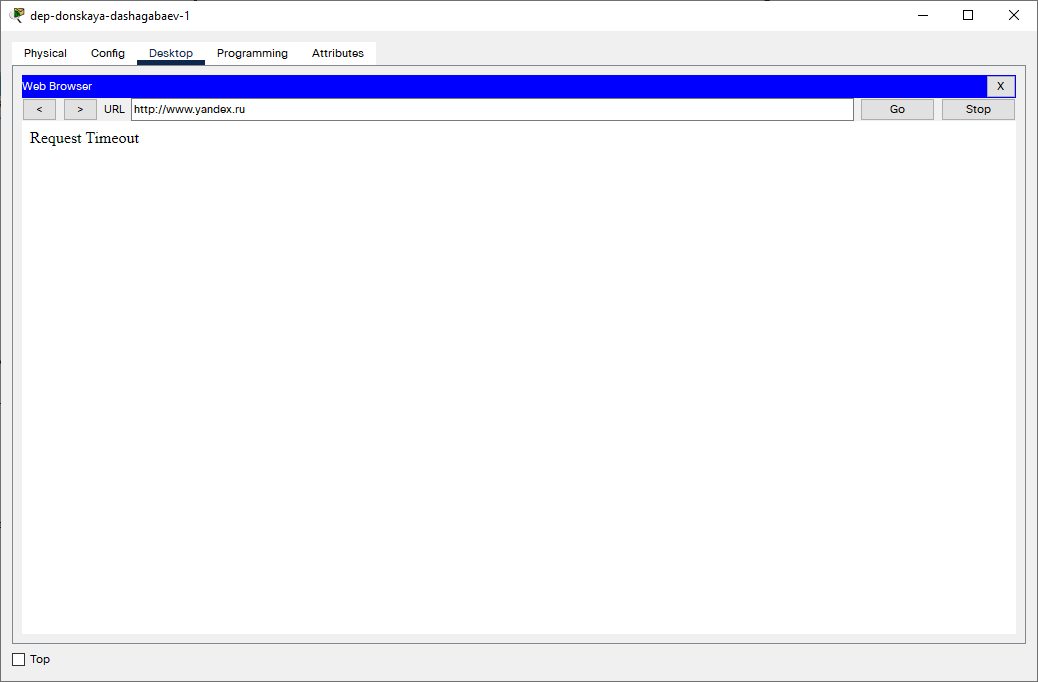


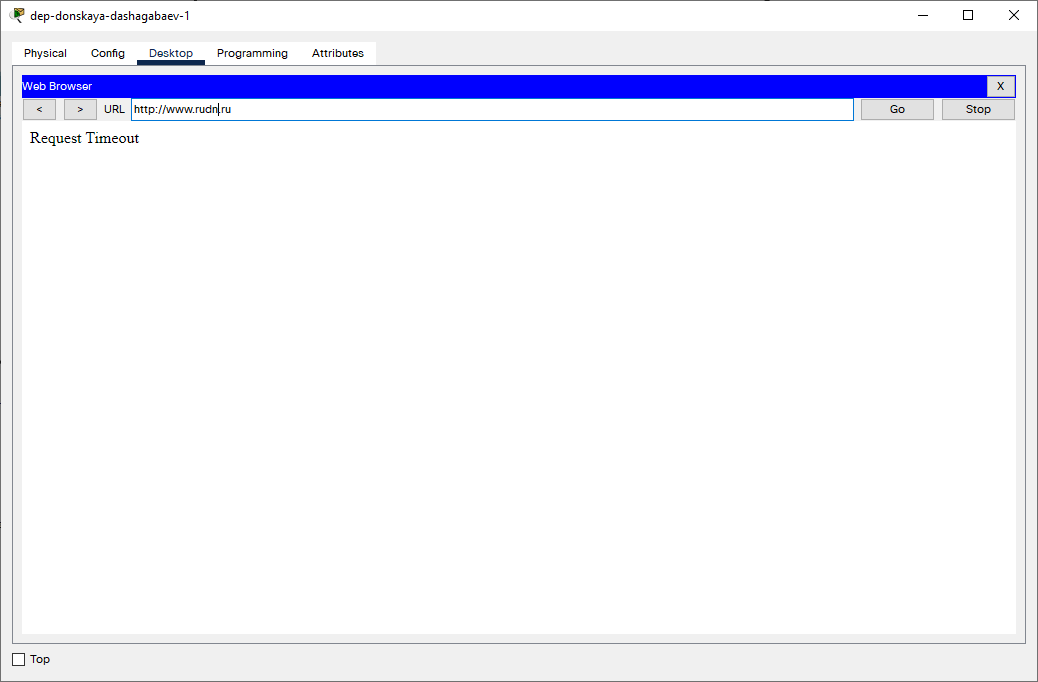


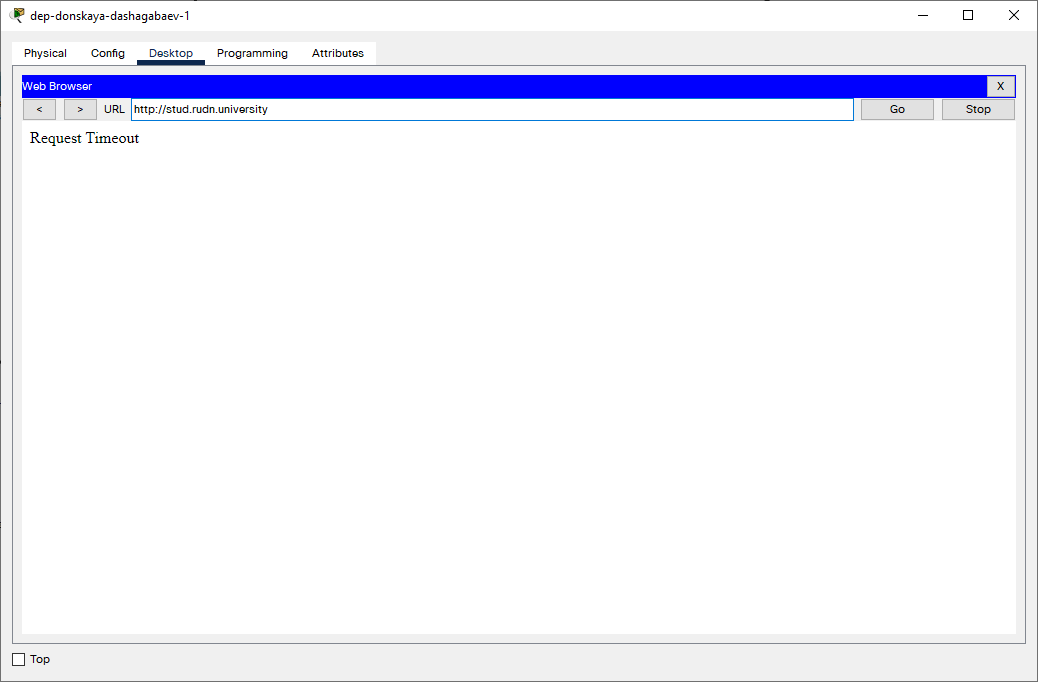


3. Оконечные устройства сети кафедр должны иметь доступ только к сайту esystem.pfur.ru.

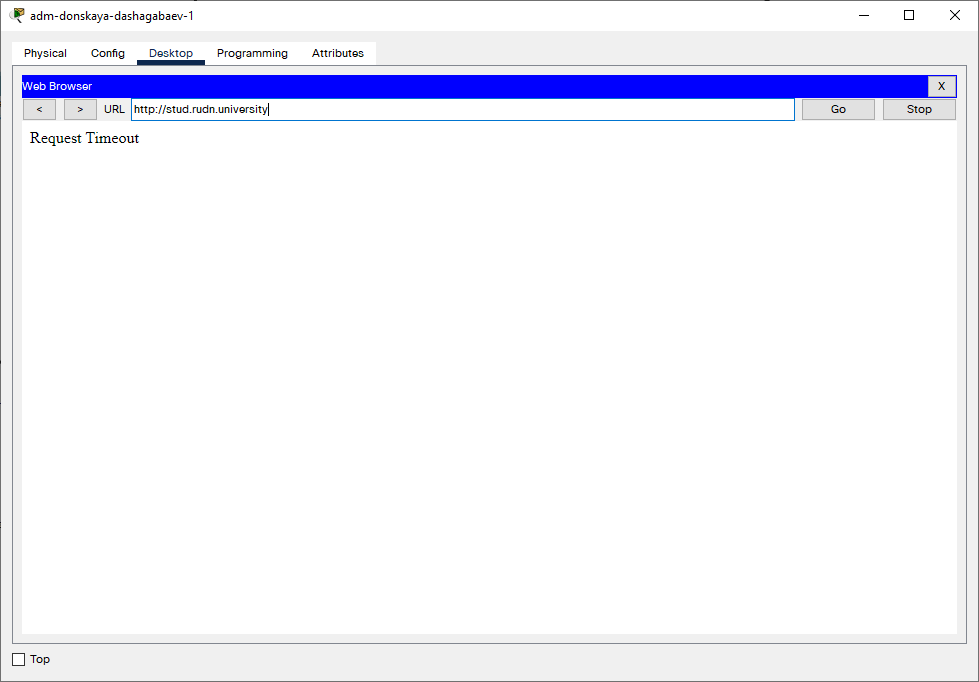


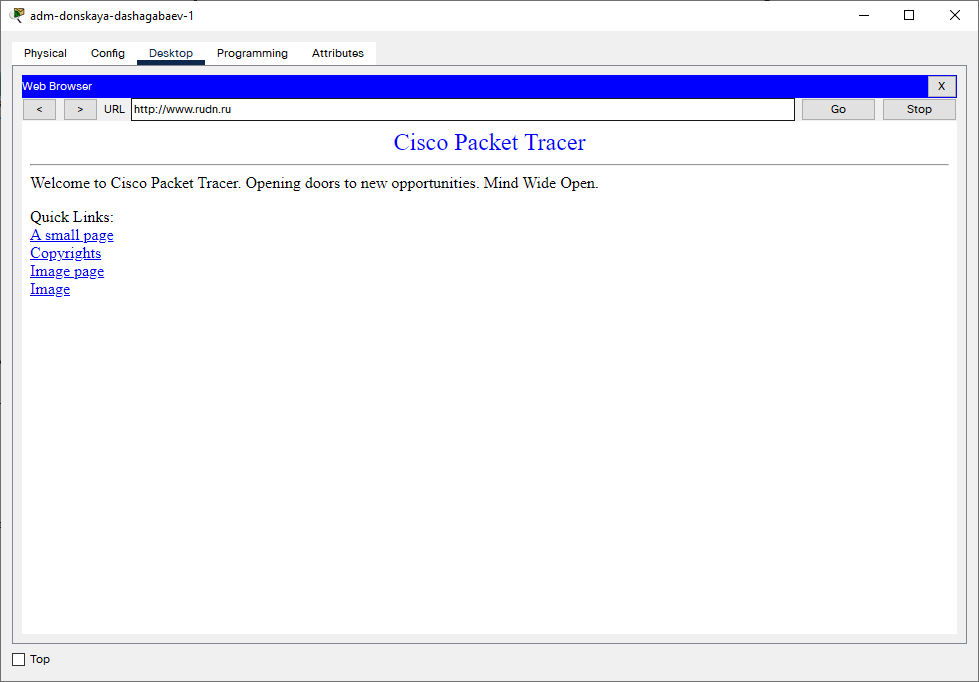


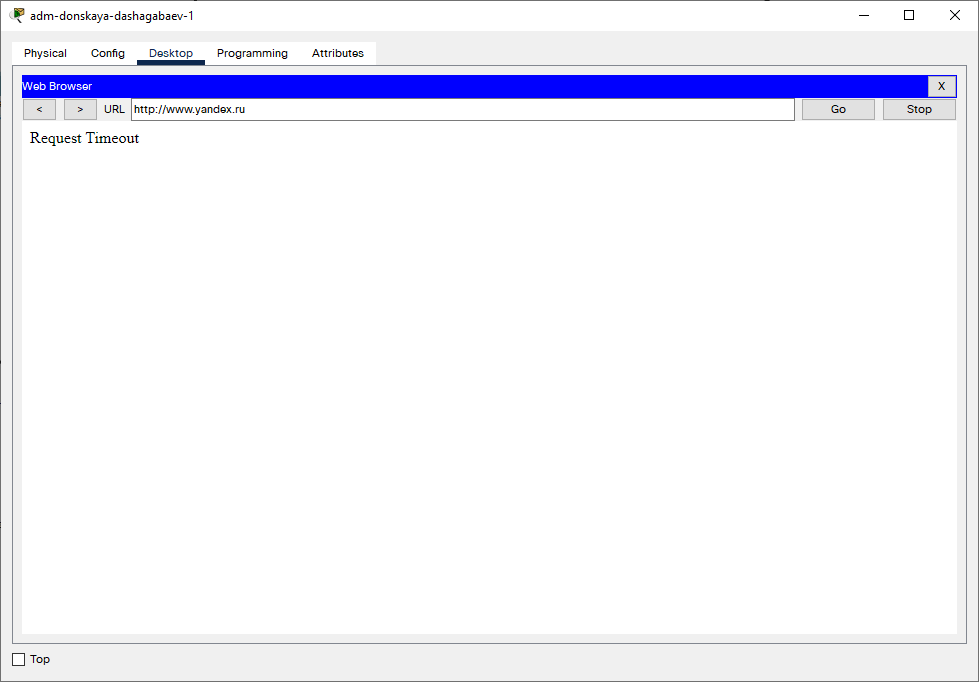


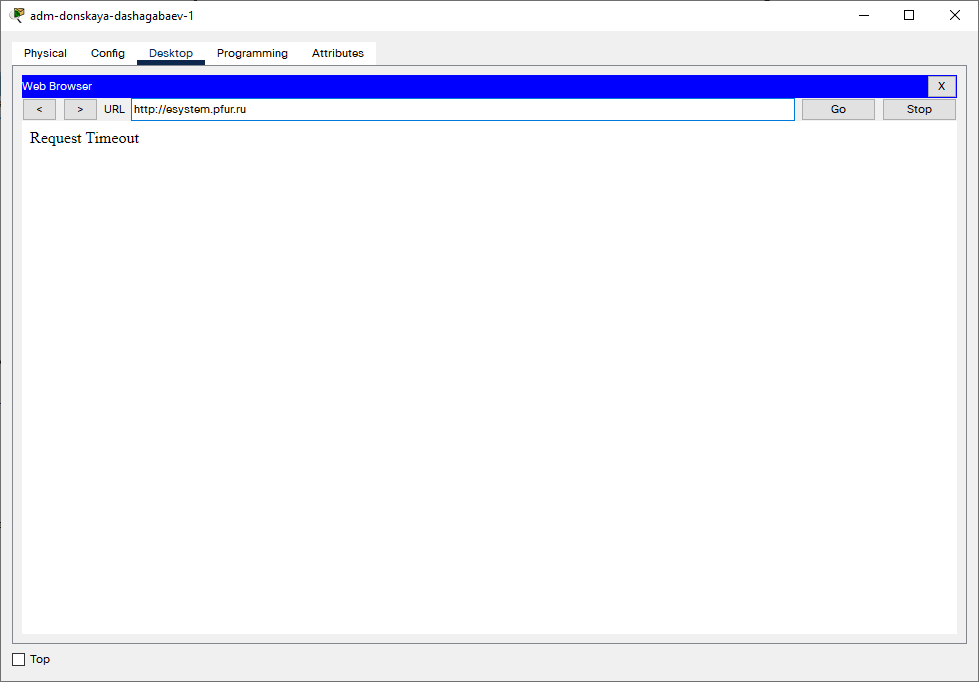


4. Оконечные устройства сети администрации должны иметь доступ только к сайту www.rudn.ru.

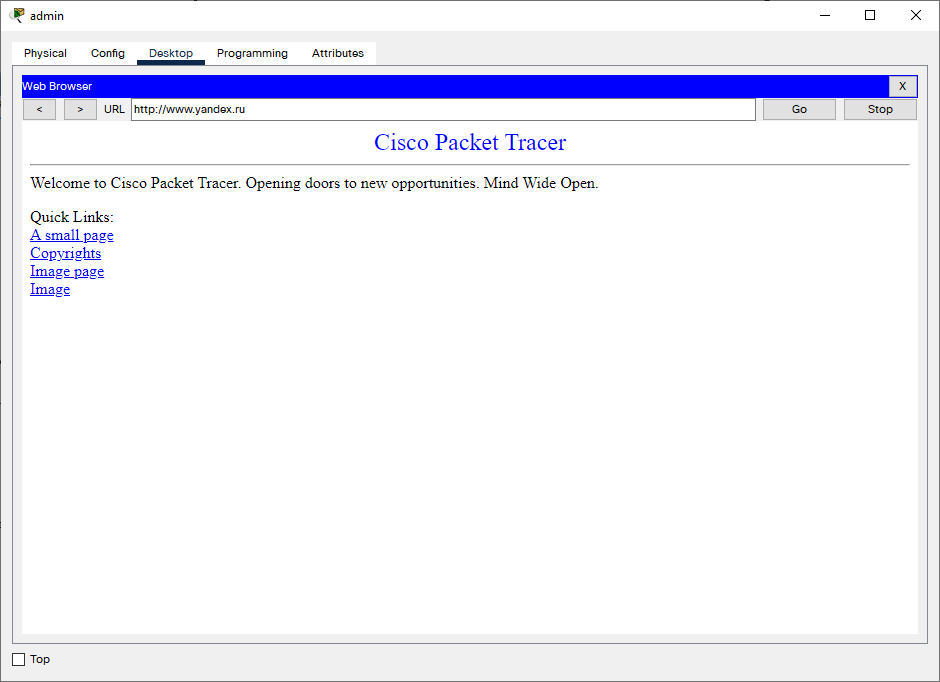


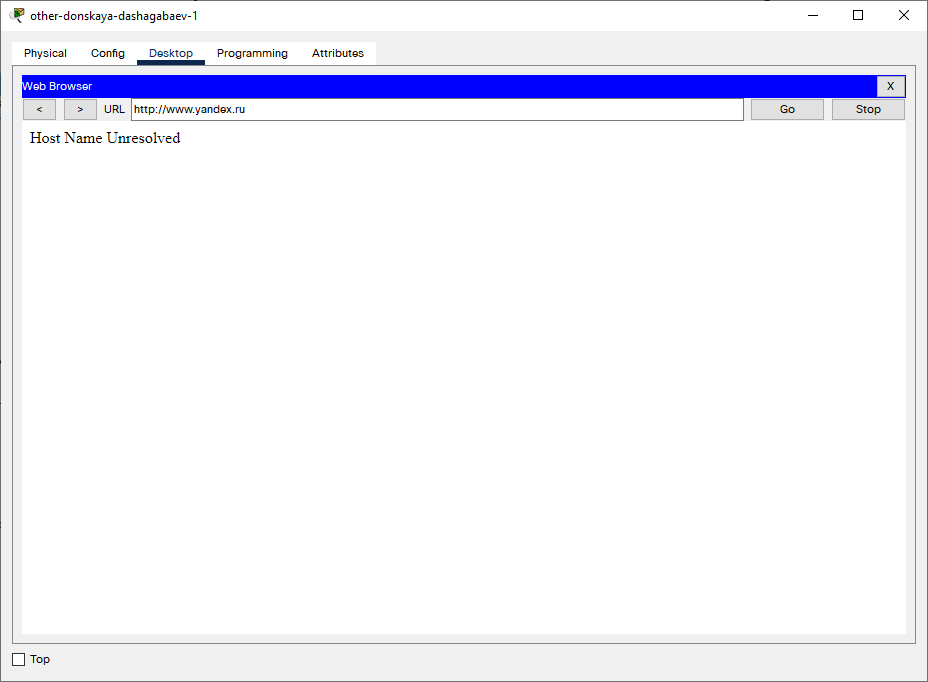




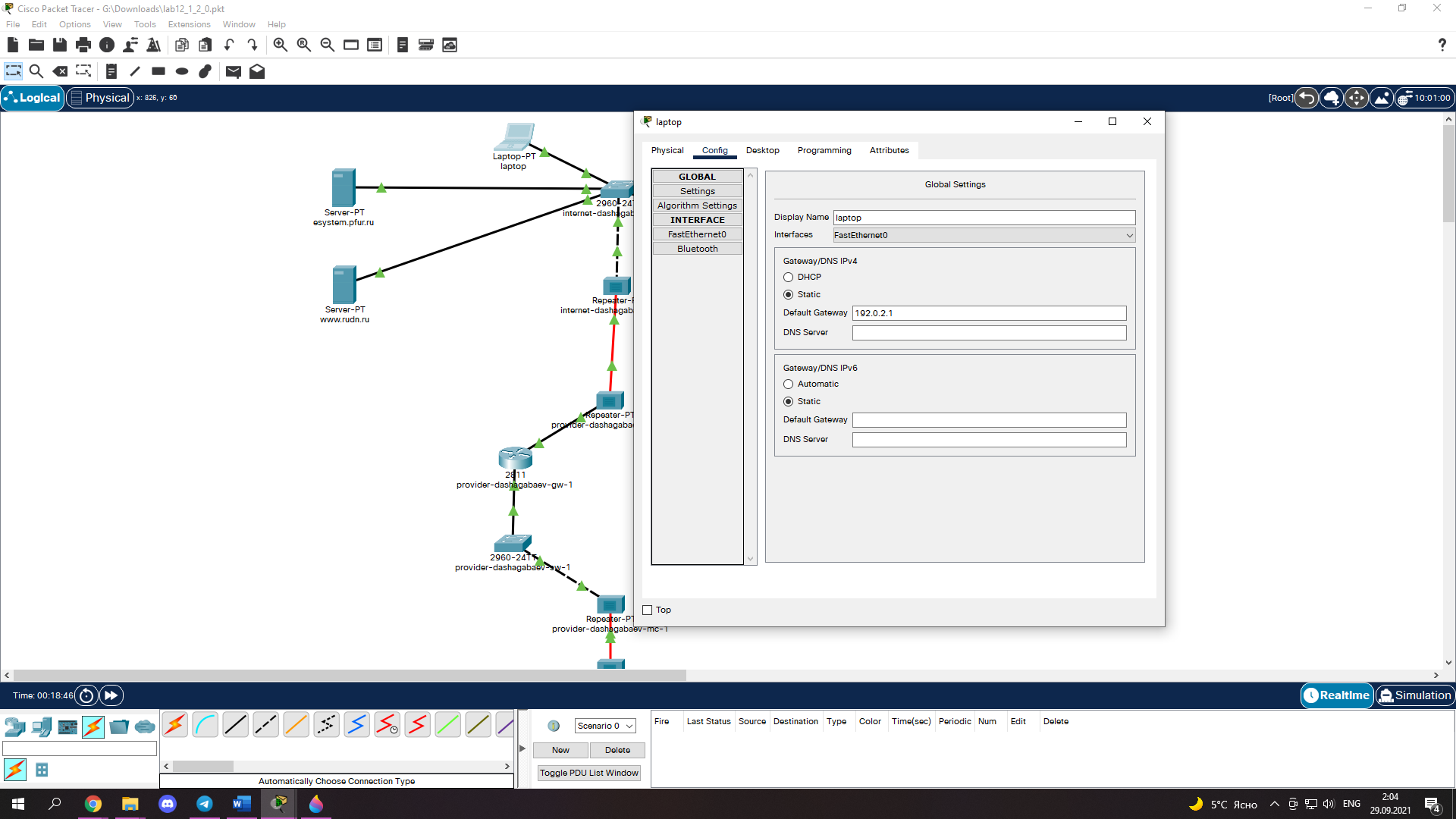


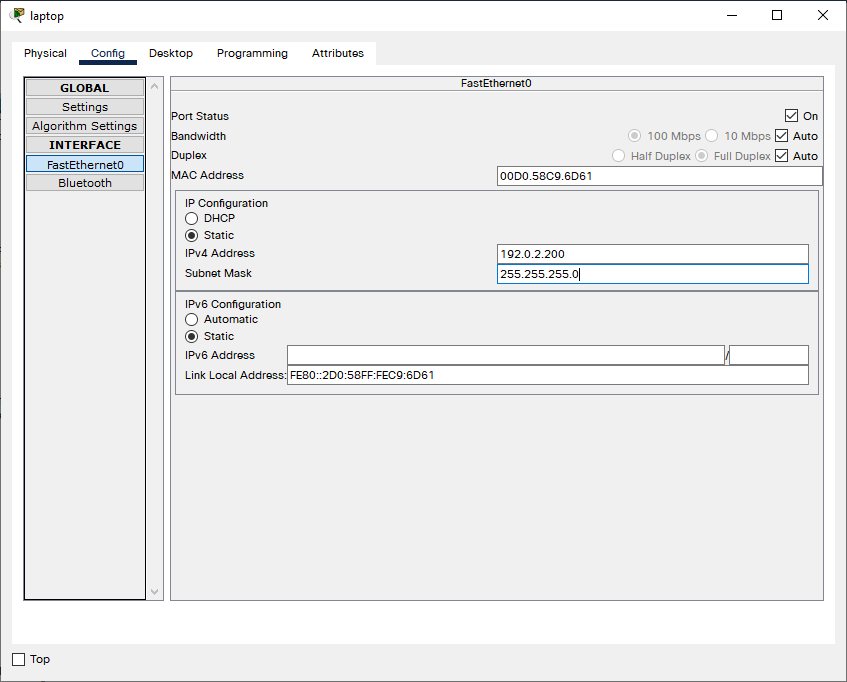
5. Компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи не должны выходить в Интернет.



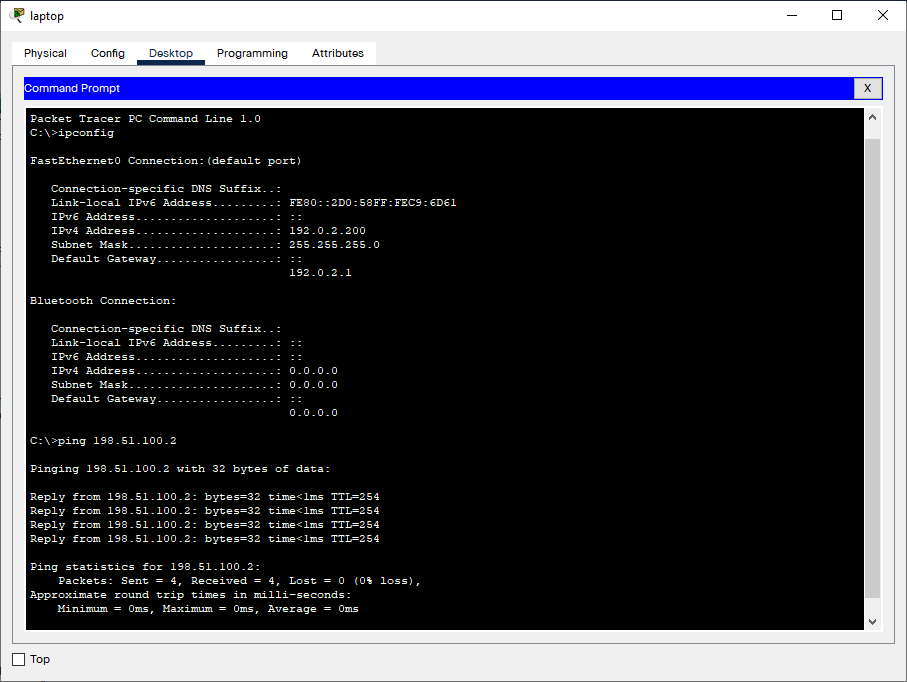


6. Добавим устройство laptop для проверки конфигурации.

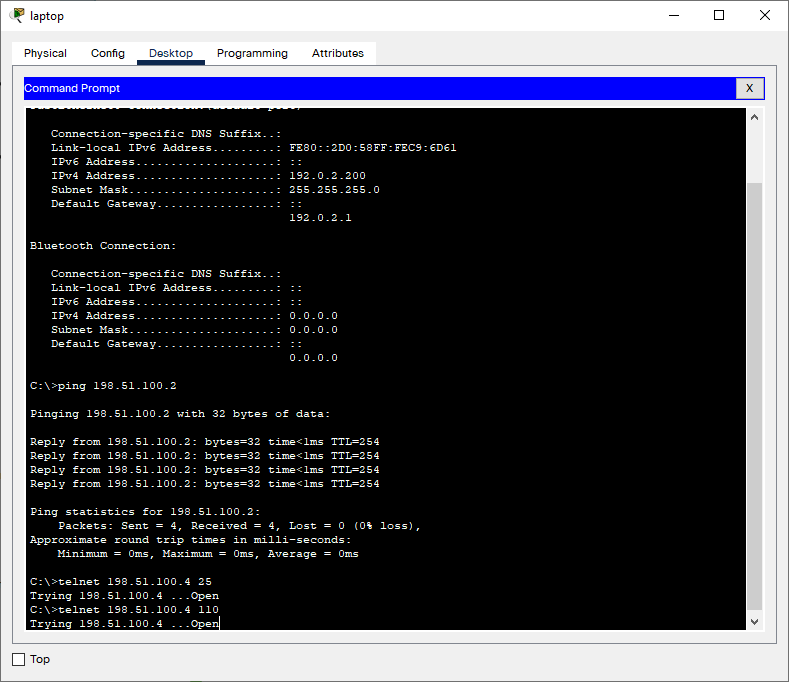




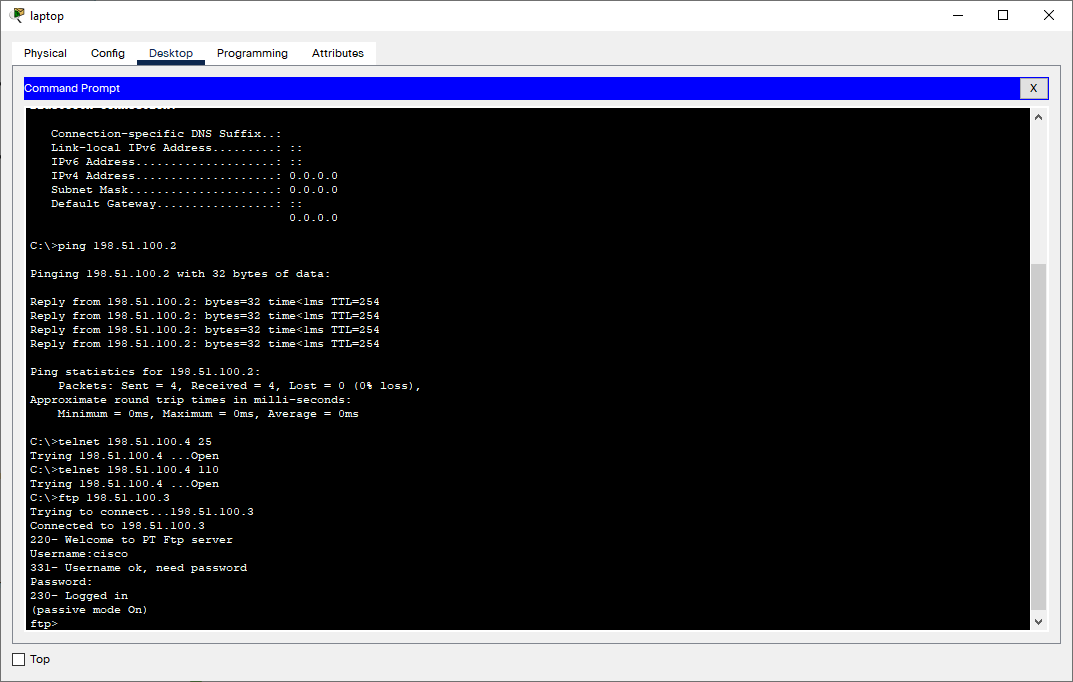
WEB сервер доступен по порту 80:



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 сеть). 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.