

# **Отчет по лабораторной работе №12**

**Администрирование локальных сетей**

Еюбоглу Тимур, НПИбд-01-22

# Содержание

<b>1</b>	<b>Цель работы</b>	<b>4</b>
<b>2</b>	<b>Задание</b>	<b>5</b>
<b>3</b>	<b>Выполнение лабораторной работы</b>	<b>6</b>
<b>4</b>	<b>Выводы</b>	<b>14</b>
<b>5</b>	<b>Контрольные вопросы</b>	<b>15</b>

## Список иллюстраций

3.1	Настройка коммутатора провайдера . . . . .	6
3.2	Присвоение адресов интерфейсам . . . . .	7
3.3	Настройка маршрутизатора . . . . .	8
3.4	Настройка маршрутизатора . . . . .	9
3.5	Администратор . . . . .	9
3.6	Пользователи . . . . .	10
3.7	Пользователи . . . . .	10
3.8	Пользователи . . . . .	11
3.9	Проверка . . . . .	12
3.10	Проверка . . . . .	12
3.11	Вход выполнен . . . . .	13
3.12	Вход выполнен . . . . .	13

# 1 Цель работы

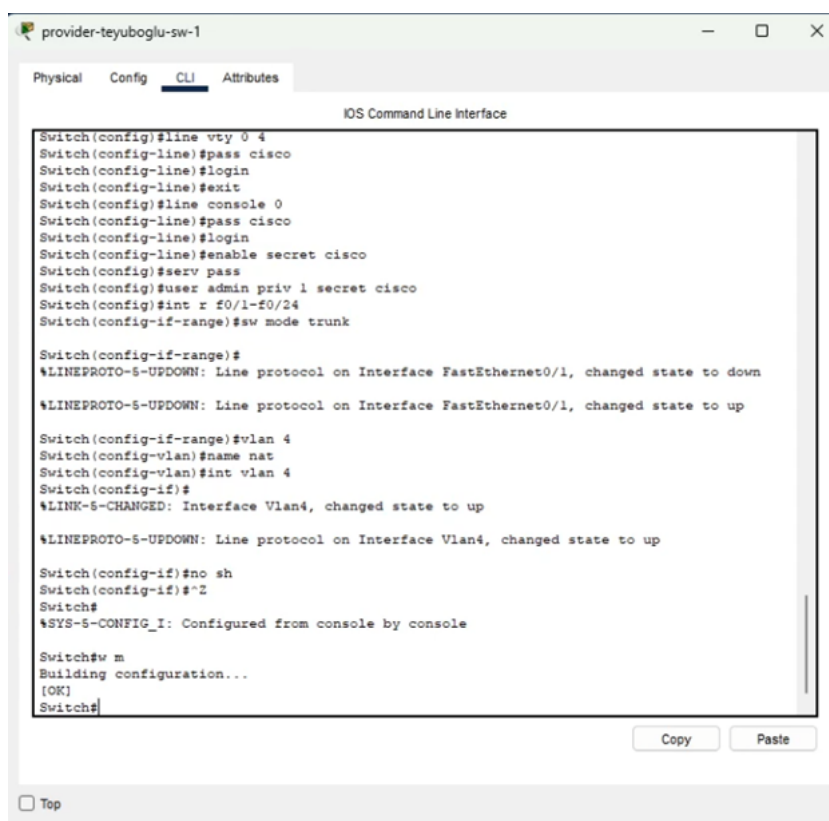
Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT.

## 2 Задание

Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT. 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](http://www.yandex.ru), [stud.rudn.university](http://stud.rudn.university)); 3) пользователям из сети кафедр разрешено работать только с образовательными сайтами (в данном случае это [esystem.pfur.ru](http://esystem.pfur.ru)); 4) пользователям сети администрации разрешено работать только с сайтом университета [www.rudn.ru](http://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).

### 3 Выполнение лабораторной работы

Настраиваем коммутатор провайдера. Все порты переводятся в транковый режим. Добавляем 4 vlan для подключения университета. (рис. 3.1).



```
provider-teyuboglu-sw-1
Physical Config CLI Attributes
IOS Command Line Interface
Switch(config)#line vty 0 4
Switch(config-line)#pass cisco
Switch(config-line)#login
Switch(config-line)#exit
Switch(config)#line console 0
Switch(config-line)#pass cisco
Switch(config-line)#login
Switch(config-line)#enable secret cisco
Switch(config)#serv pass
Switch(config)#user admin priv 1 secret cisco
Switch(config)#int r f0/1-f0/24
Switch(config-if-range)#sw mode trunk

Switch(config-if-range)#
%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

Switch(config-if-range)#vlan 4
Switch(config-vlan)#name nat
Switch(config-vlan)#int vlan 4
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 sh
Switch(config-if)#^Z
Switch#
%SYS-5-CONFIG_I: Configured from console by console

Switch# m
Building configuration...
[OK]
Switch#
```

Рис. 3.1: Настройка коммутатора провайдера

Настраиваем маршрутизатор провайдера. Присваиваем адреса интерфейсам для клиентов и для интернета. (рис. 3.2).

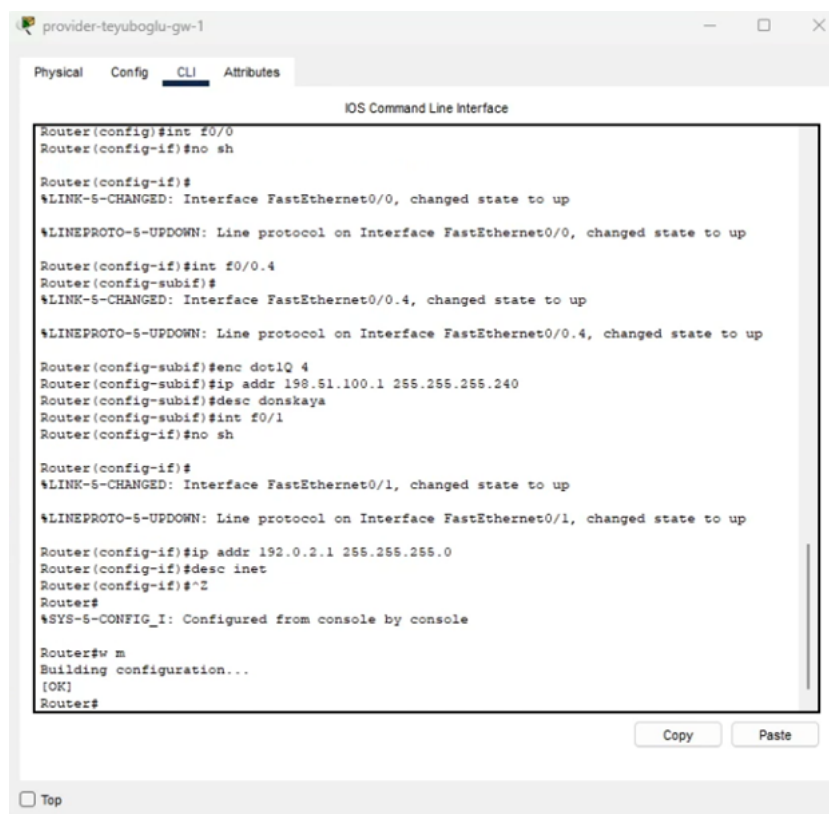


Рис. 3.2: Присвоение адресов интерфейсам

Сервера сайтов были настроены в предыдущей работе, Коммутатор интернета в настройке не нуждается

Переходим к настройке маршрутизатора университета. В соответствии с заданием создаем списки доступа. Задаем трансляцию внутренних адресов, принадлежащих серверам, во внешние. (рис. 3.3) (рис. 3.4).

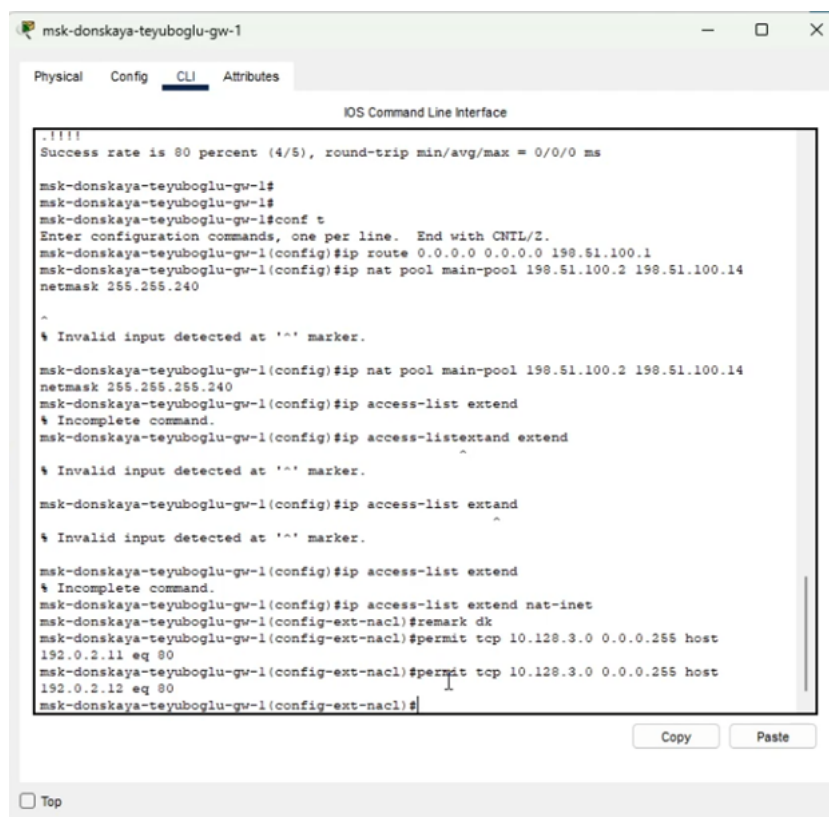


Рис. 3.3: Настройка маршрутизатора



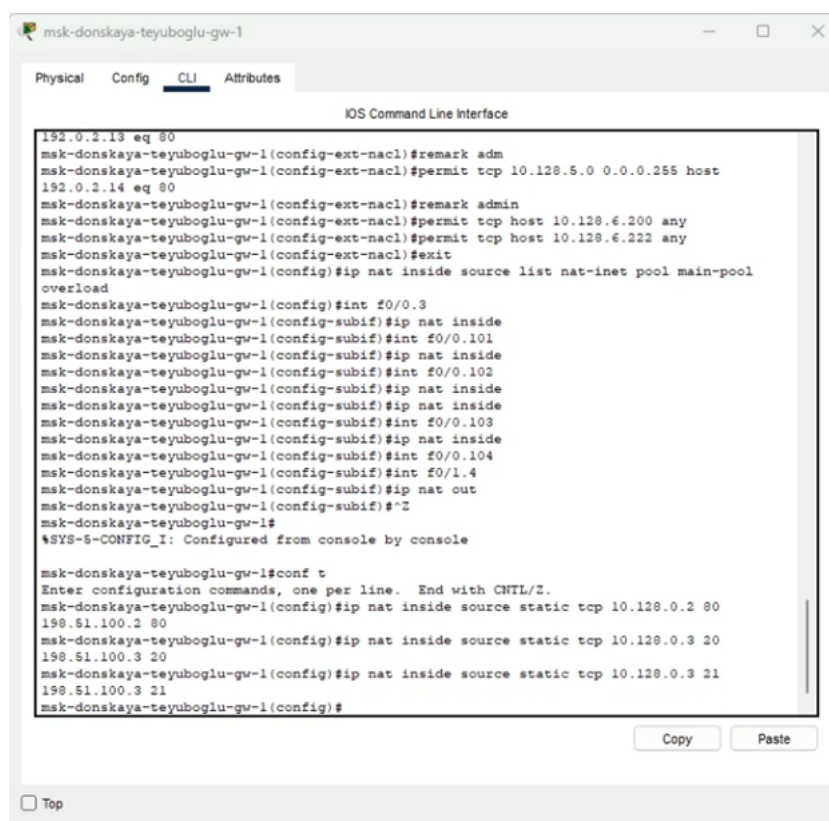


Рис. 3.4: Настройка маршрутизатора

Проверим как наши пользователи могут выходить в интернет.  
Администратору позволено все. (рис. 3.5).

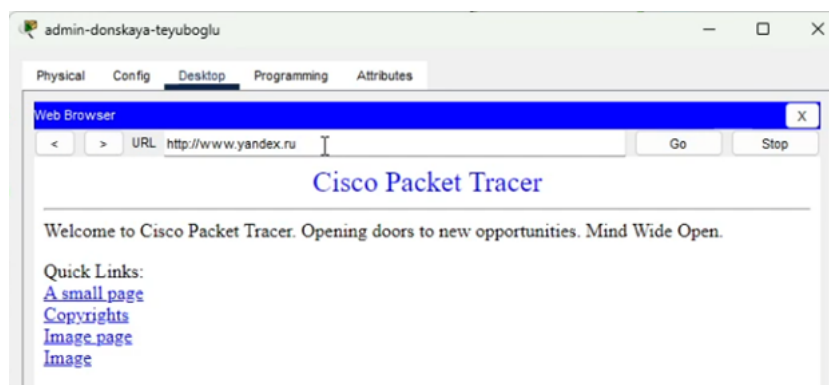


Рис. 3.5: Администратор

Пользователи – только на сайт вуза и яндекс. (рис. 3.6) (рис. 3.7) (рис. 3.8).



Рис. 3.6: Пользователи

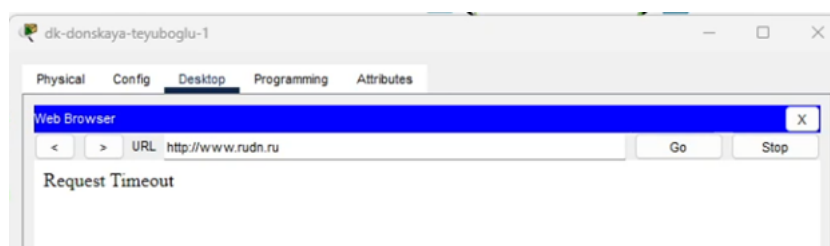


Рис. 3.7: Пользователи

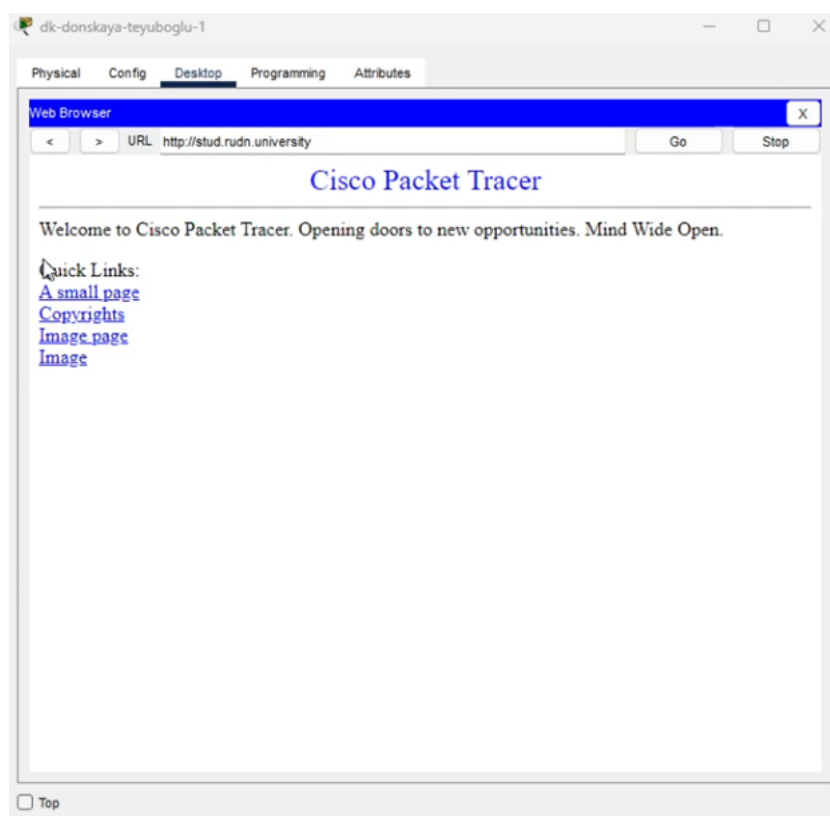


Рис. 3.8: Пользователи

В интернет нас пускает. Теперь проверим пускает ли из интернета к нам. Установим за NATом, в интернете пользователя и попробуем с него зайти на веб-сервер по http. (рис. 3.9) (рис. 3.10).

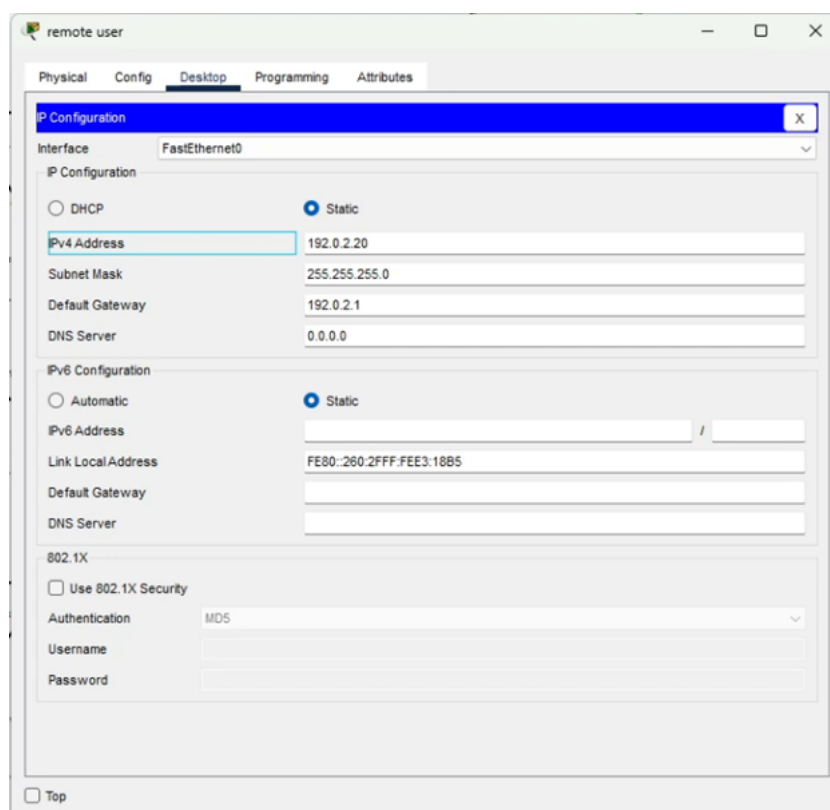


Рис. 3.9: Проверка



Рис. 3.10: Проверка

Вход выполнен. (рис. 3.11) (рис. 3.12).

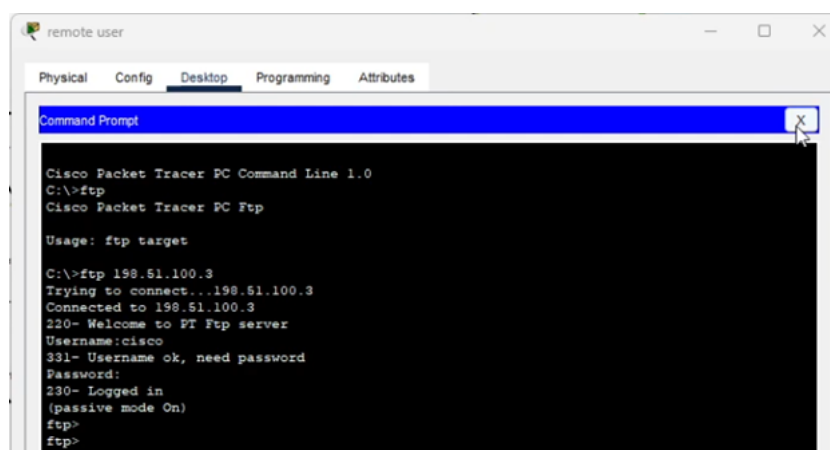


Рис. 3.11: Вход выполнен

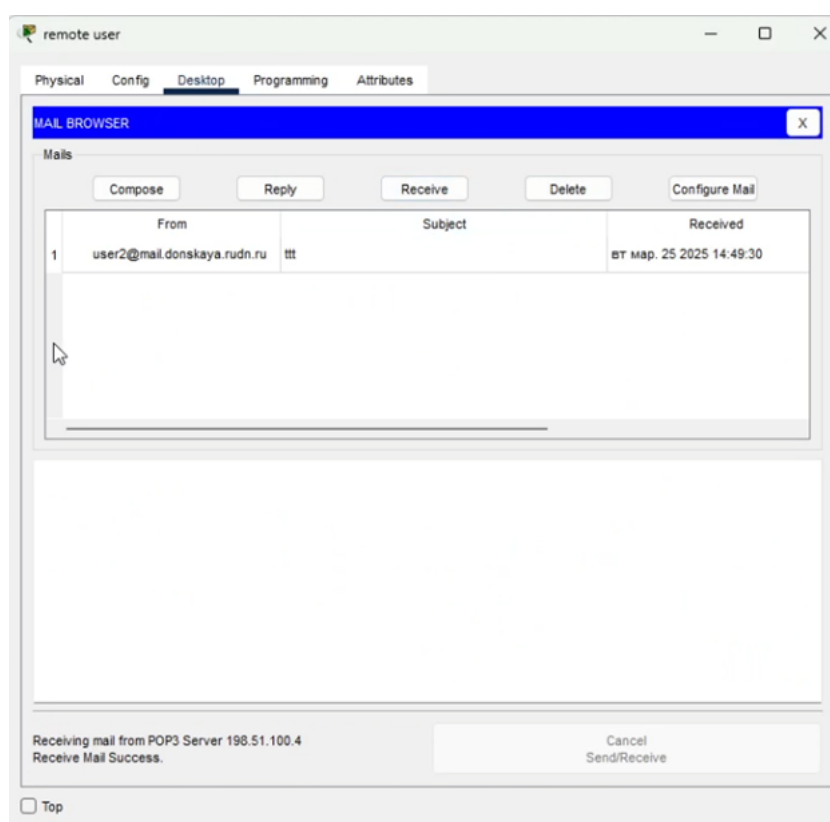


Рис. 3.12: Вход выполнен

## 4 Выводы

Настроили доступ к всемирной сети и правила NAT

## 5 Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)? - NAT на устройстве позволяет ему соединять публичные и частные сети между собой с помощью только одного IP-адреса для группы.
2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)? - Настроить интерфейсы на внутренних маршрутизаторах, наборы правил для преобразования IP.
3. Можно ли применить Cisco IOS NAT к субинтерфейсам? - Да, поскольку они существуют в энергонезависимой памяти.
4. Что такое пулы IP NAT? - Выделяемые для трансляции NAT IP.
5. Что такое статические преобразования NAT? - Взаимно однозначное преобразование внутренних IP во внешние.