**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](http://www.rudn.ru);

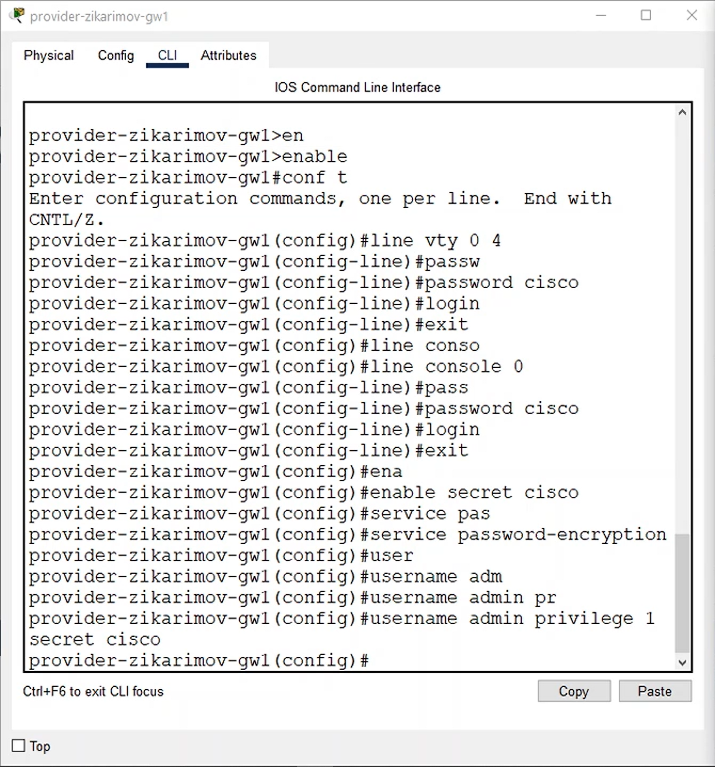
5) в сети для других пользователей компьютер администратора должен иметь полный доступ во внешнюю сеть, а другие пользователи — не должны выходить в Интернет;

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;

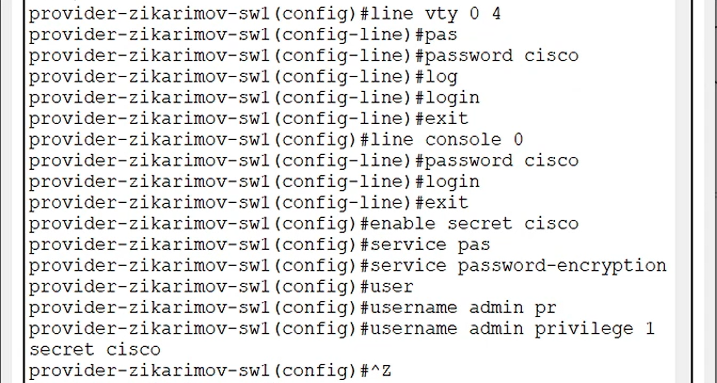
7) компьютер администратора должен быть доступен из внешней сети по протоколу удалённого рабочего стола (Remote Desktop Protocol, RDP).

**Последовательность выполнения работы**

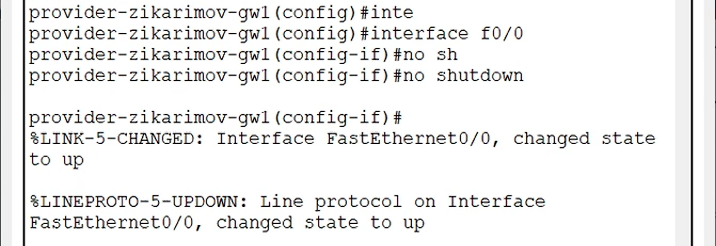
12.4.1. Первоначальная настройка маршрутизатора provider-gw-1

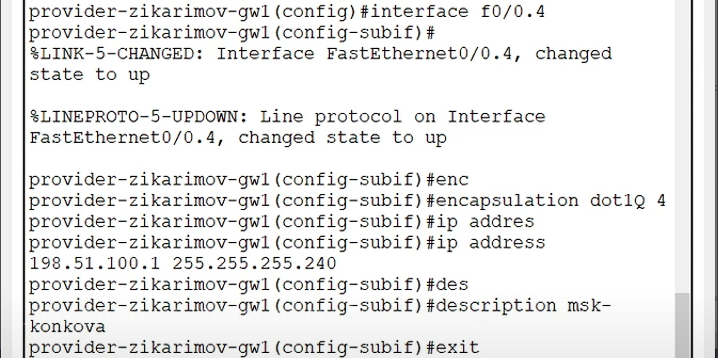


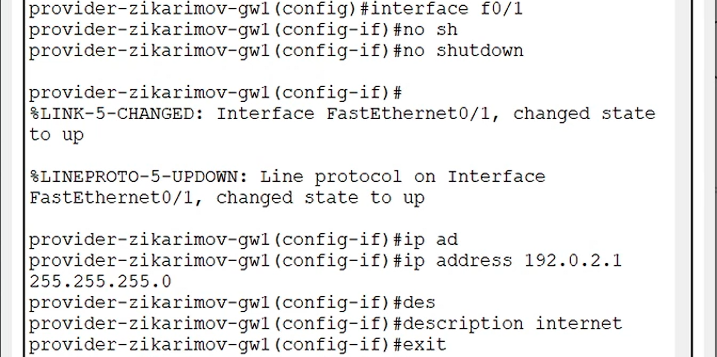
12.4.2. Первоначальная настройка коммутатора provider-sw-1



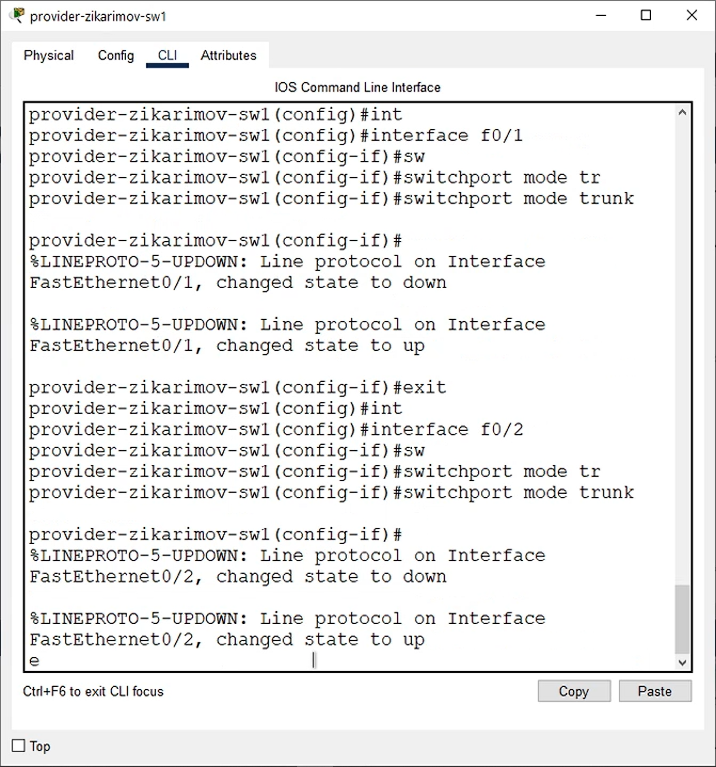
12.4.3. Настройка интерфейсов маршрутизатора provider-gw-1

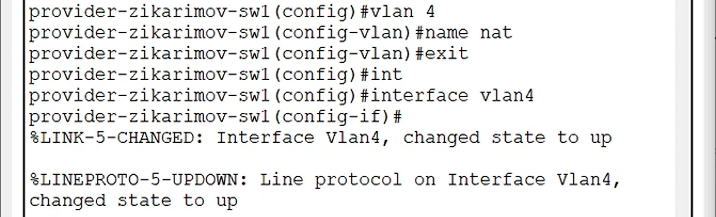




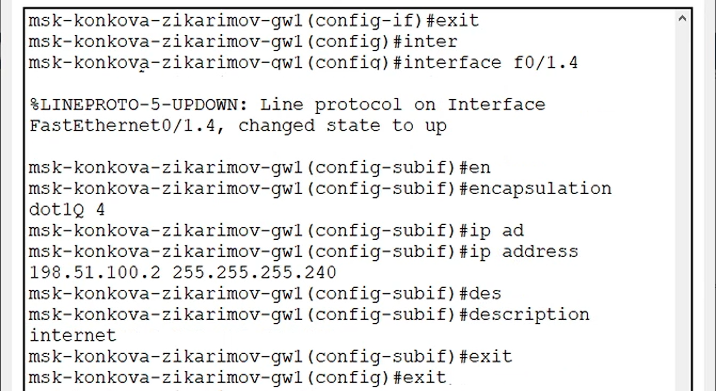
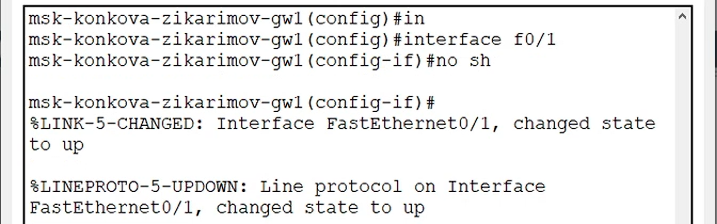


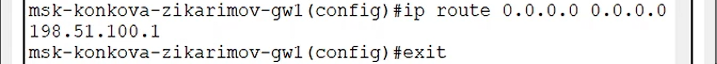
12.4.4. Настройка интерфейсов коммутатора provider-sw-1



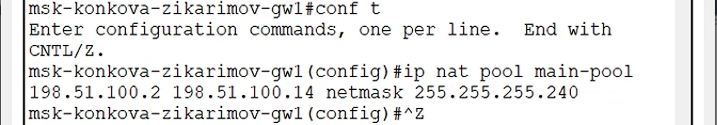


12.4.5. Настройка интерфейсов маршрутизатора msk-donskaya-gw-1

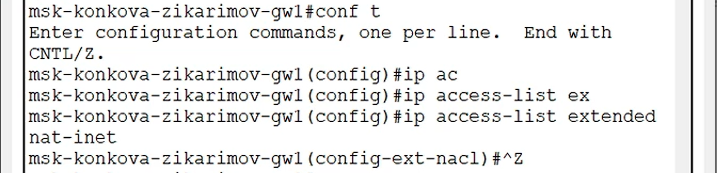




12.4.6. Настройка пула адресов для NAT



12.4.7. Настройка списка доступа для NAT

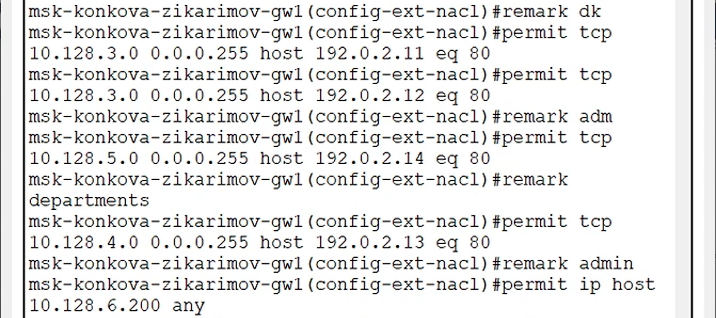


12.4.7.1. Сеть дисплейных классов

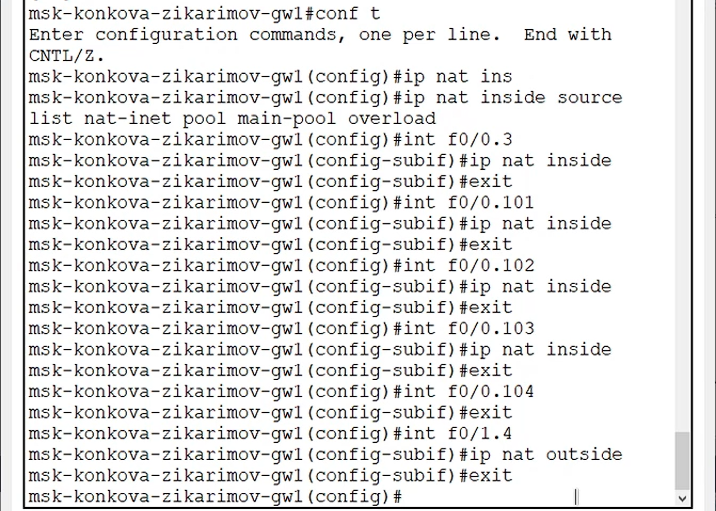
12.4.7.2. Сеть кафедр

12.4.7.3. Сеть администрации

12.4.7.4. Доступ для компьютера администратора



12.4.8. Настройка NAT



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

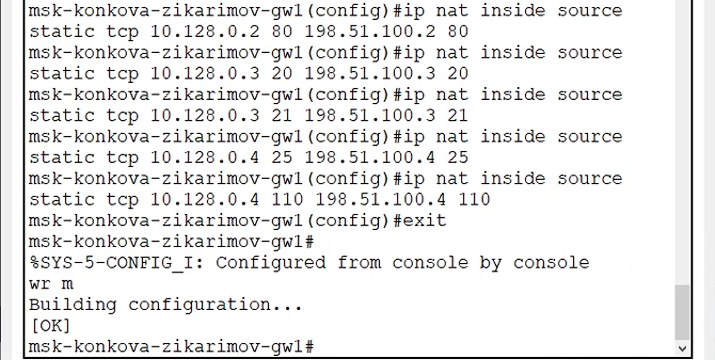


12.4.9. Настройка доступа из Интернета

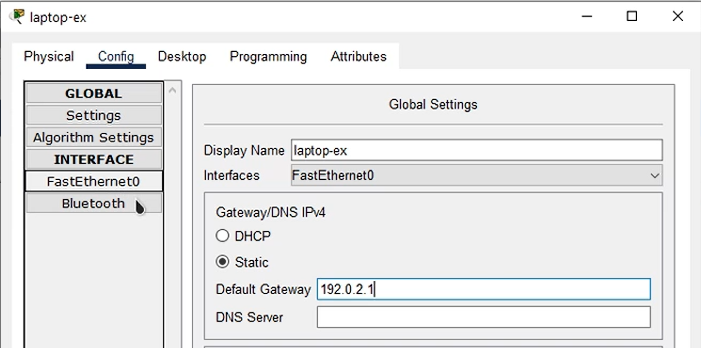
12.4.9.1. WWW-сервер

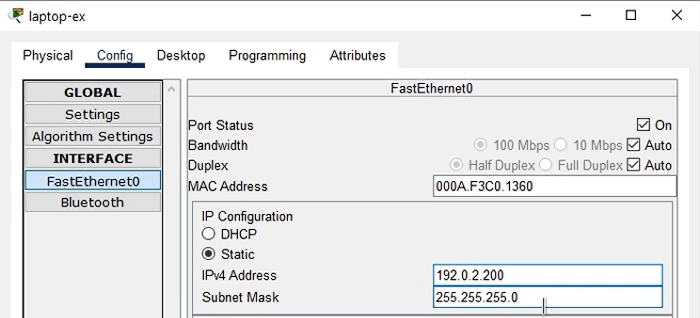
12.4.9.2. Файловый сервер

12.4.9.3. Почтовый сервер

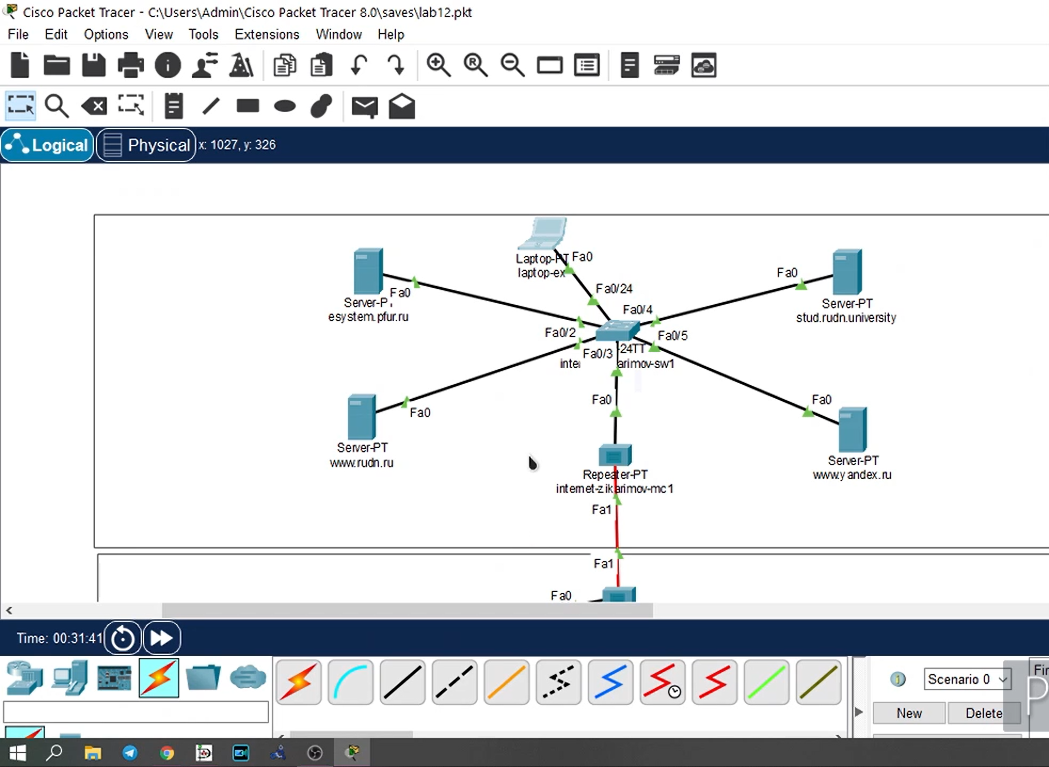


12.4.9.4. Доступ по RDP





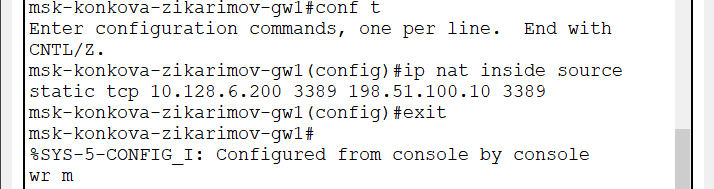




Я добавил laptop-ex в Internet и соединил с коммутатором. Также в физической рабочей области я перенес laptop-ex в Internet. И задал для данного устройства шлюз по умолчанию, ip-address и сетевую маску.

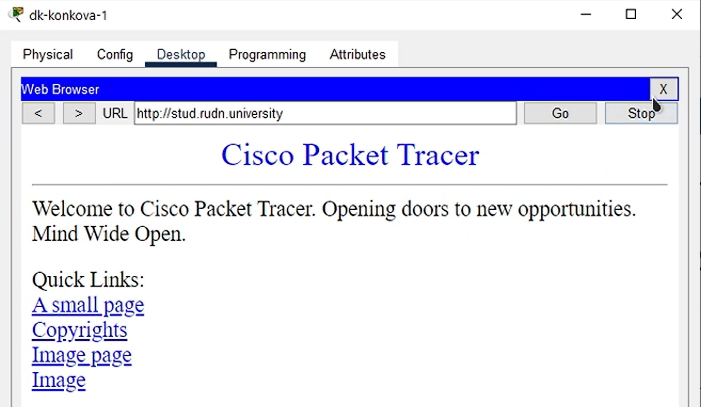
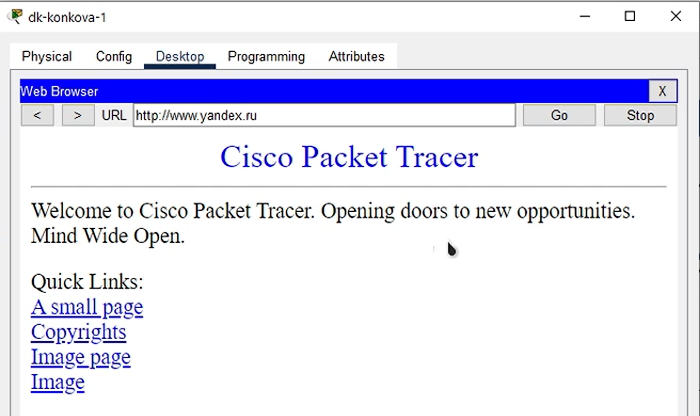
В L1 добавил laptop-ex.

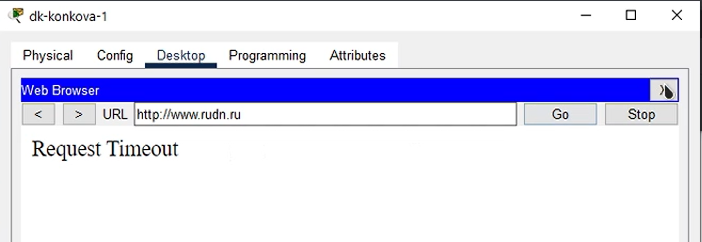




**Проверить работоспособность заданных настроек.**

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)).



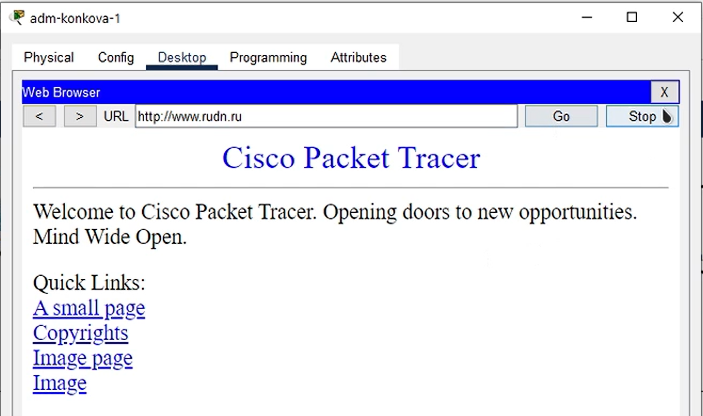


Можно увидеть, что дисплейный класс не может получить доступ к другому сайту.

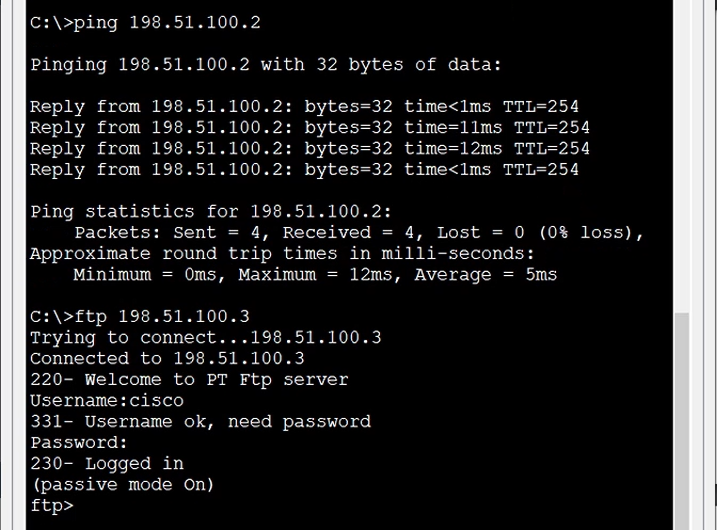
Сеть кафедр работает только с образовательными сайтами (esystem.pfur. ru (192.0.2.13)).



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



Проверка WWW-сервер и Файловый сервер.



Почтовый сервер



**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 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.