Лабораторная работа № 12

Настройка NAT

Демидова Екатерина Алексеевна

Содержание

# 1 Цель работы

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

# 2 Задание

Требуется подключить локальную сеть организации к сети Интернет с учётом ограничений, накладываемых на определённые подсети локальной сети:

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;

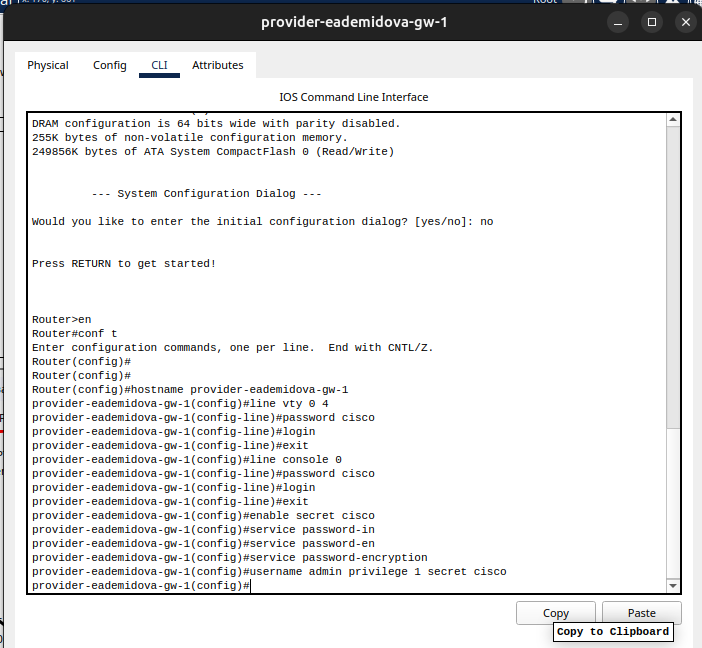
1. компьютер администратора должен быть доступен из внешней сети по протоколу удалённого рабочего стола (Remote Desktop Protocol, RDP).

**Задание**

1. Сделать первоначальную настройку маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера: задать имя, настроить доступ по паролю и т.п.
2. Настроить интерфейсы маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера:
3. Настроить интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера.
4. Настроить на маршрутизаторе сети «Донская» NAT с правилами, указанными в разделе 12.2.
5. Настроить доступ из внешней сети в локальную сеть организации, как указано в разделе 12.2.
6. Проверить работоспособность заданных настроек.

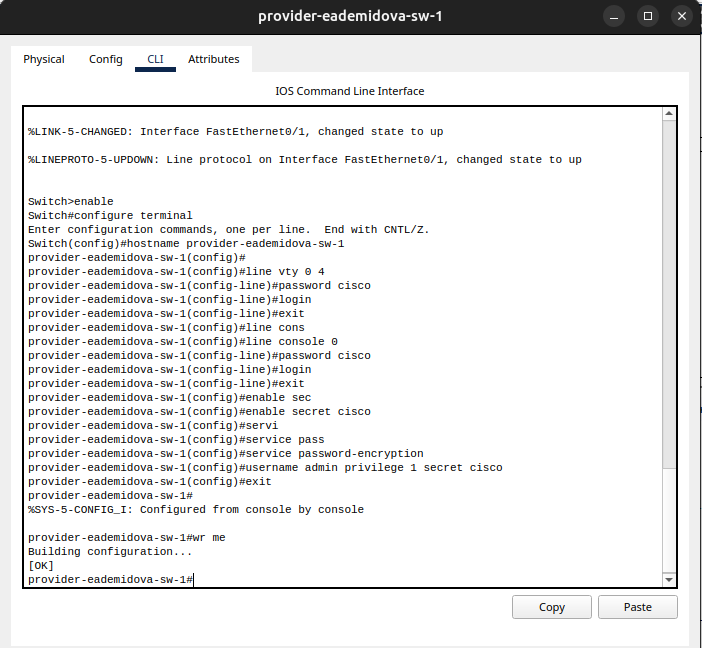
# 3 Выполнение лабораторной работы

Проведем первоначальную настройку маршрутизатора provider-eademidova-gw-1: зададим имя, настроим доступ по паролю к виртуальным терминалам(рис. [??]).



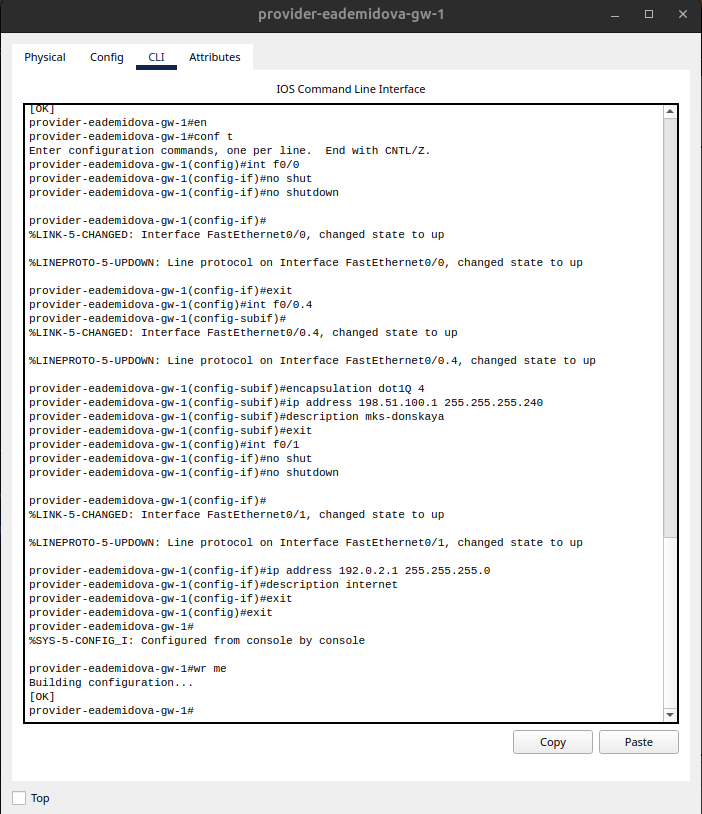
Первоначальная настройка маршрутизатора provider-eademidova-gw-1

Затем сделаем то же самое для коммутатора provider-eademidova-sw-1(рис. [??]):



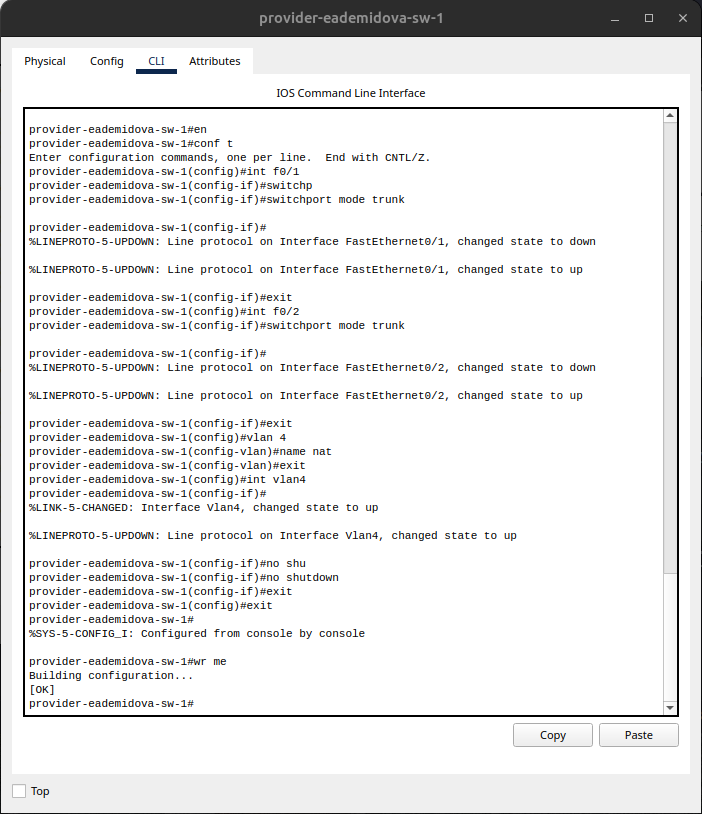
Первоначальная настройка коммутатора provider-eademidova-sw-1

Настроим интерфейсы маршрутизатора provider-eademidova-gw-1: поднимем интерфейс f0/0, создадим интерфейс f0/0.4 для 4 vlan и зададим ip-адрес, поднимем интерфейс f0/1 для доступа в интернет(рис. [??]).



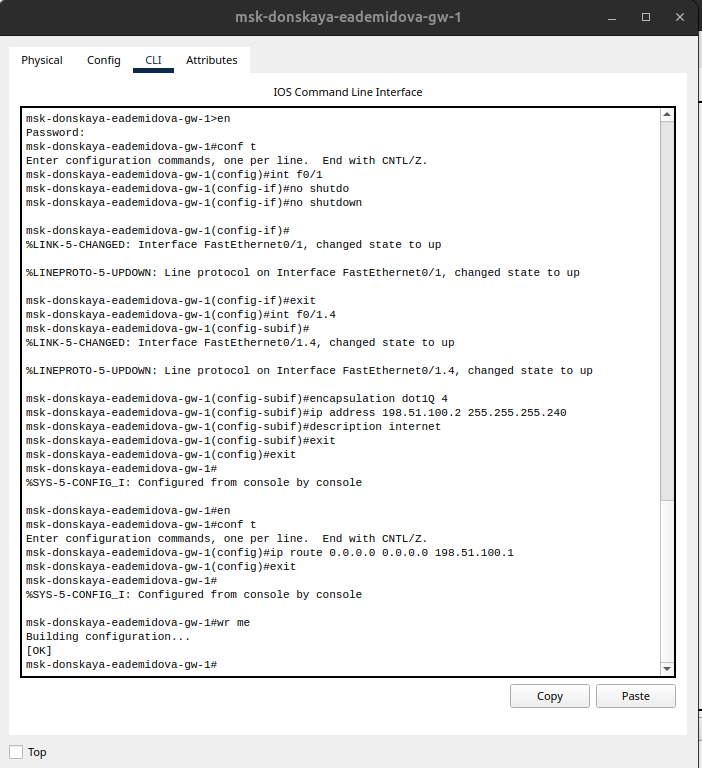
Настройка интерфейсов маршрутизатора provider-eademidova-gw-1

Настроим интерфейсы коммутатора provider-eademidova-gw-1: сделаем транковыми порты f0/1 и f0/2, зададим 4 vlan с именем nat(рис. [??]).



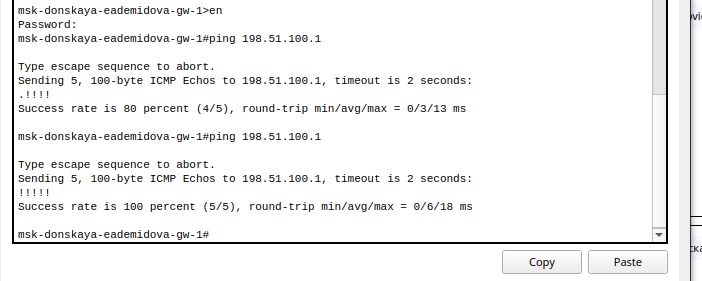
Настройка интерфейсов коммутатора provider-eademidova-sw-1

Настроим интерфейсы маршрутизатора msk-donskaya-eademidova-gw-1: поднимем интерфейс f0/1, создадим интерфейс f0/1.4 для 4 vlan и зададим ip-адрес(рис. [??]):



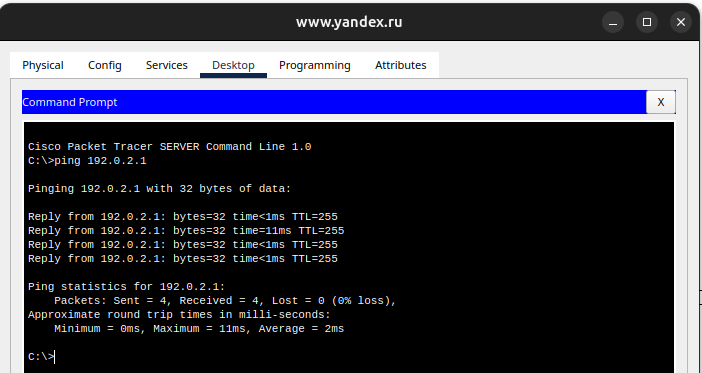
Настройка интерфейсов маршрутизатора msk-donskaya-eademidova-gw-1

Проверим доступ с маршрутизатора на Донской к маршрутизатору провайдера(рис. [??]).



Проверка связи между маршрутизаторами

А также доступ с серверов интернете на маршрутизатор провайдера(рис. [??]).



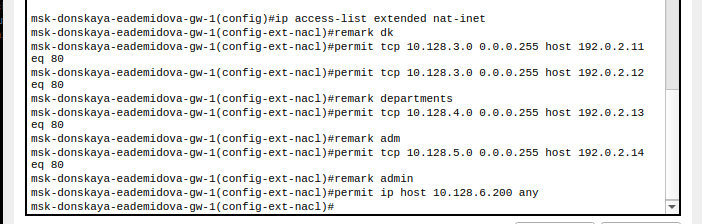
Проверка связи между сервером и маршрутизатором

Настроим пул адресов 198.51.100.2 – 198.51.100.14 для NAT(рис. [??]).

Настройка пула адресов для NAT

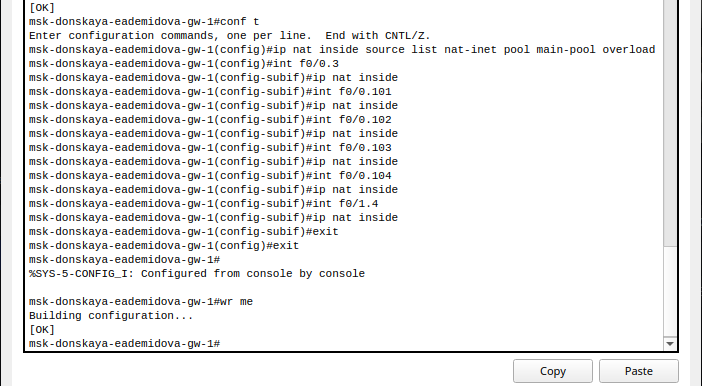
Настройка пула адресов для NAT

Теперь настроим список доступа к nat на всех подсетях для пользователей(рис. [??]):



Настройка списка доступа для NAT

Настроим Port Address Translation (PAT) на субинтерфейсах маршрутизатора с территории Донская (рис. [??]):



Настройка NAT

Настроим доступа из Интернета. Для этого добавим компьютер на территории Интернета(рис. [??]):

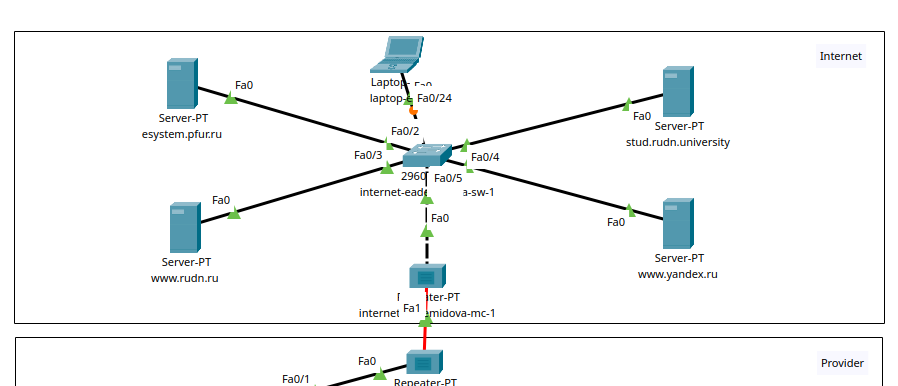
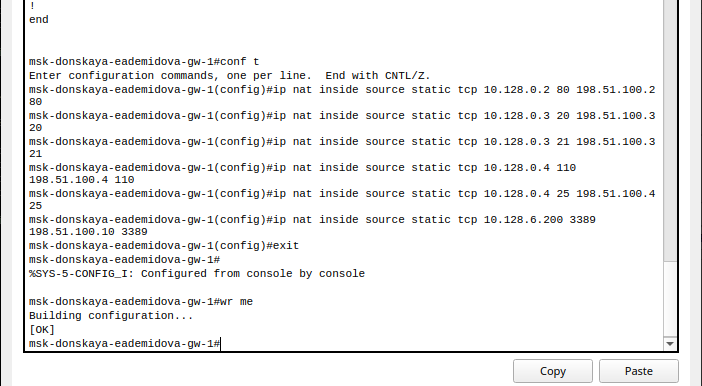


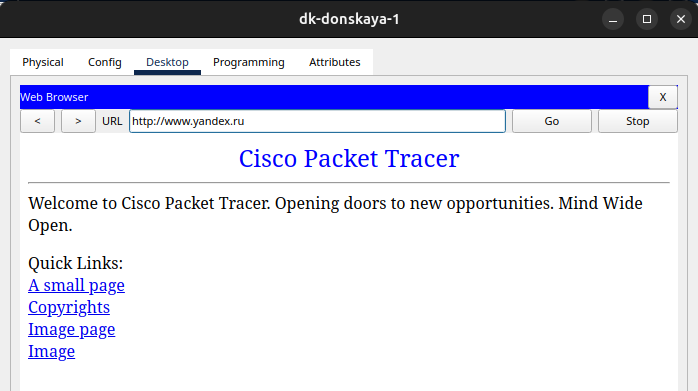
Схема сети Интернет с ноутбуком

Затем свяжем ip-адреса серверов с территории Донская с ip-адресами серверов в Интернете(рис. [??]):

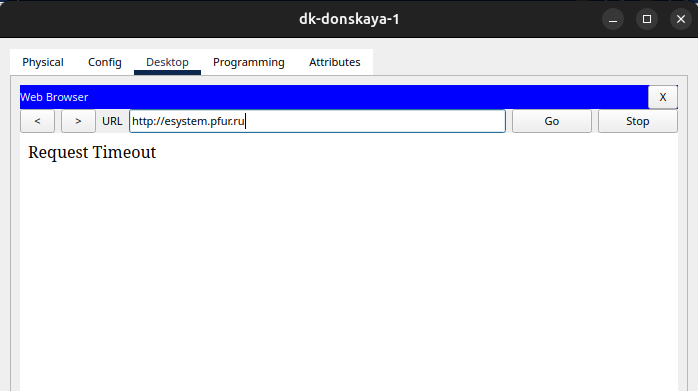


Настройка доступа из Интернета

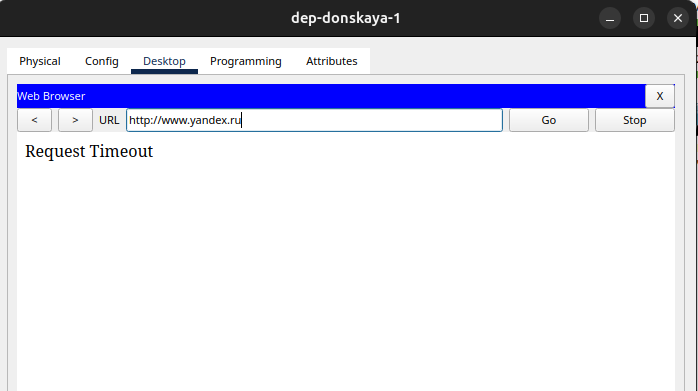
Проверим доступ к необходимым интернет-ресурсам конечных устройств сети. Убедимся, что устройствам доступны и недоступны заданные нами сайты(рис. [??] - [??]).



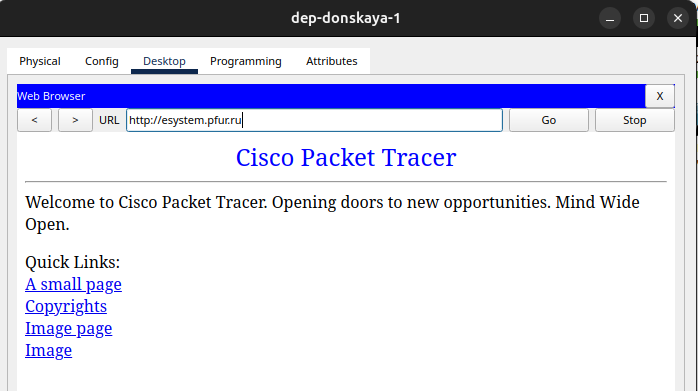
Доступ dk-donskaya-1 к www.yandex.ru



Доступ dk-donskaya-1 к esystem.pfur.ru

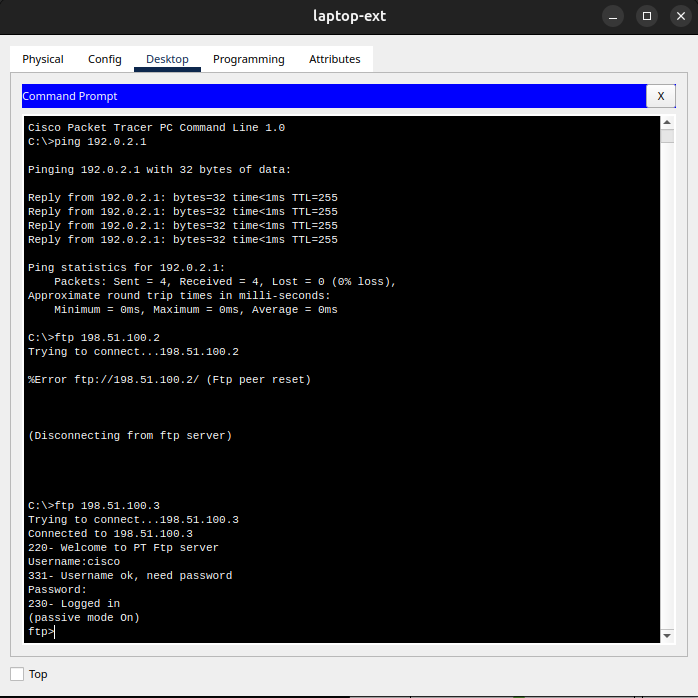


Доступ dep-donskaya-1 к www.yandex.ru

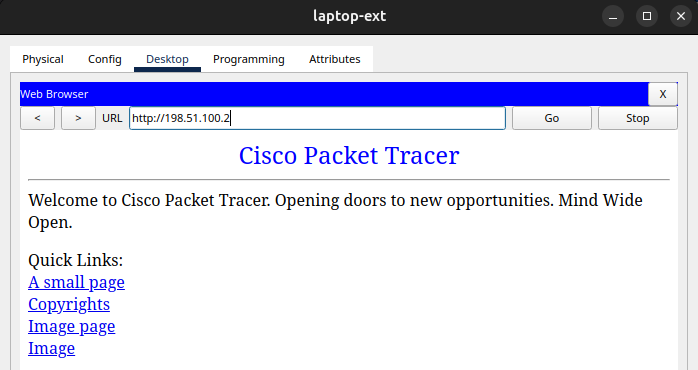


Доступ dep-donskaya-1 к esystem.pfur.ru

Также проверим работоспособность соединения из сети Интернет в сеть Донской к web-серверу и файловому серверу по ftp(рис. [??], [??]):



Проверка доступа из Интернета по ftp



Проверка доступа из Интернета к web-серверу

## 3.1 Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)?
2. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?
3. Можно ли применить Cisco IOS NAT к субинтерфейсам?
4. Что такое пулы IP NAT?
5. Что такое статические преобразования NAT?
6. Основной принцип работы NAT (Network Address Translation) заключается в том, что он позволяет скрывать внутренние IP-адреса устройств в локальной сети за одним или несколькими публичными IP-адресами, которые используются для общения с внешними сетями, такими как Интернет. Наличие NAT в сети организации позволяет экономить публичные IP-адреса и повышать безопасность защитой внутренних устройств от прямого доступа извне.
7. Для настройки NAT на оборудовании (например, маршрутизаторе или межсетевом экране) необходимо определить правила преобразования адресов. Настройка NAT позволяет установить соответствие между внутренними и внешними IP-адресами, а также определить, какие порты и протоколы будут использоваться для коммуникации между внутренней и внешней сетями.
8. Да, Cisco IOS NAT можно применить к субинтерфейсам. Субинтерфейсы позволяют разделять один физический интерфейс на несколько логических интерфейсов, каждый из которых может иметь свои собственные настройки NAT.
9. Пулы IP NAT представляют собой диапазон публичных IP-адресов, которые используются для преобразования внутренних адресов при прохождении трафика через устройство NAT. Пулы IP NAT могут быть динамическими (когда каждое внутреннее устройство получает временный доступ к одному из публичных адресов из пула) или статическими (когда определенное внутреннее устройство всегда связано с определенным публичным адресом).
10. Статические преобразования NAT (Static NAT) — это метод, при котором определенный внутренний IP-адрес связывается с определенным публичным IP-адресом, и все запросы к этому внутреннему адресу направляются на соответствующий публичный адрес. Это позволяет установить постоянное соответствие между внутренним и внешним адресами для конкретных устройств в сети.

# 4 Выводы

В результате выполнения лабораторной были приобретены практические навыки по настройке доступа локальной сети к внешней сети посредством NAT.