Отчёт по лабораторной работе №12

Администрирование локальных сетей

Ищенко Ирина НПИбд-02-22

Содержание

# 1 Цель работы

Приобретение практических навыков по настройке доступа локальной сети к внешней сети посредством NAT [1].

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

# 3 Выполнение лабораторной работы

Сделаем первоначальную настройку маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера: зададим имя, настроим доступ по паролю и т.п. (рис. 1) и (рис. 2).

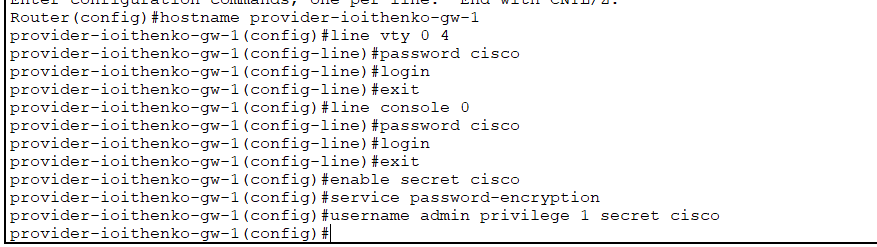


Рис. 1: Первоначальная настройка маршрутизатора

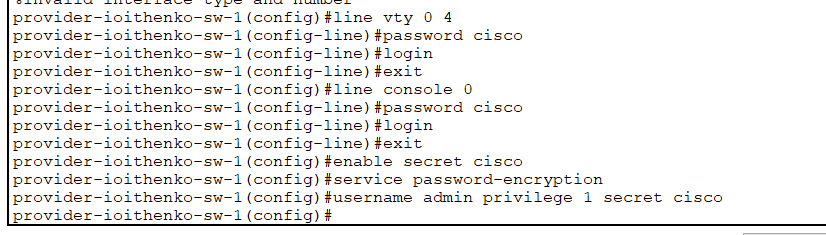


Рис. 2: Первоначальная настройка коммутатора

Настроим интерфейсы маршрутизатора provider-gw-1 и коммутатора provider-sw-1 провайдера (рис. 3) и (рис. 4).

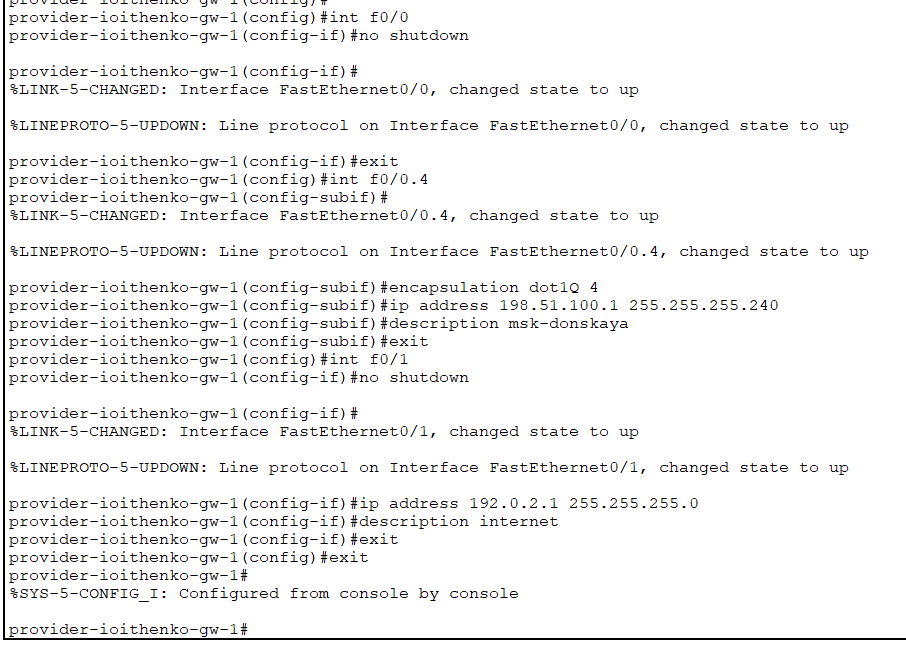


Рис. 3: Настройка интерфейсов маршрутизатора

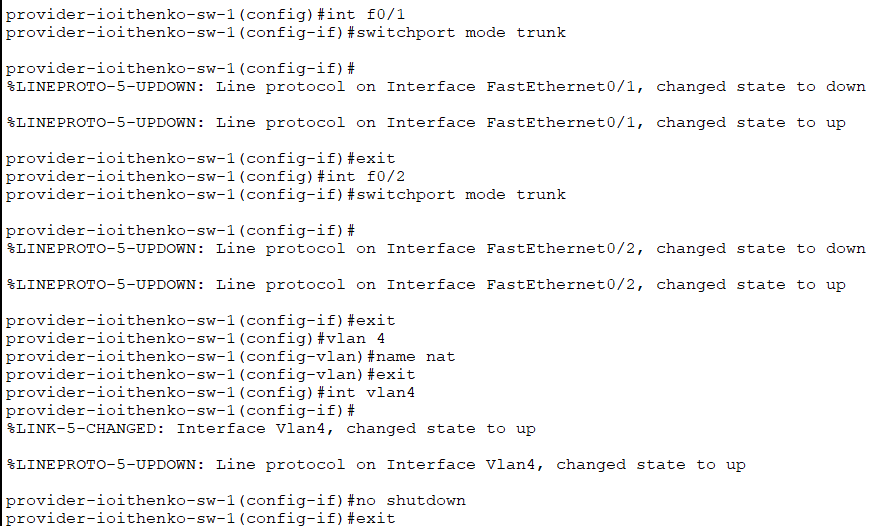


Рис. 4: Настройка интерфейсов коммутатора

Настроим интерфейсы маршрутизатора сети «Донская» для доступа к сети провайдера (рис. 5).

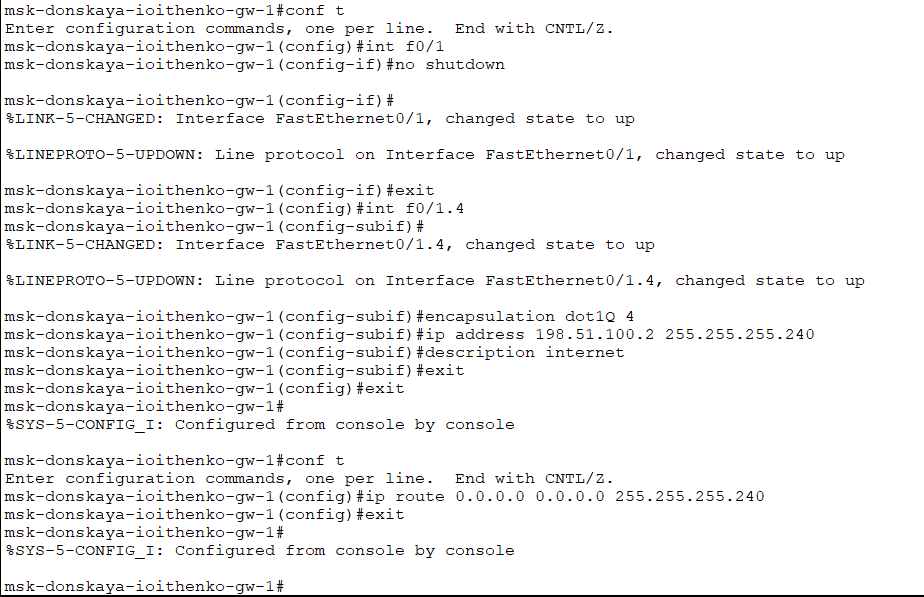


Рис. 5: Интерфейсы маршрутизатора сети Донская

Настроим на маршрутизаторе сети «Донская» NAT с правилами, описанными в задании (рис. 6).

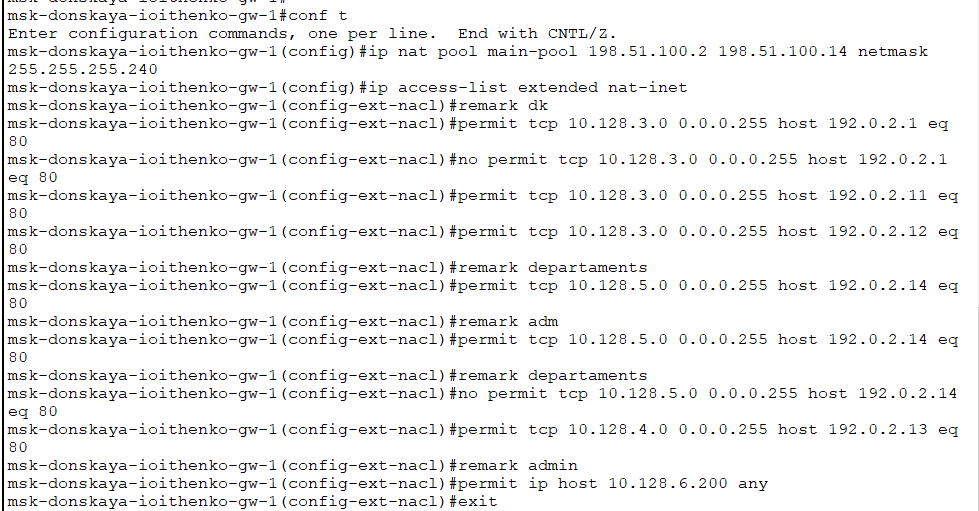


Рис. 6: Ограничения на подсети

Настроим доступ из внешней сети в локальную сеть организации (рис. 7) и (рис. 8).

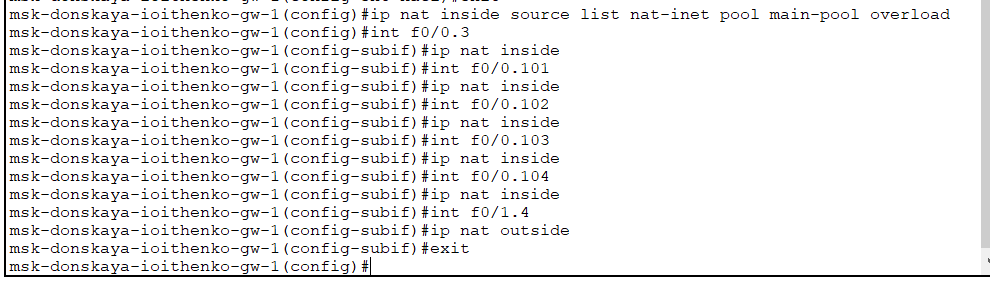


Рис. 7: Настройка интерфейсов для NAT

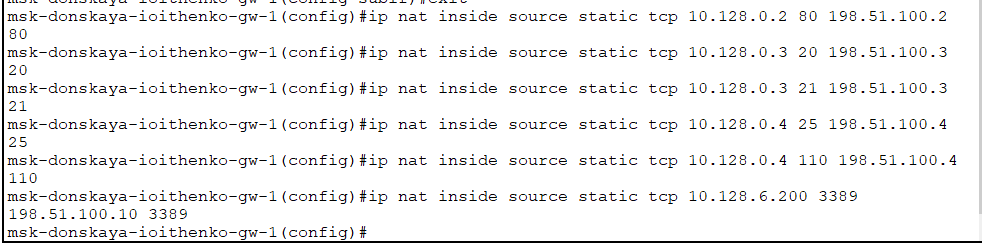


Рис. 8: Настройка доступа из интернета

Проверим работоспособность заданных настроек (рис. 9).

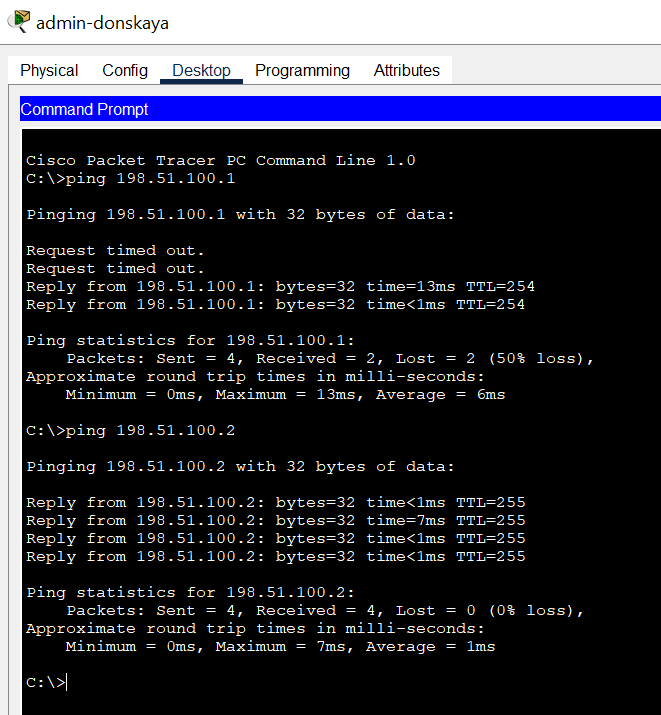


Рис. 9: Доступность устройств для admin

Добавим в сеть ноутбук и проверим работоспособность (рис. 10) и (рис. 11). Пинг успешен, подключение по FTP работает.

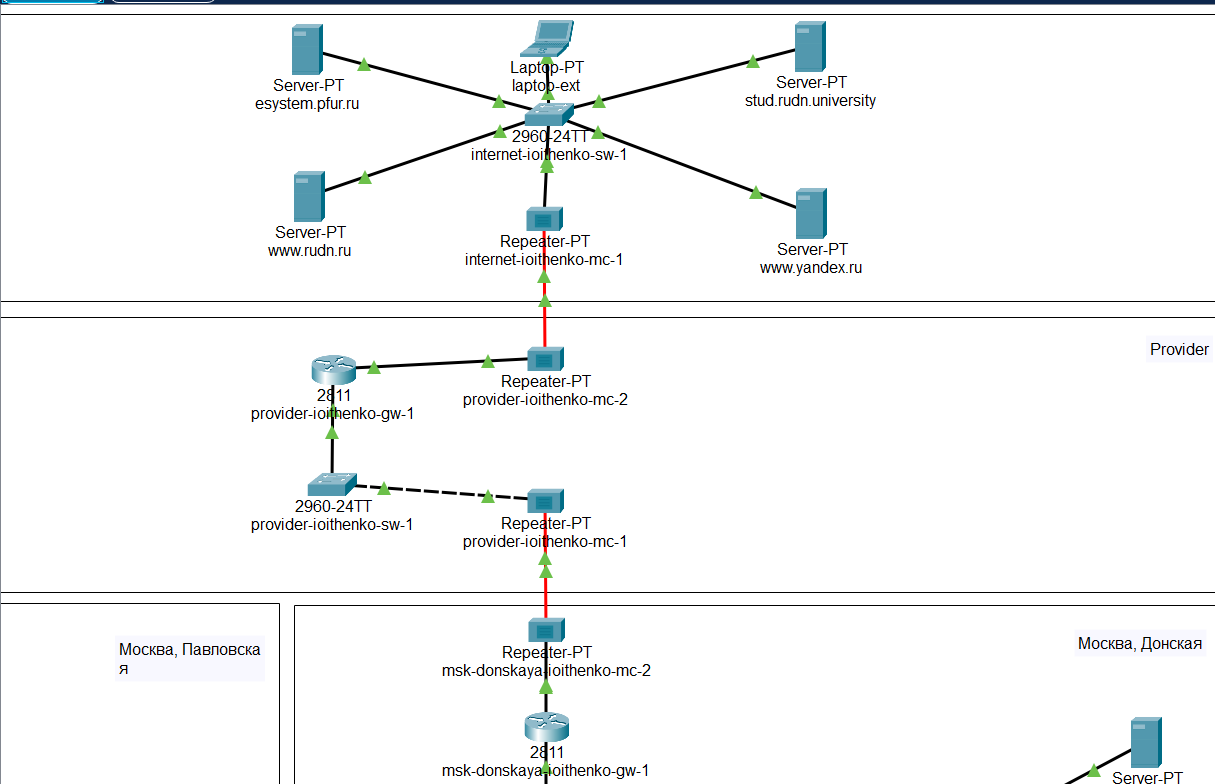


Рис. 10: Добавление ноутбука

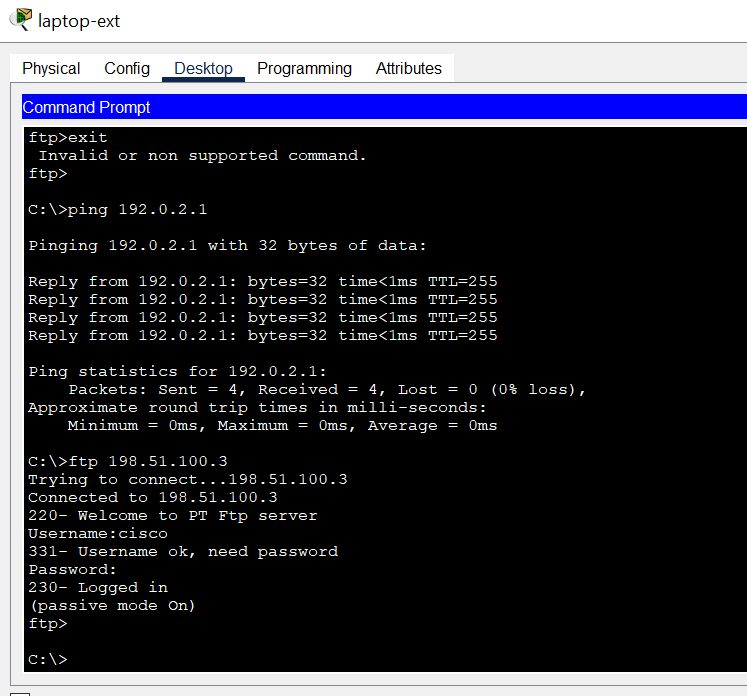


Рис. 11: Проверка

Доступ по HTTP активен (рис. 12).

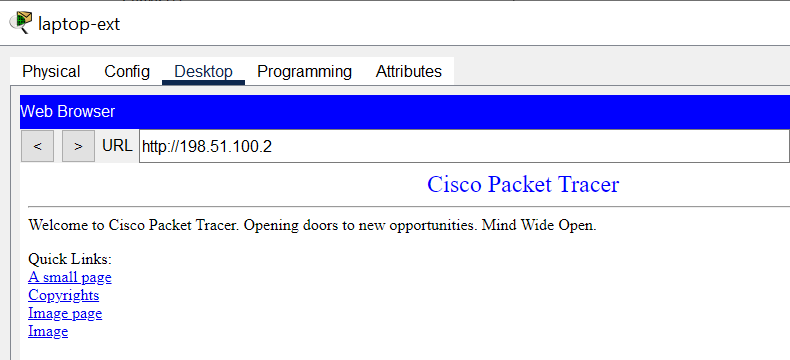


Рис. 12: Доступ по HTTP

Проверим на устройствах подсети доступ к серверам (рис. 13), (рис. 14), (рис. 15) и (рис. 16). Все корректно.

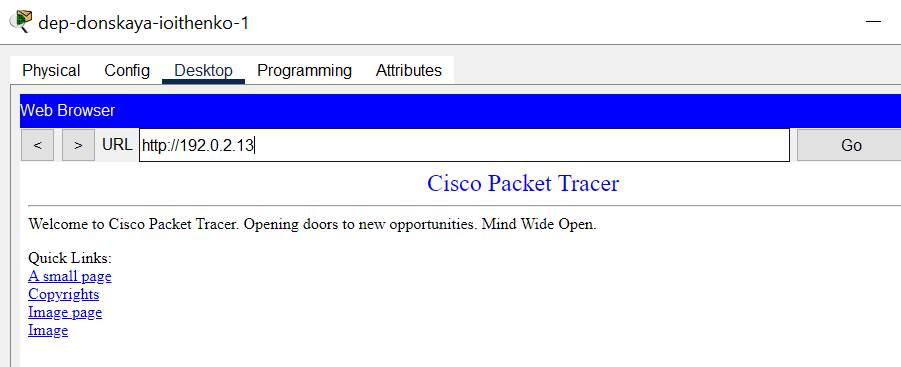


Рис. 13: dep

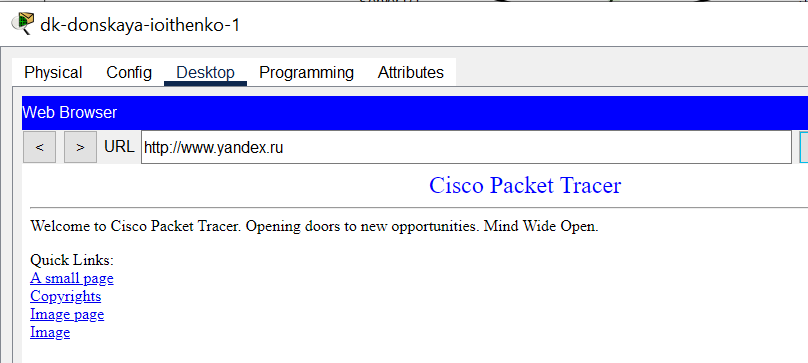


Рис. 14: dk

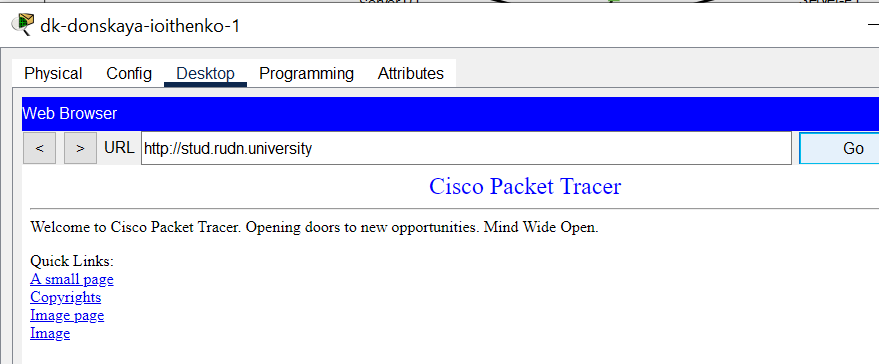


Рис. 15: dk

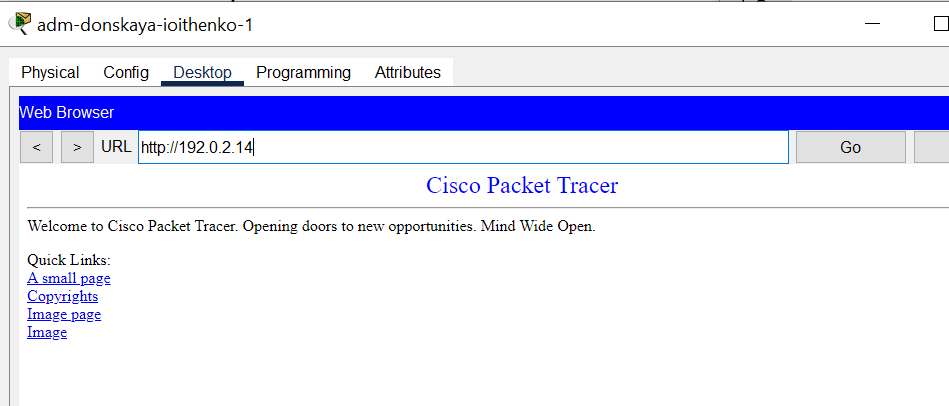


Рис. 16: adm

# 4 Выводы

В ходе выполнения лабораторной работы я приобрела практические навыки по настройке доступа локальной сети к внешней сети посредством NAT.

# 5 Контрольные вопросы

1. В чём состоит основной принцип работы NAT (что даёт наличие NAT в сети организации)?

Идея NAT заключается в том, чтобы осуществлять перевод частного локального IP-адреса в общедоступный глобальный IP-адрес и наоборот. Это необходимо для обеспечения доступа к Интернету локальным узлам, использующим частные адреса.

Наличие NAT в сети организации позволяет экономить публичные IP-адреса и повышать безопасность защитой внутренних устройств от прямого доступа извне.

1. В чём состоит принцип настройки NAT (на каком оборудовании и что нужно настроить для из локальной сети во внешнюю сеть через NAT)?

Как правило, граничный маршрутизатор настроен для NAT, то есть маршрутизатор, который имеет один интерфейс в локальной (внутренней, inside) сети и один интерфейс в глобальной (внешней, outside) сети. Когда пакет проходит за пределы локальной (inside) сети, NAT преобразует локальный (частный, private) IP-адрес в глобальный (публичный, public) IP-адрес. Когда пакет входит в локальную сеть, глобальный (public) IP-адрес преобразуется в локальный (private) IP-адрес. Граничный маршрутизатор выступает в роли шлюза между внутренней корпоративной сетью и внешней сетью, например, Интернетом.

1. Можно ли применить Cisco IOS NAT к субинтерфейсам?

Да. Преобразования NAT источника или назначения могут применяться к любому интерфейсу или подинтерфейсу с IP-адресом (включая интерфейсы программы набора номера).

1. Что такое пулы IP NAT?

Пул NAT — это набор из одного или нескольких общедоступных IPv4-адресов, которые используются в маршрутизаторе NAT.

При отправке трафика устройством из внутренней сети во внешнюю сеть маршрутизатор преобразует его внутренний IPv4-адрес в один из адресов, входящих в состав пула.

В результате действия такого механизма весь исходящий из сети трафик внешние устройства «видят» с общедоступным адресом IPv4, который можно назвать NAT IP-адресом.

1. 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.

# Список литературы

1. Королькова А. В. К.Д.С. Администрирование сетевых подсистем. Лабораторный практикум : учебное пособие. Москва: РУДН, 2021. 137 с.