

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ

РОССИЙСКОЙ ФЕДЕРАЦИИ

**ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ**

**«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ» (ДГТУ)**

Факультет Информатика и вычислительная техника

(наименование факультета)

Кафедра Кибербезопасность информационных систем

(наименование кафедры)

**ОТЧЕТ**

По практической работе по предмету: Компьютерные сети

Выполнил:

ст. гр. ВКБ31 Котелевец К.А.

Ростов-на-Дону

2025

Задание: Для практики необходимо создать корпоративную сеть, состоящую из 3-х офисов по 5 компьютеров в каждом, при этом офисы соединены через VPN. В каждом офисе есть выход в интернет через NAT.

Ход работы:

Для начала создадим схему сети, которая представлена на рисунке 1.

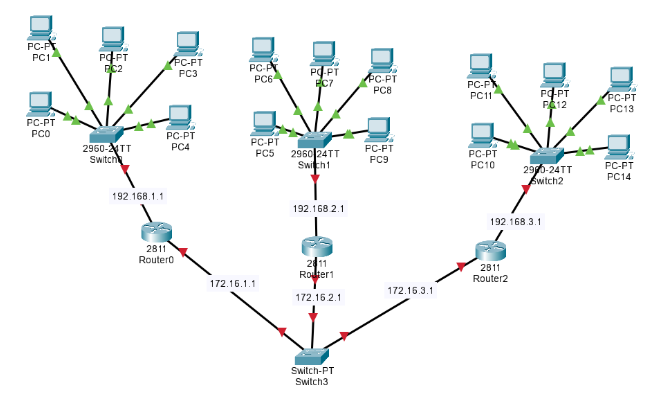


Рисунок 1 – Схема сети

Для начала сконфигурируем наши компьютеры. На рисунке 2 пример настройки первого компьютера из офиса 1.

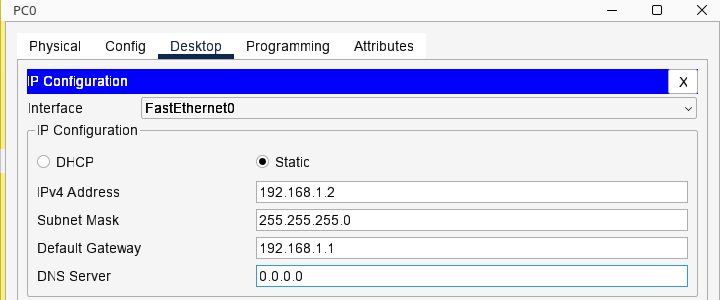


Рисунок 2 – Конфигурация ПК 1 из офиса 1

Далее настроим порты роутера. На рисунке 3 и 4 настройки интерфейсов fa0/0 и fa0/1 соответсвенно для роутера первого офиса

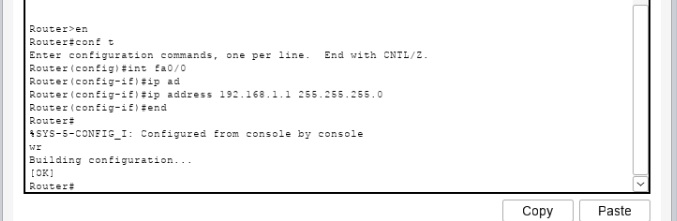


Рисунок 3 – настройка интерфейса fa0/0 на роутере офиса 1

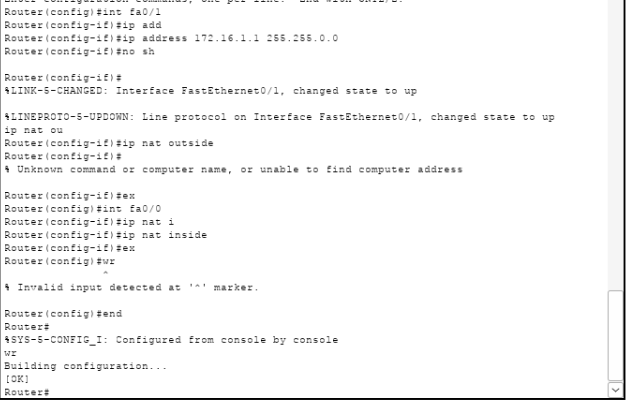


Рисунок 4 – настройка интерфейса fa0/1 на роутере офиса 1 + NAT

Аналогично настраиваем в других офисах

Также не забываем настройки Acces-list для NAT (рисунок 5)

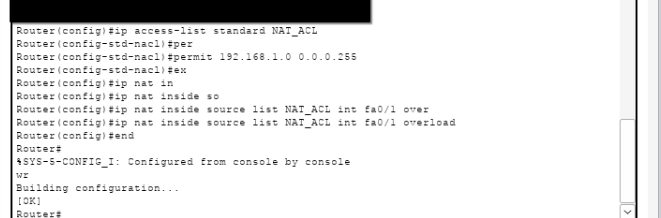


Рисунок 5 – Настройка Access-list на роутере 1 офиса

Проделаем аналогичные настройки на других роутерах.

Настроим теперь VPN. В данном случае это будет IPsec. Настройка представлена ниже для роутера офиса 1, аналогочно для других роутеров

|  |
| --- |
| Router(config)#crypto isakmp policy 10  Router(config-isakmp)#encryption aes 256  Router(config-isakmp)#hash sha  Router(config-isakmp)#authentication pre-share  Router(config-isakmp)#group 1  Router(config-isakmp)#ex  Router(config)#crypto isakmp key cisco123 address 172.16.2.1  Router(config)#crypto isakmp key cisco123 address 172.16.3.1  Router(config)#crypto ipsec transform-set VPN-SET esp-aes 256 esp-sha-hmac  Router(config)#crypto map VPN-MAP 10 ipsec-isakmp  % NOTE: This new crypto map will remain disabled until a peer  and a valid access list have been configured.  Router(config)#crypto map VPN-MAP 10 ipsec-isakmp  Router(config-crypto-map)#set peer 172.16.2.1  Router(config-crypto-map)#set peer 172.16.3.1  Router(config-crypto-map)#set transform-set VPN-SET  Router(config-crypto-map)#match address 100  Router(config-crypto-map)#ex  Router(config)#int fa0/1  Router(config-if)#crypto map VPN-MAP  \*Jan 3 07:16:26.785: %CRYPTO-6-ISAKMP\_ON\_OFF: ISAKMP is ON  Router(config-if)#ex  Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255  Router(config)#access-list 100 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255  Router(config)#end  %SYS-5-CONFIG\_I: Configured from console by console  Router#write  Building configuration...  [OK]  Router#conf t  Enter configuration commands, one per line. End with CNTL/Z.  Router(config)#ip route 192.168.2.0 255.255.255.0 172.16.2.1  Router(config)#ip route 192.168.3.0 255.255.255.0 172.16.3.1 |

Переделаем NAT\_ACL extended вместо standard для роутера офиса 1. Аналогично делаем и для других роутеров

|  |
| --- |
| Router(config)#no ip access-list standard NAT\_ACL  Router(config)#ip access-list extended NAT\_ACL  Router(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.2.0 0.0.0.255  Router(config-ext-nacl)#deny ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255  Router(config-ext-nacl)#permit ip 192.168.1.0 0.0.0.255 any |