ОРГАНІЗАЦІЯ ЗАХИЩЕНОГО КАНАЛУ НА ОСНОВІ IPsec

**Завдання**

Взяти за основу схему комп’ютерної мережі лабораторної роботи №3, при цьому доповнивши її маршрутизатором умовного сервіс-провайдера. «Внутрішні» ІР-адреси мережі та для пулу VPN для заданого числа віддалених користувачів вибрати згідно номера варіанту. Для «зовнішніх» мереж ІР-адреси вибрати довільно. Здійснити моделювання лише для першого та останнього хоста пулу VPN, привести результати роботи у звіті.

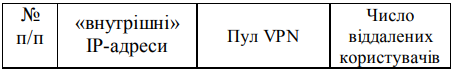
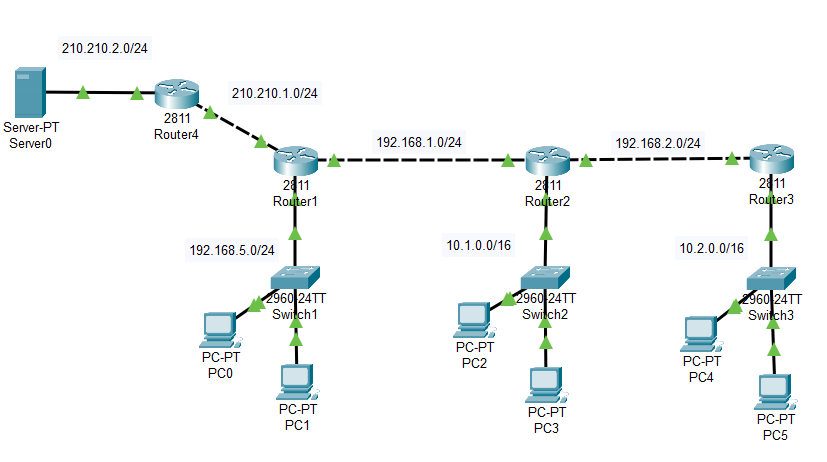




Схема змодельованої мережі



Конфігурація **Router1**

!

aaa new-model

!

aaa authentication login ABC1 local

!

aaa authorization network ABC2 local

!

username admin password 0 admin

!

crypto isakmp policy 10

encr 3des

hash md5

authentication pre-share

group 2

!

crypto isakmp client configuration group cisco

key cisco123

pool VPNPOOL

!

crypto ipsec transform-set SET1 esp-3des esp-md5-hmac

!

crypto dynamic-map MAP1 10

set transform-set SET1

reverse-route

!

crypto map MAP1 client authentication list ABC1

crypto map MAP1 isakmp authorization list ABC2

crypto map MAP1 client configuration address respond

crypto map MAP1 10 ipsec-isakmp dynamic MAP1

!

spanning-tree mode pvst

!

interface FastEthernet0/0

ip address 192.168.5.1 255.255.255.0

duplex auto

speed auto

crypto map MAP1

!

interface FastEthernet0/1

ip address 192.168.1.1 255.255.255.0

duplex auto

speed auto

!

interface FastEthernet1/0

ip address 210.210.1.1 255.255.255.0

duplex auto

speed auto

!

ip local pool VPNPOOL 172.16.0.1 172.16.0.180

ip classless

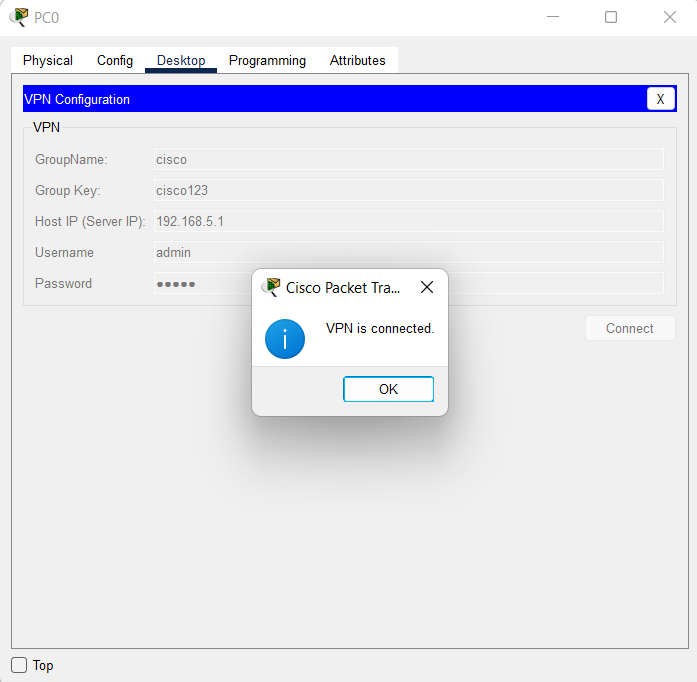
ip route 10.1.0.0 255.255.0.0 192.168.1.2

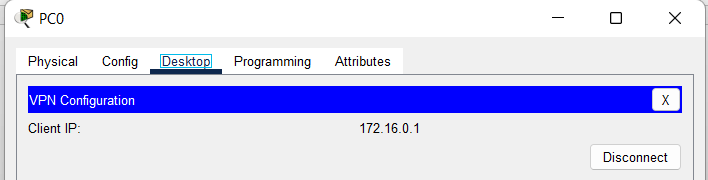
ip route 10.2.0.0 255.255.0.0 192.168.1.2

ip route 0.0.0.0 0.0.0.0 210.210.1.2

!

**Демонстрація успішного підключення VPN**





**Перевірка захисту комп’ютерного тафіку при використанні Remote access VPN**

