**Харківський національний економічний університет**

**імені Семена Кузнеця**

**ЗВІТ**

**З ВИКОНАННЯ ЛАБОРАТОРНОЇ РОБОТИ № 6**

**за дисципліною: *“*** **Корпоративні мережі та системи доступу**”

**на тему: “VPN на основі протоколу IPSec”**

**Варіант №4**

**Виконав: студент факультету Інформаційних технологій**

**3 курсу, спец. Кібербезпека,**

**групи 6.04.125.010.21.2**

**Бойко Вадим Віталійович**

**Перевірив:**

**Чугай Андрій Михайлович**

**ХНЕУ ім. С. Кузнеця**

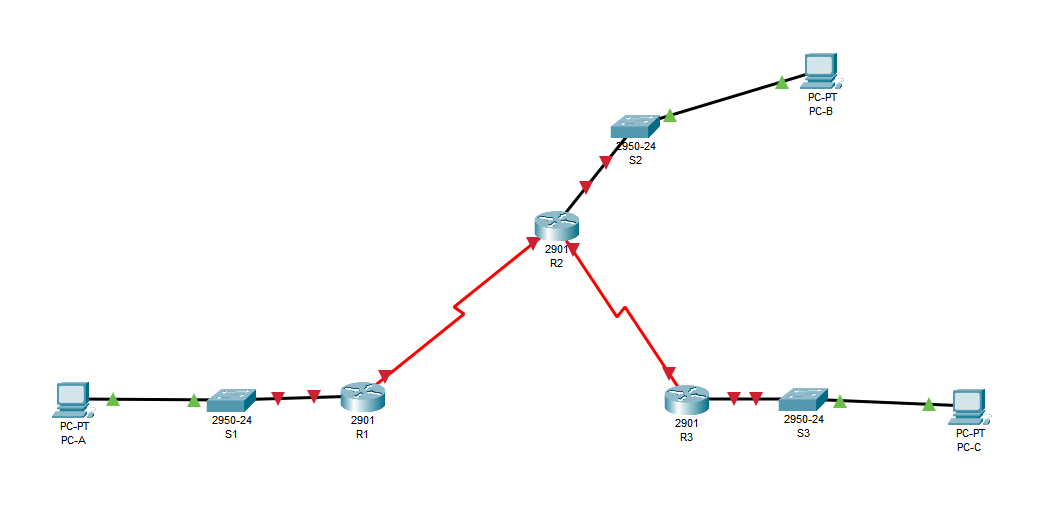
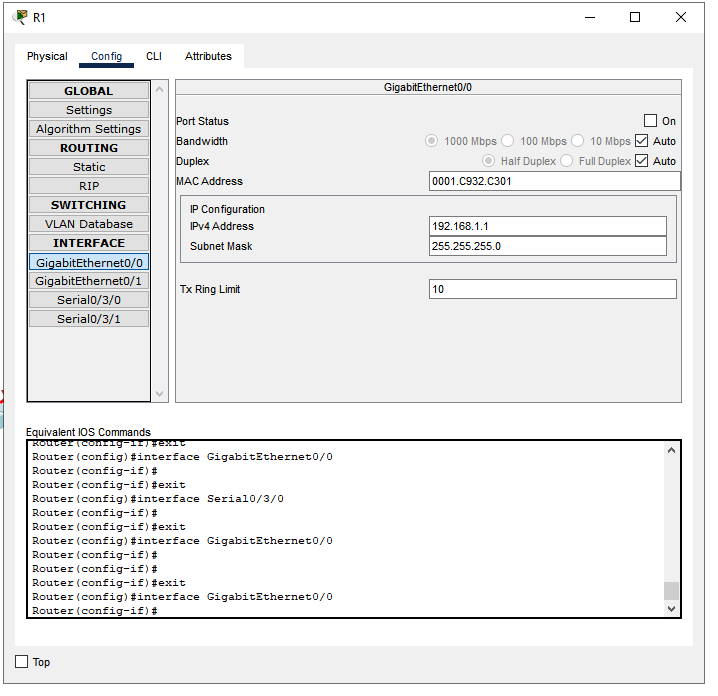
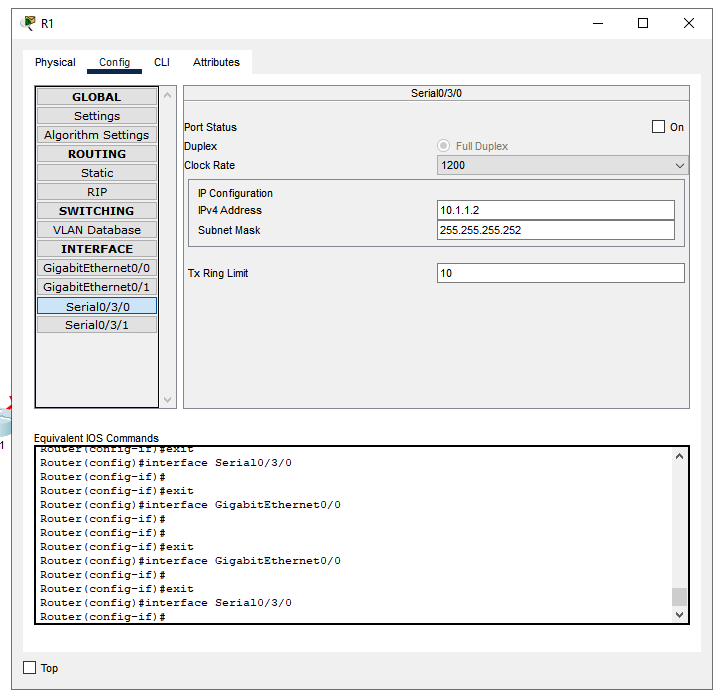
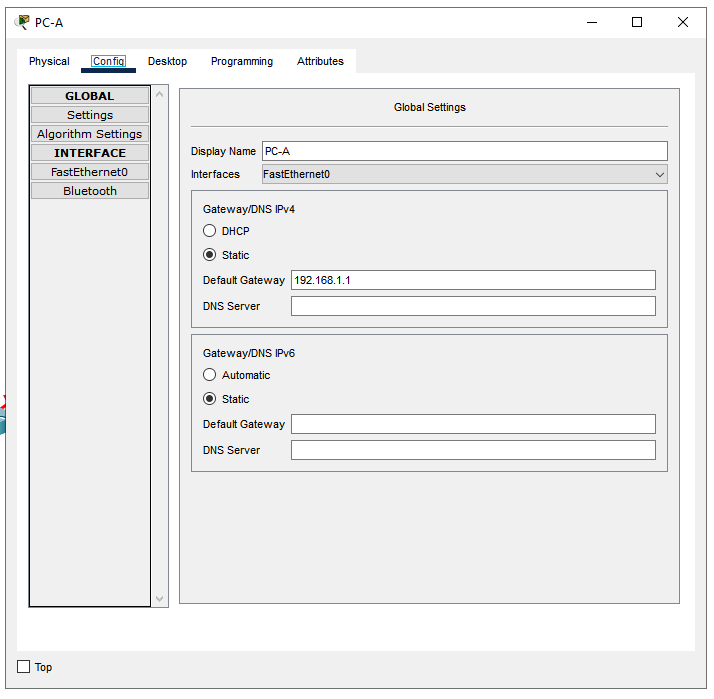
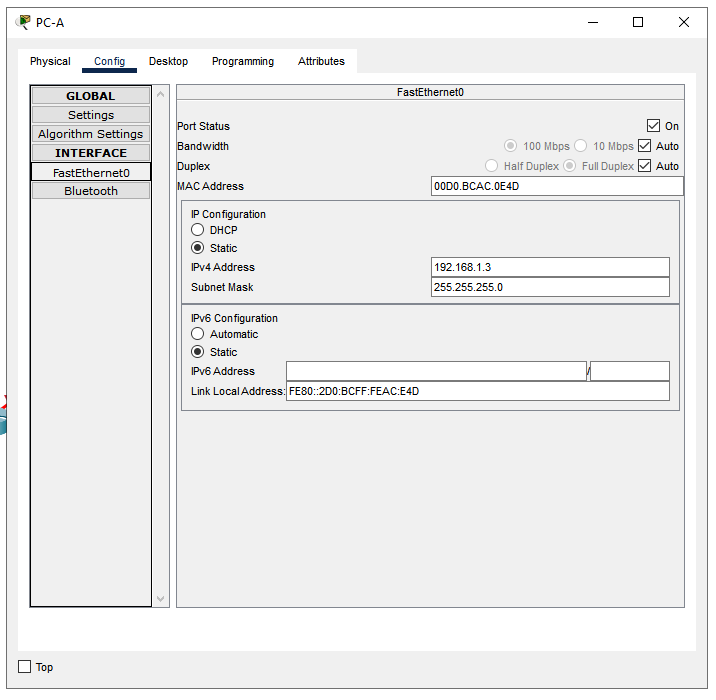
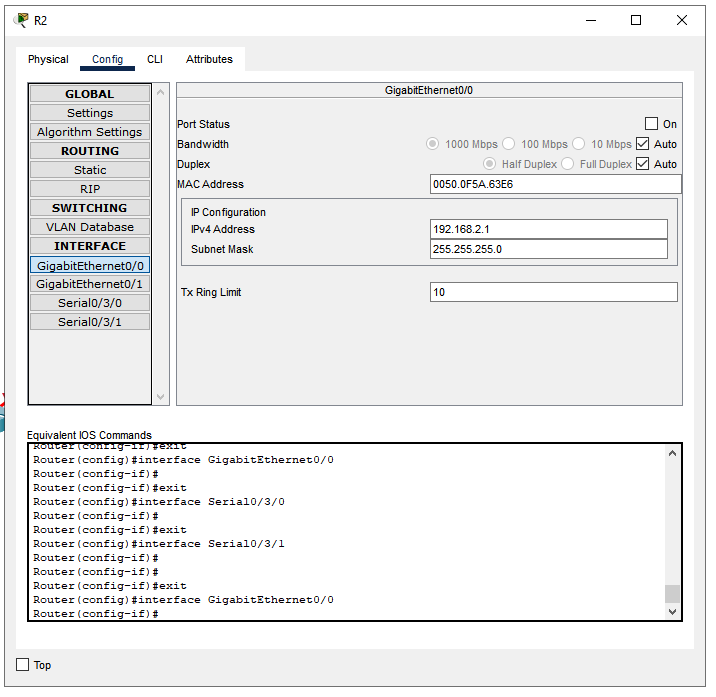
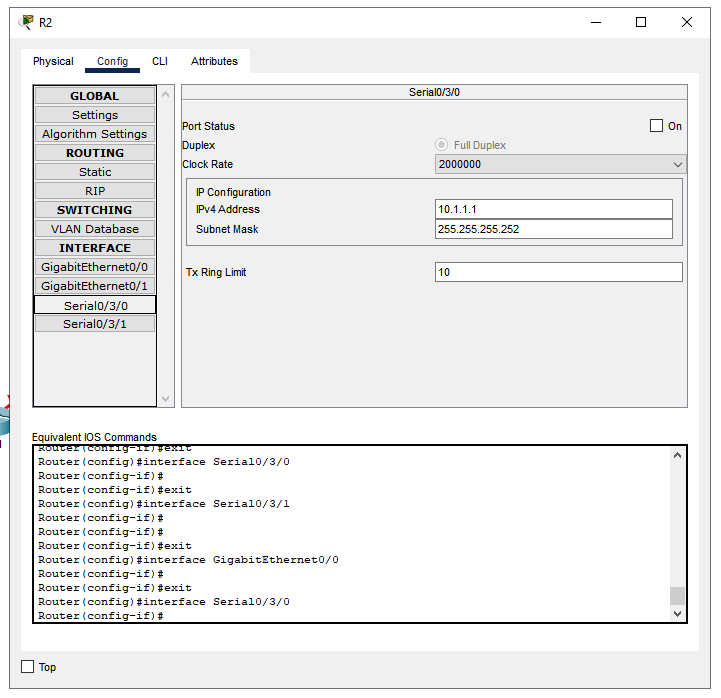
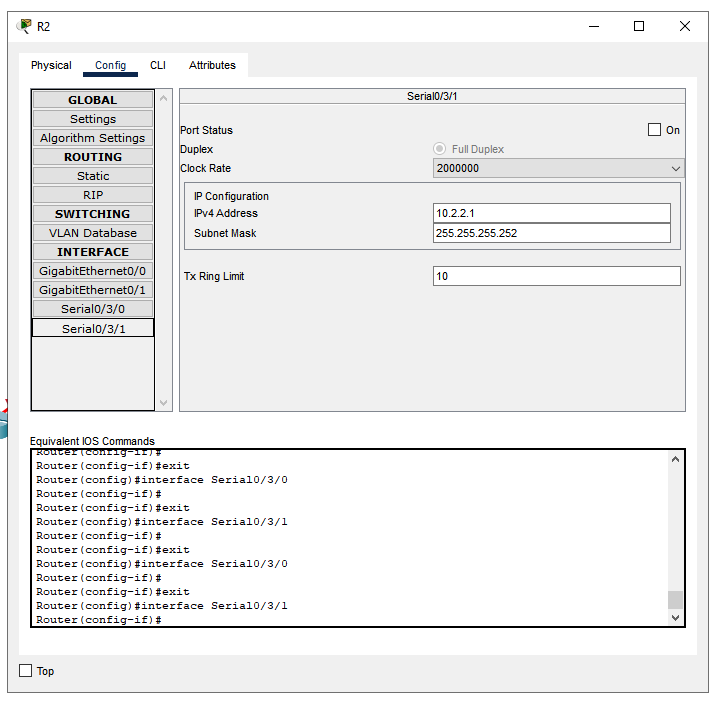
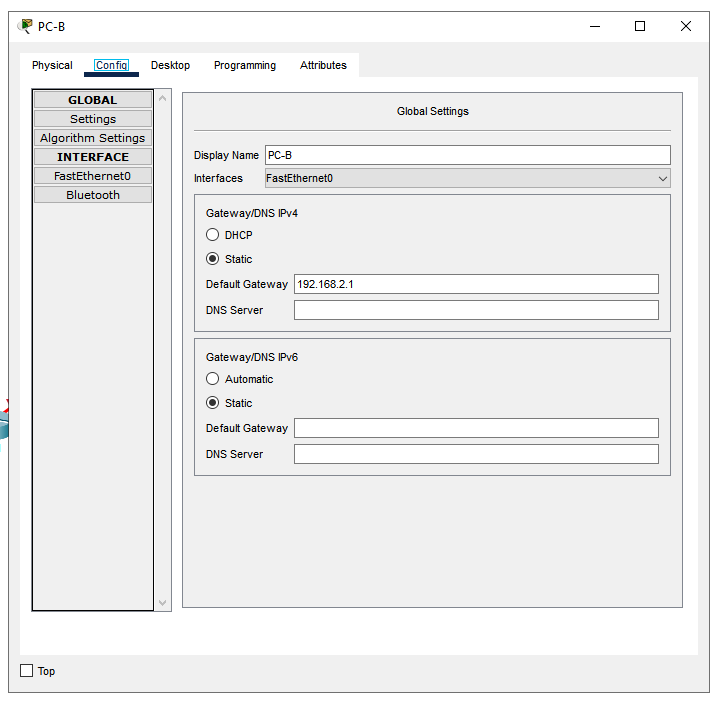
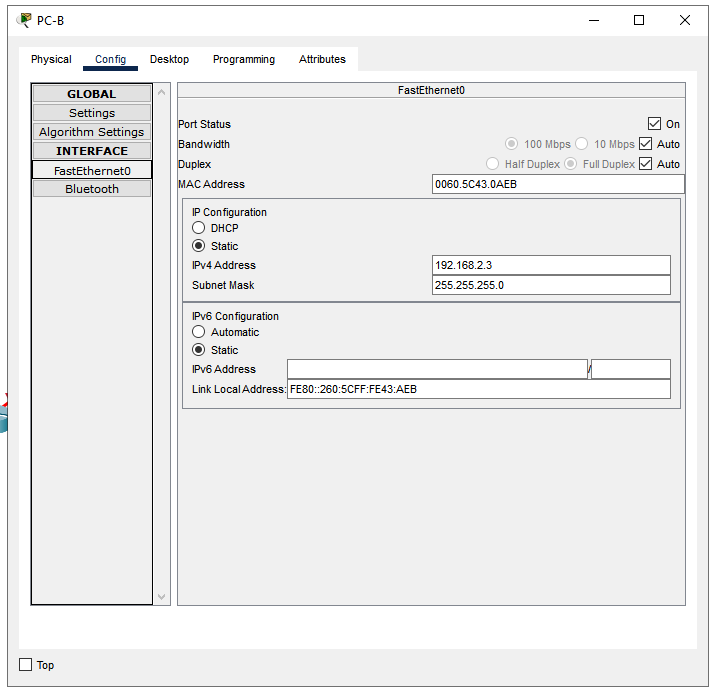
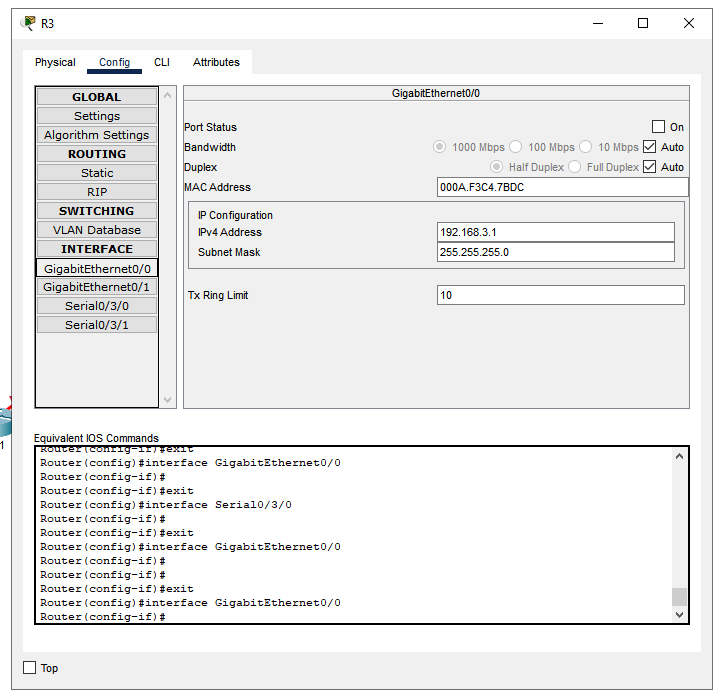
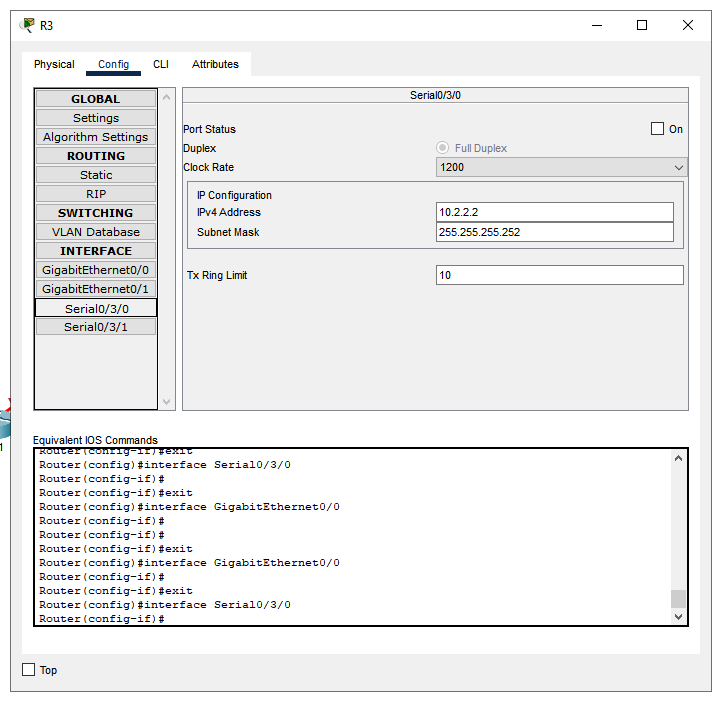
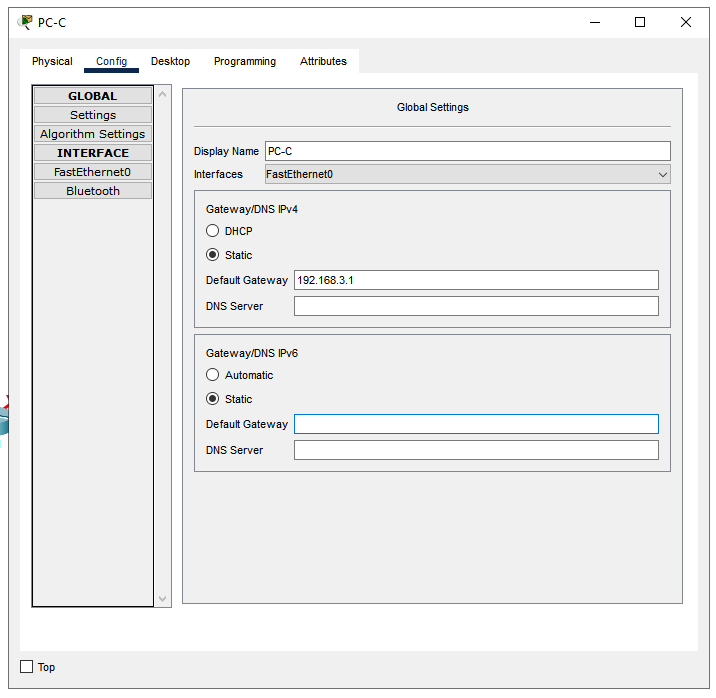
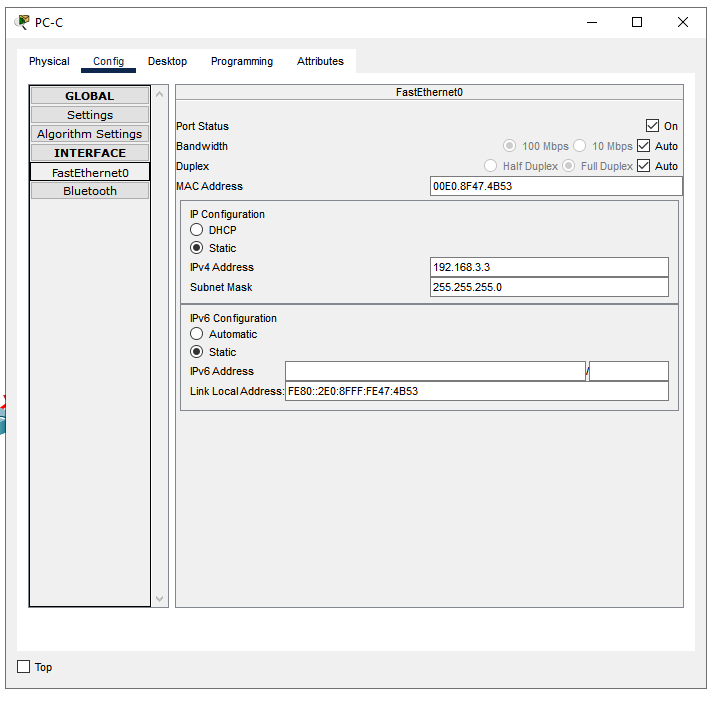
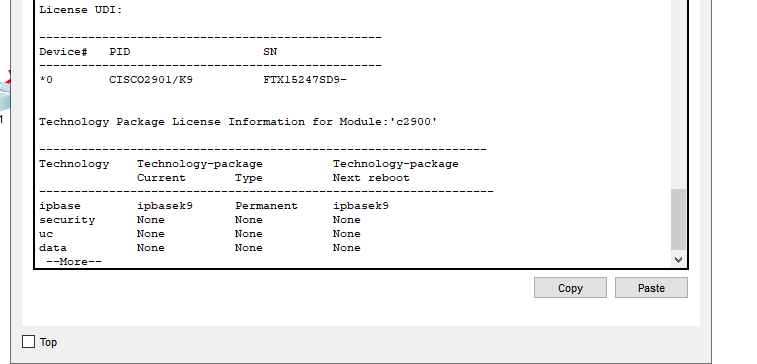
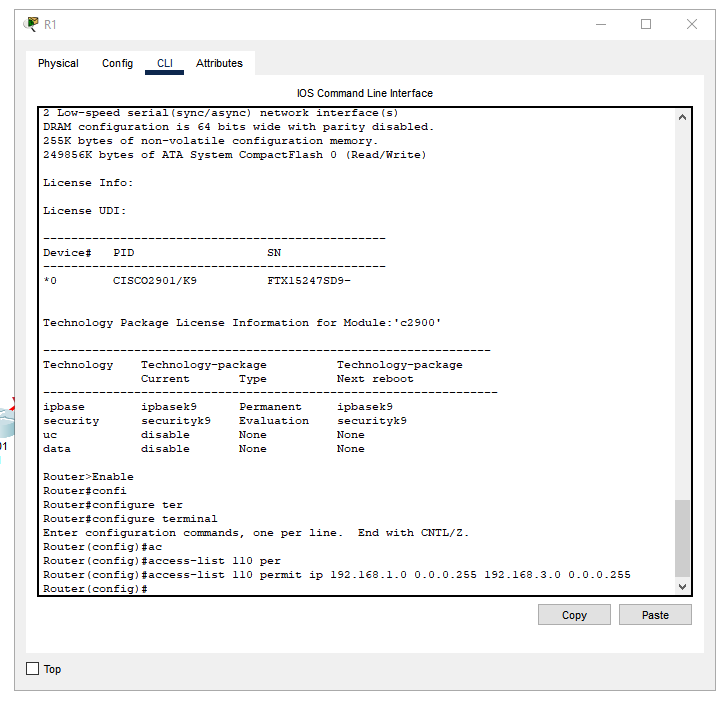
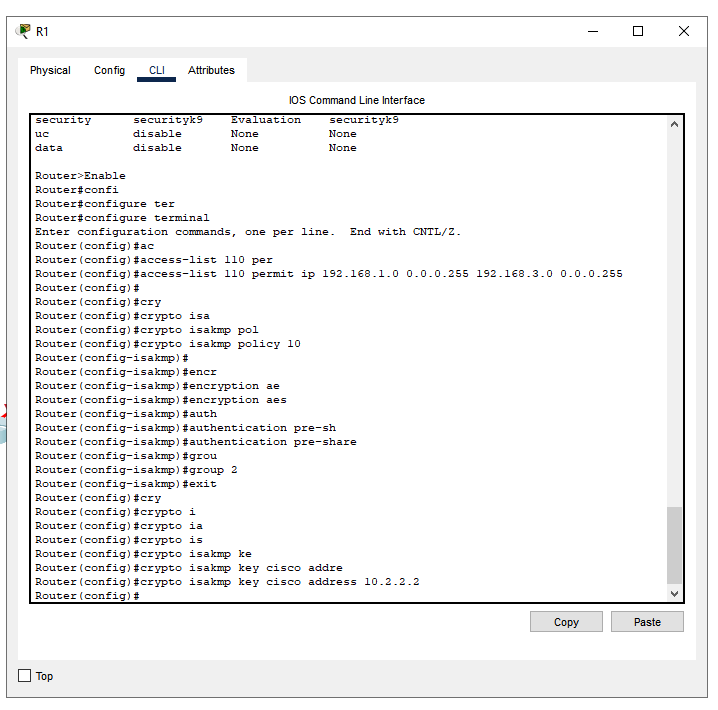
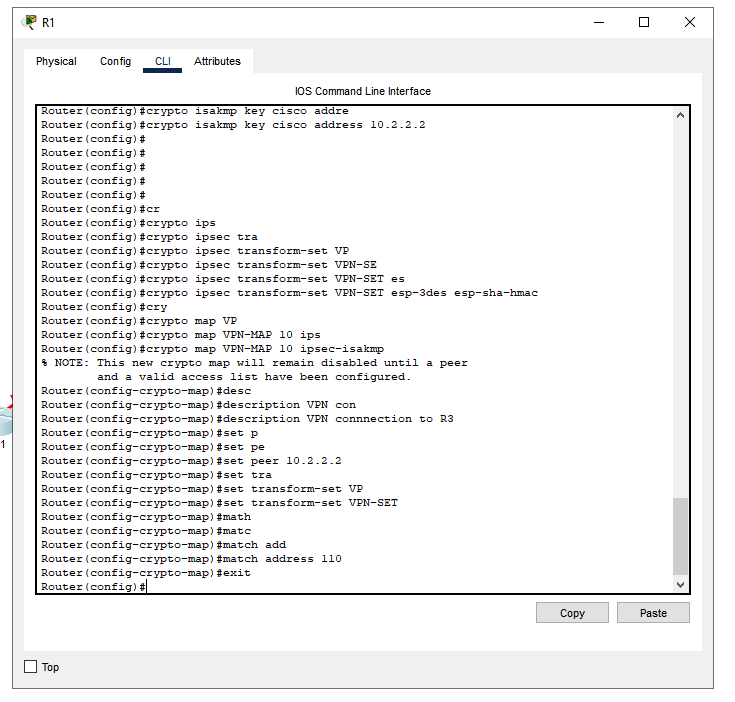
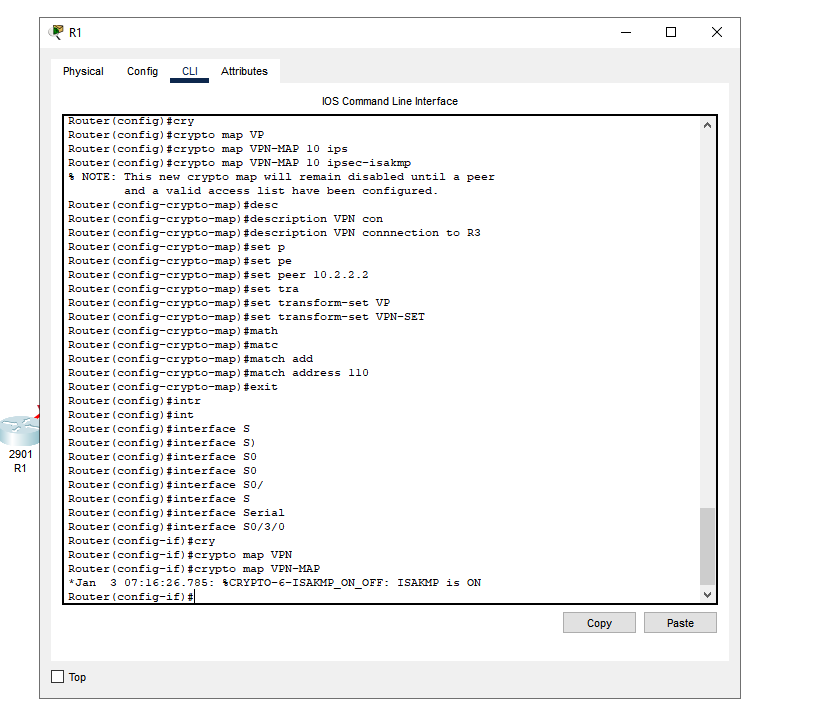
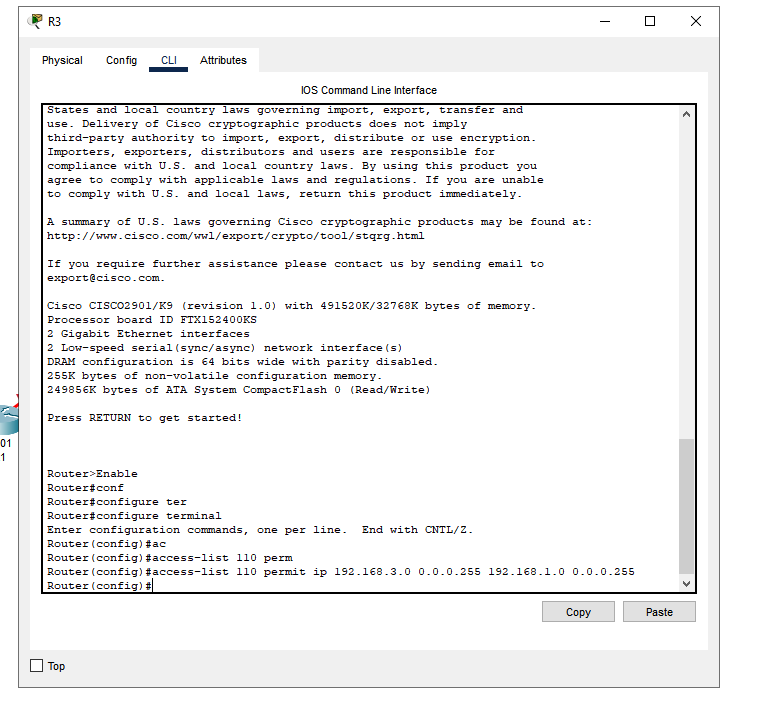
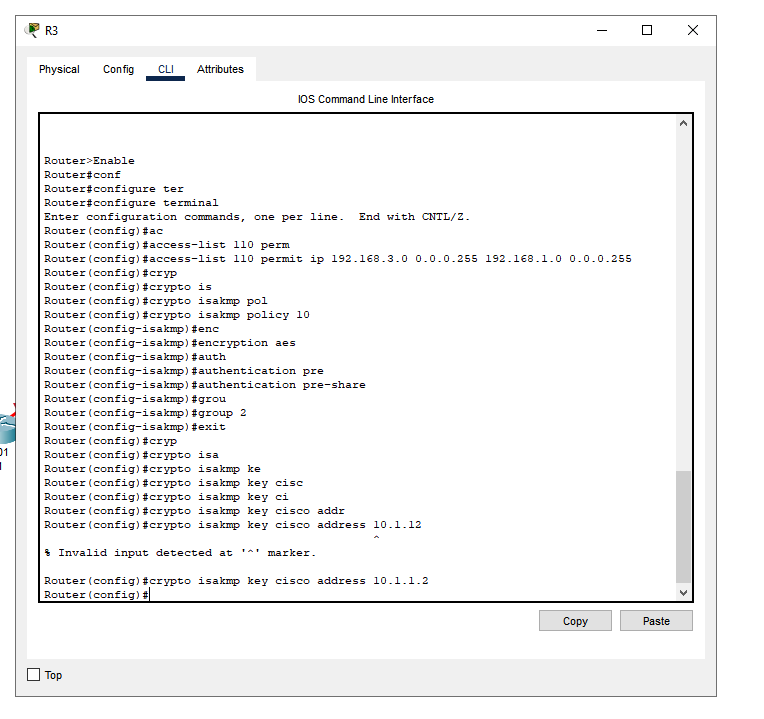
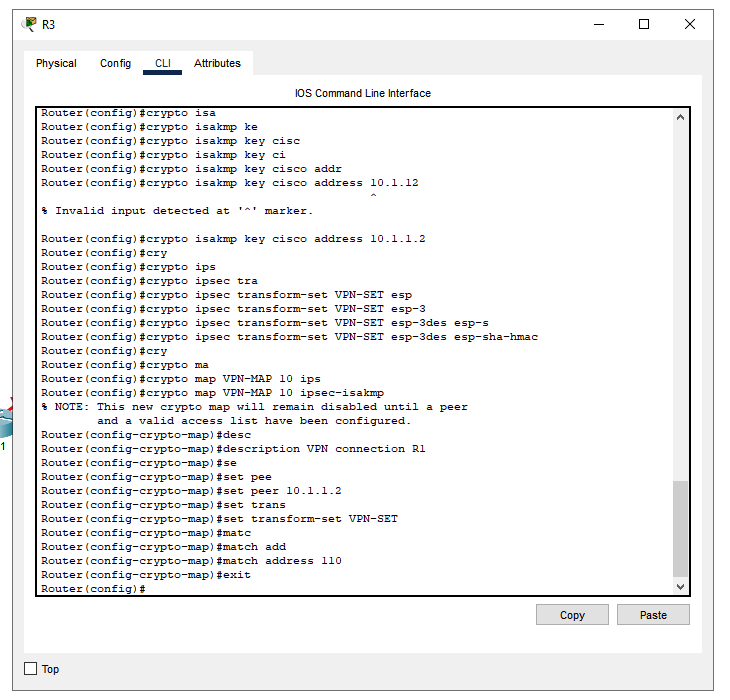
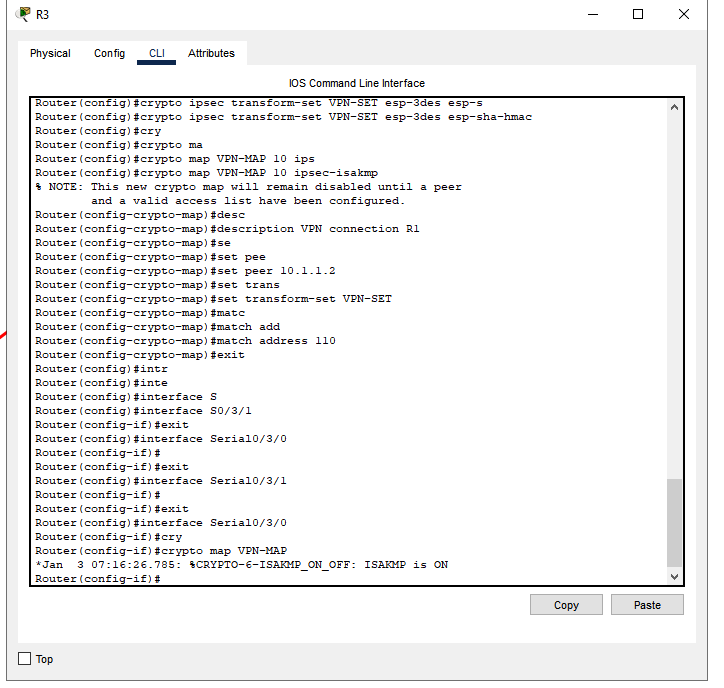
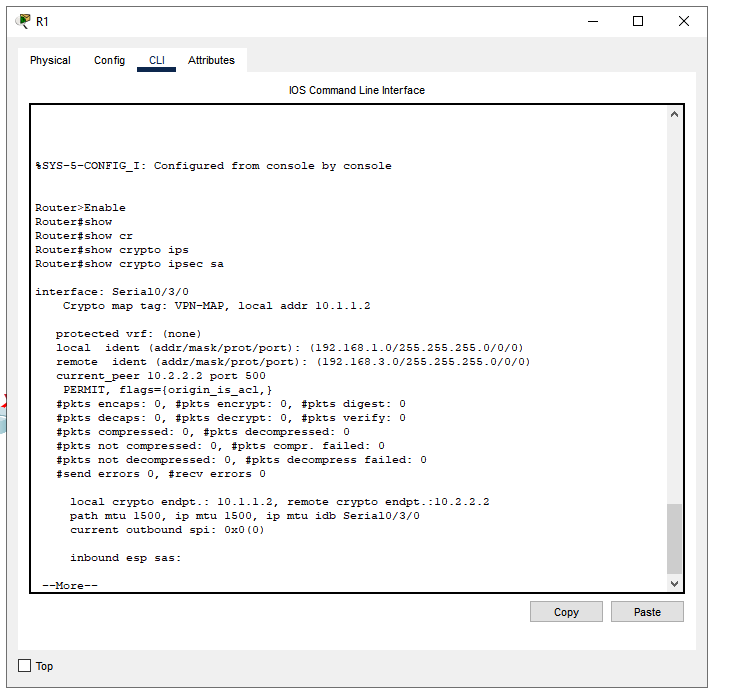
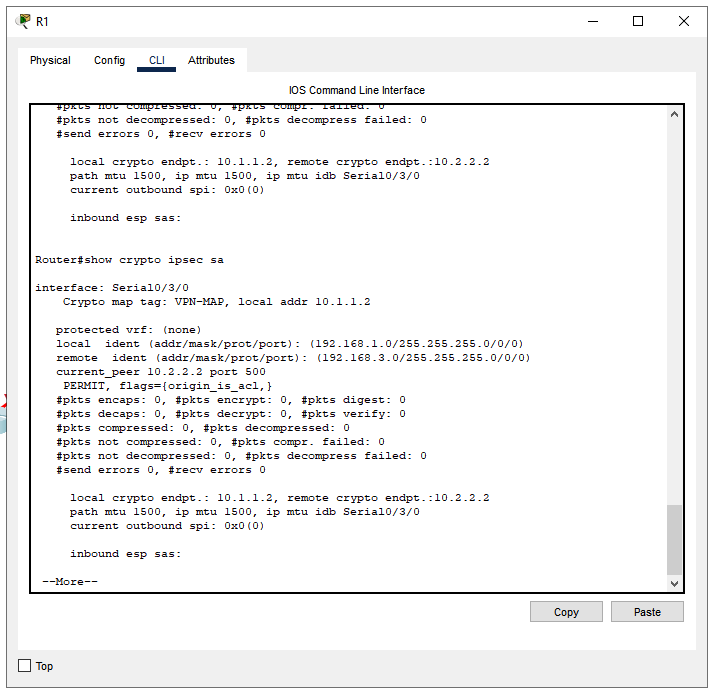
**2023**

**Мета:**

Навчитися планувати, моделювати, розробляти та

налаштовувати VPN мережі на основі протоколу IPSec

**Хід роботи:**

1. Відкриваю «Packet Tracer»
2. Збираю мережу за схемою  
   
3. Налаштовую роутери та комп’ютери  
     
     
     
     
     
     
     
     
     
     
     
     
   
4. Налаштування безпеки  
   
5. Встановлюю пакет
6. Налаштовую особливий трафік  
   
7. Налаштування ISAKMP  
   
8. Створення перетворювача VPN-SET на R1  
   
9. Налаштування мапи криптографії на вихідному інтерфейсі  
   
10. 6 Налаштування IPSec параметрів в маршрутизаторі R3
11. VPN з’єднання типу «мережа-мережа»  
    
12. Налаштування ISAKMP  
    
13. Створення перетворювача VPN-SET на R3  
    
14. Налаштування мапи криптографії на вихідному інтерфейсі  
    
15. Перевірка роботи IPSec VPN  
    
16. 

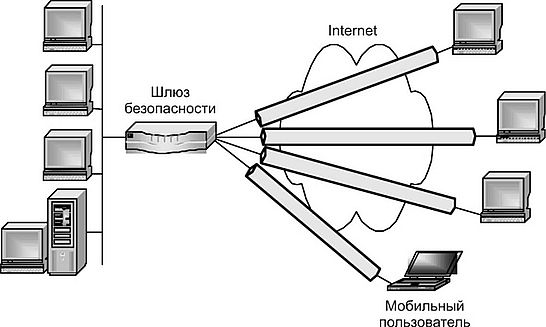
**Контрольні питання:**

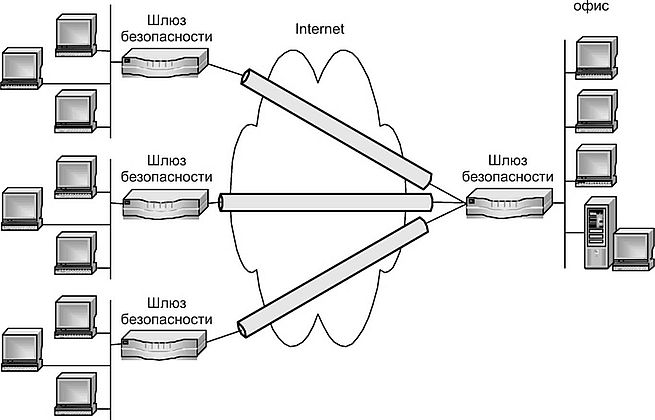
VPN (скорочення від англ. virtual private network — віртуальна приватна мережа) — узагальнена назва технологій, які дозволяють створювати віртуальні захищені мережі поверх інших мереж із меншим рівнем довіри. VPN-тунель, який створюється між двома вузлами, дозволяє приєднаному пристрою чи користувачу бути повноцінним учасником віддаленої мережі і користуватись її сервісами — внутрішніми сайтами, базами, принтерами, політиками виходу в Інтернет.

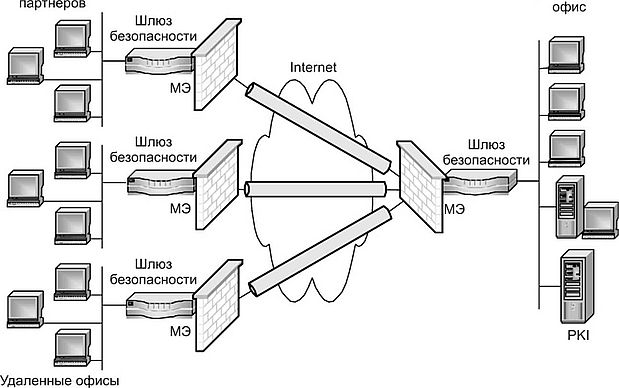
Типи VPN-у:

* IPSec (англ. IP security) — часто використовується поверх IPv4.
* PPTP (англ. Point-to-point tunneling protocol) — розроблявся спільними зусиллями декількох компаній, включаючи Microsoft.
* PPPoE або PPP (англ. Point-to-Point Protocol over Ethernet)
* L2TP (англ. Layer 2 Tunnelling Protocol) — використовується в продуктах компаній Microsoft і Cisco.
* L2TPv3 (англ. Layer 2 Tunnelling Protocol version 3).
* OpenVPN SSL VPN з відкритим вихідним кодом, підтримує режими PPP, bridge, point-to-point, multi-client server

Базові архітектури VPN-у







Група протоколів IPSec. Особливості використання

IPsec (скорочення від IP Security) — набір протоколів для забезпечення захисту даних, що передаються за допомогою протоколу IP, дозволяє здійснювати підтвердження справжності та/або шифрування IP-пакетів. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет.

Протокол IPsec використовується, в основному, для організації VPN-тунелів. В цьому випадку протоколи ESP і AH працюють в режимі тунелювання. Крім того, налаштовуючи політики безпеки певним чином, протокол можна використовувати для створення міжмережевого екрану. Сенс міжмережевого екрану полягає в тому, що він контролює і фільтрує пакети, що проходять через нього, відповідно до заданих правил. Встановлюється набір правил, і екран переглядає всі пакети які проходять через нього. Якщо передані пакети потрапляють під дію цих правил, міжмережевий екран обробляє їх відповідним чином. Наприклад, він може відхиляти певні пакети, тим самим припиняючи небезпечні з'єднання. Налаштувавши політику безпеки відповідним чином, можна, наприклад, заборонити інтернет-трафік. Для цього достатньо заборонити відсилання пакетів, в які вкладаються повідомлення протоколів HTTP та HTTPS. IPsec можна застосовувати і для захисту серверів — для цього відкидаються всі пакети, окрім пакетів, необхідних для коректного виконання функцій сервера. Наприклад, для Web-сервера можна блокувати весь трафік, за винятком з'єднань через 80-й порт протоколу TCP, або через порт TCP 443 у випадках, коли застосовується HTTPS.