1 ЗАГАЛЬНІ ВІДОМОСТІ

1.1 Технологія VPN

Технологія VPN використовує передові технології шифрування і тунелювання для створення безпечного з'єднання через Інтернет. Основою для безпеки VPN є конфіденційність даних, цілісність даних та аутентифікація.

Конфіденційність даних – спрямована на захист вмісту повідомлень від перехоплення неаутентифікованими користувачами або з несанкціонованих джерел. VPN забезпечує конфіденційність за рахунок використання механізмів інкапсуляції та шифрування.

Цілісність даних – отримувач не має жодного контролю над шляхом проходження даних і не знає, чи дані були переглянуті або оброблені під час передачі через Інтернет. Завжди існує ймовірність того, що дані були змінені. Цілісність даних гарантує, що під час передачі між джерелом і призначенням не відбуваються зміни або підробка даних. VPN, як правило, використовують хешування для забезпечення цілісності даних. Хеш, подібно як контрольна сума гарантує, що ніхто не читав вміст, але вона більш надійна.

Аутентифікація – гарантує, що повідомлення приходить з автентичного джерела і отримується автентичним отримувачем. Ідентифікація користувача дає користувачеві впевненість, що сторона, з якою користувач встановлює зв'язок є саме тим користувачем, з яким має встановлюватись з'єднання. VPN може використовувати паролі, цифрові сертифікати, смарт-карти і біометрію для ідентифікації на кінці мережі. Використання можливостей конфіденційності даних в VPN гарантує, що тільки визначені відправники та отримувачі здатні інтерпретувати оригінальний вміст повідомлення.

Тунелювання дозволяє використовувати публічні мережі для передачі даних для користувачів так, ніби користувачі мали доступ до приватної мережі. Тунелювання інкапсулює весь пакет в інший пакет і посилає новий, композитний пакет по мережі. Використовуються три класи протоколів тунелювання:

– протоколи передачі (Carrier protocol:Frame Relay, ATM, MPLS);

– протоколи інкапсуляції (Encapsulating protocol: GRE, IPSec, L2F, PPTP, L2TP);

– пасажир – інкапсульований протокол (passenger protocol:IPX, AppleTalk, IPv4, IPv6).

Тунелі - створюються на різних протоколах інкапсуляції:

– універсальна інкапсуляція маршрутизації (Generic Route Encapsulation, GRE);

– протокол безпеки IP (IPSec);

– протокол переадресації 2 рівня 2 (Layer 2 Forwarding, L2F);

– протокол туннелювання точка-точка (Point-to-Point Tunneling Protocol, PPTP);

– протокол туннелювання 2 рівня (Layer 2 TP, L2TP).

Мережа VPN імітує канал точка-точка та інкапсулює дані, у заголовку яких міститься інформація про маршрутизацію. Даний формат дозволяє даним проходити через публічну мережу, щоб досягнути призначення. Для імітації приватного каналу відбувається шифрування інкапсульованих даних, що дозволяє гарантувати конфіденційність. Алгоритми шифрування не дозволяють розшифрувати дані без ключів шифрування у випадку перехоплення пакетів у публічній мережі.

Сам по собі тунель не може забезпечити безпеку, а лише створює розширення локальної мережі в рамках WAN чи публічної мережі. Тунелі можуть передавати як зашифровані, так і незашифровані дані. Після отримання даних шлюз віддаленого вузла видаляє заголовки, дешифрує пакет і передає його на вузол призначення по приватній мережі. При віддаленому доступі до віртуальної приватної мережі клієнт VPN через ПК користувача зв'язується зі шлюзом для налаштування тунелю.

1.2 Типи VPN мереж

Протокол IPv6 вимагає, щоб кожний канал мав розмір Організації використовують site-to-site VPN мережі, щоб зв'язати розкидані підрозділи. Оскільки більшість організацій зараз мають доступ до Інтернет, є сенс скористатися перевагами site-to-site VPN. Загалом, site-to-site VPN є продовженням класичних WAN мереж, які підключають всі мережі одну з одною. Наприклад, вони можуть зв'язати мережі філії до мережі штаб-квартири компанії.

В site-to-site VPN, хости відправляють та приймають TCP/IP-трафік через VPN шлюз, яким може бути маршрутизатор, Cisco PIX (Private Internet eXchange) фаєрвол (лінійка продуктів випускалась до 2008 року), або Adaptive Security Appliance (ASA).

VPN шлюз відповідає за інкапсуляцію і шифрування вихідного трафіку та відправку його по VPN тунелю через Інтернет на VPN шлюз в пункті призначення. На приймальній стороні VPN шлюз розшифровує вміст і передає пакет до хоста призначення всередині його приватної мережі.

Мобільні користувачі та віддалені працівники інтенсивно використовують технологію VPN віддаленого доступу (remote access VPN). Більшість віддалених працівників тепер мають доступ до Інтернет з дому і можуть встановити віддалений VPN з використанням широкосмугового з'єднання. Крім того, мобільний працівник може зробити місцевий дзвінок до місцевого провайдера для доступу до корпорації через Інтернет. VPN віддаленого доступу може забезпечити потреби віддалених та мобільних користувачів в доступі до корпоративних ресурсів. При використанні VPN віддаленого доступу кожен хост, як правило, має клієнтське програмне забезпечення VPN. Кожного разу, коли користувач намагається відправити трафік, програмне забезпечення VPN-клієнт інкапсулює та шифрує трафік перед відправкою через Інтернет до VPN шлюзу в мережі призначення. Після отримання трафіку, VPN шлюз опрацьовує дані так, як він буде обробляти їх при використанні site-to-site VPN.

1.3 Організація захисту VPN мереж

Сьогодні існують ***чотири види архітектури організації захисту інформації на базі застосування технології VPN***:

– ***локальна*** мережа (Local Area Network - LAN). Забезпечує захист потоків даних та інформації від НСД всередині мережі компанії, інформаційну безпеку на рівні розмежування доступу, системних і персональних паролів, безпеки функціонування ОС, а також ведення журналу колізій і шифрування конфіденційної інформації;

– ***внутрішньокорпоративна мережа VPN*** (Intranet-VPN). Підтримує безпечні з'єднання між внутрішніми підрозділами розподіленої компанії;

– ***мережі VPN з віддаленим доступом*** (Internet-VPN). Забезпечує захищений дистанційний доступ віддалених підрозділів розподіленої компанії і мобільних співробітників і відділів через відкритий простір Internet;

– ***міжкорпоративні мережі VPN*** (Extranet-VPN). Гарантує ефективний захищений обмін інформацією з постачальниками, партнерами, філіями корпорації в інших країнах. Передбачає використання стандартизованих і надійних VPN-продуктів, що працюють у відкритих гетерогенних середовищах і забезпечують максимальну захищеність конфіденційного трафіку, що включає музику і дивитися потокове інформації - конфіденційні телефонні переговори і телеконференції з клієнтами.

VPN-тунель має всі властивості захищеної виділеній лінії, що проходить через відкритий простір Інтернету. Особливість технології тунелювання полягає в тому, що вона дозволяє зашифрувати не тільки поле даних, але весь вихідний пакет, включаючи заголовки.

Це важлива деталь, оскільки з заголовка вихідного пакету зловмисник може витягти дані про внутрішню структуру мережі, наприклад інформацію про кількість локальних мереж і вузлів і їх IP-адресах. Зашифрований пакет інкапсулюється в інший пакет з відкритим заголовком, який транспортується по відповідному тунелю. При досягненні кінцевої точки тунелю із зовнішнього пакету витягується внутрішній, після чого відбувається його дешифрування, а його заголовок використовується для подальшої передачі по внутрішній мережі або підключеному до локальної мережі мобільному користувачеві.

Засоби побудови захищеної VPN досить різноманітні. Вони можуть включати маршрутизатори з механізмом фільтрації пакетів (Filtering Router), багатофункціональні міжмережеві екрани (Multifunction Firewall), проміжні пристрої доступу в мережу (Proxy Server), програмно-апаратні шифратори (Firmware Cryptograph) і т.д.

1.4 Протокол безпеки IPSec

IPsec – це набір протоколів для забезпечення IP комунікацій, який забезпечує шифрування, цілісність та аутентифікацію. Протокол IPSec включає криптографічні методи, які задовольняють потреби керування

ключами на мережевому рівні безпеки. IPsec також містить в собі протоколи для захищеного обміну ключами в мережі Інтернет. Протоколи IPsec можна розділити на два класи: протоколи, які відповідають за захист потоку пакетів та протоколи обміну криптографічними ключами. На даний момент визначений тільки один протокол обміну криптографічними ключами – IKE (Internet Key Exchange) – та два протоколи, які забезпечують захист потоку інформації, що передається:

– Authentication Header (AH) – використовується коли конфіденційність не потрібна, або не вимагається. AH забезпечує перевірку достовірності і цілісності даних для IP пакетів, переданих між двома системами. Даний алгоритм перевіряє відсутність змін під час передачі повідомлення та підтверджує, що дані належать визначеним відправнику та отримувачу. AH не забезпечує конфіденційність даних шляхом шифрування пакетів. При використанні лише AH протоколу забезпечується слабкий захист. Тому він використовується з протоколом ESP, щоб забезпечити шифрування даних і захист від підробок;

– Encapsulating Security Payload (ESP) – забезпечує цілісність та конфіденційність шляхом шифрування IP-пакетів. Шифрування IP-пакетів забезпечує приховування даних та відомостей про відправника та отримувача. Хоча шифрування та аутентифікація є обов'язковими для ESP, як мінімум, одна з цих функцій має бути вибрана.

IPsec реалізований на основі існуючих алгоритмів шифрування, аутентифікації та обміну ключами. Деякі з стандартних алгоритмів, що використовує IPsec:

– DES – шифрує та розшифровує пакети даних;

– 3DES – забезпечує кращу ефективність шифрування ніж 56-бітний DES;

– AES – забезпечує кращий рівень шифрування, в залежності від довжини ключа, і більшу пропускну здатність;

– MD5 – аутентифікація пакетної передачі даних з використанням 128-бітного спільного секретного ключа.

– SHA-1 – аутентифікує дані, використовуючи 160-бітний спільний секретний ключ;

– DH – дозволяє двом сторонам створити спільний секретний ключ, що використовується для шифрування та хеш-алгоритмів, наприклад, DES та MD5, при передачі даних по незахищеному каналі.

Для виконання шифрування та дешифрування за допомогою алгоритмів, які використовують симетричний секретний ключ коллективного використання, необхідно його створити та роздати. Налаштування ключів може здійснюватись вручну мережевим адміністратором, або за допомогою методу обміну ключами. Погодження ключа Діффі-Хеллмана (DH) – це публічний метод обміну ключами, який дозволяє двом сторонам встановлювати секретний ключ, що використовується при передачі даних по незахищеному каналі. В групах Діффі-Хеллмана має бути вказаний тип криптографії:

– DH GROUP 1 – використовується 768-бітна криптографія;

– DH GROUP 2 – тільки для пристроїв Cisco IOS, PIX Firewall та пристрою адаптивного захисту Cisco (ASA), використовується 1024-бітне шифрування;

– DH GROUP 5 – підтримується при умові виконання вимог програмної системи, використовується 1536-бітне шифрування.

2 ЛАБОРАТОРНА РОБОТА
VPN на основі протоколу IPSec

Мета роботи: навчитися планувати, моделювати, розробляти та налаштовувати VPN мережі на основі протоколу IPSec.

2.1 Налаштування мережі
2.1.1 Модель мережі (схема)

Виконайте етапи з'єднання мережного обладнання:

– запустіть ярлик на робочу столі Packet Tracer (або виконайте установку програми запустивши файл Packet Tracer.exe з папки Install);

– зберіть мережу за схемою представленою на рисунку 2.1, з основними параметрами комутаційного обладнання та інтерфейсів (табл. 2.1). Для цього виконайте наступні дії:

1) з панелі приладів в робочу область перенесіть 3 маршрутизатора 2901 (для зручності їх краще перейменувати у R1, R2 і R3);

2) в робочу область перенесіть 3 комутатора 2950-24 (перейменуйте їх у S1, S2 і S3);

3) в робочу область перенесіть 3 робочих станції PC-PT (перейменуйте у PC-A, PC-B та PC-C).

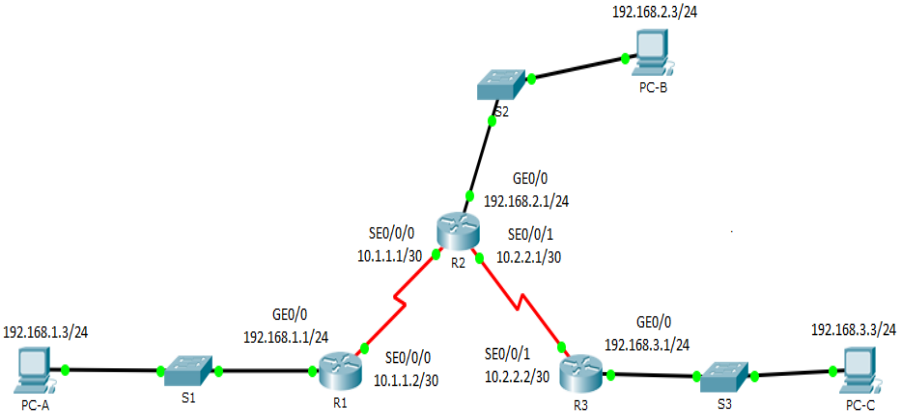

Рисунок 2.1 – Схема мережі

Для установки маршрутизаторів на панелі приладів необхідно вибрати перший елемент – Routers (рис.2.2). З показаних пристроїв треба вибрати 2901 (підкреслений) і перетягнути у робочу область.

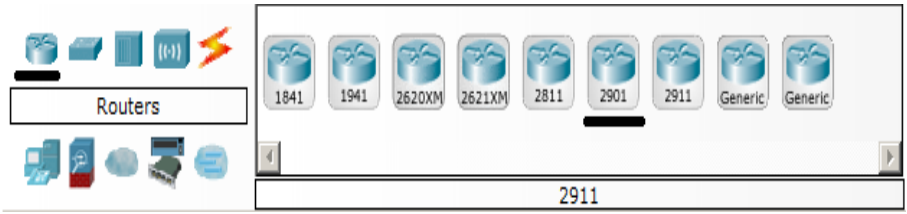

Рисунок 2.2 – Вибір маршрутизаторів

Для вставки комутаторів необхідно перейти на закладку Switches (рис. 2.3) і перетягти 2950-24 (підкреслений) елемент у робочу область.

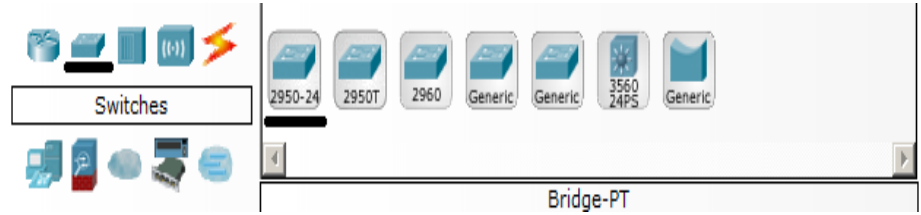

Рисунок 2.3 – Вибір комутаторів

Для вставки комп'ютерів необхідно перейти на закладку End devices (рис.2.4) і перетягти Generic (підкреслений) елемент у робочу область.

Рисунок 2.4 – Вибір комп'ютерів

Таблиця 2.1 – Параметри інтерфейсів

Пристрій	Інтерфейс	IP-адреса	Маска	Default Gateway
R1	Gigabit Ethernet 0/0	192.168.1.1	255.255.255.0	***
	Serial 0/0/0	10.1.1.2	255.255.255.252	***
R2	Gigabit Ethernet 0/0	192.168.2.1	255.255.255.0	***
	Serial 0/0/0	10.1.1.1	255.255.255.252	***
	Serial 0/0/1	10.2.2.1	255.255.255.252	***
R3	Gigabit Ethernet 0/0	192.168.3.1	255.255.255.0	***
	Serial 0/0/1	10.2.2.2	255.255.255.252	***
PC-A	***	192.168.1.3	255.255.255.0	192.168.1.1
PC-B	***	192.168.2.3	255.255.255.0	192.168.2.1
PC-C	***	192.168.3.3	255.255.255.0	192.168.3.1

В процесі налаштування на маршрутизатори необхідно додати спеціальні модулі. Для цього клацніть на піктограмі маршрутизатора, яка знаходиться у робочій області. Далі відкриється вікно налаштувань даного пристрою (рис. 2.5). У відкритому вікні у вкладці Physical зліва оберіть модуль HWIC-2T.

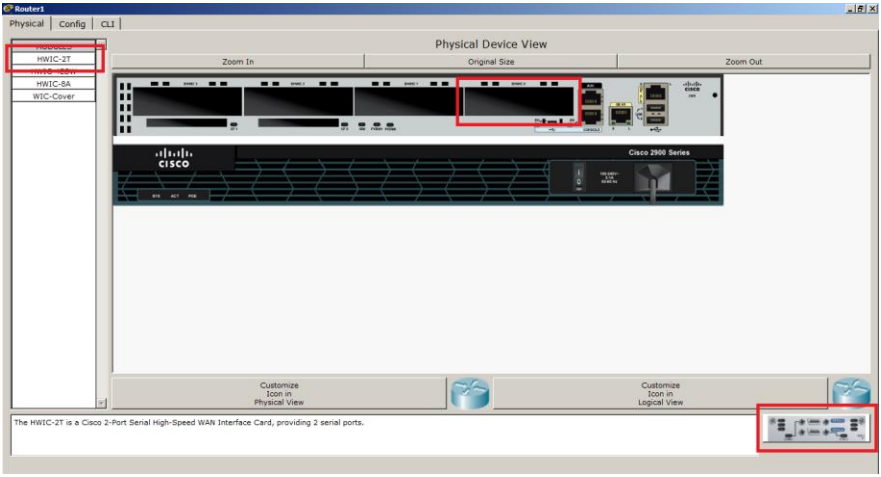

Рисунок .2.5 – Вікно налаштувань маршрутизатора

Тепер вимкніть живлення маршрутизатора і перетягніть зображення модуля з правого нижнього кута вікна на крайній правий вільний роз'єм розширення (це важливо, так як розташування модуля впливає на його кінцеву назву), як показано на рисунку 2.6. Після закінчення налаштувань необхідно увімкнути живлення.

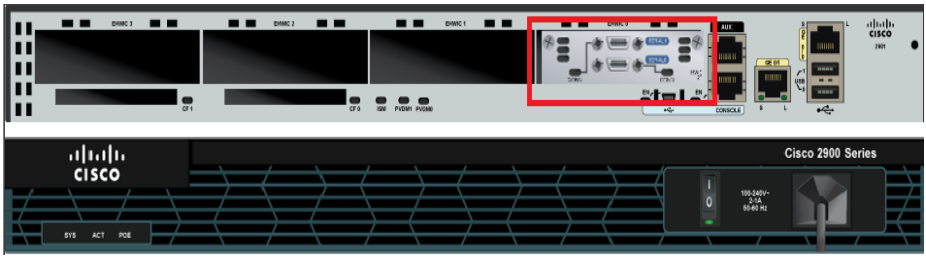

Рисунок 2.6 – Маршрутизатор з встановленим модулем

Аналогічні дії необхідно повторити для R2 і R3.

Наступним кроком є з'єднання між собою маршрутизаторів за допомогою кабелів. У даному випадку використовується кабель DCE - він призначений для з'єднання між собою послідовних портів маршрутизаторів (Serial портів).

Для того, щоб вибрати даний тип кабелю, треба клацнути на кладку Connections та обрати кабель Serial DTE (рис. 2.7).

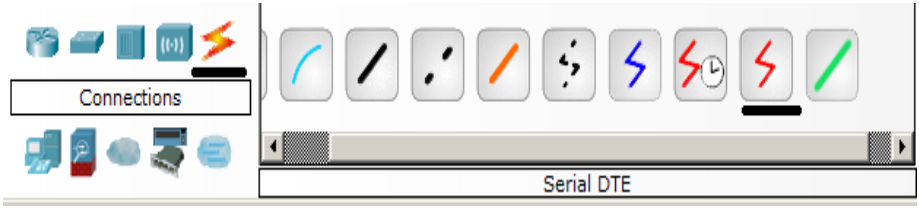

Рисунок 2.7 – Вибір кабелю для з'єднання маршрутизаторів

Для з'єднання двох пристроїв необхідно:

– вибрати кабель для з'єднання (рис. 2.7);

– натиснути на першому пристрої який необхідно з'єднати та вибрати порт (рис. 2.8);

– протягнути кабель до другого пристрою і так само обрати порт (рис. 2.9).

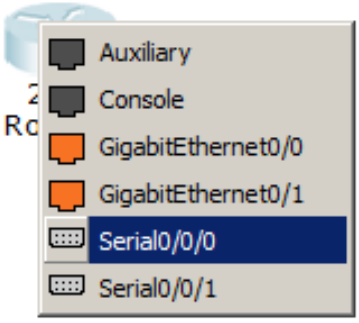

Рисунок 2.8 – Вибір порту на першому пристрої

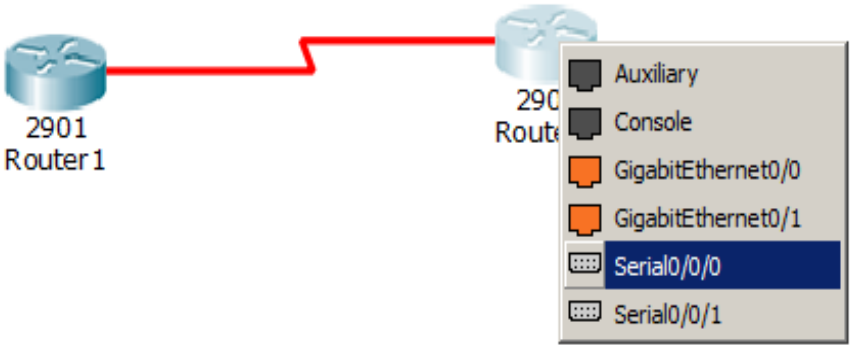

Рисунок 2.9 – Вибір порту на другому пристрої

Для підключення комп’ютера до комутатора, а комутатора у свою чергу до маршрутизатора використовується інший тип кабелю – вита пара (рис. 2.10).

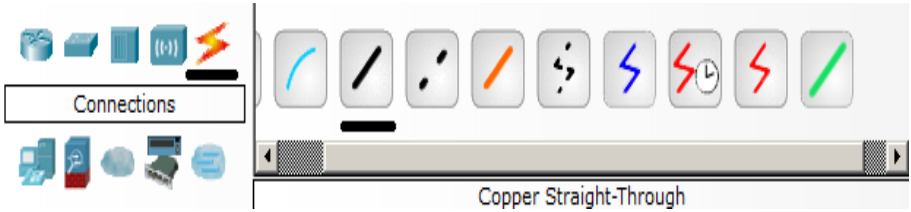

Рисунок 2.10 – Вибір звитої пари

Для спрощення налаштувань необхідно кабель підключати на ті порти, які вказані у таблиці 2.1.

2.2 Налаштування IP адресації

Тепер треба виконати необхідні налаштування, згідно параметрам наведеним в таблиці 2.1.

Для налаштування комп'ютера PC-A необхідно:

– клацнути на піктограмі PC-A у робочій області лівою кнопкою миші;

– у відкритому вікні обрати вкладку Desktop;

– натиснути на кнопці IP Configuration і ввести налаштування з таблиці 2.1 (рис. 2.11, 2.12)

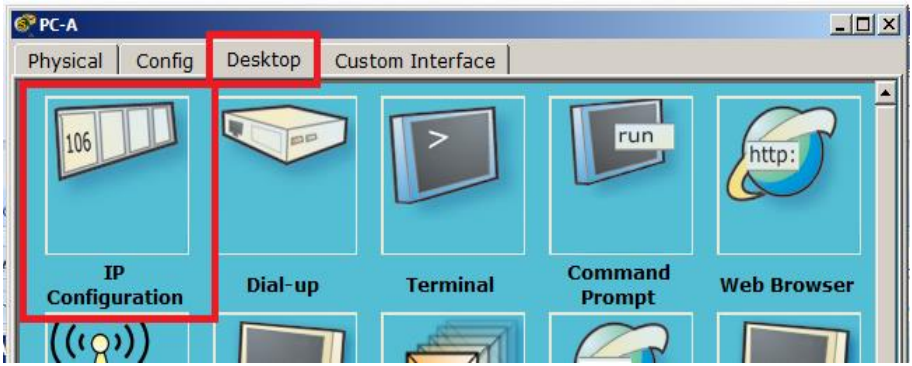

Рисунок 2.11 – Налаштування PC-A

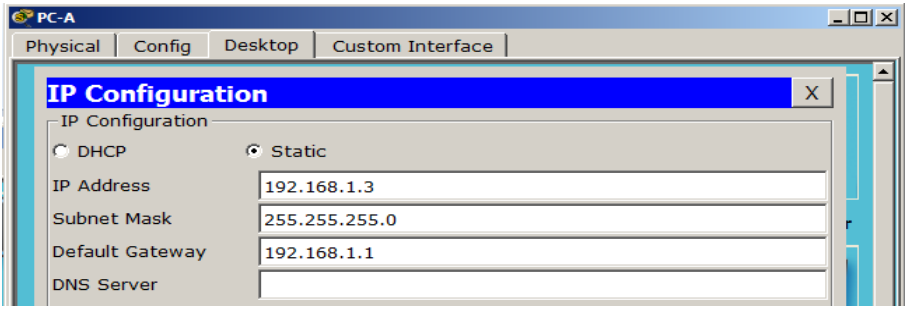

Рисунок 2.12 – Налаштування IP адресації PC-A

Аналогічним чином повторіть попередні пункти для PC-B та PC-C. Необхідні параметри (IP-адреса, маска підмережі та Default Gateway) візьміть з таблиці 2.1.

Для налаштування маршрутизатора R1 необхідно:

– клацнути на піктограмі R1 у робочій області лівою кнопкою миші;

– у відкритому вікні обрати вкладку Config;

– налаштувати інтерфейси згідно таблиці 2.1 (рис. 2.13, 2.14).

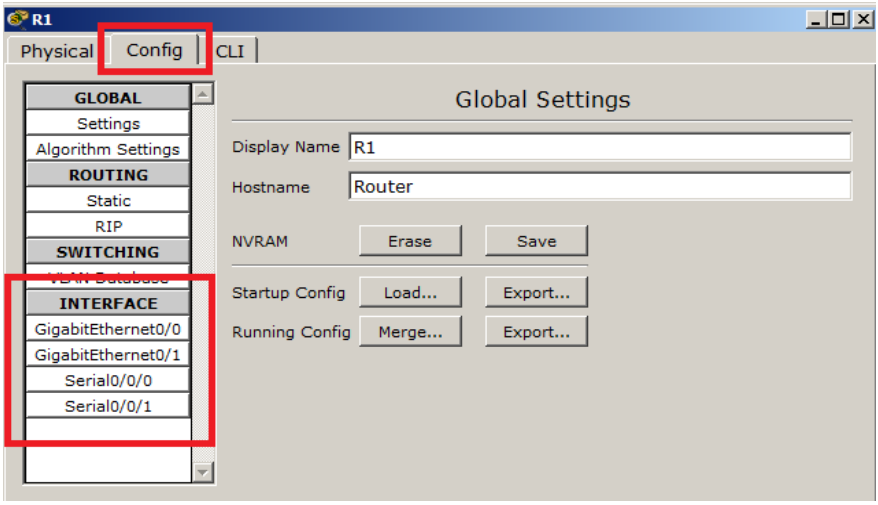

Рисунок 2.13 – Налаштування R1

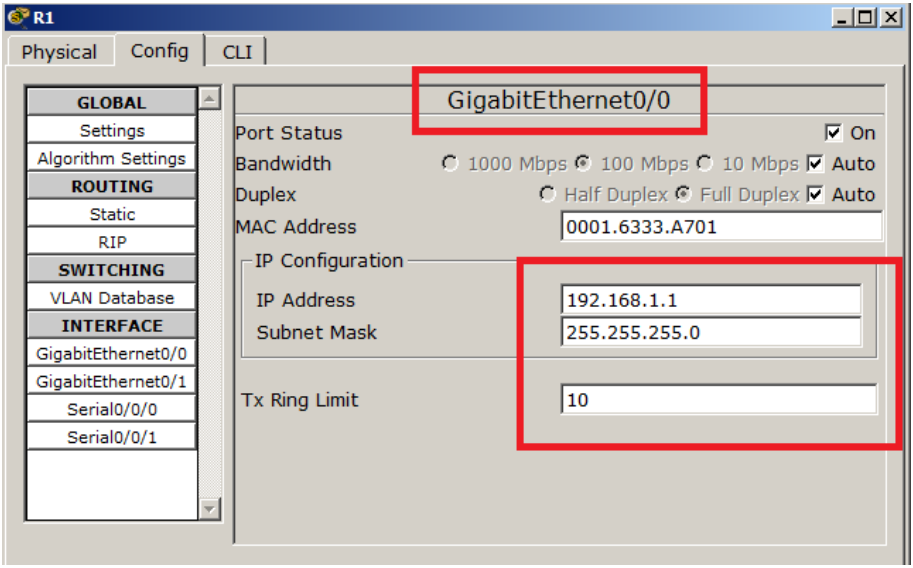

Рисунок 2.14 – Налаштування IP адресації R1

Аналогічним чином повторіть попередні пункти для роутерів R1 та R2. Необхідні параметри (IP-адреса і маска підмережі) візьміть з таблиці 2.1.

2.3 Налаштування статичної маршрутизації

Так як PC-A та PC-B з'єднані через R1 та R3, а вони в свою чергу через R2, то для забезпечення обміну даними між різними мережами, необхідно виконати настройку маршрутизації – статичної, або динамічної. У даному випадку налаштуємо статичну маршрутизацію.

Для налаштувань статичної маршрутизації необхідно виконати наступні дії.

– клацнути на маршрутизаторі R1 лівою кнопкою миші;

– у відкритому вікні перейти у вкладку CLI (рис.2.15) і виконати необхідні команди.

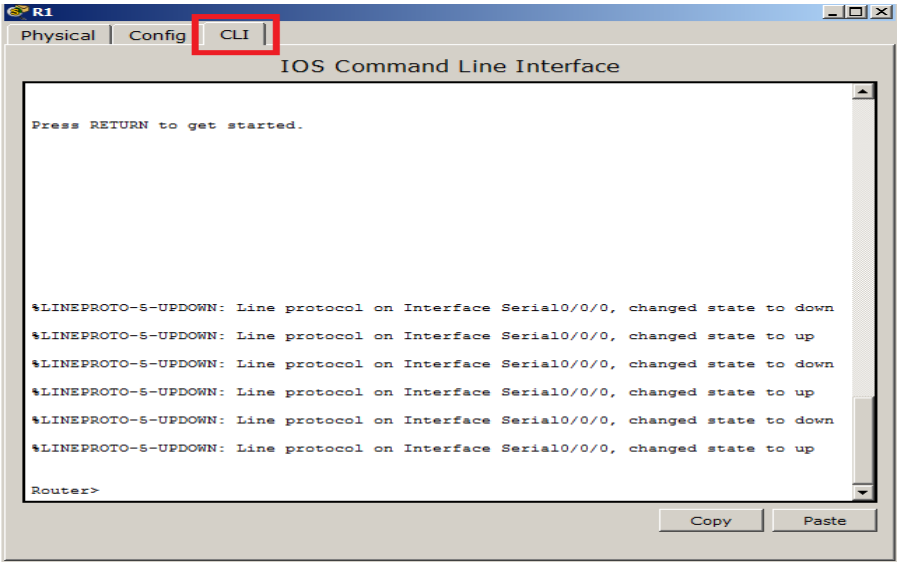

Рисунок 2.15 – Вкладка CLI

Для налаштування статичної маршрутизації необхідно в кожному маршрутизаторі прописати адреси і маски мереж, які безпосередньо НЕ підключені до даного маршрутизатора. Таким чином для маршрутизатора R1 необхідно додати такі мережі:

– 192.168.2.0/24;
– 10.2.2.0/30;
– 192.168.3.0/24.

Примітка. Усі подальші команди виконуються у вікні CLI.

Розглянемо етапи підключення та налаштування на прикладі однієї мережі, для цього:

– входимо в привілейований режим – в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– далі безпосередньо вкажіть мережу, прописуючи в терміналі:

> IP route 192.168.2.0 255.255.255.0 s0/0/0

Замість s0/0/0 можна також ввести IP-адресу інтерфейсу маршрутизатора, до якого підключена дана мережа (у даному випадку – 10.1.1.2);

– вводимо вище наведену команду для налаштування інших мереж, змінюючи IP-адресу і маску згідно з таблицею 2.1;

– якщо допущена помилка при налаштуванні, то видалити запис з таблиці маршрутизації можна за допомогою команди:

> no IP route 192.168.2.0 255.255.255.0 s0/0/0 (або з ім'ям (адресою) інтерфейсу);

Виконайте, за попередньою схемою, налаштування маршрутизаторів R2 і R3, з урахуванням мереж до яких вони підключені і адрес їх інтерфейсів (таблиця 2.1).

Для маршрутизатора R2 необхідно додати такі мережі:

– 192.168.1.0/24;

– 192.168.3.0/24.

Для маршрутизатора R3 необхідно додати такі мережі:

– 192.168.1.0/24;

– 10.1.1.0/30;

– 192.168.2.0/24.

Після усіх налаштувань перевіряємо чи працює статична маршрутизація. Для цього необхідно виконати команду «ping» від PC-A до PC-B та PC-C і також від PC-B до PC-C (це можна зробити за допомогою гарячої клавіші «P», для цього після натискання клавіші треба клацнути лівою кнопкою миші на об’єкті від якого буде йти пінг-пакет, а потім клацнути на об’єкті до якого буде йти пінг-пакет). Якщо пінг пройшов у всіх напрямках то статична маршрутизація налаштована правильно і можна переходити до безпосереднього шифрування трафіку.

2.4 Налаштування функції безпеки

2.4.1 Активація модуля securityk9

Пакет ліцензії Security Technology Package має бути доступним для виконання дій, які стосуються безпеки трафіку.

Для перевірки чи встановлений пакет (модуль) securityk9 необхідно виконати наступні дії:

– клацнути лівою кнопкою миші на маршрутизаторі R1;

– перейти у вкладку CLI;

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– виконуємо команду щоб переконатися що ліцензія Security Technology Package активирована:

– show version;

Якщо відповідь на введену команду є такою як на рисунку 2.16, то це означає що пакет не встановлений.

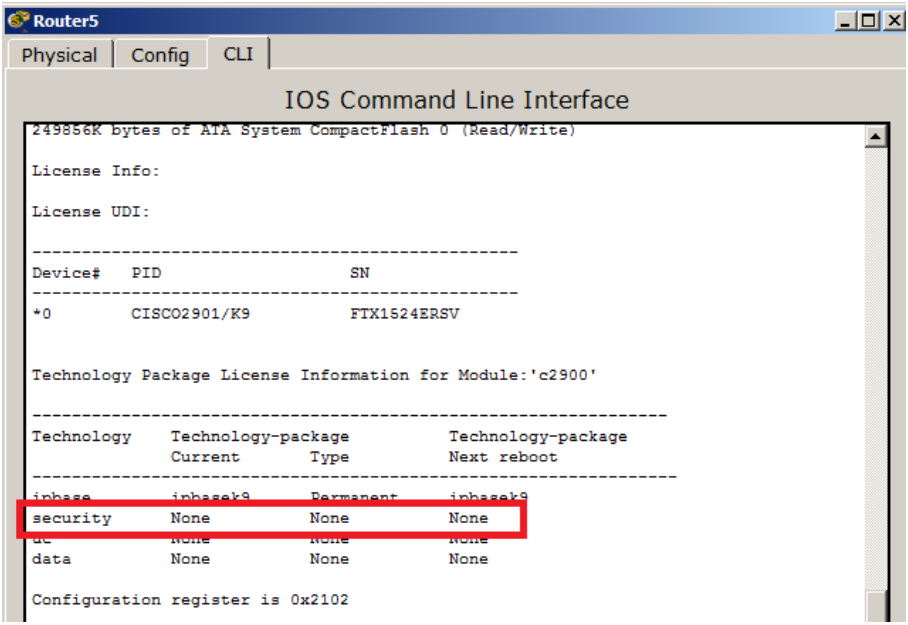

Рисунок 2.16 – Налаштування безпеки у маршрутизаторі

Для активації ліцензії, тобто встановлення пакету securityk9, необхідно виконати наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконаємо встановлення модуля c2900, який пов'язаний з ліцензією securityk9:

> license boot module c2900 technology-package securityk9;

> end;

– запис поточних параметрів у параметри при завантаженні:

> copy running-config startup-config;

– перезавантаження маршрутизатора:

> reload.

Після перевантаження маршрутизатора повторіть команду show version. Результат має бути таким як на рисунку 2.17.

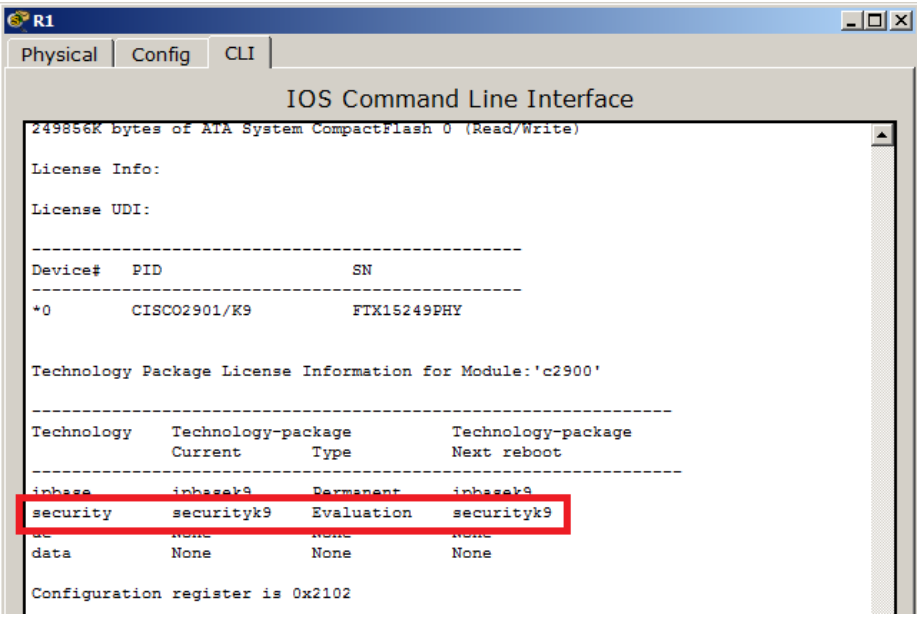

Рисунок 2.17 – Встановлений пакет ліцензії безпеки

Такі саме дії необхідно виконати і на маршрутизаторі R3.

2.4.2 Ідентифікація «особливого» трафіку

Для ідентифікації трафіку з локальної мережі R1 до локальної мережі R3 як «особливого» необхідно налаштувати ACL 110.

Примітка. Розширені списки ACL можуть фільтрувати за протоколом, IP-адресами джерела і призначення, номерами портів джерела і призначення.

Додатковою політикою для мережі говориться, що пристроям з наступної локальної мережі дозволяється тільки, досягнення внутрішньої мережі. Комп'ютерам на цій локальній мережі не дозволений доступ до Інтернету. Таким чином користувачі повинні бути заблоковані від досягнення відкритої IP-адреси (для виходу в Інтернет). Так як ця вимога діє і для джерела і для призначення, то необхідна розширена ACL.

Під ACL в роботі мається на увазі access-list, який фільтрує за адресами джерела і отримувача трафік протоколів 3 і 4 рівнів. Він повинен мати номер у діапазоні від 100 до 199. Цей «особливий» трафік буде використовувати протокол IPSec кожного разу як проходитиме між локальними мережами через R1 та R3.

Для його ідентифікації необхідно виконати наступні команди: (на маршрутизаторі R1).

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– входимо в режим налаштування конфігурацій, вводимо команду:

> Configure terminal;

– налаштовуємо трафік між R1 та R3 як «особливий»:

> access-list 110 permit ip 192.168.1.0 0.0.0.255 192.168.3.0 0.0.0.255.

Усі основні параметри, які пов’язані з налаштуваннями безпеки при передачі «особливого» трафіку наведено у таблиці 2.2.

Таблиця 2.2 – Параметри ISAKMP

Параметри		R1	R2
Спосіб розповсюдження ключа	Згідно інструкції чи **ISAKMP**	ISAKMP	ISAKMP
Алгоритм шифрування	**DES**, 3DES, or AES	AES	AES
Алгоритм хешування	MD5 or **SHA-1**	SHA-1	SHA-1
Метод аутентифікації	Попередньо поширені ключі або **RSA**	Попередньо поширені ключі	Попередньо поширені ключі
Обмін ключами	Група DG **1**, 2 або 5	DH 2	DH 2
Час життя IKE SA	88640 сек або менше	88640	88640
ISAKMP ключ		cisco	cisco

2.5 Налаштування ISAKMP

2.5.1 Налаштування політики криптографії

Налаштуємо політику криптографії ISAKMP 10 на маршрутизаторі R1 с використанням ключа «cisco». Повернемося до таблиці ISAKMP (табл. 2.2) для вибору конкретних параметрів. Не можна залишати параметри за замовченням, необхідно налаштувати спосіб обміну ключами та DH-метод.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування вводимо команду:

> Configure terminal;

– виконуємо налаштування:

> crypto isakmp policy 10
> encryption aes
> authentication pre-share
> group 2
> exit
> crypto isakmp key cisco address 10.2.2.2

2.5.2 Створення перетворювача VPN-SET на R1

Необхідно створити перетворювач VPN-SET для того, щоб використовувати криптографічні алгоритми шифрування esp-3des та esp-sha-hmac. Після цього зможемо налаштувати мапу криптографії VPN-MAP, яка зв'яже усі параметри разом.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконуємо налаштування:

> crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
> crypto map VPN-MAP 10 ipsec-isakmp
> description VPN connection to R3
> set peer 10.2.2.2
> set transform-set VPN-SET
> match address 110
> exit

2.5.3 Налаштування мапи криптографії на вихідному інтерфейсі S0/0/0

Кінцевим налаштуванням мапи криптографії VPN-MAP є її прив'язка до вихідного інтерфейсу S0/0/0 на маршрутизаторі R1.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконуємо налаштування:

> interface S0/0/0
> crypto map VPN-MAP

2.6 Налаштування IPSec параметрів в маршрутизаторі R3

2.6.1 VPN з'єднання типу «мережа-мережа»

Тепер необхідно налаштувати зворотні параметри для даної VPN мережі на маршрутизаторі R3. Налаштування ACL 110 для ідентифікації трафіку з локальної мережі R3 у локальну мережу R1 як «особливого».

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

- і виконуємо налаштування:

> access-list 110 permit ip 192.168.3.0 0.0.0.255 192.168.1.0 0.0.0.255

2.6.2 Налаштування ISAKMP

Налаштування політики криптографії ISAKMP 10 на маршрутизаторі R3 с використанням ключа «cisco». Поверніться до таблиці ISAKMP (поки ще нема) для завдання конкретних параметрів. Не можна залишати параметри за замовченням, необхідно налаштувати спосіб обміну ключами та DH-метод.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконуємо налаштування:

> crypto isakmp policy 10

> encryption aes

> authentication pre-share

> group 2

> exit
> crypto isakmp key cisco address 10.1.1.2

2.6.3 Створення перетворювача VPN-SET на R3

Так як і на маршрутизаторі R1 необхідно створити набір для перетворення VPN-SET, для можливості використання esp-3des та esp-sha-hmac на маршрутизаторі R3. Після цього створюється мапа криптографії, яка зв'яже необхідні параметри разом.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконуємо налаштування:

> crypto ipsec transform-set VPN-SET esp-3des esp-sha-hmac
> crypto map VPN-MAP 10 ipsec-isakmp
> description VPN connection to R1
> set peer 10.1.1.2
> set transform-set VPN-SET
> match address 110
> exit.

2.6.4 Налаштування мапи криптографії на вихідному інтерфейсі S0/0/1

Кінцевим налаштуванням мапи криптографії VPN-MAP є її прив'язка до вихідного інтерфейсу S0/0/1 на маршрутизаторі R3.

Для цього необхідно ввести наступні команди:

– входимо в привілейований режим, для цього в терміналі вводимо команду:

> Enable;

– для входу в режим налаштування конфігурацій вводимо команду:

> Configure terminal;

– виконуємо налаштування:
> interface S0/0/1
> crypto map VPN-MAP

2.6.5 Перевірка роботи IPSec VPN

Виконайте команду **show crypto ipsec sa** на маршрутизаторі R1 (рис.2.18). Зверніть увагу що кількість інкапсульованих, зашифрованих, декапсульованих, розшифрованих пакетів встановлена в 0.

– входимо в привілейований режим, для цього в терміналі вводимо команду:
> Enable;
– виконуємо команду:
> show crypto ipsec sa

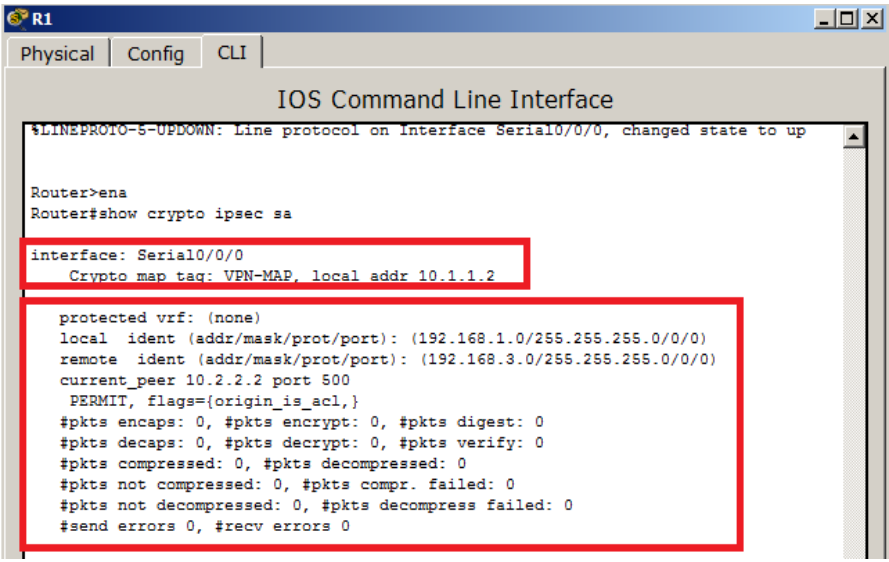

Рисунок 2.18 – Результати виконання команди show crypto ipsec sa

Для того, щоб так званий «особливий» трафік пройшов від локальної мережі R3 до локальної мережі R1 виконаємо команду «Ping»

від PC-C до PC-A (це можна зробити за допомогою гарячої клавіші «P», для цього після натискання клавіші треба клацнути лівою кнопкою миші на об'єкті від якого буде йти пінг-пакет, а потім клацнути на об'єкті до якого буде йти пінг-пакет).

Повторимо команду show crypto ipsec sa на маршрутизаторі R1 (рис.2.19). Зверніть увагу на те, що кількість пакетів змінилась. Це означає, що налаштований IPSec працює.

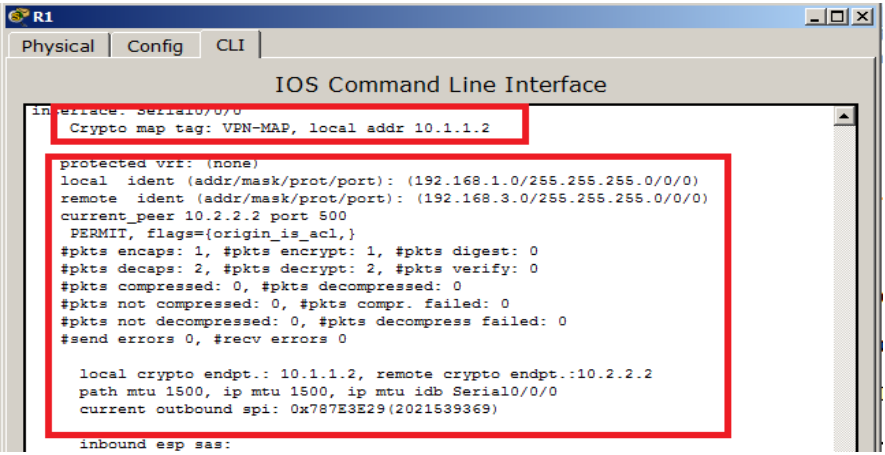

Рисунок 2.19 - Результати виконання команди show crypto ipsec sa

Тепер виконайте команду «Ping» від PC-B до PC-A. Після цього знову виконайте команду show crypto ipsec sa на маршрутизаторі R1 (рис. 2.20) і переконайтеся що кількість пакетів не змінилася.

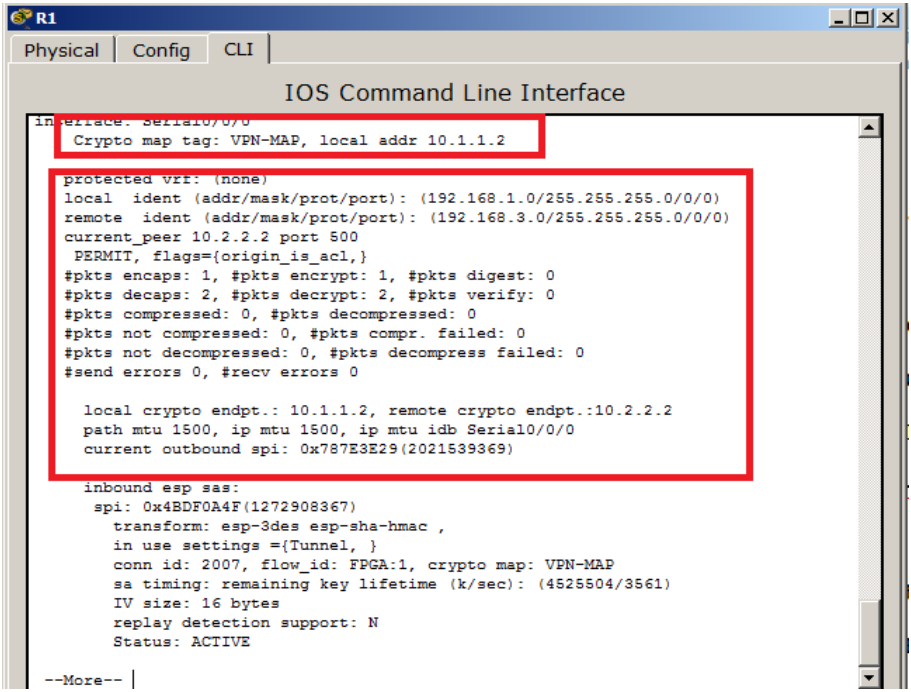

Рисунок 2.20 - Результати виконання команди show crypto ipsec sa після команди «Ping»

2.7 Зміст звіту

- хід роботи;
- індивідуальна схема з зазначенням конфігурації інтерфейсів;
- відповіді на контрольні питання.

2.8 Контрольні питання

1. Визначення та види VPN.
2. Базові архітектури VPN.
3. Група протоколів IPSec. Особливості використання.
4. Схема передачі пакету з використанням IPSec шифрування. Особливості налаштування та адресації.