

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Національний університет «Запорізька політехніка»

МЕТОДИЧНІ ВКАЗІВКИ

до виконання лабораторних робіт з дисципліни

"Технології проектування телекомунікаційних мереж"

для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні
програми «Комп'ютерні системи та мережі» та «Спеціалізовані
комп'ютерні системи», усіх форм навчання.

Реалізація GRE тунелю

Методичні вказівки до виконання лабораторних робіт з дисципліни "Технології проектування телекомунікаційних мереж" для магістрів спеціальності 123 "Комп'ютерна інженерія", освітні програми «Комп'ютерні системи та мережі» та «Спеціалізовані комп'ютерні системи», усіх форм навчання. Реалізація GRE тунелю / Укл. Г.Г. Киричек. – Запоріжжя: НУ «Запорізька політехніка», 2020. – 34 с.

Укладачі:

Г.Г. Киричек, доцент, к.т.н.

Рецензент:

М.Ю. Тягунова, доцент, к.т.н.

Відповідальний за випуск:

Г.Г. Киричек, доцент, к.т.н.

Затверджено
на засіданні кафедри КСМ
Протокол № 2 від 04.09.2020

Рекомендовано до видання
НМК КНТ
Протокол № 2/1 від 15.09.2020

ЗМІСТ

1 Лабораторна робота. Реалізація GRE тунелю	4
1.1 GRE тунель	4
1.2 Налаштування мережі	6
1.2.1 Модель мережі (схема)	6
1.2.2 Налаштування IP адресації	13
1.2.3 Налаштування статичної маршрутизації	18
1.3 Налаштування функції безпеки	22
1.3.1 Активація модуля securityk9	22
1.3.2 Ідентифікація «особливого» трафіку	24
1.4 Налаштування ISAKMP	25
1.4.1 Налаштування політики криптографії	25
1.4.2 Створення перетворювача VPN-SET	26
1.4.3 Налаштування мапи криптографії на вихідному інтерфейсі S0/0/0	27
1.5 Налаштування IPSec параметрів в маршрутизаторах R2 і R3	27
1.5.1 VPN з'єднання типу «мережа-мережа»	27
1.5.2 Налаштування ISAKMP	28
1.5.3 Створення перетворювача VPN-SET	29
1.5.4 Налаштування мапи криптографії на вихідному інтерфейсі S0/0/1	30
1.6 Налаштування GRE тунелю через IPSec	31
1.7 Перевірка роботи тунелю GRE скрізь IPsec	33
1.8 Зміст звіту	33
1.9 Контрольні питання	33
Рекомендована література	34

1 ЛАБОРАТОРНА РОБОТА.

Реалізація GRE тунелю

Мета роботи: навчитися планувати, моделювати, розробляти та налаштовувати GRE тунелі та реалізовувати їх прокладку через протокол IPSec.

1.1 GRE тунель

GRE (англ. *Generic Routing Encapsulation* - загальна інкапсуляція маршрутів) - протокол тунелювання мережних пакетів, розроблений компанією Cisco Systems. Його основне призначення - інкапсуляція пакетів мережного рівня моделі OSI в IP пакети.

Сам по собі GRE не забезпечує ніякої безпеки переданих даних - це site-to-site VPN тунель у чистому вигляді. Використовується зазвичай такий тунель, коли є специфічні завдання, пов'язані з маршрутизацією і немає вимог до безпеки. Не варто забувати, що чистий GRE тунель - не навантажує обладнання, а навантаження при шифруванні великого обсягу даних досить істотне.

Протокол GRE інкапсулюється безпосередньо в IP, мінаючи TCP або UDP, в IP пакеті є спеціальне поле «Protocol type», в якому міститься число, що позначає протокол, інкапсульований в даний IP пакет, для GRE код protocol type дорівнює 47. У зв'язку з цим, якщо в мережі є GRE тунелі, то варто уважно ставитися до написання розширених списків контролю доступу (ACL), так як `permit tcp any any` і `permit udp any any` приведуть до заборони на GRE через те, що він інкапсулюється безпосередньо в пакет, тому треба писати або `permit ip any any` або `permit gre any any`.

У зв'язку зі службовим заголовком розмір переданих даних усередині IP пакета через GRE-тунель зменшується при збереженні загального розміру пакета. У IP-пакеті передбачено наявність біта DF (do not fragment), який забороняє поділ пакета на декілька частин при передачі через середовище з меншим розміром MTU. У цьому випадку пакет з розміром корисної області даних, яка перевищує MTU IP пакету в GRE-тунелі, відкидається, що призводить до втрат пакетів при істотному навантаженні (проходять пакети малого розміру, такі як SYN пакети TCP, ICMP повідомлення (ping), але губляться пакети з даними

в TCP потоці (тобто з'єднання рветься)). Для вирішення цієї проблеми рекомендується використовувати path-mtu-discovery (визначення TCP MSS, тобто максимального розміру IP-пакетів на всьому шляху) при передачі даних через GRE-тунель, щоб уникнути надмірної фрагментації або втрати великих пакетів.

Тунелювання забезпечується трьома протоколами:

- пасажир - інкапсульований протокол (в різних стеках свій - IP, CLNP, IPX, AppleTalk, DECnet Phase IV, XNS, VINES і Apollo);
- протокол інкапсуляції (GRE);
- транспортний протокол (IP).

Дана робота описує принцип дії GRE тунелю на прикладі віртуальної приватної мережі (VPN), яка складається з 2 віддалених філіалів та одного центрального офісу, у якому встановлено сервер підприємства. Філіали можуть обмінюватися інформацією з сервером через закриту мережу, але при цьому не можуть обмінюватися даними між собою напряму, тобто обмін даними відбувається виключно через центральний офіс.

Такий обмін інформацією дозволяє забезпечити захист трафіку, який передається і, одночасно, спрощує роботу користувачів з базою даних підприємства, так як при такій взаємодії виключається створення помилкових записів, видалення одних і тих же записів з бази двічі чи їх дублювання.

Реалізована таким чином віртуальна приватна мережа дозволяє забезпечити зв'язок між сегментами різних мереж так, ніби ці сегменти об'єднані прямим з'єднанням (кабелем або віртуальним каналом).

Приклад стека протоколів наведено у таблиці 1.1.

Таблиця 1.1 – Приклад стека протоколів

Рівень моделі OSI	Протокол
5. Сеансовий	X.225
4. Транспортний	UDP
3. Мережевий (GRE-інкапсуляція)	IPv4
Інкапсуляція	GRE
3. Мережний	IPv4
2. Канальний	Ethernet
1. Фізичний	Ethernet

Як видно з таблиці, будь-яка інкапсуляція (не обов'язково GRE) порушує ієрархію в моделі OSI. Це явище можна розглядати як роздільник між двома стеками протоколів, де один виступає «постачальником послуг» для іншого.

1.2 Налаштування мережі

1.2.1 Модель мережі (схема)

Виконайте етапи з'єднання мережного обладнання:

- запустіть ярлик Packet Tracer на робочому столі (або виконайте установку програми запустивши файл Packet Tracer.exe з папки Install);
- зберіть мережу за схемою, представленою на рисунку 1.1, з основними параметрами комутаційного обладнання та інтерфейсів (табл. 1.2);

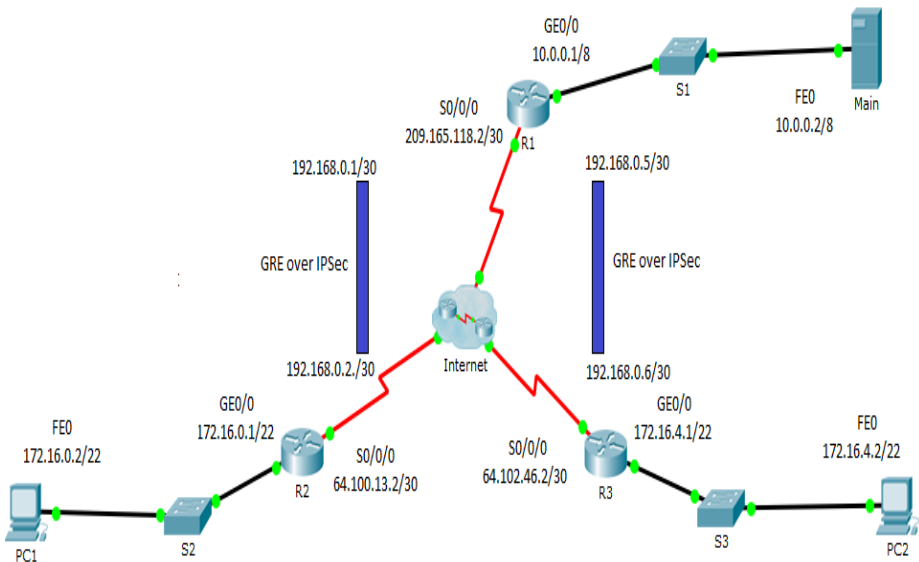


Рисунок 1.1 – Схема мережі

- для цього виконайте наступні дії:

1) з панелі приладів в робочу область перенесіть 4 маршрутизатора 2901 (для зручності їх краще перейменувати у R1, R2, R3 та Bridge);

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

3) в робочу область перенесіть 2 робочі станції PC-PT (перейменуйте у PC1 та PC2);

4) в робочу область перенесіть 2 сервери Server (перейменуйте у Main та Google).

Для установки маршрутизаторів на панелі приладів необхідно вибрати перший елемент – Routers (рис.1.2). З показаних пристроїв треба вибрати 2901 (підкреслений) і перетягнути у робочу область.

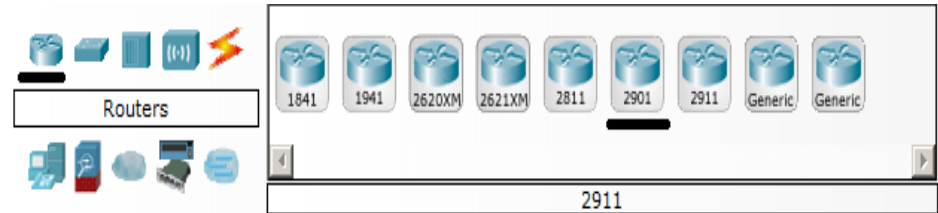


Рисунок 1.2 – Вибір маршрутизаторів

Для вставки комутаторів необхідно перейти на закладку Switches (рис.1.3) і перетягти 2950-24 (підкреслений) елемент у робочу область.

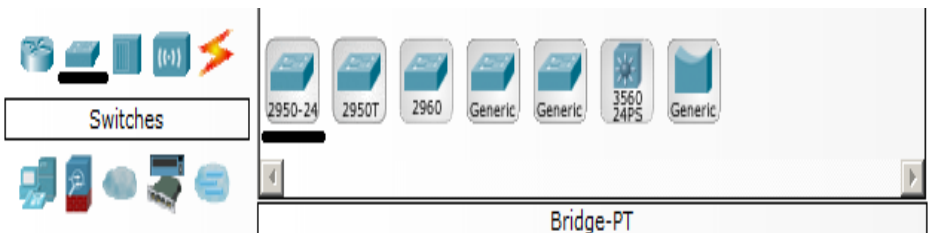


Рисунок 1.3 – Вибір комутаторів

Для вставки комп'ютерів необхідно перейти на закладку End devices (рис.1.4) і перетягти Generic (підкреслений) елемент у робочу область.



Рисунок 1.4 – Вибір комп'ютерів

Для вставки серверів необхідно перейти на закладку End devices (рис.1.5) і перетягти Generic (підкреслений) елемент у робочу область.



Рисунок 1.5 – Вибір серверів

Таблиця 1.2 – Параметри інтерфейсів

Пристрій	Інтерфейс	IP-адреса	Маска	Default Gateway
R1	Gigabit Ethernet 0/0	10.0.0.1	255.0.0.0	***
	Serial 0/0/0	209.165.118.2	255.255.255.252	***
	Tunnel 0	192.168.0.1	255.255.255.252	***
	Tunnel 1	192.168.0.5	255.255.255.252	***

Продовження таблиці 1.2

R2	Gigabit Ethernet 0/0	172.16.0.1	255.255.252.0	***
	Serial 0/0/0	64.100.13.2	255.255.255.252	***
	Tunnel 0	192.168.0.2	255.255.255.252	***
R3	Gigabit Ethernet 0/0	172.16.4.1	255.255.252.0	***
	Serial 0/0/0	64.102.46.2	255.255.255.252	***
	Tunnel 0	192.168.0.6	255.255.255.252	***
Bridge	Gigabit Ethernet 0/0	8.1.1.1	255.0.0.0	***
	Serial 0/0/0	64.100.13.1	255.255.255.252	***
	Serial 0/0/1	209.165.118.1	255.255.255.252	***
	Serial 0/1/0	64.102.46.1	255.255.255.252	***
PC1	Fast Ethernet 0	172.16.0.2	255.255.252.0	172.16.0.1
PC2	Fast Ethernet 0	172.16.4.2	255.255.252.0	172.16.4.1
Main	Fast Ethernet 0	10.0.0.2	255.0.0.0	10.0.0.1
Google	Fast Ethernet 0	8.8.8.8	255.0.0.0	8.1.1.1

В процесі налаштування на маршрутизаторах необхідно додати спеціальні модулі. Для цього клацніть на піктограмі маршрутизатора, яка знаходиться у робочій області. Далі відкриється вікно налаштувань даного пристрою (рис.1.6). У відкритому вікні у вкладці Physical зліва оберіть модуль HWIC-2T.

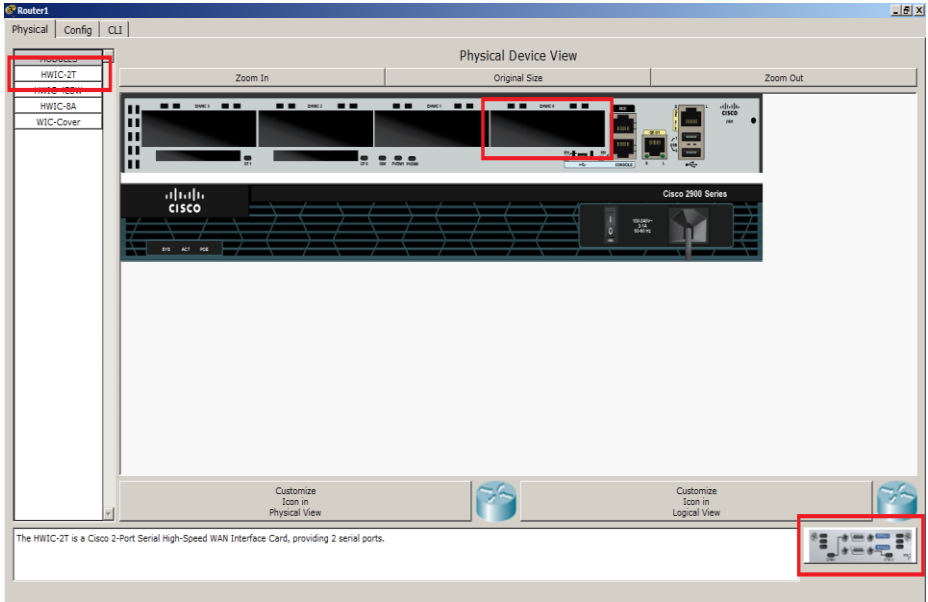


Рисунок .1.6 – Вікно налаштувань маршрутизатора

Тепер треба вимкнути живлення маршрутизатора і перетягнути 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 1.7.

Після закінчення налаштувань необхідно увімкнути живлення.

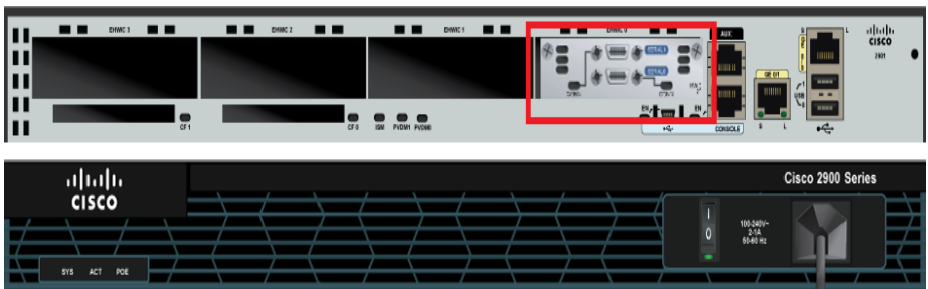


Рисунок .1.7 – Маршрутизатор з встановленим модулем

Аналогічні дії необхідно повторити для маршрутизаторів R2 і R3. У випадку маршрутизатора Bridge треба встановити два таких модуля у крайні праві роз'єми.

Наступним кроком налаштувань є з'єднання між собою маршрутизаторів за допомогою кабелю. У даному випадку використовується кабель який 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.1.8).



Рисунок 1.8 – Вибір кабелю для з'єднання маршрутизаторів

Для з'єднання двох пристроїв необхідно:

- вибрати кабель для з'єднання (рис.1.8);
- натиснути на першому пристрої який необхідно з'єднати та вибрати порт (рис.1.9);
- протягнути кабель до другого пристрою і так само обрати порт (рис.1.10).

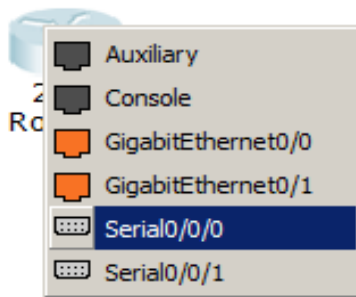


Рисунок 1.9 – Вибір порту на першому пристрої

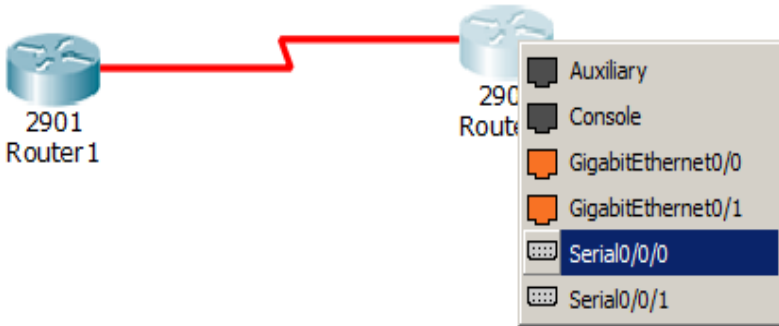


Рисунок 1.10 – Вибір порту на другому пристрої

Для підключення комп'ютера до комутатора, а комутатора у свою чергу до маршрутизатора використовується інший тип кабелю – вита пара (рис.1.11).

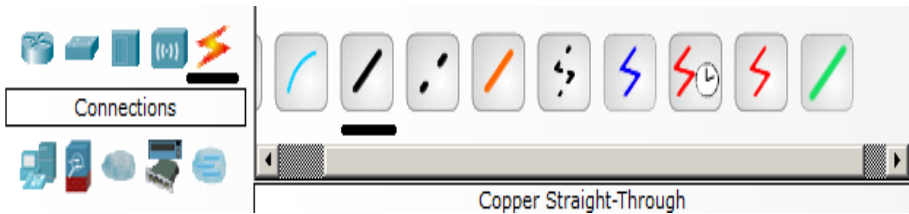


Рисунок 1.11 – Вибір витиї пари

Для спрощення налаштувань необхідно кабель підключати на ті порти, які вказані у таблиці 1.2.

Користуючись вказаними вище вказівками необхідно зібрати наступну локальну мережу (рис. 1.12).

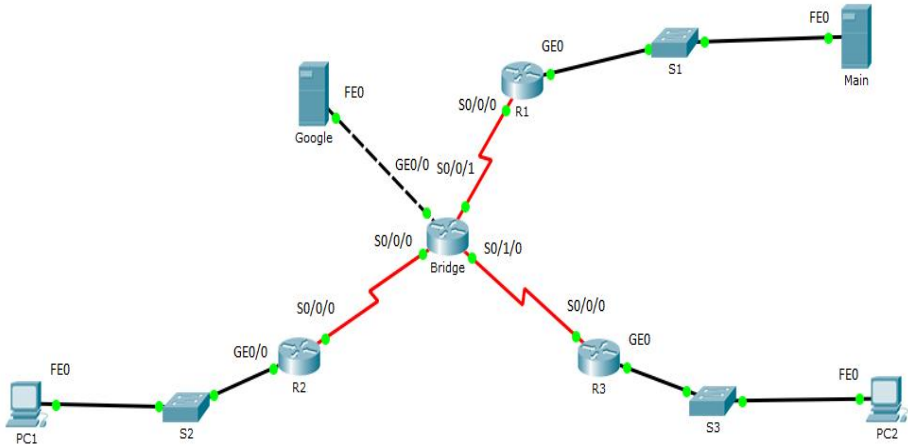


Рисунок 1.12 – Загальна схема мережі

Для того щоб придати схемі мережі вигляд, як на рисунку 1.1 необхідно зробити наступні дії:

- виділити елементи Google і Bridge;
- натиснути на панелі управління кнопку New Cluster;
- підписати отриманий об'єкт як Internet.

1.2.2 Налаштування IP адресації

У цьому розділі описано, як виконати необхідні налаштування IP адресації, згідно параметрам наведеним в таблиці 1.2.

Для налаштування комп'ютера PC1 необхідно:

- клацнути на піктограмі PC1 у робочій області лівою кнопкою миші;
- у відкритому вікні обрати вкладку Desktop;
- натиснути на кнопці IP Configuration і ввести налаштування з таблиці 1 (рис. 1.13, 1.14).

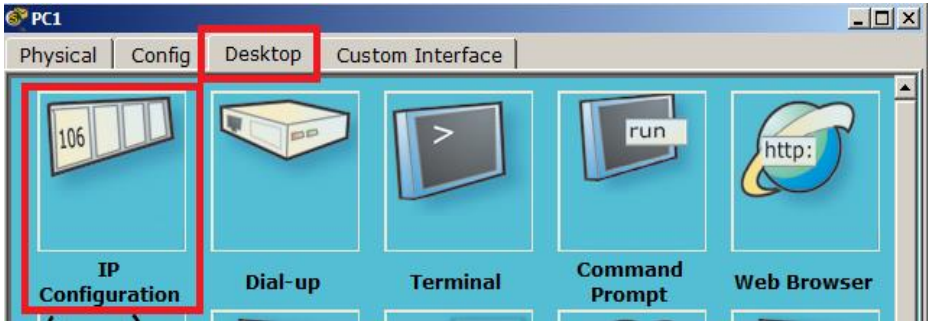


Рисунок 1.13 – Налаштування PC1

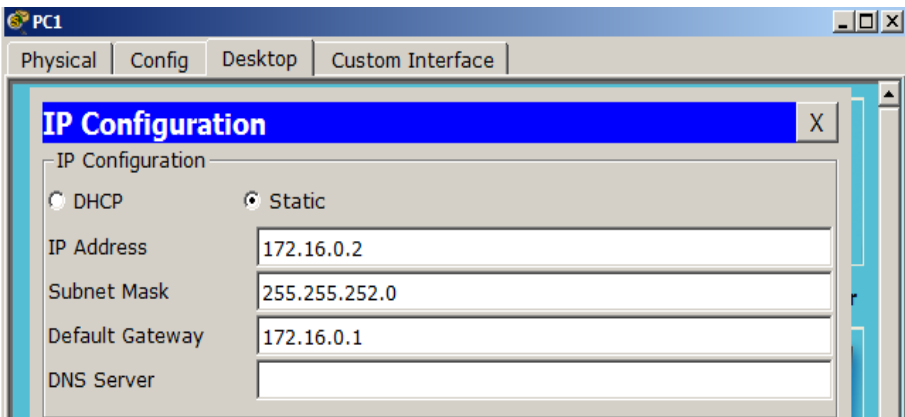


Рисунок 1.14 – Налаштування IP адресації PC1

Аналогічним чином повторіть попередні пункти для PC2. Необхідні параметри (IP-адреса, маска підмережі та Default Gateway) візьміть з таблиці 1.2.

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 1.2 (рис. 1.15, 1.16).

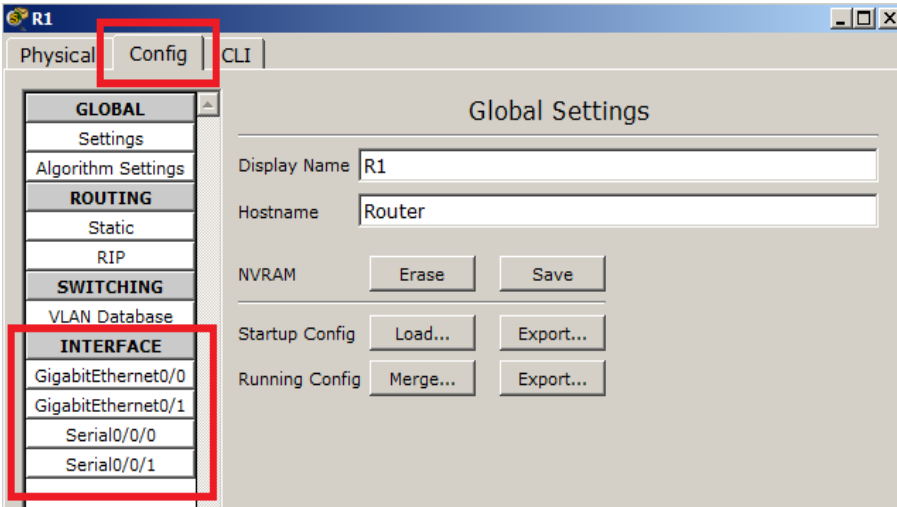


Рисунок 1.15 – Налаштування R1

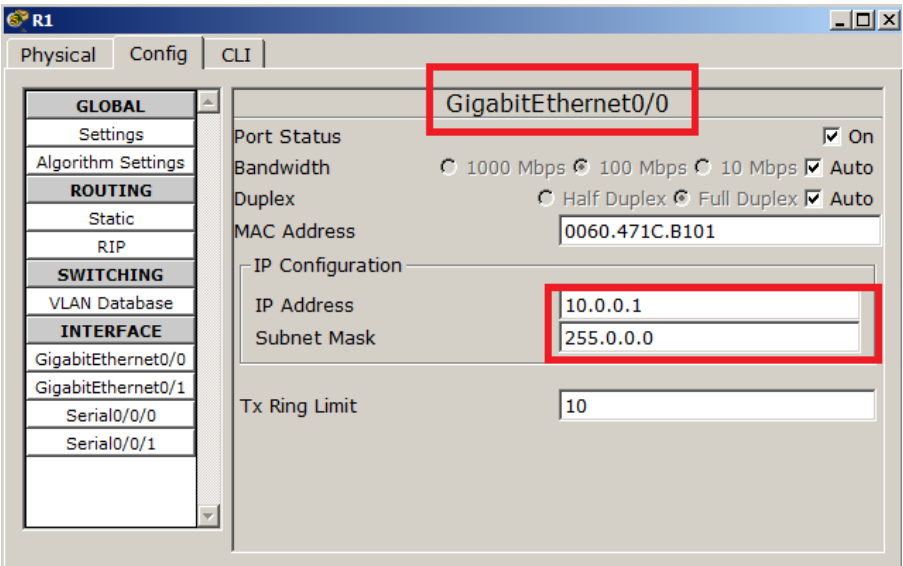


Рисунок 1.16 – Налаштування IP адресації R1

Аналогічним чином повторіть попередні пункти для маршрутизаторів R2, R3 та Bridge. Необхідні параметри (IP-адреса та маска підмережі) візьміть з таблиці 1.2.

Для налаштування сервера Main треба:

- клацнути на піктограмі Main у робочій області лівою кнопкою миші;
- у відкритому вікні обрати вкладку Desktop;
- натиснути на кнопці IP Configuration і ввести налаштування з таблиці 1.2 (рис. 1.17, 1.18).

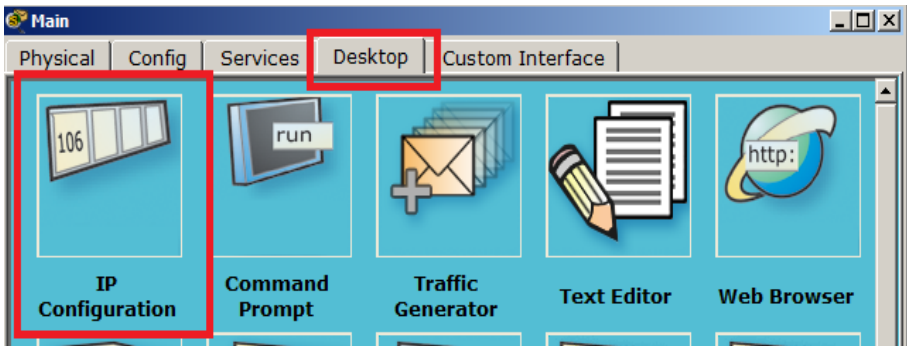


Рисунок 1.17 – Налаштування Main

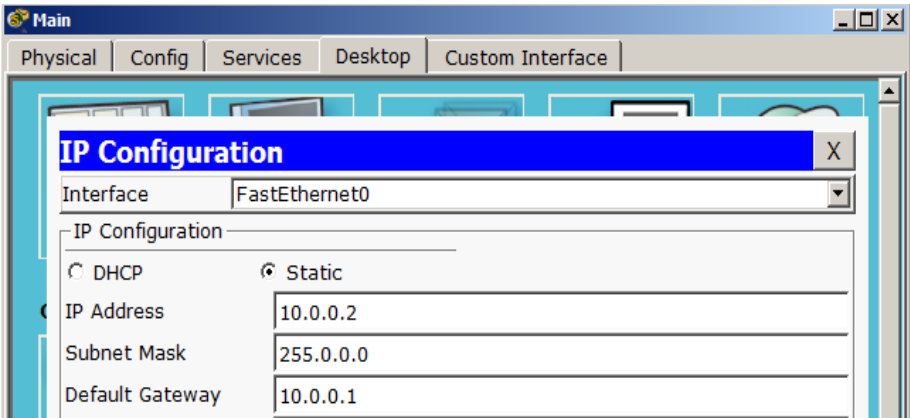


Рисунок 1.18 – Налаштування IP адресації Main

Аналогічним чином повторіть попередні пункти для Google. Необхідні параметри (IP-адреса, маска підмережі та Default Gateway) візьміть з таблиці 1.2.

Додатково сервер Google треба налаштувати наступним чином:

- перейти у вкладку Services, натиснути на сервісі HTTP, увімкнути його і змінити одну зі строчок тексту сторінки на «Welcome to GOOGLE» (рис. 1.19);
- перейти у сервіс DNS, у полі Name ввести адресу google.com, у полі Address – 8.8.8.8 і натиснути кнопку Add (рис. 1.20).

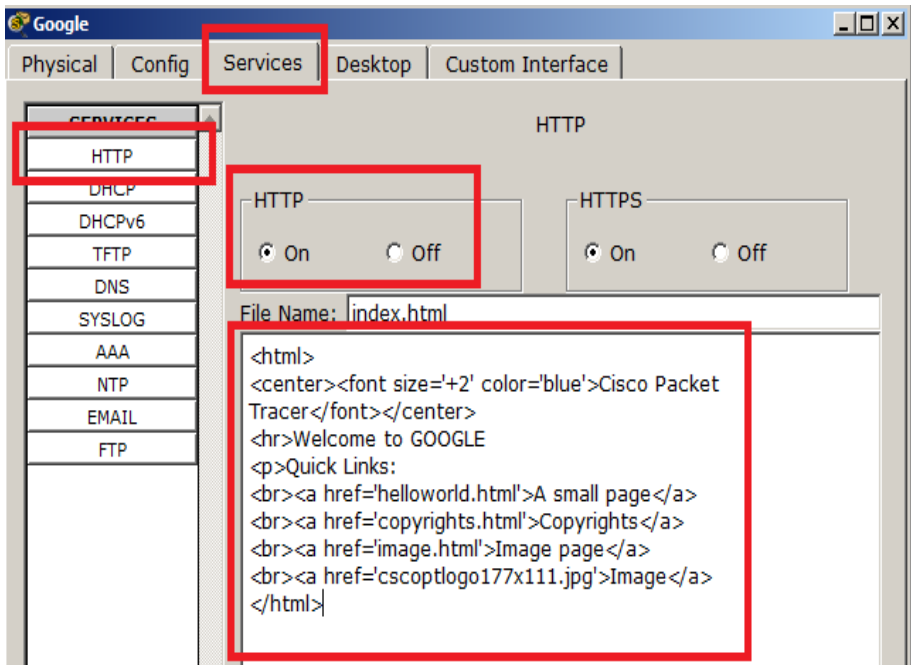


Рисунок 1.19 – Налаштування HTTP сервісу на сервері Google

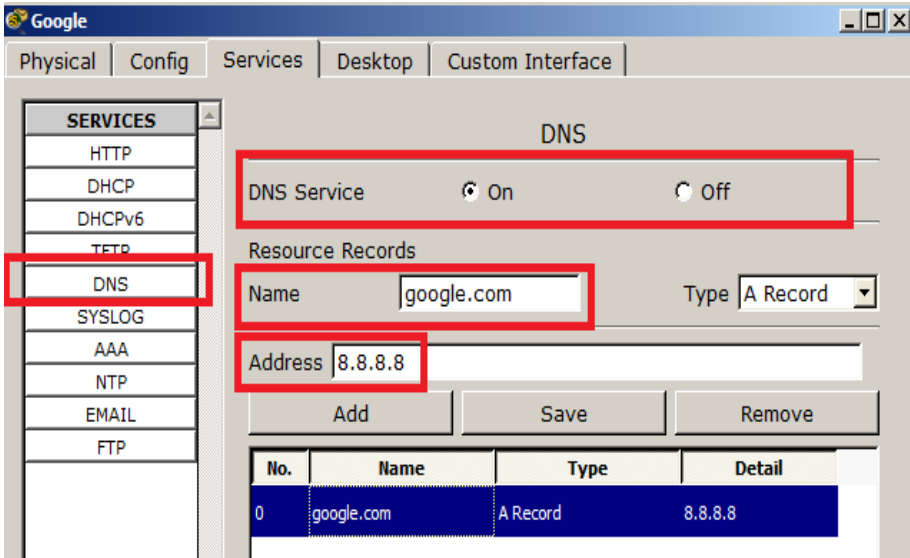


Рисунок 1.20 – Налаштування DNS сервісу на сервері Google

1.2.3 Налаштування статичної маршрутизації

Налаштуємо маршрути на маршрутизаторі R1.

Для налаштувань статичної маршрутизації необхідно виконати наступні дії.

- клацнути на маршрутизаторі R1 лівою кнопкою миші;
- у відкритому вікні перейти у вкладку CLI (рис.1.21) і виконати необхідні команди.

Для налаштування статичної маршрутизації треба для кожного маршрутизатора прописати адреси і маски мереж, які безпосередньо НЕ підключені до даного маршрутизатора. Таким чином для маршрутизатора R1 необхідно додати такі мережі (у скобках вказано інтерфейс, який необхідно вказати при налаштуванні):

- 64.100.13.0/30 (S0/0/0);
- 64.102.46.0/30 (S0/0/0).

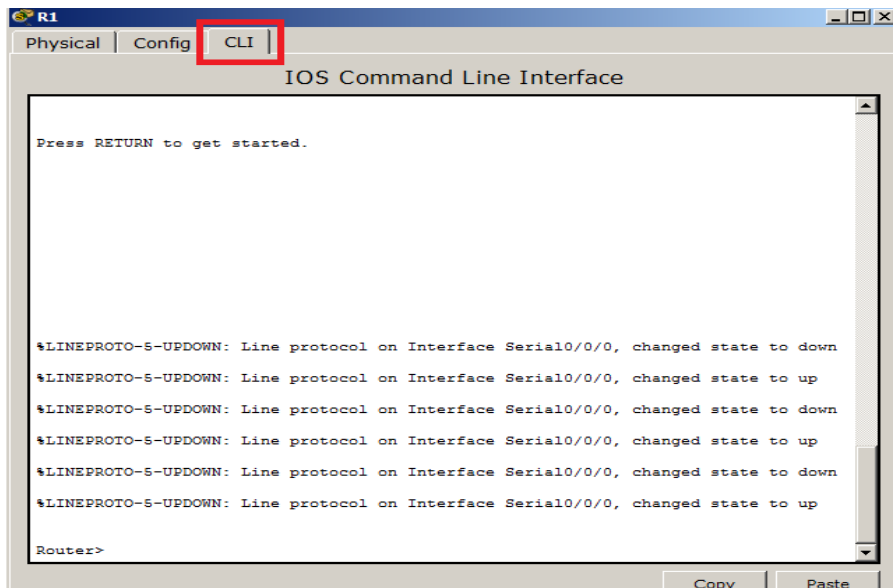


Рисунок 1.21 – Вкладка CLI

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 64.100.13.0 255.255.255.252 s0/0/0.

Замість s0/0/0 можна ввести IP-адресу інтерфейсу маршрутизатора, до якого підключена дана мережа;

- вводимо вище наведену команду для налаштування інших мереж, змінюючи IP-адресу і маску згідно з таблицею 1.2;

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

> по IP route 64.100.13.0 255.255.255.252 s0/0/0 (або з ім'ям (адресою) інтерфейсу).

Виконайте, за попередньою схемою, налаштування маршрутизаторів R2, R3 та Bridge, з урахуванням мереж до яких вони підключені і адрес їх інтерфейсів (табл.1.2).

Для маршрутизатора R2 необхідно додати такі мережі:

- 209.165.118.0/30 (S0/0/0);
- 64.102.46.0/30 (S0/0/0);
- 8.0.0.0/8 (S0/0/0).

Для маршрутизатора R3 необхідно додати такі мережі:

- 209.165.118.0/30 (S0/0/0);
- 64.100.13.0/30 (S0/0/0);
- 8.0.0.0/8 (S0/0/0).

Для маршрутизатора Bridge необхідно додати такі мережі:

- 64.102.46.0/30 (S0/0/0);
- 64.102.46.0/30 (S0/0/1);
- 209.165.118.0/30 (S0/0/0);
- 209.165.118.0/30 (S0/1/0);
- 64.100.13.0/30 (S0/0/1);
- 64.100.13.0/30 (S0/1/0);
- 172.16.0.0/22 (S0/0/0);
- 172.16.4.0/22 (S0/1/0).

Після усіх налаштувань перевіряємо чи працює статична маршрутизація. Для цього необхідно виконати команду «ping» від PC1 до Google, а потім від PC2 до Google (це можна зробити за допомогою гарячої клавіші «P», для цього після натискання клавіші треба клацнути лівою кнопкою миші на об'єкті від якого відправляємо пінг-пакет, а потім клацнути на об'єкті який отримає пінг-пакет).

Далі перевіряються наступні з'єднання:

- R1->R2;
- R1->R3;
- R1->Bridge;
- R2->R3;
- R2->Bridge;
- R3->Bridge.

Якщо пінг пройшов у всіх напрямках, то статична маршрутизація налаштована правильно і на даний момент «вихід в інтернет» реалізований.

Ще одним варіантом перевірки є використання DNS сервера.

Для цього необхідно повернутися до налаштувань IP конфігурації комп'ютерів PC1 та PC2 (рис.1.12, 1.13). У налаштуваннях необхідно додати IP- адресу DNS серверу.

У якості DNS сервера вказуємо IP-адресу сервера Google (8.8.8.8). Далі потрібно перейти у вкладку Web Browser (рис. 1.22) і вести у строку адреси наступну адресу <http://google.com>. Сторінка має прийняти вигляд як на рисунку 1.23.

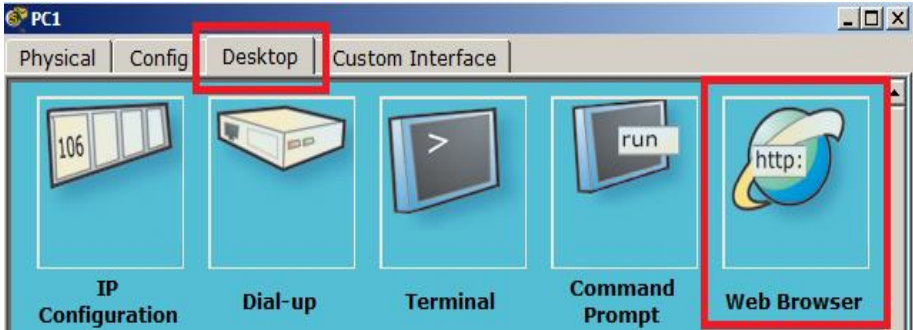


Рисунок 1.22 – Відкриття Web-браузера на PC

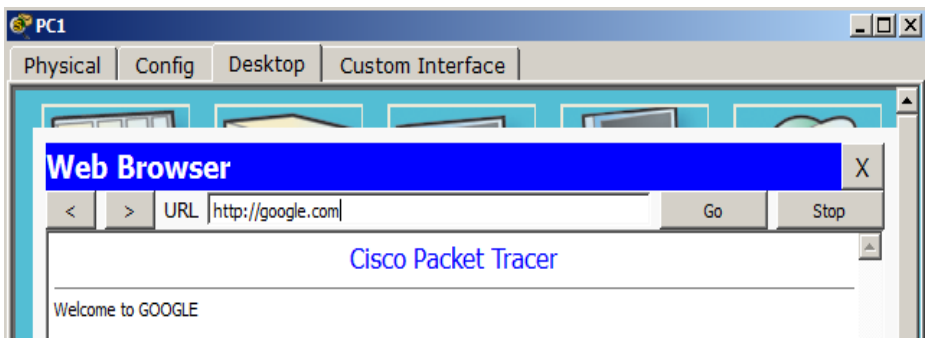


Рисунок 1.23 – Сторінка «Google»

1.3 Налаштування функції безпеки

1.3.1 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 активована:

- show version.

Якщо відповідь на введену команду є такою як на рисунку 1.24, то це означає що пакет не встановлений.

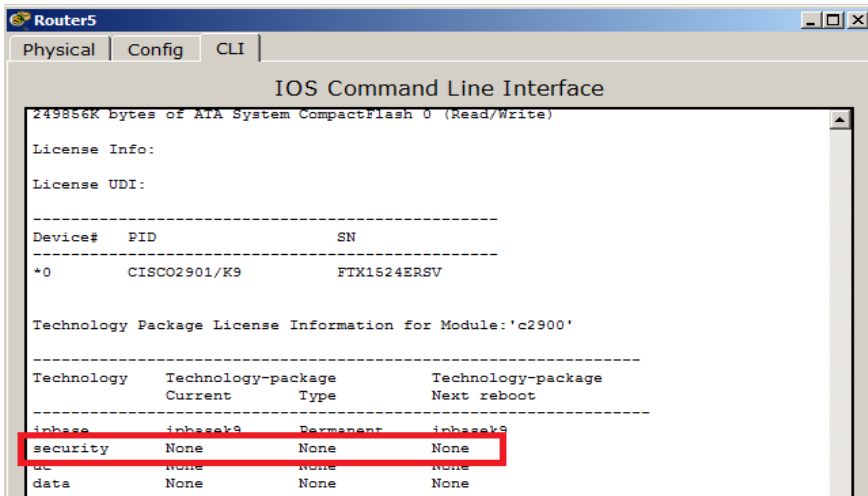


Рисунок 1.24 – Налаштування безпеки у маршрутизаторі

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 (на запит «АССЕРТ? [yes/no]:») після виконання команди необхідно обов'язково ввести відповідь «yes»);

> 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 1.25.

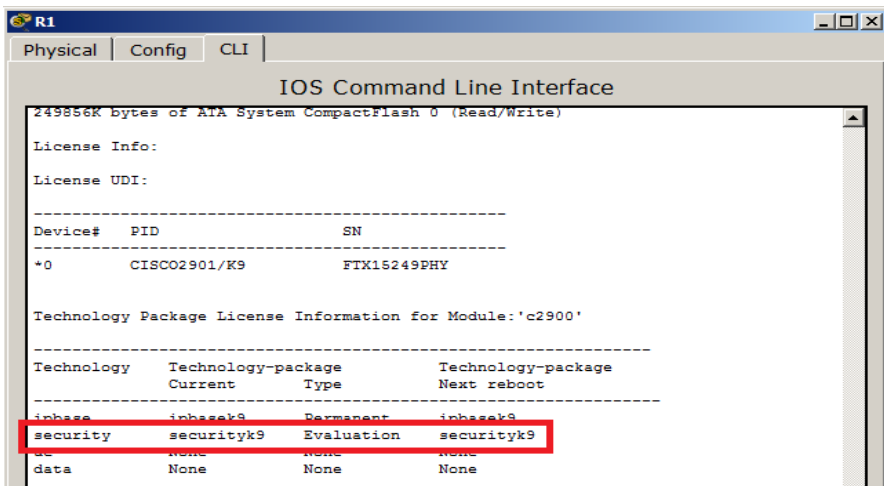


Рисунок 1.25 – Встановлений пакет ліцензії безпеки

Такі саме дії необхідно виконати на маршрутизаторах R2 та R3.

1.3.2 Ідентифікація «особливого» трафіку

Для ідентифікації трафіку з локальної мережі R1 до локальної мережі R2 як «особливого» необхідно налаштувати ACL 102.

Примітка. Розширені списки ACL можуть фільтрувати за протоколом та IP-адресами джерела і призначення, номерами портів джерела і призначення. Додатковою політикою для мережі визначається, що пристроям з наступної локальної мережі дозволяється тільки досягнення внутрішньої мережі. Комп'ютерам цієї локальної мережі не дозволений доступ до Інтернету. Таким чином користувачі повинні бути заблоковані від отримання 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 використовує протокол IPsec кожного разу як проходить між локальними мережами через R1 та R2.

Для його ідентифікації виконаємо наступні команди (маршрутизатор 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 R2 як «особливий»:
 - > access-list 102 permit ip 10.0.0.0 0.255.255.255 172.16.0.0 0.0.3.255.

Для ідентифікації трафіку з локальної мережі R1 до локальної мережі R3 як «особливого» необхідно налаштувати ACL 103.

- налаштовуємо трафік між R1 та R3 як «особливий»:
 - > access-list 103 permit ip 10.0.0.0 0.255.255.255 172.16.4.0 0.0.3.255.

1.4 Налаштування ISAKMP

1.4.1 Налаштування політики криптографії

Налаштуємо політику криптографії ISAKMP 102 на маршрутизаторі R1 з використанням ключа «cisco». 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 102

> encryption aes

> authentication pre-share

> group 5

> exit

> crypto isakmp key cisco address 64.100.13.2.

Налаштуємо політику криптографії ISAKMP 103 на маршрутизаторі R1 з використанням ключа «cisco». 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 103

> encryption aes

> authentication pre-share

```

> group 5
> exit
> crypto isakmp key cisco address 64.102.46.2.

```

1.4.2 Створення перетворювача VPN-SET

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

Для цього необхідно ввести наступні команди (маршрутизатор R1):

- 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 R1_R2_Set esp-aes esp-sha-hmac
```

```
> crypto map R1_R2_Map 102 ipsec-isakmp
```

```
> set peer 64.100.13.2
```

```
> set transform-set R1_R2_Set
```

```
> match address 102
```

```
> exit.
```

Необхідно повторити ці дії для налаштування R1_R3_Set та R1_R3_Map. Продовжуємо працювати в CLI маршрутизатора R1.

```
> crypto ipsec transform-set R1_R3_Set esp-aes esp-sha-hmac
```

```
> crypto map R1_R3_Map 103 ipsec-isakmp
```

```
> set peer 64.102.46.2
```

```
> set transform-set R1_R3_Set
```

```
> match address 103
```

```
> exit.
```

1.4.3 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 R1_R2_Map;

> crypto map R1_R3_Map.

1.5 Налаштування IPSec параметрів в маршрутизаторах R2 і R3

1.5.1 VPN з'єднання типу «мережа-мережа»

Тепер необхідно налаштувати зворотні параметри для даних VPN мережі на маршрутизаторах R2 і R3 та виконати налаштування ACL 102 для ідентифікації трафіку з локальної мережі R2 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 102 permit ip 172.16.0.0 0.0.3.255 209.165.118.2 0.0.0.3.

Налаштування ACL 103 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 103 permit ip 172.16.4.0 0.0.3.255 209.165.118.2 0.0.0.3.

1.5.2 Налаштування ISAKMP

Налаштування політики криптографії ISAKMP 102 на маршрутизаторі R2 з використанням ключа «cisco». 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 102

> encryption aes

> authentication pre-share

> group 5

> exit

> crypto isakmp key cisco address 209.165.118.2.

Налаштування політики криптографії ISAKMP 103 на маршрутизаторі R3 з використанням ключа «cisco». 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 103

> encryption aes

> authentication pre-share

> group 5

> exit

> crypto isakmp key cisco address 209.165.118.2.

1.5.3 Створення перетворювача VPN-SET

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

Для цього необхідно ввести наступні команди (маршрутизатор R2):

– 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 R1_R2_Set esp-aes esp-sha-hmac

> crypto map R1_R2_Map 102 ipsec-isakmp

> description VPN connection R1_R2

> set peer 209.165.118.2

> set transform-set R1_R2_Set

> match address 102

> exit.

Для цього введемо наступні команди (маршрутизатор R3):

– 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 R1_R3_Set esp-aes esp-sha-hmac

> crypto map R1_R3_Map 103 ipsec-isakmp

> description VPN connection R1_R3

> set peer 209.165.118.2

> set transform-set R1_R3_Set

> match address 103

> exit.

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

Кінцевим налаштуванням мапи криптографії VPN-MAP є її прив'язка до вихідного інтерфейсу S0/0/0 на маршрутизаторі R2.

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 R1_R2_Map.

Кінцевим налаштуванням мапи криптографії VPN-MAP є її прив'язка до вихідного інтерфейсу S0/0/0 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 S0/0/0
- > crypto map R1_R3_Map.

1.6 Налаштування GRE тунелю через IPSec

Для початку налаштуємо тунель Tunnel 0 на R1 (тунель між локальними мережами R1 та R2).

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 tunnel 0
- > ip address 192.168.0.1 255.255.255.252
- > tunnel source s0/0/0
- > tunnel destination 64.100.13.2
- > tunnel mode gre ip
- > exit.

Потім налаштуємо тунель Tunnel 1 на R1 (тунель між локальними мережами R1 та 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 tunnel 1

```
> ip address 192.168.0.5 255.255.255.252  
> tunnel source s0/0/0  
> tunnel destination 64.102.46.2  
> tunnel mode gre ip  
> exit.
```

Налаштуємо зворотнє підключення, створимо тунелі на маршрутизаторах R2 та R3.

Для початку налаштуємо тунель Tunnel 0 на R2 (тунель між локальними мережами R1 та R2).

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 tunnel 0
```

```
> ip address 192.168.0.2 255.255.255.252
```

```
> tunnel source s0/0/0
```

```
> tunnel destination 209.165.118.2
```

```
> tunnel mode gre ip
```

```
> exit.
```

Далі налаштуємо тунель Tunnel 1 на R3 (тунель між локальними мережами R1 та 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 tunnel 1
```

```
> ip address 192.168.0.6 255.255.255.252
```

```
> tunnel source s0/0/0  
> tunnel destination 209.165.118.2  
> tunnel mode gre ip  
> exit.
```

Додатково описуємо маршрутизацію між віртуальними тунелями та реальними IP адресами.

R1:

- ip route 172.16.0.0 255.255.255.252 192.168.0.2;
- ip route 172.16.4.0 255.255.255.252 192.168.0.6.

R2:

- ip route 10.0.0.0 255.0.0.0 192.168.0.1.

R3:

- ip route 10.0.0.0 255.0.0.0 192.168.0.5.

1.7 Перевірка роботи тунелю GRE скрізь IPsec

Для перевірки достатньо виконати команду «Ping» від комп'ютерів PC1 та PC2 до сервера Main. Якщо пакети пройдуть успішно, це означає що GRE тунель налаштований і правильно працює. При цьому пакети між PC1 та PC2 проходити не будуть.

1.8 Зміст звіту

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

1.9 Контрольні питання

1. Визначення протоколу GRE.
2. Етапи побудови GRE-тунелю.
3. Принципи інкапсуляції при створенні тунелю GRE.

РЕКОМЕНДОВАНА ЛІТЕРАТУРА

1. Олифер В. Г. Компьютерные сети. Принципы, технологии, протоколы / В.Г. Олифер, Н.А.Олифер. // Учебник для вузов. – 5-е изд. – СПб.: Питер, 2016. – 992с.: ил.
2. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCENT/CCNA ICND1 100-101 / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 912 с. – ISBN 978-5-8459-1906-9.
3. Одом, Уэнделл. Официальное руководство Cisco по подготовке к сертификационным экзаменам CCNA ICND2 200-101: маршрутизация и коммутация / У. Одом. – акад. изд.: Пер. с англ. – М.; ООО “И. Д. Вильямс”, 2015. – 736 с. – ISBN 978-5-8459-1907-6.
4. Шапорін Р.О. Моделі та методи проектування комунікаційних систем комп'ютерних мереж масштабу підприємства [Текст]: автореф. дис... канд. техн. наук: 05.13.12 / Р.О.Шапорін ; Одеський національний політехнічний ун-т. - О., 2007. - 22 с.
5. Таненбаум Э. Компьютерные сети / Э. Таненбаум, Д.Уэзеролл. – 5-е изд. – СПб.: Питер, 2012. – 960 с.
6. Бакланов И.Г. NGN: принципы построения и организации. – М. : Эко–Трендз, 2008. – 400 с.
7. Гольдштейн А.Б. Технология и протоколы MPLS / А.Б.Гольдштейн, Б.С.Гольдштейн. – СПб.: БХВ, 2005. – 304 с.
8. Глотиков К. IMS (IP multimedia Subsystem). М.: Эко-трендз. 2009. – 100 с.
9. Гольдштейн Б.С. Сети связи. Учебник для вузов / Б.С. Гольдштейн, Н.А.Соколов, Г.Г.Яновский. – СПб. : БХВ, 2009. – 400 с.
10. Hucaby D. CCNP Routing and Switching SWITCH 300-115 Official Cert Guide / D. Hucaby. – 2nd Edition. – USA: Cisco Press, 2015. – 578 p.
11. Платунова С.М. Методы проектирования фрагментов компьютерной сети – СПб: НИУ ИТМО, 2012. – 51 с.