UNIVERSIDAD DE LAS FUERZAS ARMADAS-ESPE

SEDE SANTO DOMINGO DE LOS TSÁCHILAS

DEPARTAMENTO DE CIENCIAS DE LA COMPUTACIÓN - DCCO-SS

CARRERA DE INGENIERÍA EN TECNOLOGÍAS DE LA INFORMACIÓN

PERIODO	:	202450 mayo 2024 – septiembre 2024
ASIGNATURA	:	Seguridad Informática
TEMA	:	Laboratorio 4
ESTUDIANTE	:	Steeven Joel Riofrio Zambrano
NIVEL-PARALELO – NRC	:	7mo 17690
DOCENTE	:	Ing. Germán Rodríguez
FECHA DE ENTREGA	:	20 de Julio de 2024

SANTO DOMINGO – ECUADOR

2024

Contenido

Índice de figuras

1. Introducción

.

2. Objetivos

2.1. Objetivo general

.

2.2. Objetivos específicos

- .
-
-

3. Desarrollo

3.1. Elaboración del escenario

El diseño del escenario se lo hiso según la guía del laboratorio correspondiente

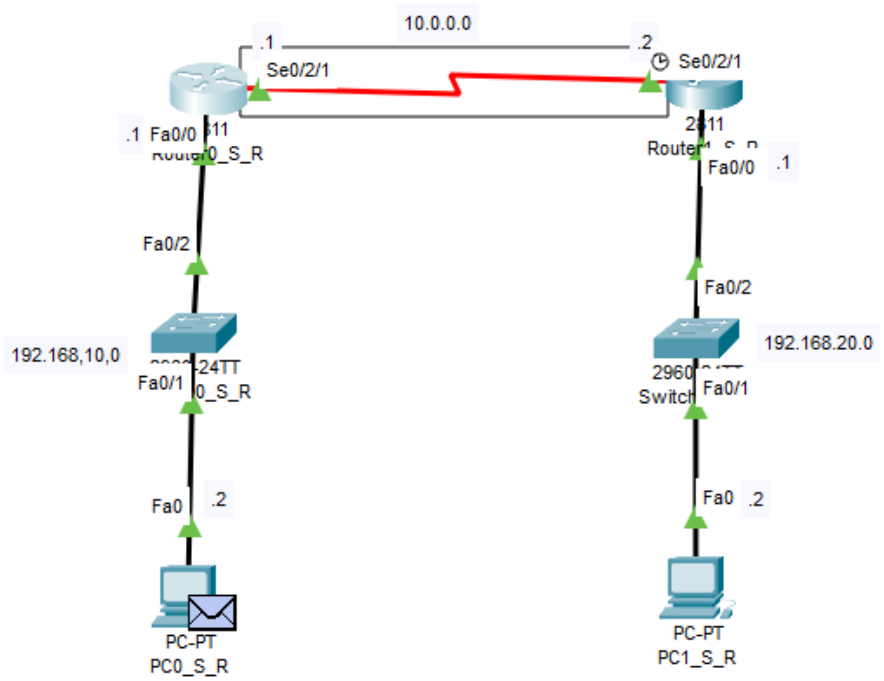

Figura 1 Topología

3.2. Configuración de IPs de los puertos del Router0_S_R

En el Router0_S_R,nos dirigimos a la sección config en la parte INTERFACE FastEthernet0/0 para asignarle la ip 192.168.10.1 con su respectiva Mask activando el puerto Port Status

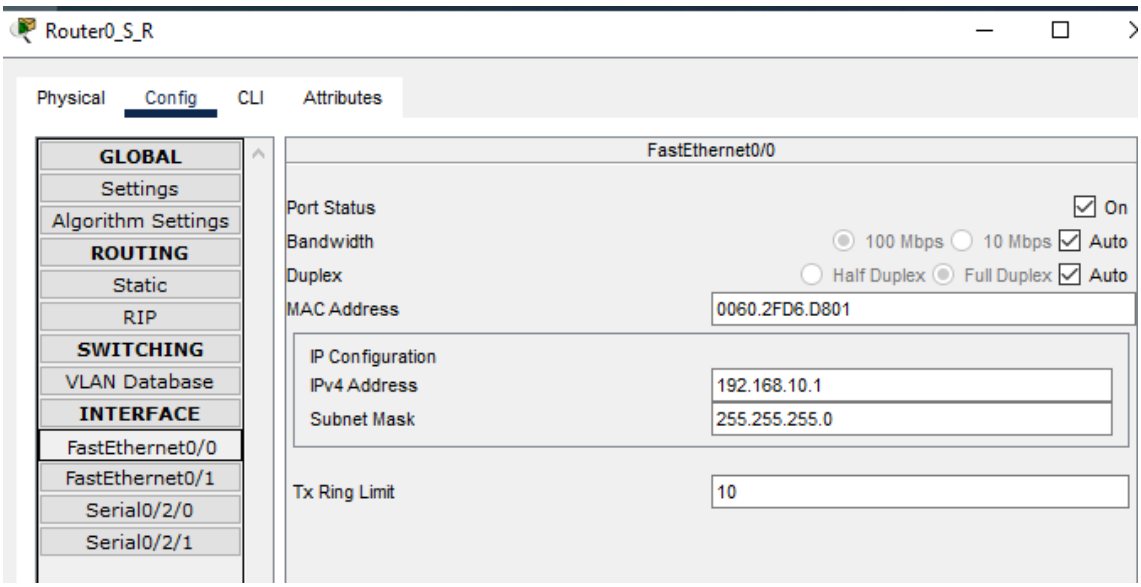

Figura 2 Configuración de IPs de los puertos del Router0_S_R

De igual manera en INTERFACE Serial0/2/1 para asignarle la ip 10.0.0.1 con su respectiva Mask activando el puerto Port Status

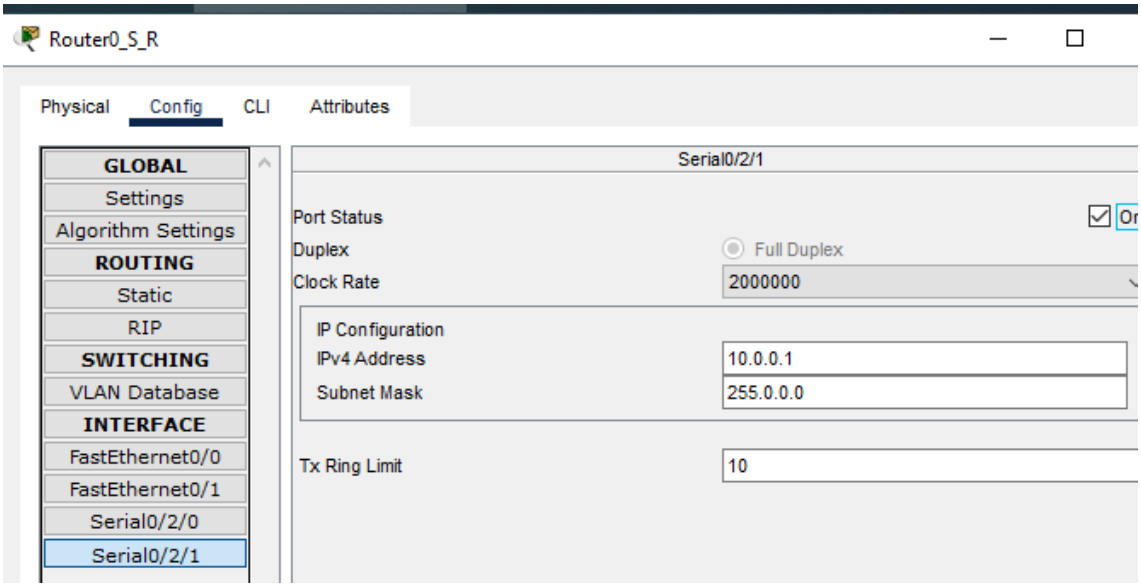

Figura 3 Configuración de IPs de los puertos del Router0_S_R

3.3. Configuración de IPs de los puertos del Router1_S_R

En el Router1_S_R,nos dirigimos a la sección config en la parte INTERFACE FastEthernet0/0 para asignarle la ip 192.168.20.1 con su respectiva Mask activando el puerto Port Status.

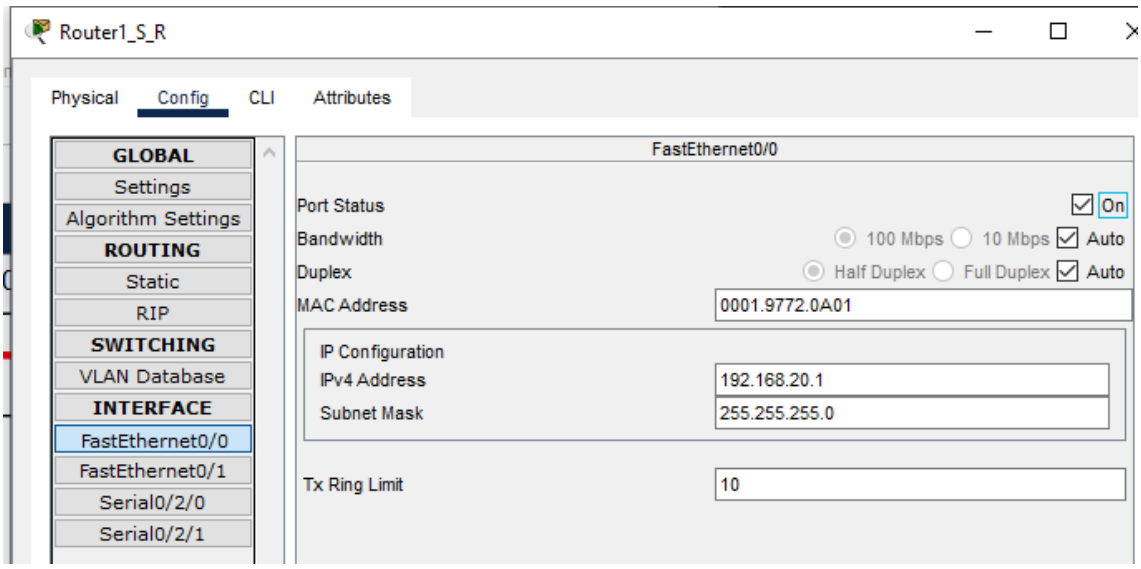

Figura 4 Configuración de IPs de los puertos del Router1_S_R

De igual manera en INTERFACE Serial0/2/1 para asignarle la ip 10.0.0.2 con su respectiva Mask activando el puerto Port Status

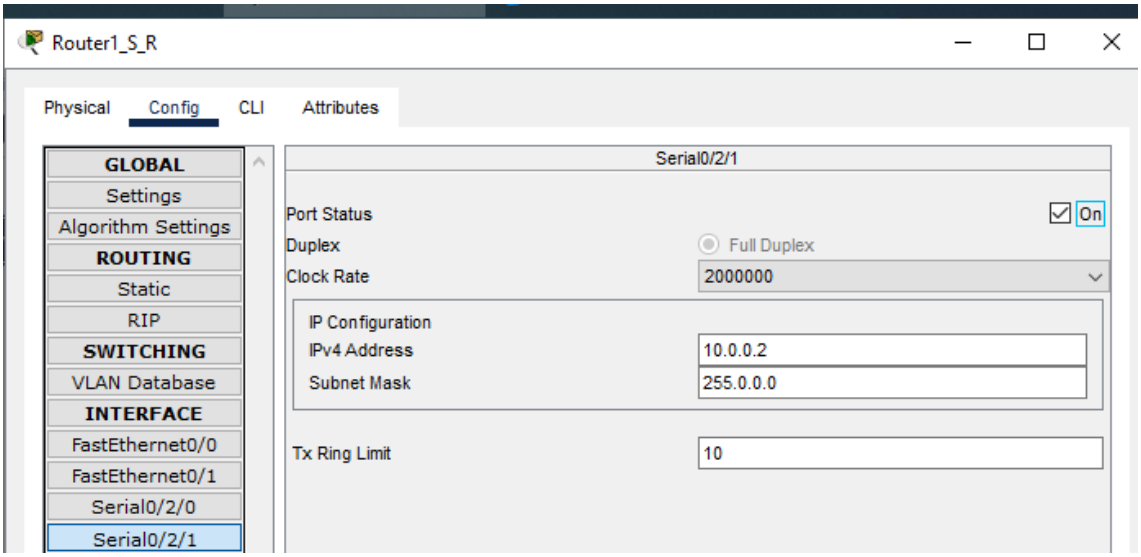

Figura 5 Configuración de IPs de los puertos del Router1_S_R

3.4. Asignación IP a la PC0

En PC0_S_R,nos dirigimos a la sección desktop en la parte IP Configuration para asignarle la ip 192.168.10.2 con su respectiva Mask y Gateway.

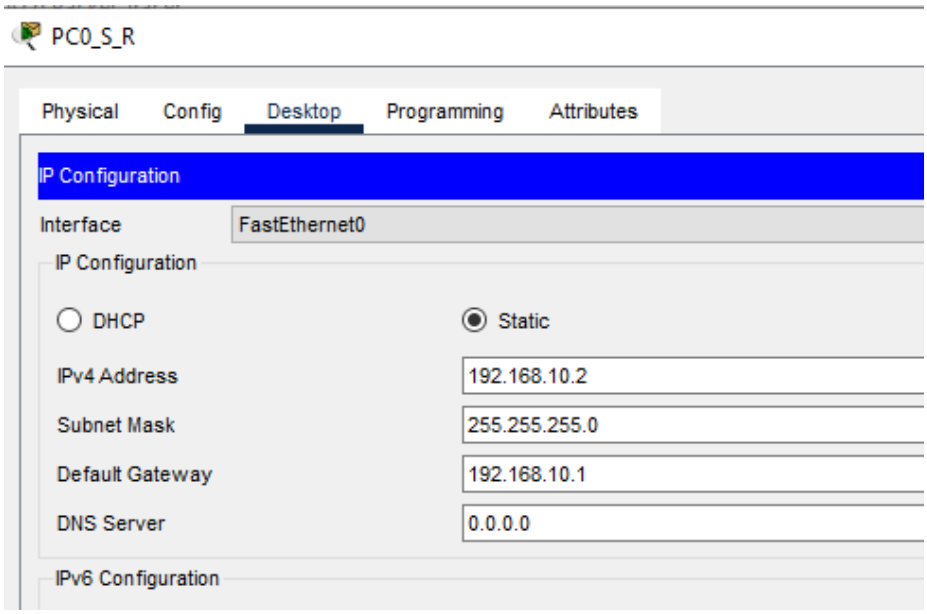

Figura 6 Asignación IP a las PCs

3.5. Asignación IP a la PC1

En PC1_S_R,nos dirigimos a la sección desktop en la parte IP Configuration para asignarle la ip 192.168.20.2 con su respectiva Mask y Gateway.

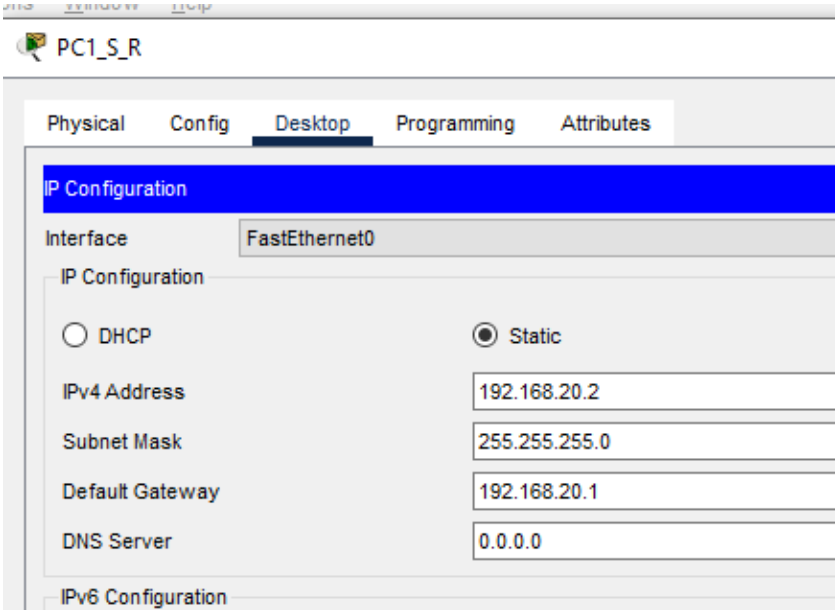

Figura 7 Asignación IP a las PCs

3.6. Protocolo de enrutamiento dinámico Rip

Para tener comunicación entre los 2 equipos utilizamos el protocolo de enrutamiento dinámico rip para poder enviar paquetes de la PC0 a la PC1 en el Router0_S_R en Config donde dice ROUTING RIP agregamos la network que son las redes más cercanas el router que según el escenario son 10.0.0.0 y la 192.168.10.0

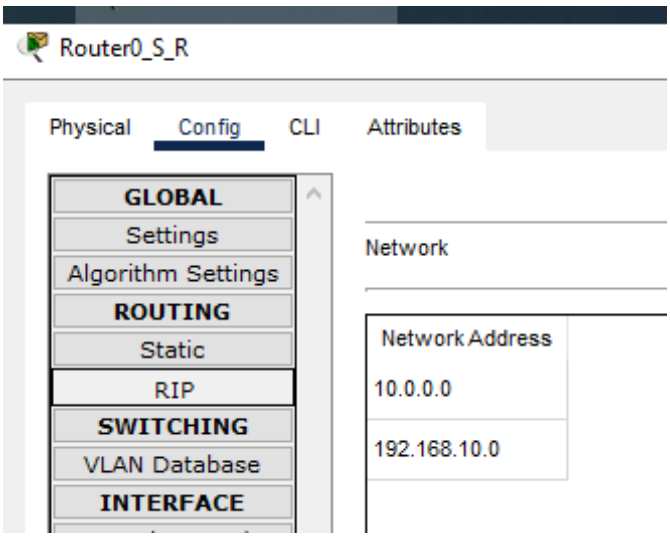

Figura 8 Enrutamiento dinámico Rip

Para tener comunicación entre los 2 equipos utilizamos el protocolo de enrutamiento dinámico rip para poder enviar paquetes de la PC0 a la PC1 en el Router1_S_R en Config donde dice ROUTING RIP agregamos la network que son las redes más cercanas el router que según el escenario son 10.0.0.0 y la 192.168.20.0

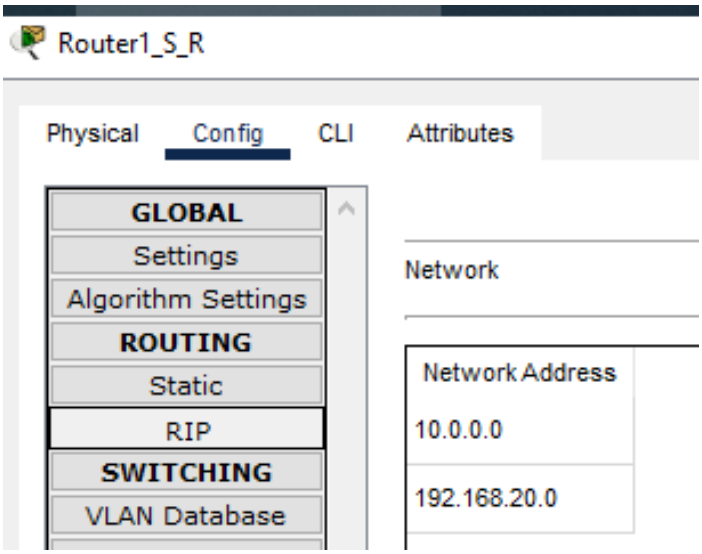

Figura 9 Enrutamiento dinámico Rip

3.7. Prueba de conexión ping

Como nos damos cuenta si se hace un ping de la la PC0_S_R a la Router1_S_R se muestra una prueba de conexión exitosa a un dispositivo con la dirección IP 10.0.0.2. El comando ping ha verificado que la comunicación entre ambos dispositivos es rápida y estable.

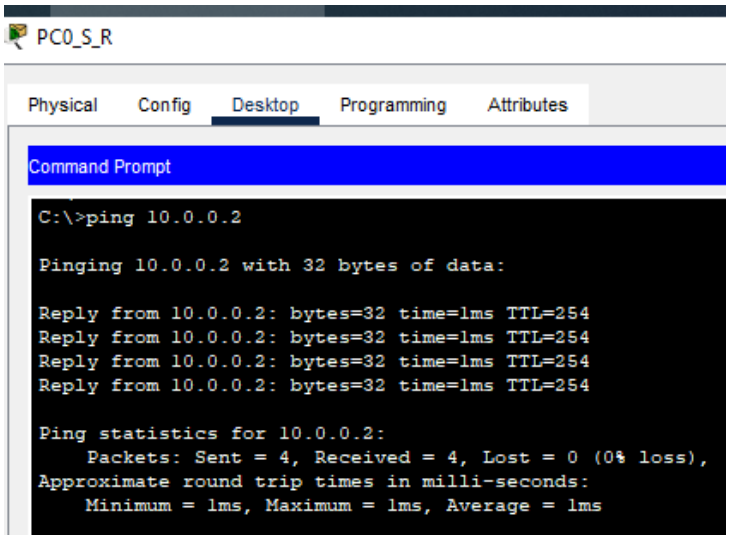

Figura 10 Comunicación de paquetes ping

De igual manera si se hace un ping de la la PC0_S_R a la PC1_S_R se muestra una prueba de conexión exitosa a un dispositivo con la dirección IP 192.168.20.2.El comando ping ha verificado que la comunicación entre ambos dispositivos es rápida y estable.

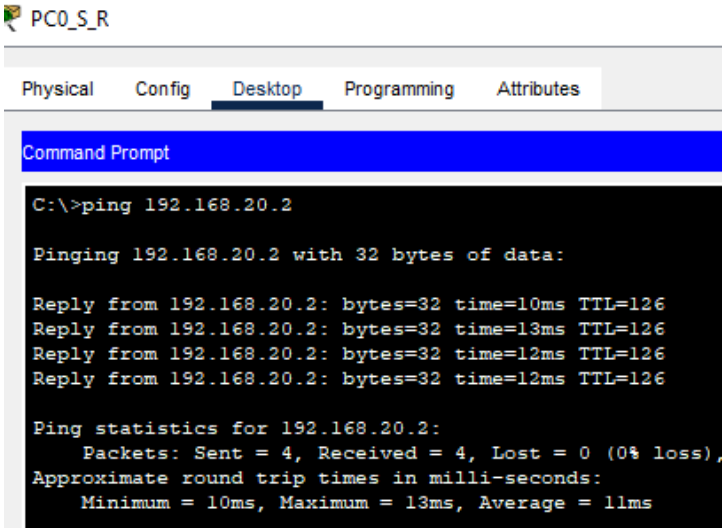

Figura 11 Comunicación de paquetes ping

3.8. Configuración de encriptación mediante de protocolo IPSEC e ISAKMP del Router0_S_R

Para mostrar la configuración aplicamos con el comando show run, se puede ver que se establece una política ISAKMP que es el que define cómo se asegurarán las negociaciones del túnel VPN.

`encr aes 256` usa un cifrado AES con una clave de 256 bits para proteger la comunicación, `authentication pre-share` se utiliza una clave precompartida para la autenticación y group 2 que especifica el grupo de Diffie-Hellman que ayuda al intercambio de claves

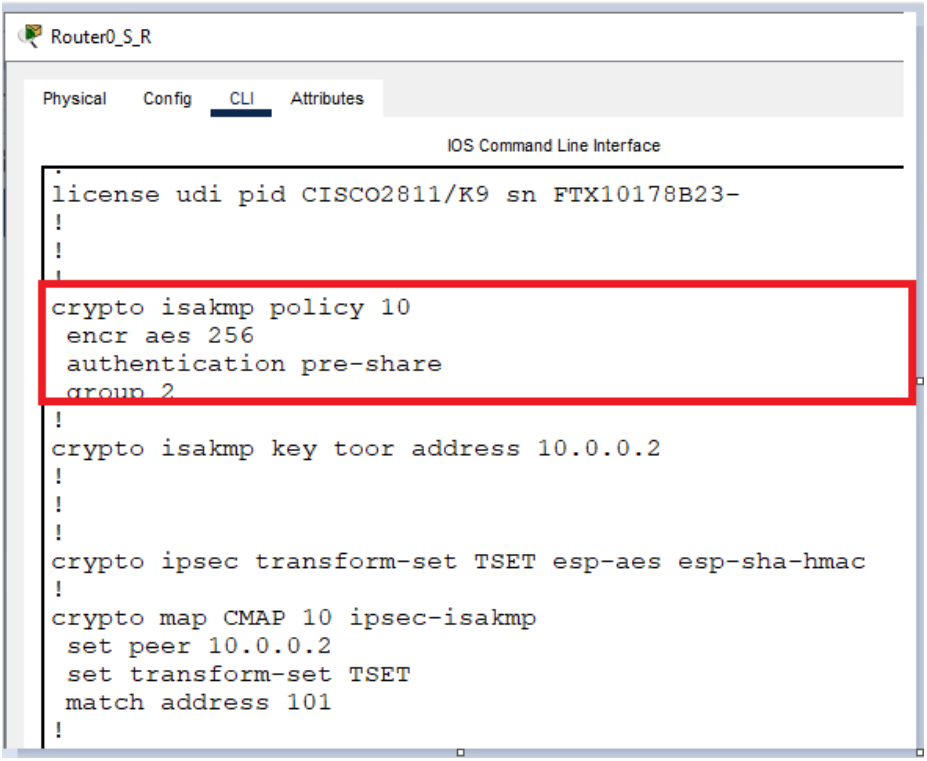

Figura 12 Política ISAKMP

Se define la clave precompartida `toor` que se usará para la autenticación del peer con la dirección IP 10.0.0.2.

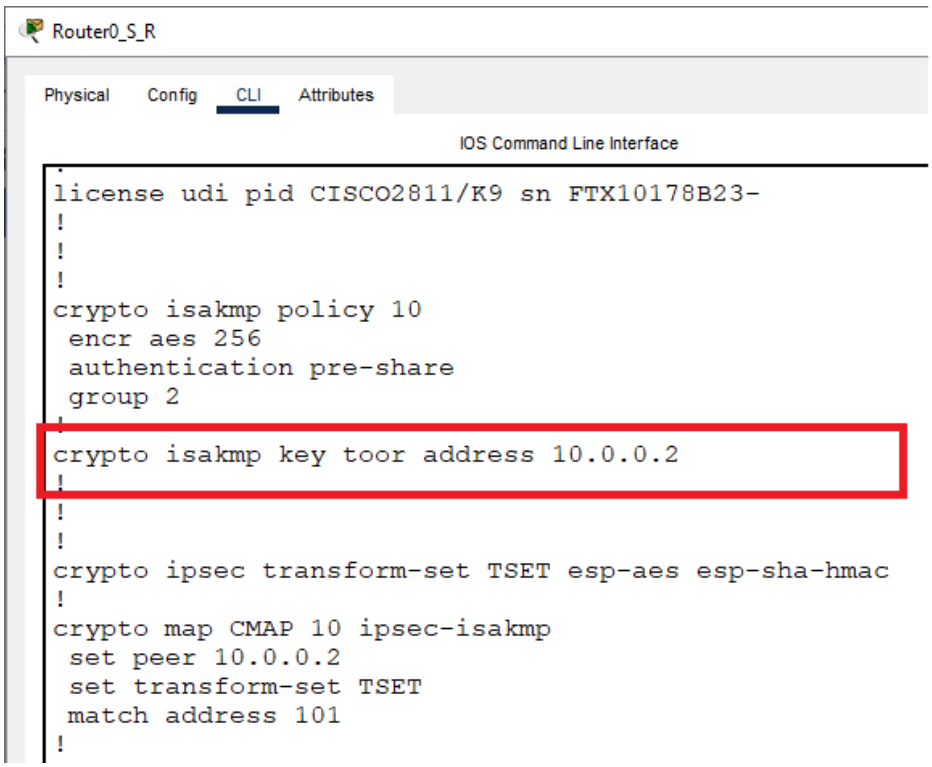

Figura 13 Clave Precompartida

Se asigna el conjunto de transformaciones que especifican cómo se cifrarán y autenticará el tráfico de datos, con `esp-aes` especifica que se usará AES para el cifrado del paquete esp y el `esp-sha-hmac` con el que se usará SHA para la autenticación HMAC

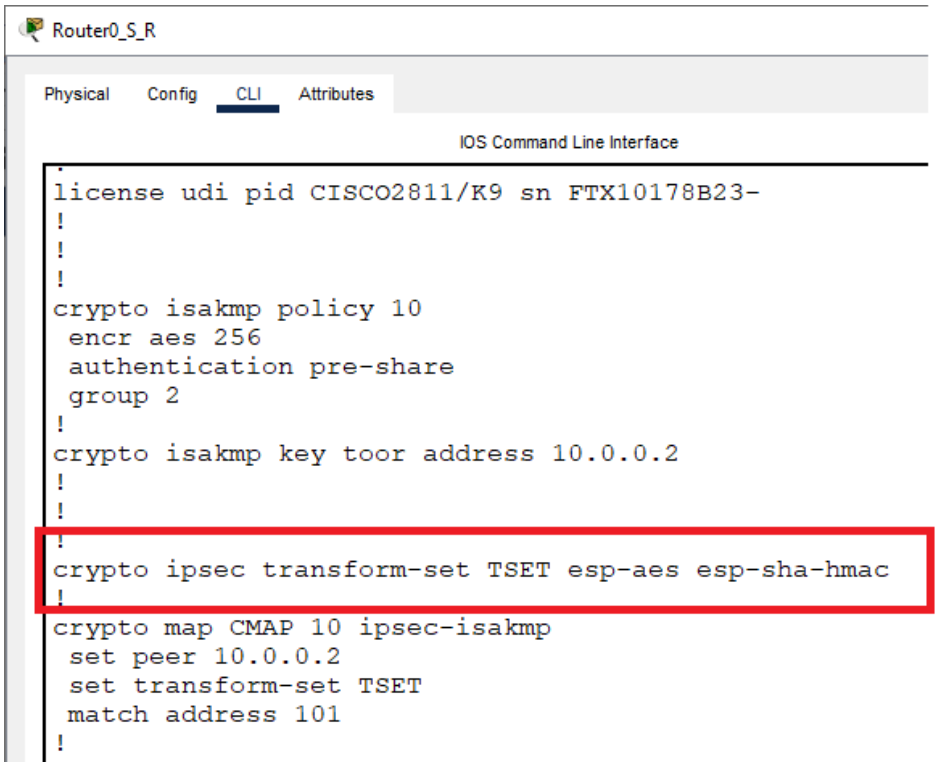

Figura 14 Conjunto de Transformaciones IPSec

Se crea un mapa de criptografía aplicando la configuracion IPSec a las interfaces designadas, set peer 10.0.0.2 muestra la dirección IP del peer con el que se establecerá el túnel, set transform-set TSET une el conjunto de transformaciones TSET con este mapa de criptografía y match address 101 muestra la lista de acceso 101 para determinar qué tráfico se debe cifrar y enviar a través del túnel IPSec.

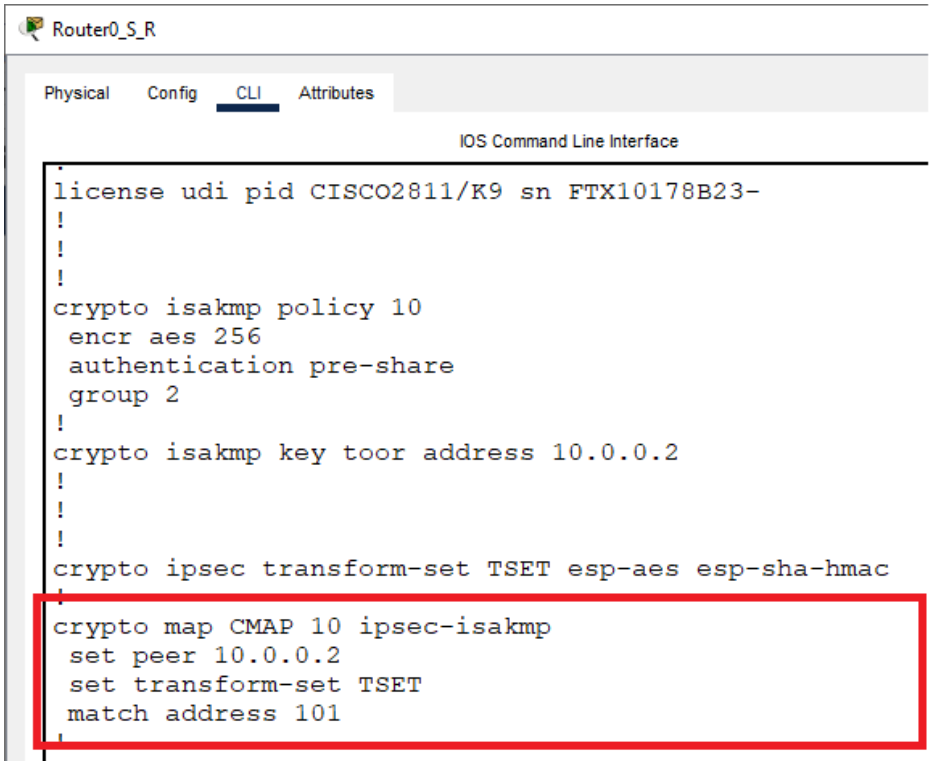

Figura 15 Mapa de Criptografía

Muestra la lista de acceso 101 permite tráfico IP entre las redes 192.168.10.0/24 y 192.168.20.0/24 para cifrado IPSec.

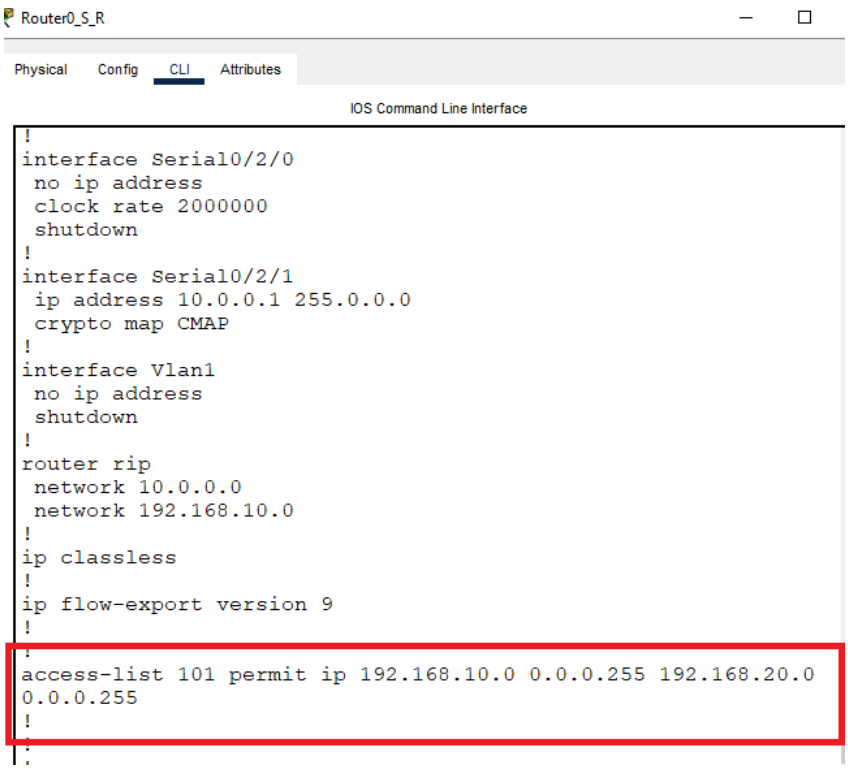

Figura 16 Lista de acceso 101

Por ultimo la interfaz Serial0/2/1 se le aplica el mapa de criptografía CMAP para proteger el tráfico.

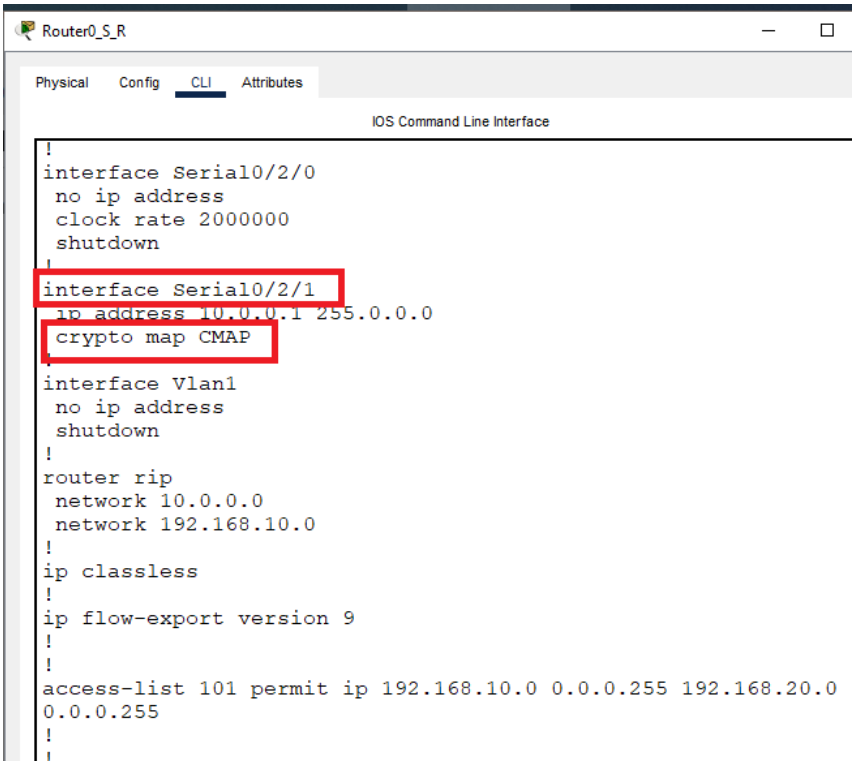

Figura 17 Mapa de criptografía CMAP

3.9. Configuración de encriptación mediante de protocolo IPSEC e ISAKMP del Router0_S_R

Para mostrar la configuración aplicamos con el comando show run, se puede ver que se establece una política ISAKMP que es el que define cómo se asegurarán las negociaciones del túnel VPN.

encr aes 256 usa un cifrado AES con una clave de 256 bits para proteger la comunicación, authentication pre-share se utiliza una clave precompartida para la autenticación y group 2 que especifica el grupo de Diffie-Hellman que ayuda al intercambio de claves

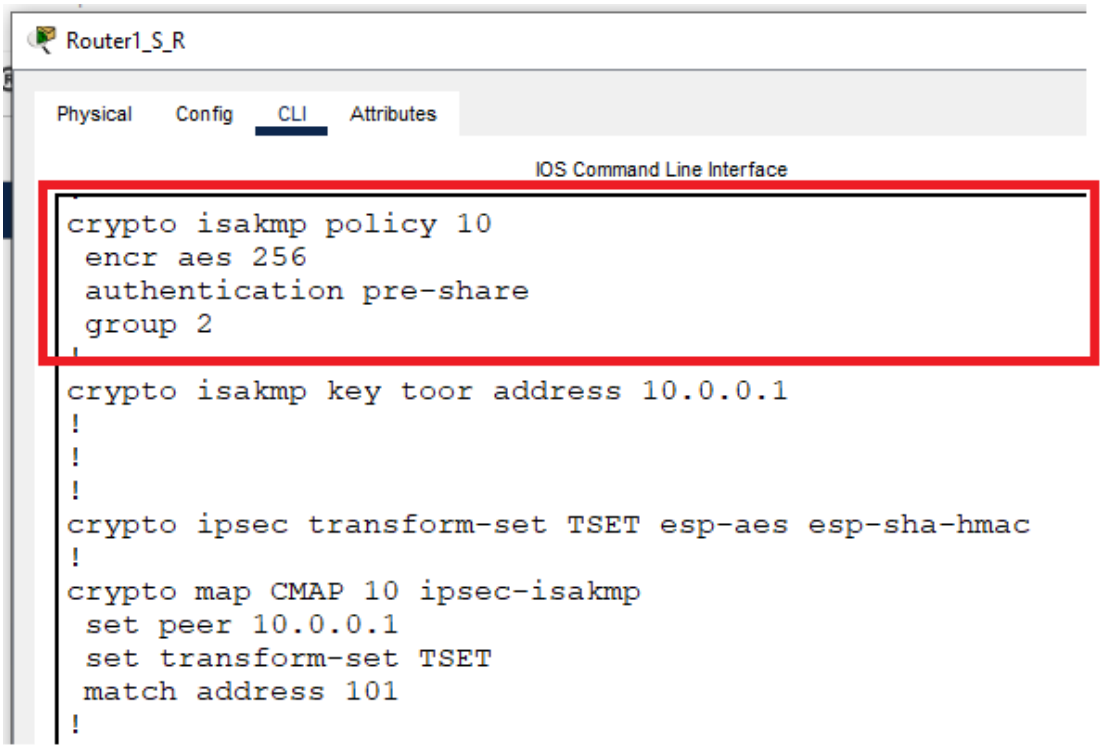

Figura 18 Política ISAKMP

Se define la clave precompartida `toor` que se usará para la autenticación del peer con la dirección IP 10.0.0.1

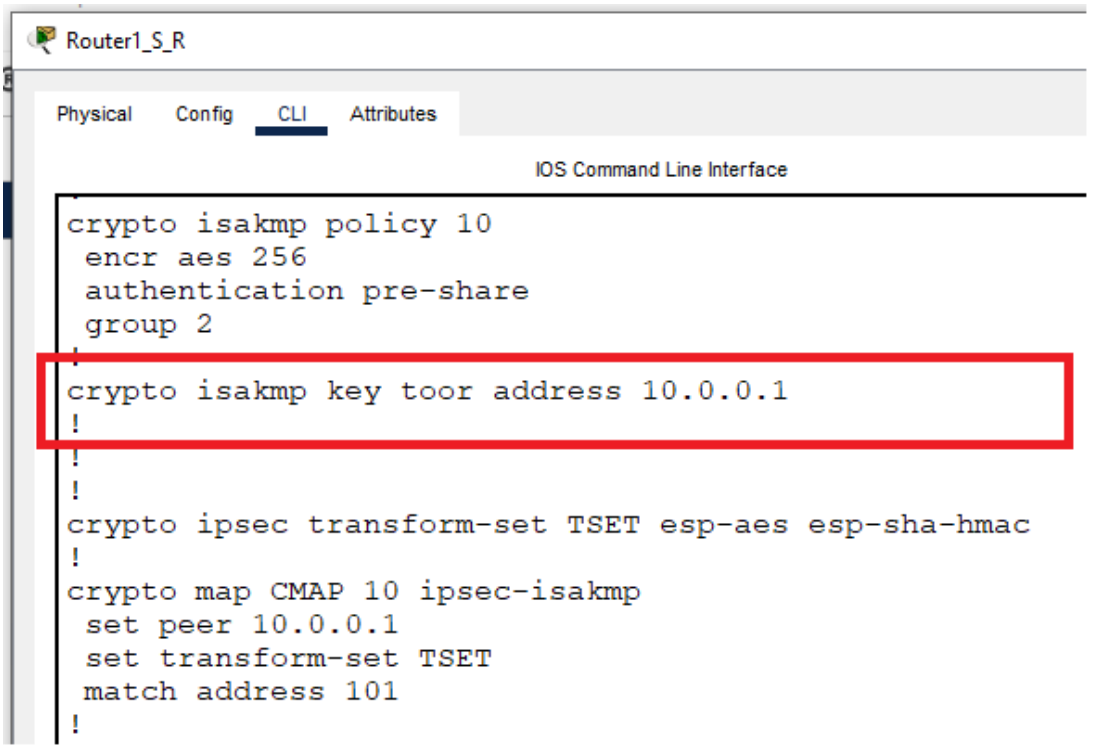

Figura 19 Clave Precompartida

Se asigna el conjunto de transformaciones que especifican cómo se cifrarán y autenticará el tráfico de datos, con `esp-aes` especifica que se usará AES para el cifrado del paquete esp y el `esp-sha-hmac` con el que se usará SHA para la autenticación HMAC

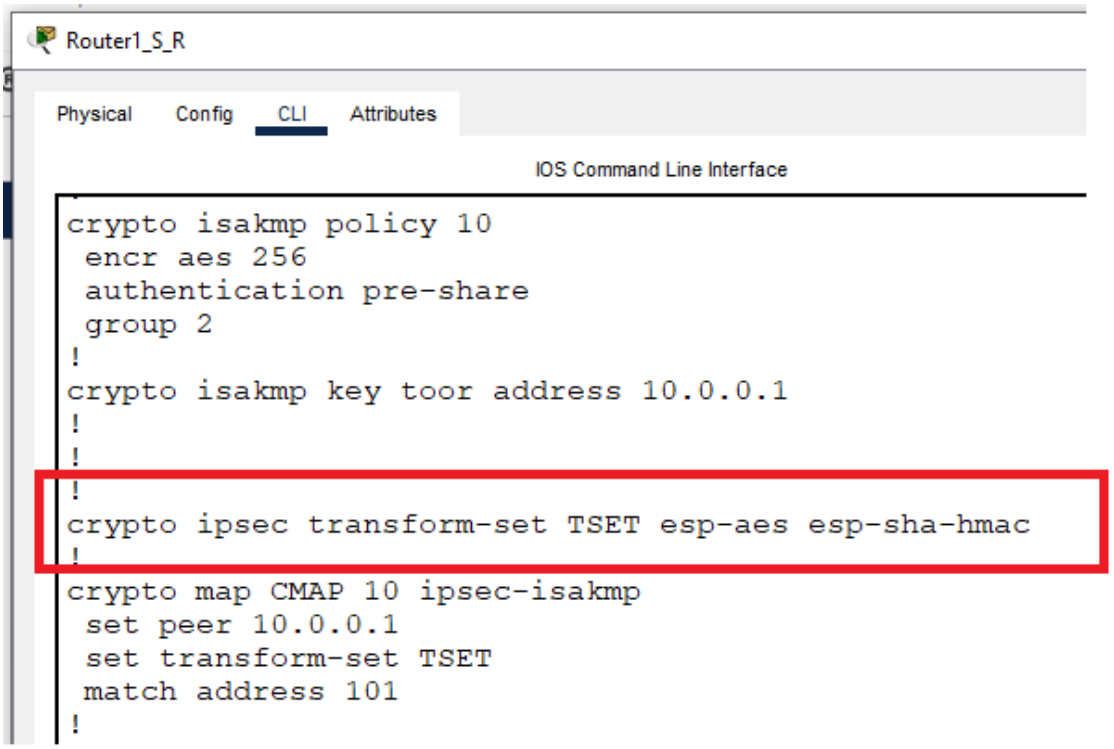

Figura 20 Conjunto de Transformaciones IPSec

Se crea un mapa de criptografía aplicando la configuracion IPSec a las interfaces designadas, set peer 10.0.0.1 muestra la dirección IP del peer con el que se establecerá el túnel, set transform-set TSET une el conjunto de transformaciones TSET con este mapa de criptografía y match address 101 muestra la lista de acceso 101 para determinar qué tráfico se debe cifrar y enviar a través del túnel IPSec.

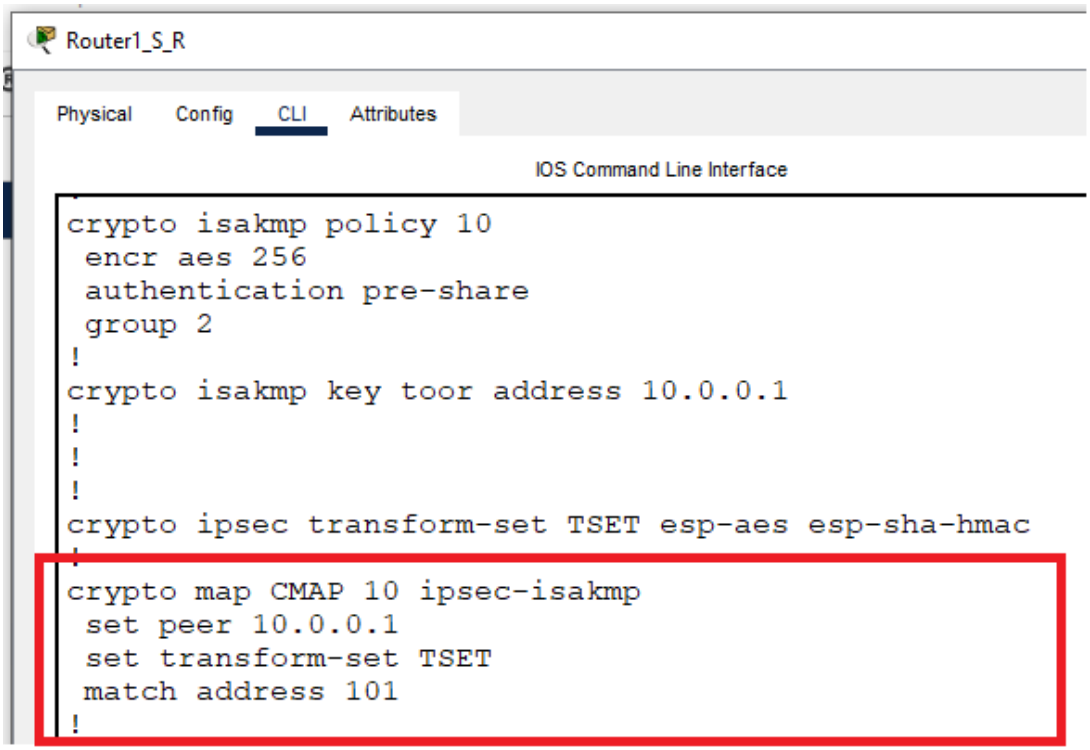

Figura 21 Mapa de Criptografía

Muestra la lista de acceso 101 permite tráfico IP entre las redes 192.168.20.0/24 y 192.168.10.0/24 para cifrado IPSec.

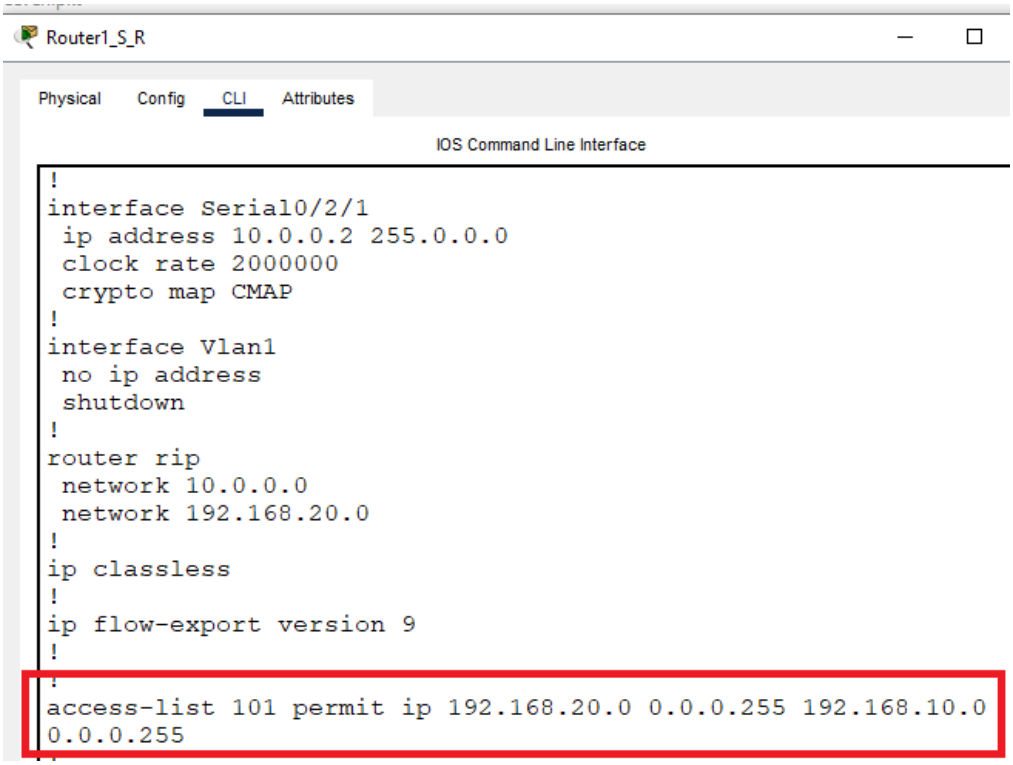

Figura 22 Lista de acceso 101

Por último la interfaz Serial0/2/1 se le aplica el mapa de criptografía CMAP para proteger el tráfico.

Figura 23 Mapa de criptografía CMAP

3.10. Verificación de pruebas mediante el protocolo ICMP

Como resultado vemos una simulación de una red básica en donde permite visualizar el flujo de paquetes de datos entre estos equipos, utilizando protocolos como ICMP y RIP como parte de enrutamiento.

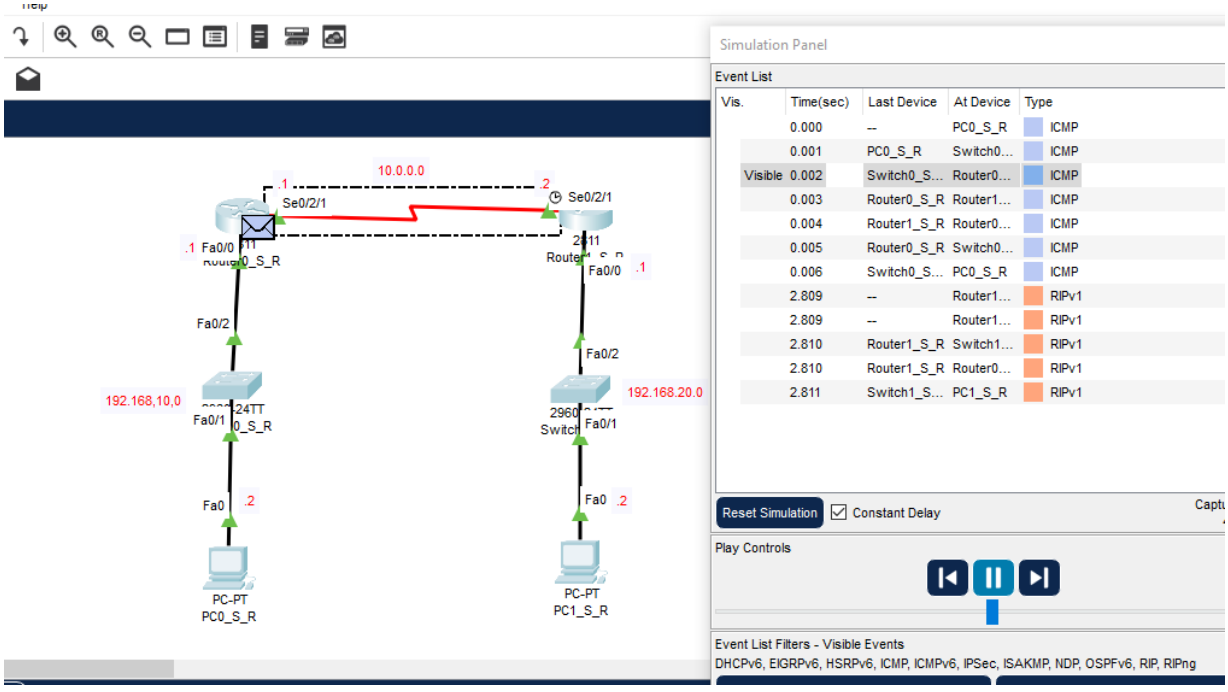

Figura 24 Verificación de pruebas mediante el protocolo ICMP

3.11. Actividad adicional

4. Conclusiones

5. Recomendación