Instituto Politécnico Nacional

Escuela Superior de Cómputo



**Nombre**: Garibay Huerta Valery Viridiana

**Grupo**: 3CM8

**Profesora**: Henestrosa Carrasco Leticia

**Asignatura**: Administración de servicios de red

**Práctica no. 2**

**Protocolo RIPv2 con SSH**

**INTRODUCCIÓN**

En esta práctica se pusieron a prueba nuestros conocimientos de redes l y de investigación, así como recordar los protocolos que se habían usado, como RIP, el uso de las contraseñas, telnet, pero sobre todo SSH. Así mismo, la segunda práctica de la asignatura pretende introducir al alumno en las redes de computadores de forma práctica usando Packet Tracer y dándole continuidad a la primera práctica, ya que solo se detectó el error de las versiones de RIP, ya que con VLSM solo se puede utilizar la segunda versión, así mismo, se introdujo SSH.

SSH o Secure Shell, es un protocolo de administración remota que le permite a los usuarios controlar y modificar sus servidores remotos a través de Internet. El servicio se creó como un reemplazo seguro para el Telnet sin cifrar y utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada. Proporciona un mecanismo para autenticar un usuario remoto, transferir entradas desde el cliente al host y retransmitir la salida de vuelta al cliente.

Cualquier usuario de Linux o macOS puede usar SSH en su servidor remoto directamente desde la ventana del terminal. Los usuarios de Windows pueden aprovechar los clientes SSH como Putty, ya que se puede ejecutar comandos shell de la misma manera que lo harías si estuvieras operando físicamente el equipo remoto.

La ventaja significativa ofrecida por SSH sobre sus predecesores es el uso del cifrado para asegurar la transferencia segura de información entre el host y el cliente. Host se refiere al servidor remoto al que estás intentando acceder, mientras que el cliente es el equipo que estás utilizando para acceder al host. Hay tres tecnologías de cifrado diferentes utilizadas por SSH:

1. **Cifrado simétrico:** El cifrado simétrico es una forma de cifrado en la que se utiliza una clave secreta tanto para el cifrado como para el descifrado de un mensaje, tanto por el cliente como por el host. Efectivamente, cualquiera que tenga la clave puede descifrar el mensaje que se transfiere. Se llama clave compartida (shared key) o cifrado secreto compartido. Normalmente sólo hay una clave que se utiliza, o a veces un par de claves donde una clave se puede calcular fácilmente con la otra clave.
2. **Cifrado asimétrico :** A diferencia del cifrado simétrico, el cifrado asimétrico utiliza dos claves separadas para el cifrado y el descifrado. Estas dos claves se conocen como la clave pública (public key) y la clave privada (private key). Juntas, estas claves forman el par de claves pública-privada (public-private key pair).
3. **Hashing:** El hashing unidireccional es otra forma de criptografía utilizada en Secure Shell Connections. Las funciones de hash unidireccionales difieren de las dos formas anteriores de encriptación en el sentido de que nunca están destinadas a ser descifradas. Generan un valor único de una longitud fija para cada entrada que no muestra una tendencia clara que pueda explotarse. Esto los hace prácticamente imposibles de revertir.

**OBJETIVO**

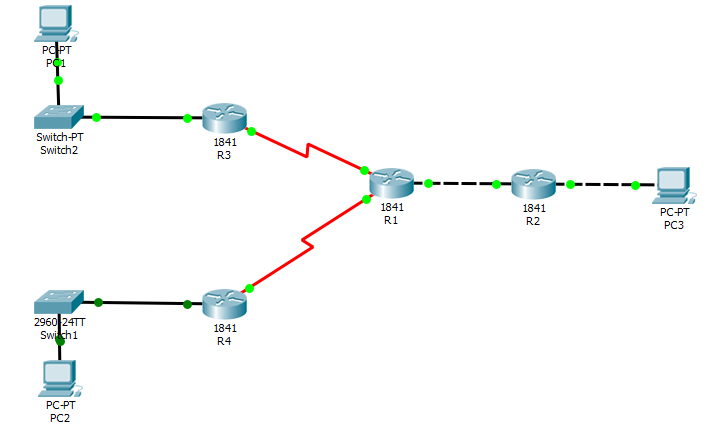


Imagen 1.1

Con base en la imagen 1.1 aplicar los siguiente:

* PROTOCOLO RIPv2
* VLSM
* NOMBRES DE HOST
* APLICAR CONTRASEÑAS
* Usar SSH
* PROBAR CONECTIVIDAD

**DESARROLLO**

Una vez identificada que RIP versión 1 no se podía implementar con el Subneteo VLSM (VLSM Subnetting), se tuvo que poner los comandos de la imagen 1.1 para poder implementar RIP v2 en todos los routers.

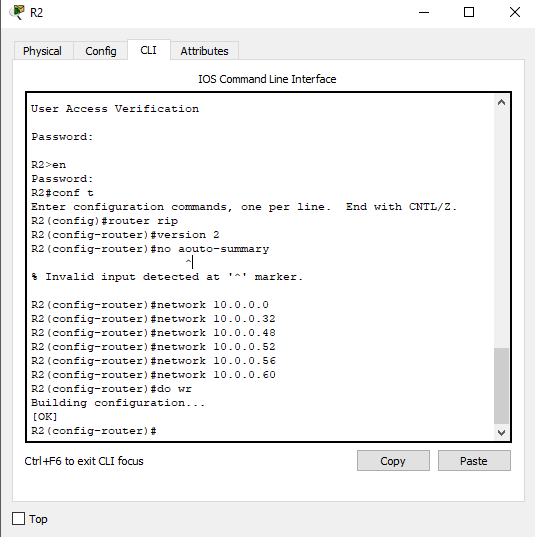


Imagen 1.1

Posteriormente se realizaron pruebas exitosas como se muestra en la figura 1.2 mandando paquetes entre todos los PC para ver si el RIP v2 estaba funcionando correctamente.

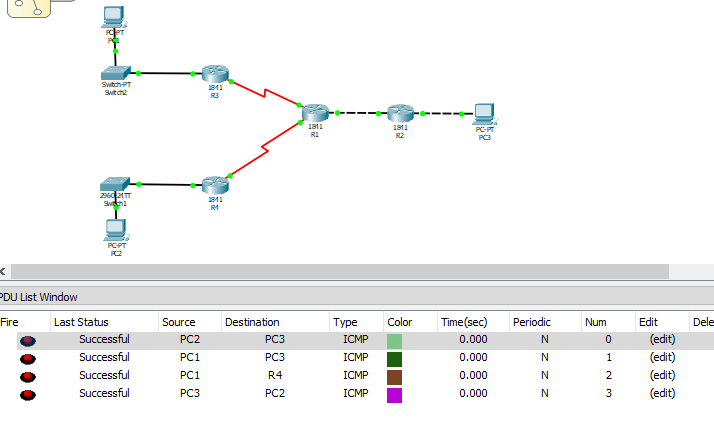


Imagen 1.2

Una vez teniendo las pruebas exitosas se paso a implementar los SSH en todos los routers con los siguientes comandos que se muestran en la imagen 1.3

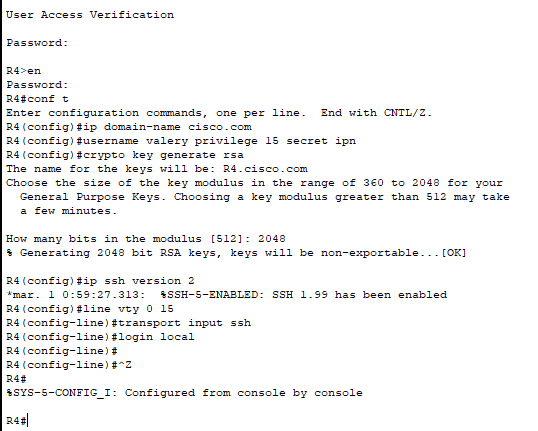
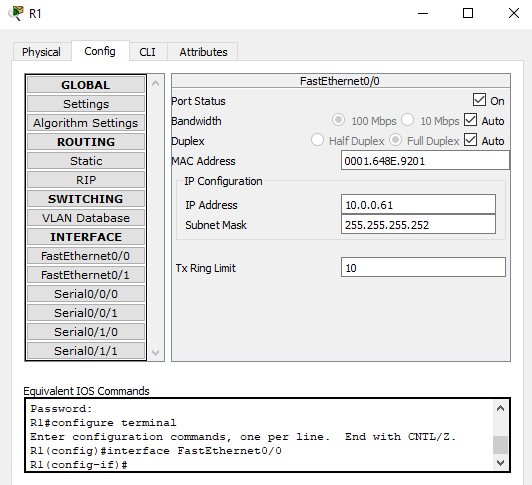
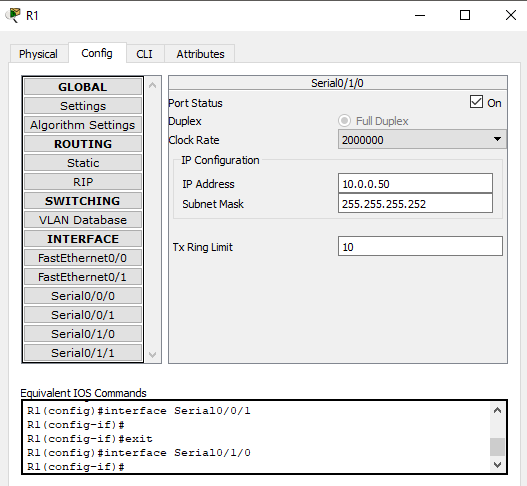
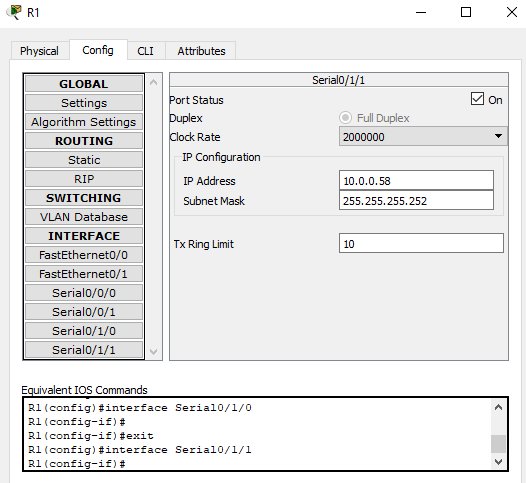


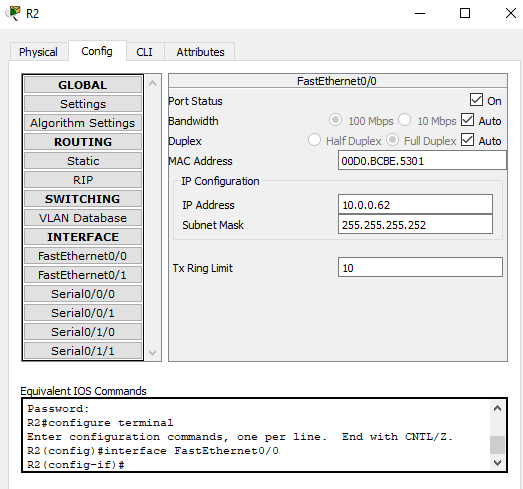
Imagen 1.3

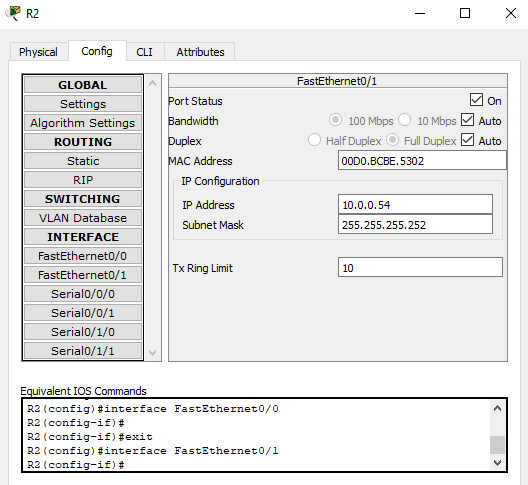
Las contraseñas y los nombres de los routers, así como las IP se configuraron en la práctica no. 1

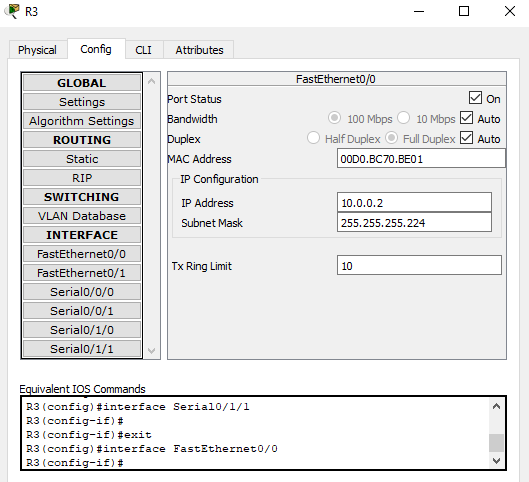


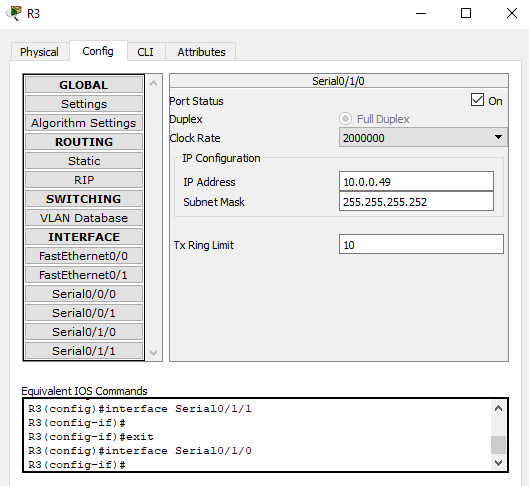


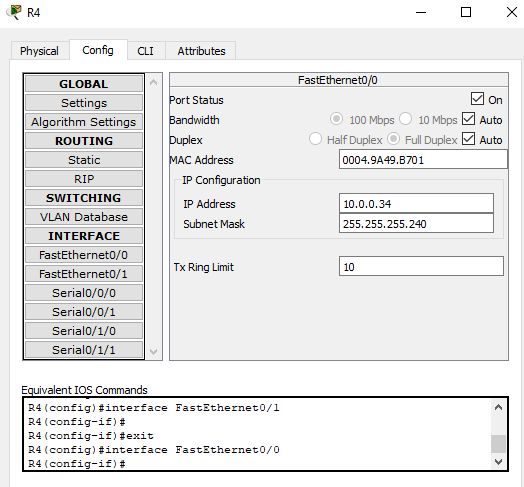


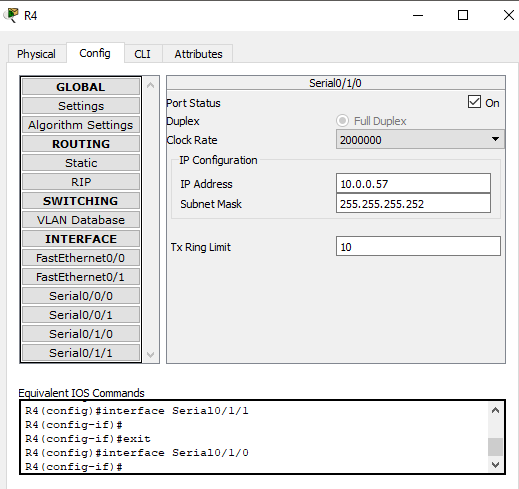




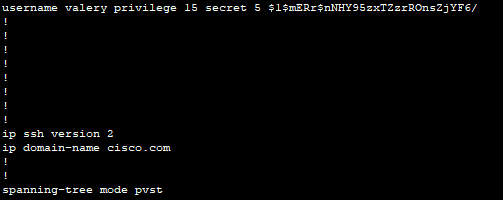
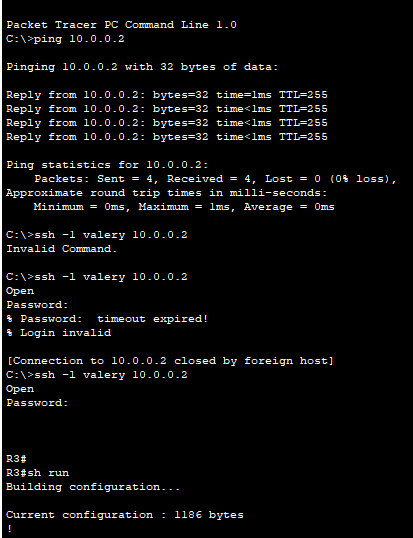








Por último, en consola se verifico todo el SSH de varios routers exitosamente, como se muestra en la figura 1.4, ya que primero se realizó un ping y posterior el ssh de la misma dirección.



**CONCLUSIONES**

En esta práctica me quedo más claro el protocolo RIP, ya que modifiqué mi error de la práctica 1 y entendí el porque no se podían pasar los paquetes, además pude darme cuenta que SSH es muchísimo mas seguro que telnet, ya que utiliza técnicas criptográficas para garantizar que todas las comunicaciones hacia y desde el servidor remoto sucedan de manera encriptada.

**BIBLIOGRAFIA O REFERENCIAS**

[1] B.Hill, “Manual de referencia CISCO.”McGraw-Hill,pp.631-700,2002.

[2] Routing Information Protocol, RFC1058,Jun 1988

[3] Cisco Networking Academy, “Packet Tracer: Configuración de SSH”, 2014.