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

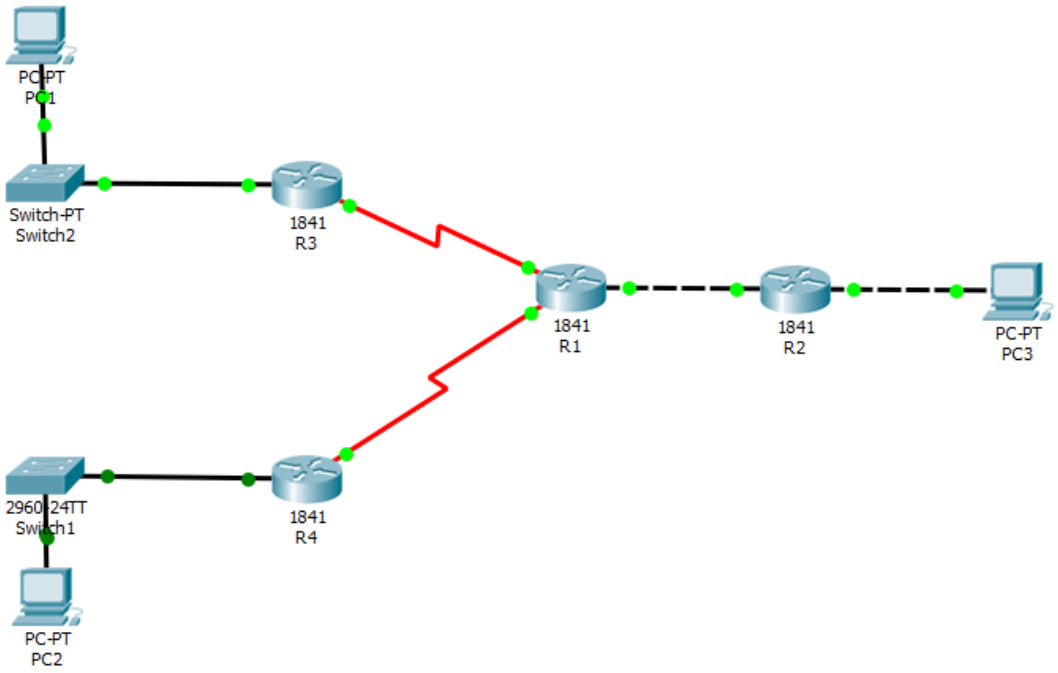


Imagen 1.1

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.

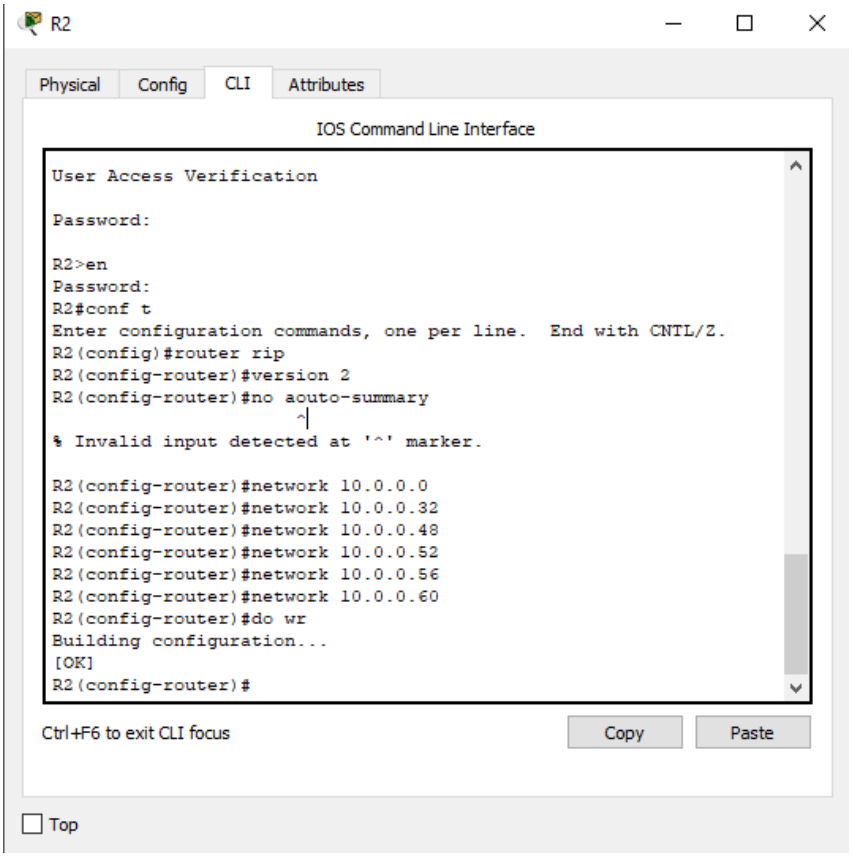


Imagen 1.1

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.

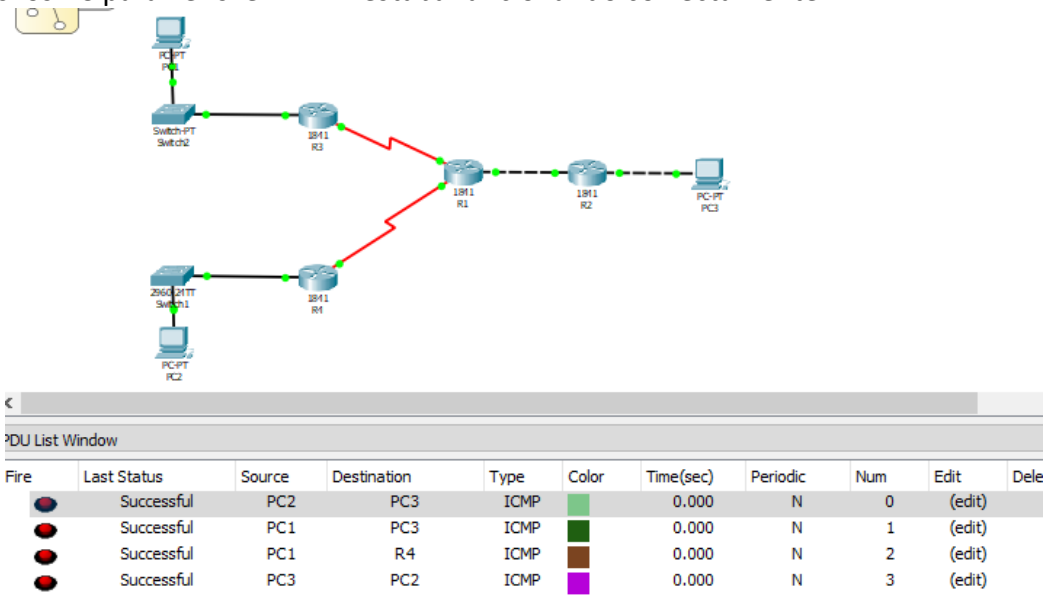


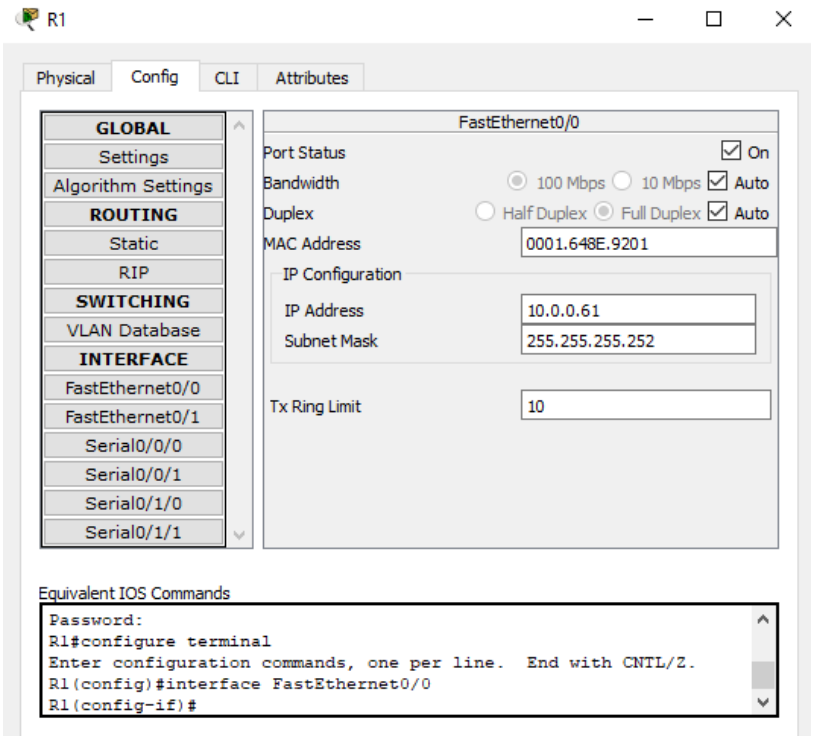
Imagen 1.2

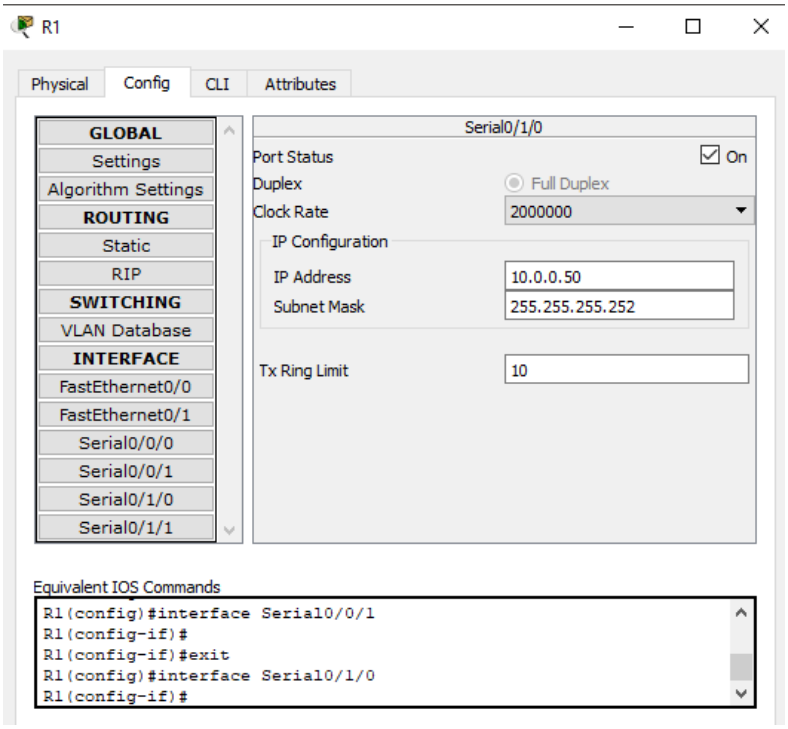
Una vez teniendo las pruebas exitosas se paso a implementar los SSH en todos los routers con los siguientes comandos que se muestran en la imagen 1.3

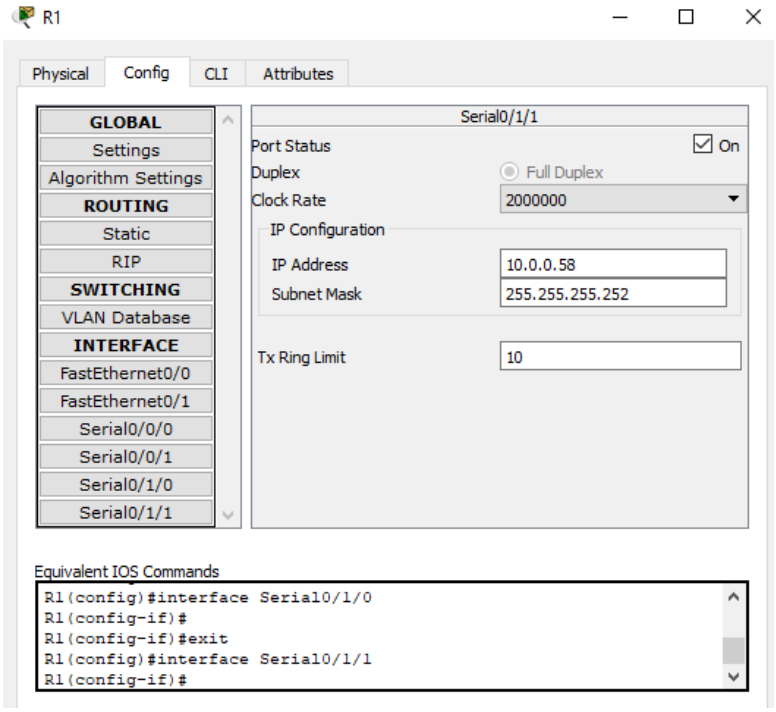
```
User Access Verification

Password:

R4>en
Password:
R4#conf t
Enter configuration commands, one per line.  End with CNTL/Z.
R4(config)#ip domain-name cisco.com
R4(config)#username valery privilege 15 secret ipn
R4(config)#crypto key generate rsa
The name for the keys will be: R4.cisco.com
Choose the size of the key modulus in the range of 360 to 2048 for your
  General Purpose Keys. Choosing a key modulus greater than 512 may take
  a few minutes.

How many bits in the modulus [512]: 2048
% Generating 2048 bit RSA keys, keys will be non-exportable...[OK]

R4(config)#ip ssh version 2
*mar. 1 0:59:27.313:  %SSH-5-ENABLED: SSH 1.99 has been enabled
R4(config)#line vty 0 15
R4(config-line)#transport input ssh
R4(config-line)#login local
R4(config-line)#
R4(config-line)#^Z
R4#
%SYS-5-CONFIG_I: Configured from console by console

R4#
```

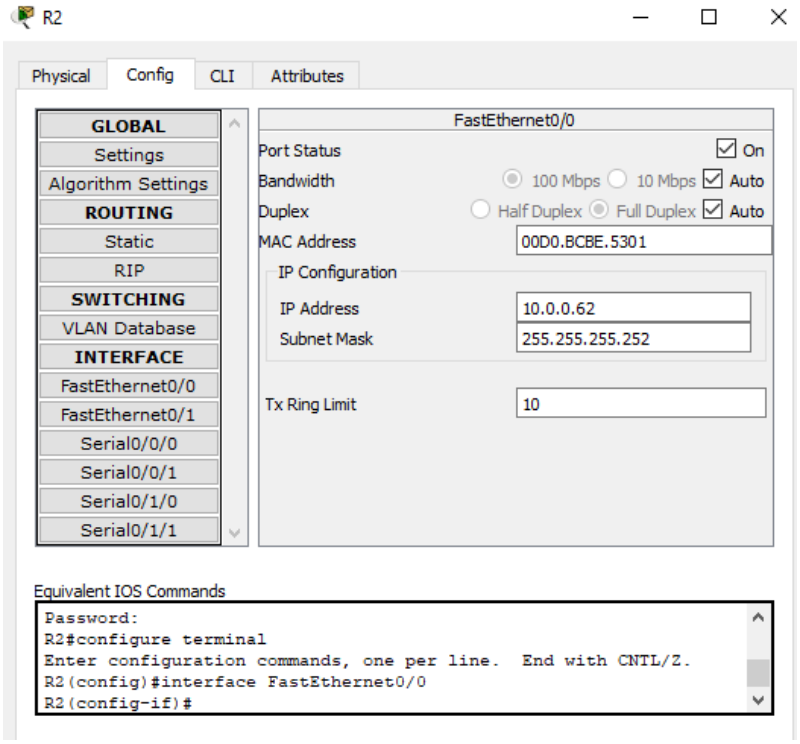
Imagen 1.3

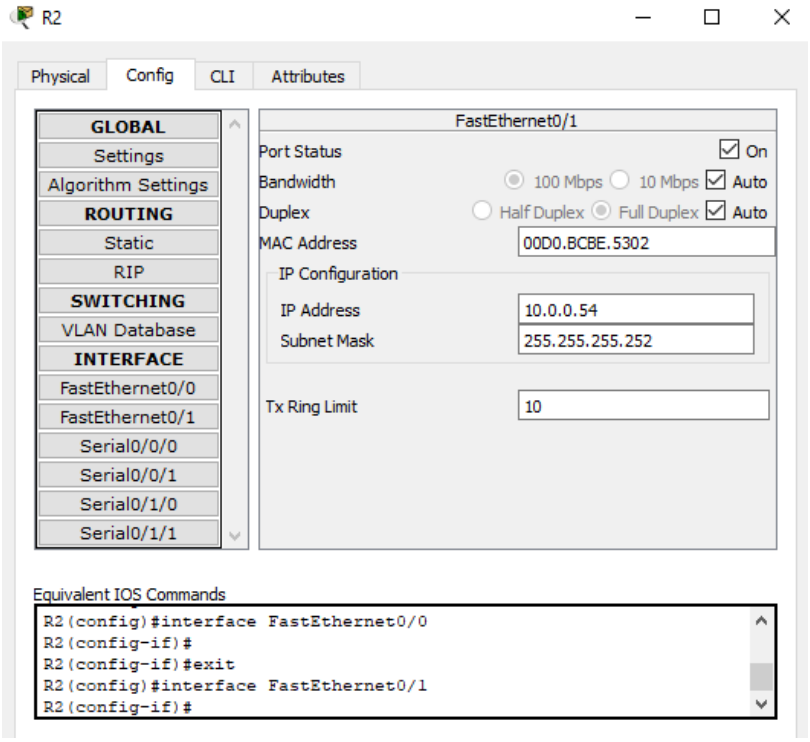
Las contraseñas y los nombres de los routers, así como las IP se configuraron en la práctica no. 1

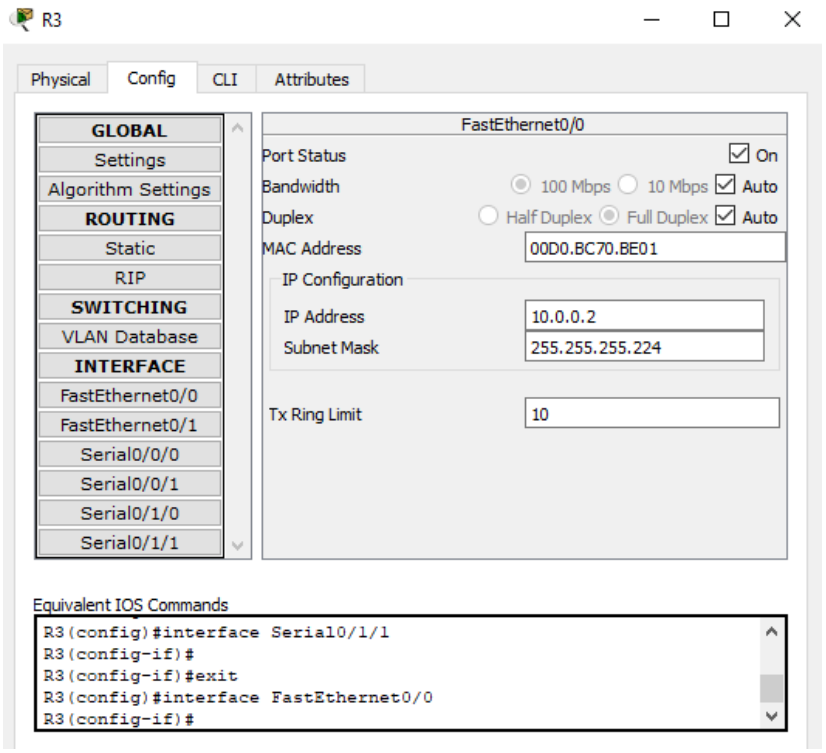


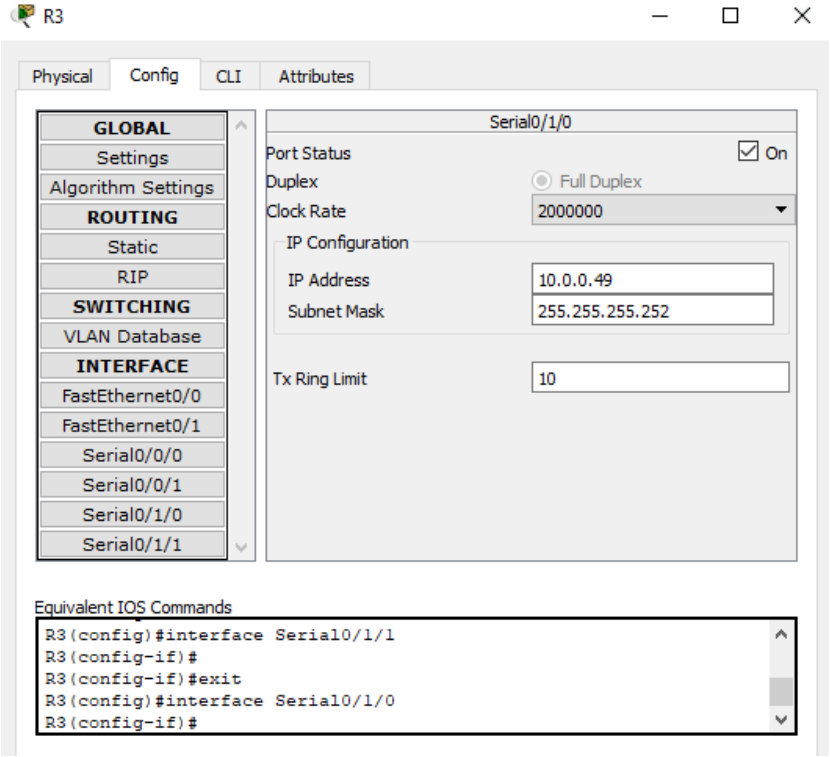

R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
10.0.0.50
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
R1(config)#interface Serial0/0/1
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/0
R1(config-if)#

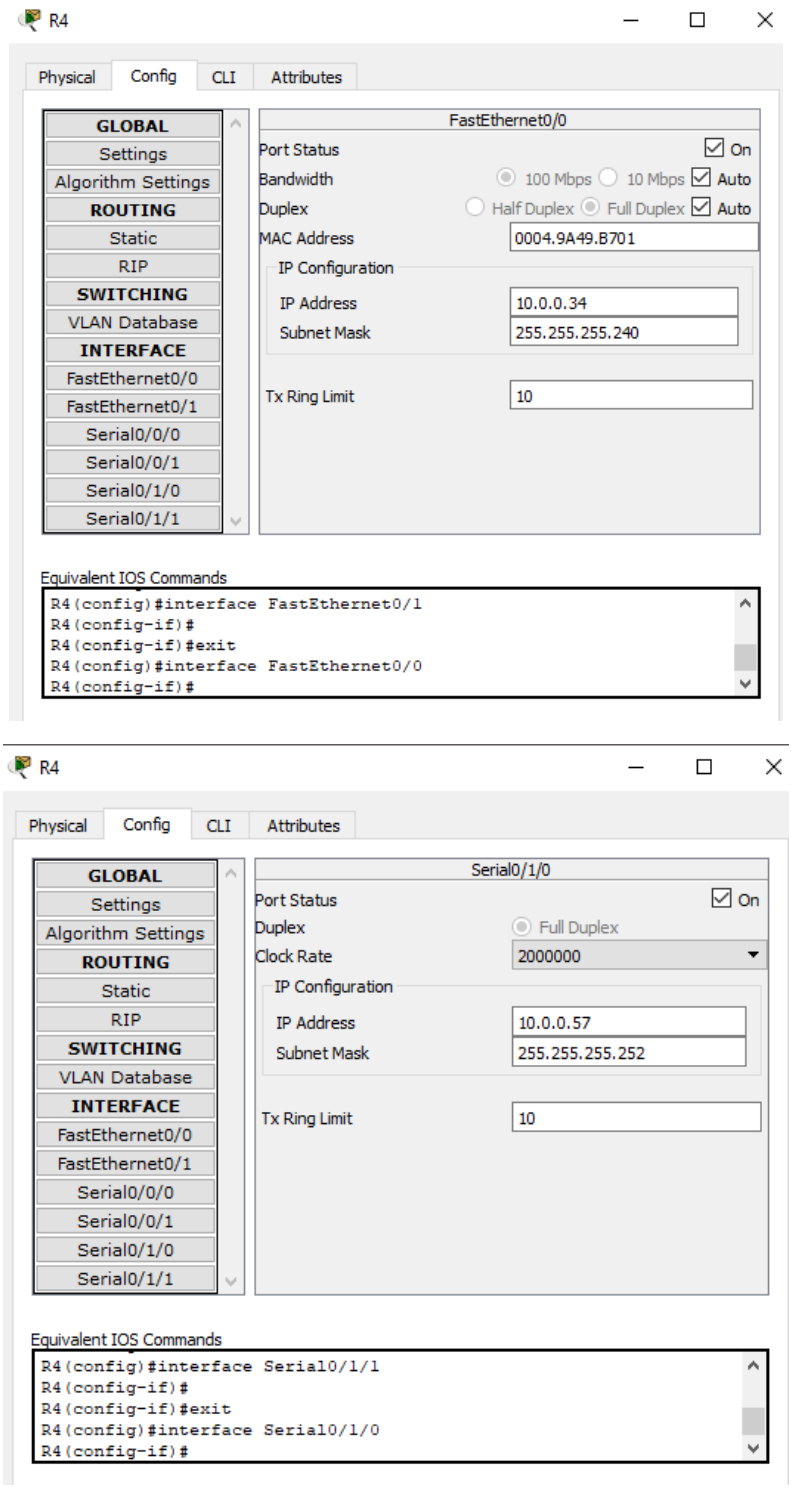

R1
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/1/1
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
10.0.0.58
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
R1(config)#interface Serial0/1/0
R1(config-if)#
R1(config-if)#exit
R1(config)#interface Serial0/1/1
R1(config-if)#


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BCBE.5301
IP Configuration
IP Address
10.0.0.62
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
Password:
R2#configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
R2(config)#interface FastEthernet0/0
R2(config-if)#


R2
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/1
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BCBE.5302
IP Configuration
IP Address
10.0.0.54
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
R2(config)#interface FastEthernet0/0
R2(config-if)#
R2(config-if)#exit
R2(config)#interface FastEthernet0/1
R2(config-if)#


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
FastEthernet0/0
Port Status
On
Bandwidth
100 Mbps
10 Mbps
Auto
Duplex
Half Duplex
Full Duplex
Auto
MAC Address
00D0.BC70.BE01
IP Configuration
IP Address
10.0.0.2
Subnet Mask
255.255.255.224
Tx Ring Limit
10
Equivalent IOS Commands
R3(config)#interface Serial0/1/1
R3(config-if)#
R3(config-if)#exit
R3(config)#interface FastEthernet0/0
R3(config-if)#


R3
Physical
Config
CLI
Attributes
GLOBAL
Settings
Algorithm Settings
ROUTING
Static
RIP
SWITCHING
VLAN Database
INTERFACE
FastEthernet0/0
FastEthernet0/1
Serial0/0/0
Serial0/0/1
Serial0/1/0
Serial0/1/1
Serial0/1/0
Port Status
On
Duplex
Full Duplex
Clock Rate
2000000
IP Configuration
IP Address
10.0.0.49
Subnet Mask
255.255.255.252
Tx Ring Limit
10
Equivalent IOS Commands
R3(config)#interface Serial0/1/1
R3(config-if)#
R3(config-if)#exit
R3(config)#interface Serial0/1/0
R3(config-if)#



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.

```
Packet Tracer PC Command Line 1.0
C:\>ping 10.0.0.2

Pinging 10.0.0.2 with 32 bytes of data:

Reply from 10.0.0.2: bytes=32 time=1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255
Reply from 10.0.0.2: bytes=32 time<1ms TTL=255

Ping statistics for 10.0.0.2:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\>ssh -l valery 10.0.0.2
Invalid Command.

C:\>ssh -l valery 10.0.0.2
Open
Password:
% Password:  timeout expired!
% Login invalid

[Connection to 10.0.0.2 closed by foreign host]
C:\>ssh -l valery 10.0.0.2
Open
Password:



R3#
R3#sh run
Building configuration...

Current configuration : 1186 bytes
!
```

```
username valery privilege 15 secret 5 $1$mERr$nNHY95zxTZzrROnsZjYF6/
!
!
!
!
!
!
!
!
ip ssh version 2
ip domain-name cisco.com
!
!
spanning-tree mode pvst
```

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.