



INSTITUTO POLITÉCNICO NACIONAL
ESCUELA SUPERIOR DE CÓMPUTO
Administración de servicios en red



Práctica 3:

Configuración routers pexpect

Alumnos:

Meza Vargas Brandon David
Romero Angeles Abraham

Equipo:

ADR

Grupo:

4CM13

Profesor:

Gaspar Medina Fabian

Introducción

El método de cifrado de clave pública RSA.

RSA es un algoritmo de cifrado de clave pública que utiliza una clave pública para cifrar datos y una clave privada para descifrar los datos cifrados. Fue inventado en 1977 por Ron Rivest, Adi Shamir y Leonard Adleman, de ahí su nombre.

El algoritmo RSA se basa en la dificultad de factorizar grandes números enteros en números primos. La seguridad de RSA radica en la dificultad de factorizar el producto de dos números primos muy grandes. La clave pública consiste en dos números, un número de clave pública y un número de módulo, mientras que la clave privada consiste en un número de clave privada y el mismo número de módulo.

RSA se utiliza ampliamente en la seguridad de la información para proteger la comunicación en línea y para proteger datos sensibles almacenados en sistemas informáticos.

RSA es un algoritmo de cifrado de clave pública que utiliza una clave pública para cifrar datos y una clave privada para descifrar los datos cifrados. Es uno de los algoritmos de cifrado más utilizados en la seguridad de la información y se utiliza ampliamente en la protección de datos confidenciales y en la seguridad de las comunicaciones en línea.

El algoritmo RSA se basa en la dificultad de factorizar grandes números enteros en números primos. En el proceso de generar las claves públicas y privadas, se eligen dos números primos grandes al azar y se calcula el producto de estos dos números, que se utiliza como el número de módulo para el cifrado y descifrado. Se calculan dos valores más para cada clave: el valor de la clave pública y el valor de la clave privada. El valor de la clave pública se comparte ampliamente para permitir que cualquiera pueda cifrar datos y enviarlos al propietario de la clave privada. El valor de la clave privada debe ser mantenido en secreto para permitir que el propietario de la clave pueda descifrar los datos cifrados.

Para cifrar datos utilizando RSA, el remitente utiliza la clave pública del destinatario para cifrar los datos y los envía al destinatario. El destinatario utiliza su clave privada para descifrar los datos cifrados y leer el mensaje original. Como la clave privada sólo la posee el destinatario, los datos cifrados sólo pueden ser descifrados por el destinatario, lo que garantiza la confidencialidad de la comunicación.

RSA también se utiliza en la autenticación de datos, mediante la firma digital. La firma digital es un esquema de autenticación que permite a los usuarios firmar digitalmente documentos y mensajes para verificar su autenticidad e integridad. El remitente utiliza su clave privada para firmar digitalmente los datos y el destinatario utiliza la clave pública del remitente para verificar la firma digital y garantizar la autenticidad e integridad de los datos.

En resumen, RSA es un algoritmo de cifrado de clave pública que se utiliza ampliamente en la seguridad de la información para proteger la confidencialidad y la autenticidad de los datos y la comunicación en línea.

Lineas virtuales

Las líneas virtuales son una tecnología que permite a los usuarios tener múltiples números de teléfono en un solo dispositivo o línea telefónica física. Esto se logra mediante la utilización de un software de línea virtual que funciona como un teléfono virtual y permite la gestión de múltiples números de teléfono en un solo dispositivo.

La línea virtual es una solución práctica para las empresas y los profesionales que necesitan tener varios números de teléfono para diferentes propósitos, como la separación de las llamadas personales y de negocios, la utilización de diferentes números para diferentes campañas de marketing, la atención a clientes de diferentes regiones, etc.

Una línea virtual puede ser utilizada en cualquier dispositivo que tenga acceso a internet, como un teléfono inteligente, una tableta o una computadora. Los usuarios pueden descargar una aplicación de línea virtual o utilizar un servicio en línea para crear una línea virtual y asignar un número de teléfono. Algunas aplicaciones de línea virtual también ofrecen funciones adicionales como grabación de llamadas, transferencia de llamadas y llamadas en conferencia.

Además de la gestión de múltiples números de teléfono, las líneas virtuales también ofrecen ventajas como la reducción de los costos de las llamadas internacionales y la eliminación de la necesidad de tener múltiples dispositivos para gestionar diferentes números de teléfono.

Las líneas virtuales también son posibles entre computadoras. De hecho, una de las formas más comunes de líneas virtuales entre computadoras es a través de aplicaciones de software de telefonía por Internet, también conocida como VoIP (Voz sobre Protocolo de Internet).

Estas aplicaciones de VoIP permiten a los usuarios realizar llamadas de voz y video a través de Internet utilizando un software especializado en lugar de un dispositivo de telefonía convencional. Algunas de las aplicaciones de VoIP más populares son Skype, Zoom, WhatsApp y Google Meet.

A través de estas aplicaciones, los usuarios pueden crear una línea virtual y asignar un número de teléfono virtual a su cuenta. Este número de teléfono virtual se puede utilizar para realizar y recibir llamadas de voz y video a través de Internet, y también para enviar y recibir mensajes de texto.

Además, las líneas virtuales entre computadoras también son posibles utilizando servicios de telefonía en la nube que ofrecen funciones avanzadas de telefonía y comunicaciones empresariales. Estos servicios permiten a las empresas crear líneas virtuales para sus empleados y clientes en cualquier lugar del mundo, lo que puede ser beneficioso para la gestión de equipos remotos y la atención al cliente global.

TELNET

TELNET es un acrónimo que significa "Red de Terminales" en inglés, que se refiere a la capacidad de conectarse a un dispositivo remoto y controlarlo a través de una conexión de terminal virtual. La palabra "TELNET" se utiliza tanto para referirse al protocolo de red como a la aplicación de software que se utiliza para conectarse a un dispositivo remoto utilizando el protocolo TELNET.

El protocolo TELNET es un protocolo de red que se utiliza para establecer una conexión remota entre dispositivos a través de una red. Se utiliza comúnmente para acceder a equipos informáticos remotos, como servidores, routers, switches y otros dispositivos de red.

El protocolo TELNET permite a los usuarios conectarse a un dispositivo remoto y controlarlo como si estuvieran sentados frente a él. Esto se logra a través de una conexión de terminal virtual, que proporciona una interfaz de usuario basada en texto que permite enviar y recibir comandos y datos a través de la red.

Una de las principales ventajas del protocolo TELNET es que permite a los usuarios conectarse a dispositivos remotos desde cualquier lugar del mundo, siempre y cuando haya una conexión de red disponible. Esto puede ser beneficioso para la gestión remota de equipos informáticos, especialmente en entornos empresariales y de red.

Sin embargo, una de las desventajas del protocolo TELNET es que toda la información se transmite en texto sin cifrar, lo que puede ser un riesgo de seguridad en entornos en los que la información confidencial se está transmitiendo. Por lo tanto, se recomienda el uso de alternativas más seguras, como el protocolo SSH (Secure Shell), que utiliza cifrado para proteger la información transmitida.

SSH

El protocolo SSH (Secure Shell) es un protocolo de red que se utiliza para establecer una conexión segura y cifrada entre dos dispositivos a través de una red. Se utiliza comúnmente para acceder a equipos informáticos remotos, como servidores, routers, switches y otros dispositivos de red.

El protocolo SSH permite a los usuarios conectarse a un dispositivo remoto y controlarlo como si estuvieran sentados frente a él, al igual que el protocolo TELNET. Sin embargo, a diferencia del protocolo TELNET, el protocolo SSH cifra toda la información transmitida entre los dispositivos, lo que proporciona una capa adicional de seguridad.

Además de proporcionar una conexión segura, el protocolo SSH también admite la autenticación de usuarios mediante el uso de contraseñas o claves de acceso. Esto permite a los administradores de sistemas limitar el acceso a los dispositivos remotos solo a usuarios autorizados.

Otra característica importante del protocolo SSH es que admite la transferencia segura de archivos a través del protocolo SFTP (Secure File Transfer Protocol). Esto permite a los usuarios transferir archivos de forma segura entre dispositivos remotos, lo que puede ser beneficioso para la gestión remota de archivos en entornos empresariales y de red.

SSH es un protocolo de red seguro que se utiliza para conectarse de forma remota a dispositivos y sistemas informáticos a través de una red. El protocolo SSH proporciona una conexión segura y encriptada, lo que significa que la información que se envía a través de la conexión no puede ser interceptada o leída por terceros. SSH es una alternativa segura al protocolo TELNET, que transmite información en texto sin cifrar.

Una de las principales características de SSH es la capacidad de autenticar a los usuarios mediante el uso de contraseñas o claves de acceso. Los usuarios deben proporcionar credenciales válidas para conectarse a un sistema remoto utilizando SSH. El uso de claves de acceso en lugar de contraseñas puede ser aún más seguro, ya que las claves son más difíciles de adivinar o descifrar que las contraseñas.

Además, SSH admite la transferencia segura de archivos a través del protocolo SFTP (Secure File Transfer Protocol). SFTP es similar a FTP (File Transfer Protocol), pero utiliza SSH para encriptar y proteger los archivos que se transfieren.

SSH se utiliza ampliamente en entornos empresariales y de red, donde la seguridad es una preocupación importante. Los administradores de sistemas utilizan SSH para conectarse de forma remota a servidores y dispositivos de red, lo que les permite administrar y configurar estos sistemas sin tener que estar físicamente presentes en la ubicación del dispositivo. Además, los usuarios pueden utilizar SSH para conectarse de forma segura a sistemas informáticos desde ubicaciones remotas, lo que les permite trabajar desde cualquier lugar.

Niveles de privilegios de CISCO

En Cisco IOS (Internetwork Operating System), hay diferentes niveles de privilegios o modos de operación que determinan el nivel de acceso y control que un usuario puede tener sobre el dispositivo. A continuación, se describen los niveles de privilegios de Cisco y sus definiciones:

Modo Usuario (User Mode): El Modo Usuario es el nivel de privilegio más bajo y restringido. Los usuarios solo pueden ver el estado básico del dispositivo, como la configuración actual, la carga de CPU y la cantidad de memoria libre. Para ingresar a este modo, se debe iniciar sesión con un nombre de usuario válido.

Modo Privilegiado (Privileged Mode): El Modo Privilegiado es el nivel de privilegio más alto antes del modo de configuración. Los usuarios pueden ejecutar comandos de supervisión, ver información detallada sobre el dispositivo y ejecutar ciertas tareas de administración de red. Para acceder a este modo, se debe ingresar el comando "enable" en el modo de usuario y proporcionar la contraseña de privilegiado.

Modo de Configuración Global (Global Configuration Mode): El Modo de Configuración Global permite a los usuarios realizar cambios en la configuración global del dispositivo, como la configuración de la interfaz, la asignación de direcciones IP y la configuración de enrutamiento. Para ingresar a este modo, se debe ingresar el comando "configure terminal" en el modo de privilegiado.

Modo de Configuración de Interfaz (Interface Configuration Mode): El Modo de Configuración de Interfaz permite a los usuarios configurar parámetros específicos de la interfaz, como la velocidad, el dúplex, la dirección IP y la máscara de subred. Para acceder

a este modo, se debe ingresar el comando "interface [nombre de la interfaz]" en el modo de configuración global.

Modo de Configuración de Línea (Line Configuration Mode): El Modo de Configuración de Línea se utiliza para configurar los parámetros de línea de la consola, VTY o interfaz auxiliar. Por ejemplo, los usuarios pueden configurar la contraseña de la consola o especificar la velocidad y el control de flujo para una línea VTY. Para acceder a este modo, se debe ingresar el comando "line [nombre de la línea]" en el modo de configuración global.

Modo de Configuración de Protocolo (Protocol Configuration Mode): El Modo de Configuración de Protocolo permite a los usuarios configurar protocolos específicos de la red, como OSPF, EIGRP o BGP. Para acceder a este modo, se debe ingresar el comando "router [nombre del protocolo]" en el modo de configuración global.

Desarrollo

En esta práctica vamos a configurar la siguiente topología para conectarnos entre routers usando ssh o telnet, de igual manera nos vamos a conectar a los routers desde una máquina virtual.

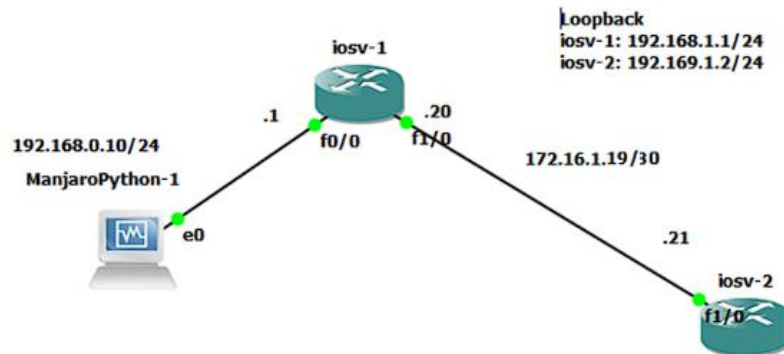


Ilustración 1. Topología para armar

En la siguiente imagen podemos ver la topología armada en nuestro ambiente GNS3.

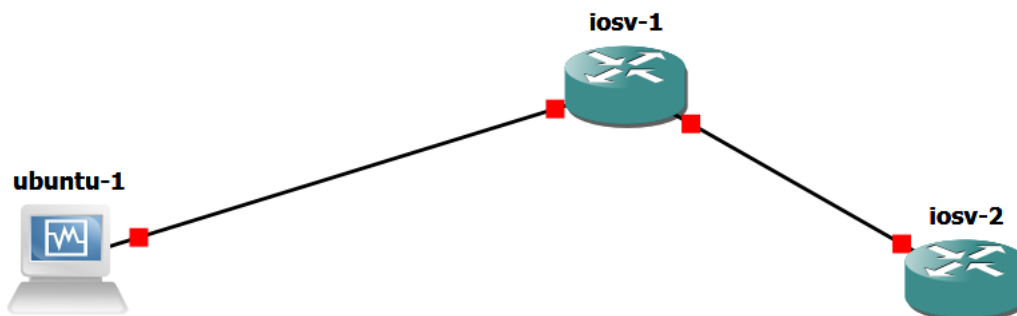


Ilustración 2. Topología armada

Ahora vamos a realizar las configuraciones correspondientes en los routers comenzando por el router **iosv-1**. En la siguiente imagen podemos ver la habilitación de la encriptación, encriptación de contraseña y la habilitación y descripción de la interfaz de loopback indicada en la ilustración 1.

```
iosv-1#config t
Enter configuration commands, one per line. End with CNTL/Z.
iosv-1(config)#enable secret 1234
iosv-1(config)#service password-encryption
iosv-1(config)#interface loopback0
iosv-1(config-if)#description loopback0
iosv-1(config-if)#ip address 192.168.1.1 255.255.255.255
iosv-1(config-if)#no shutdown
```

Ilustración 3. Configuración iosv-1

Posteriormente esta la configuración de las interfaces y el enrutamiento, en este caso se usó ospf, de igual manera la declaración de interfaces pasivas.

```
iosv-1(config)#interface fastEthernet1/0
iosv-1(config-if)#ip address 172.16.1.20 255.255.255.0
iosv-1(config-if)#no shutdown
iosv-1(config-if)#exit
iosv-1(config)#interface fastEthernet0/0
iosv-1(config-if)#ip address 192.168.0.1 255.255.255.0
iosv-1(config-if)#no shutdown
iosv-1(config-if)#exit
iosv-1(config)#router ospf 1
iosv-1(config-router)#passive-interface loopback0
iosv-1(config-router)#passive-interface fa0/0
iosv-1(config-router)#network 172.16.1.0 0.0.0.255 area 0
iosv-1(config-router)#network 192.168.0.0 0.0.0.255 area 0
iosv-1(config-router)#exit
iosv-1(config)#
```

Ilustración 4. Configuración iosv-1

Ahora vamos con el levantamiento de SSH, para esto se necesitan llaves publicas y privadas y la creación de usuarios y un dominio, este se ve a continuación.

```
iosv-1(config)#ip domain-name adminredes.escom.ipn.mx
iosv-1(config)#ip ssh rsa keypair-name sshkey
iosv-1(config)#crypto key generate rsa usage-keys label sshkey modulus 1024
% You already have RSA keys defined named sshkey.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]
% Generating 1024 bit RSA keys, keys will be non-exportable...
*May  1 15:49:15.567: %SSH-5-DISABLED: SSH 2.0 has been disabled[OK]

iosv-1(config)#
*May  1 15:49:18.763: %SSH-5-ENABLED: SSH 2.0 has been enabled
iosv-1(config)#ip ssh v 2
iosv-1(config)#ip ssh time-out 30
iosv-1(config)#ip ssh authentication-retries 3
iosv-1(config)#line vty 0 15
iosv-1(config-line)#password cisco
iosv-1(config-line)#login local
iosv-1(config-line)#transport input ssh telnet
iosv-1(config-line)#exit
iosv-1(config)#username cisco privilege 15 password cisco
iosv-1(config)#end
iosv-1#
*May  1 15:50:32.891: %SYS-5-CONFIG_I: Configured from console by console
iosv-1#
```

Ilustración 5. Configuración iosv-1

El router **iosv-2** se va a configurar de manera similar al router **iosv-1** , a continuación se adjuntan las capturas de esta configuración.


```

iosv-2(config)#
iosv-2(config)#enable secret 1234
iosv-2(config)#service password-encryption
iosv-2(config)#interface loopback0
iosv-2(config-if)#description loopback0
iosv-2(config-if)#ip address 192.169.1.2 255.255.255.255
iosv-2(config-if)#no shutdown
iosv-2(config-if)#exit
iosv-2(config)#interface fa1/0
iosv-2(config-if)#ip address 172.16.1.21 255.255.255.0
iosv-2(config-if)#no shutdown
iosv-2(config-if)#exit
iosv-2(config)#router ospf 1
iosv-2(config-router)#network 192.168.0.0 0.0.0.255 area 0
iosv-2(config-router)#exit
iosv-2(config)#ip domain-name adminredes.escom.ipn.mc
iosv-2(config)#ip domain-name adminredes.escom.ipn.mx
iosv-2(config)#ip ssh rsa keypair-name sshkey
iosv-2(config)#crypto generate rsa usage-keys label sshket modulus 1024
^
% Invalid input detected at '^' marker.

iosv-2(config)#crypto generate rsa usage-keys label sshkey modulus 1024
^
% Invalid input detected at '^' marker.

iosv-2(config)#crypto key generate rsa usage-keys label sshkey modulus 1024
% You already have RSA keys defined named sshkey.
% They will be replaced.

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
*May  1 15:55:15.583: %SSH-5-DISABLED: SSH 2.0 has been disabled[OK]
% Generating 1024 bit RSA keys, keys will be non-exportable...[OK]

iosv-2(config)#
*May  1 15:55:22.355: %SSH-5-ENABLED: SSH 2.0 has been enabled
iosv-2(config)#ip ssh v 2
iosv-2(config)#ip ssh time-out 30
iosv-2(config)#ip ssh authentication-retries 3
iosv-2(config)#line vty 0 15
iosv-2(config-line)#password cisco
iosv-2(config-line)#login local
iosv-2(config-line)#transport input ssh telnet
iosv-2(config-line)#exit
iosv-2(config)#username cisco privilege 15 password cisco
iosv-2(config)#end
iosv-2#

```

Ilustración 6. Configuración iosv-2

Una vez tengamos los dos routers configurados procedemos a conectarlos.

Conexión con telnet y ssh de router 2 a router 1

```
iosv-2#ssh -l cisco 172.16.1.20
Password:
iosv-1#exit
[Connection to 172.16.1.20 closed by foreign host]
iosv-2#telnet 172.16.1.20
Trying 172.16.1.20 ... Open

User Access Verification

Username: cisco
Password:
iosv-1#
```

Ilustración 7. Conexión router 2 a router 1

Conexión con telnet y ssh de router 1 a router 2

```
iosv-1#ssh -l cisco 172.16.1.21
Password:
iosv-2#exit
[Connection to 172.16.1.21 closed by foreign host]
iosv-1#telnet 172.16.1.21
Trying 172.16.1.21 ... Open

User Access Verification

Username: cisco
Password:
iosv-2#
iosv-2#
```

Ilustración 8. Conexión router 1 a router 2

Ahora veremos la configuración de la máquina virtual y la conexión a los routers desde esta.

Configuración de la máquina virtual:

Debemos configurar la IP de máquina virtual dado click en configuración de red:

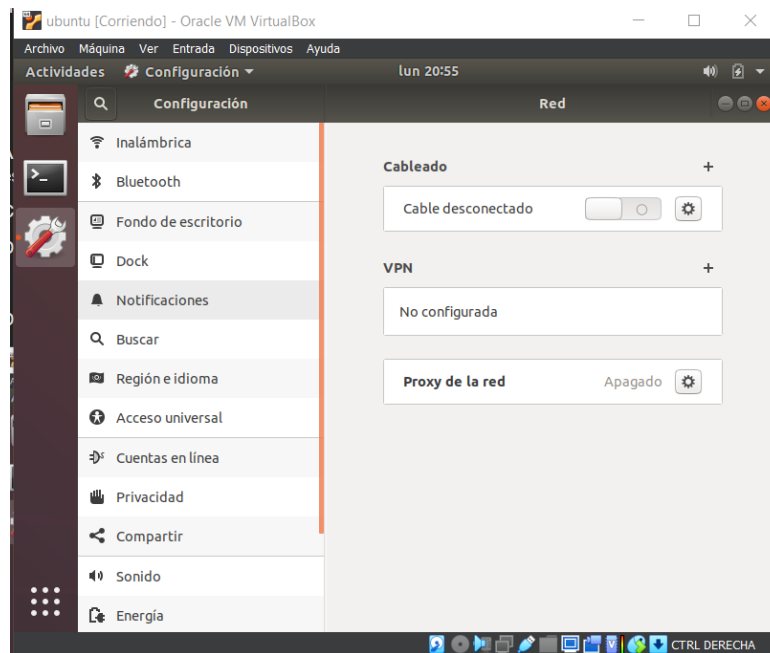


Ilustración 9. Ventana de red la maquina virtual

Damos en cableado al símbolo del engrane para que nos abra la configuración de la IP y el DNS

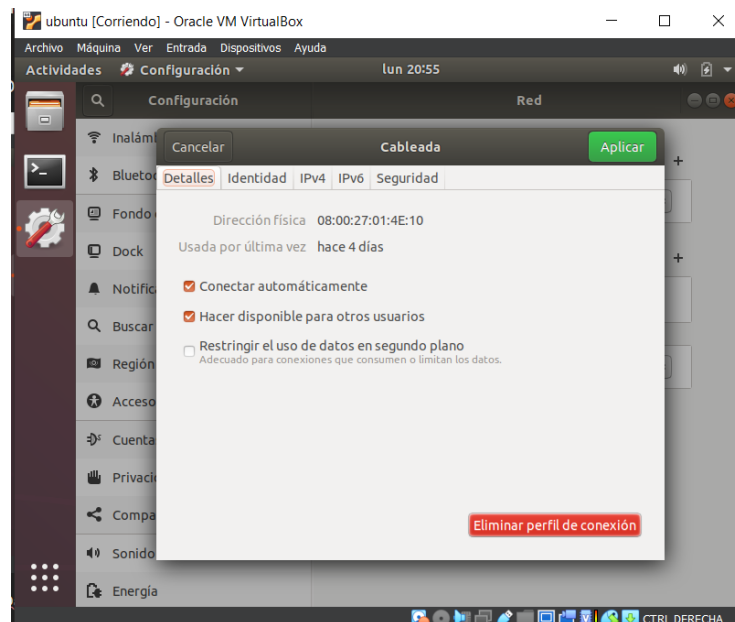


Ilustración 10. Detalles de la configuración de la red de la maquina virtual

Damos click en el apartado de IPv4 y ponemos la IP “192.192.0.10”

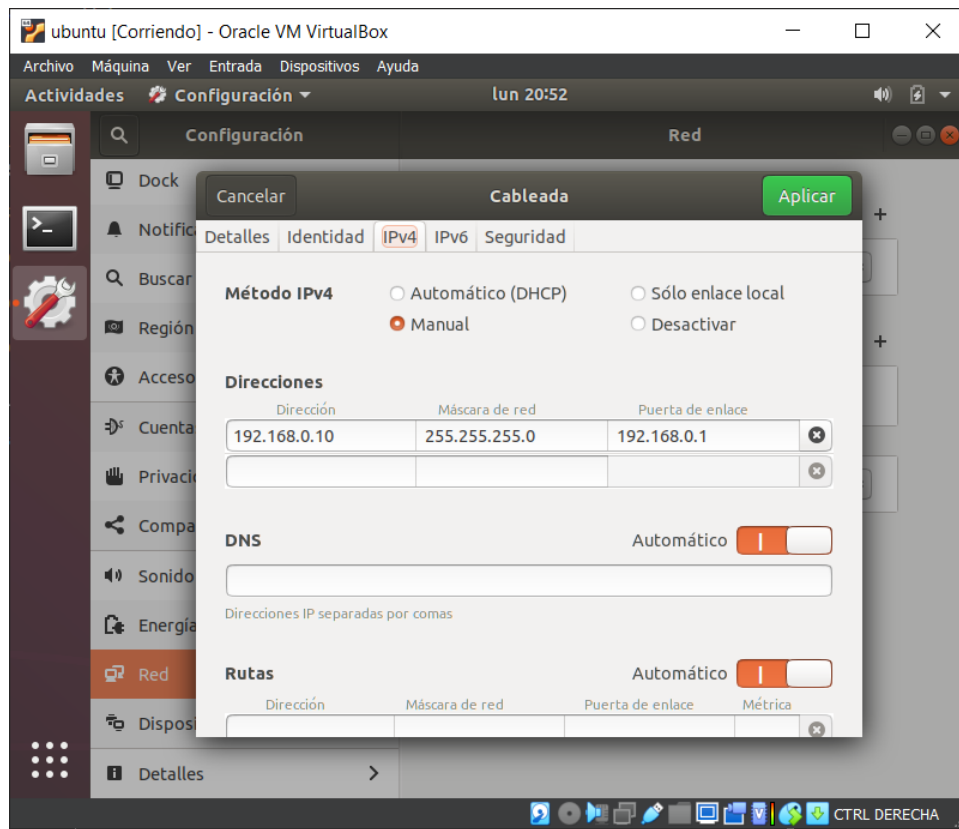


Ilustración 11. Configuración de la IP de la maquina virtual

Damos en "Aceptar" y la PC ya está configurada con su IP y servidor DNS

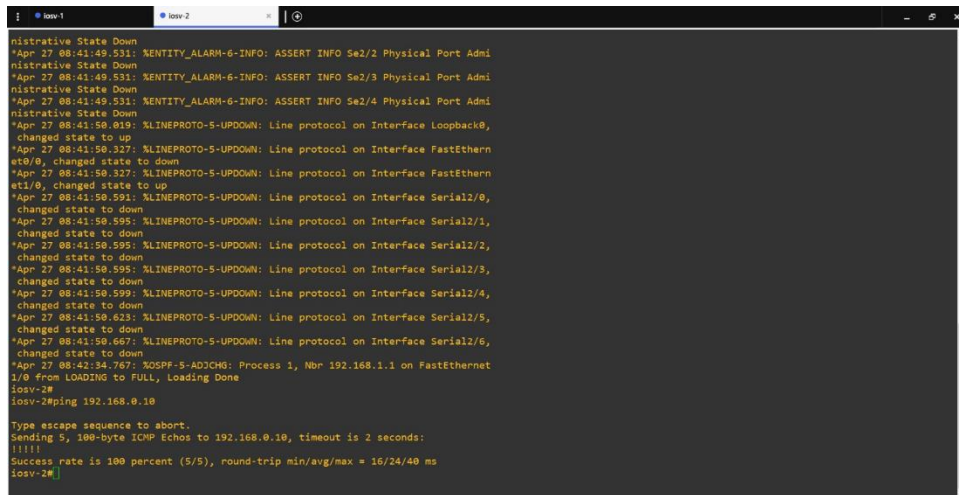
Ejecución

Hacemos ping del router 1 a la PC



Ilustración 12. Ping del router 1 a la máquina virtual

Hacemos ping del router 2 a la PC

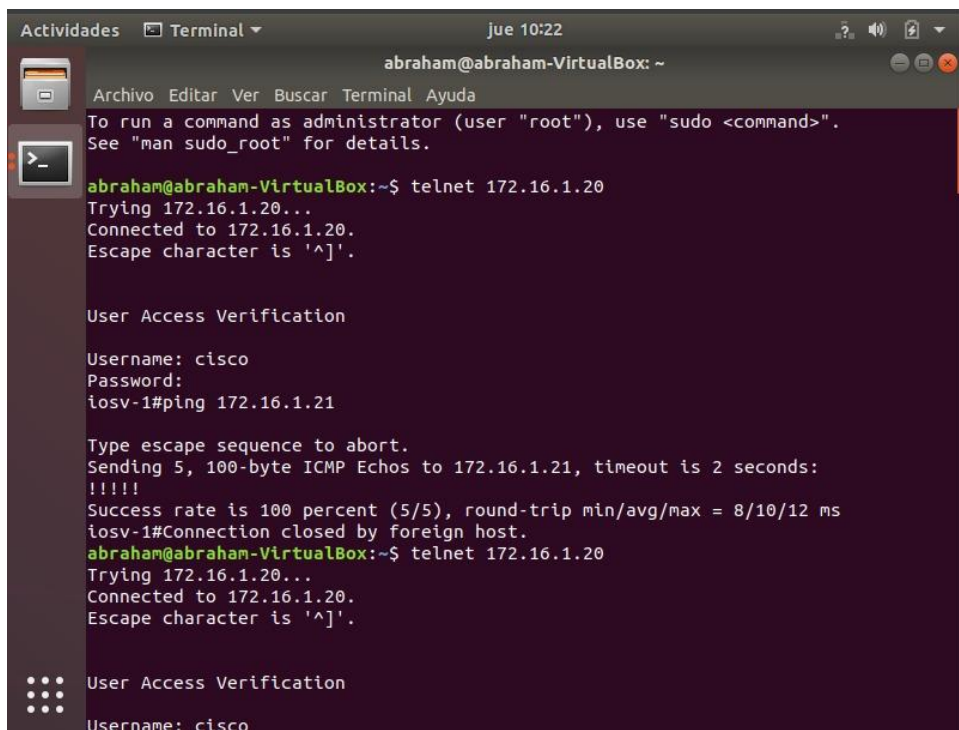


```
Administrative State Down
*Apr 27 08:41:49.531: %ENTITY_ALARM-6-INFO: ASSERT INFO Se2/3 Physical Port Admini
Administrative State Down
*Apr 27 08:41:49.531: %ENTITY_ALARM-6-INFO: ASSERT INFO Se2/3 Physical Port Admini
Administrative State Down
*Apr 27 08:41:49.531: %ENTITY_ALARM-6-INFO: ASSERT INFO Se2/4 Physical Port Admini
Administrative State Down
*Apr 27 08:41:50.019: %LINEPROTO-5-UPDOWN: Line protocol on Interface Loopback0,
changed state to up
*Apr 27 08:41:50.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et0/0, changed state to down
*Apr 27 08:41:50.327: %LINEPROTO-5-UPDOWN: Line protocol on Interface FastEthernet
et1/0, changed state to up
*Apr 27 08:41:50.591: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/0,
changed state to down
*Apr 27 08:41:50.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/1,
changed state to down
*Apr 27 08:41:50.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/2,
changed state to down
*Apr 27 08:41:50.595: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/3,
changed state to down
*Apr 27 08:41:50.599: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/4,
changed state to down
*Apr 27 08:41:50.623: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/5,
changed state to down
*Apr 27 08:41:50.667: %LINEPROTO-5-UPDOWN: Line protocol on Interface Serial2/6,
changed state to down
*Apr 27 08:42:34.767: %OSPF-5-ADJCHG: Process 1, Nbr 192.168.1.1 on FastEthernet
1/0 #from LOADING to FULL, Loading Done
iosv-2#
iosv-2#ping 192.168.0.10

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 192.168.0.10, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/24/40 ms
iosv-2#
```

Ilustración 13. Ping del router 2 a la máquina virtual

Desde la máquina virtual nos conectamos al router 1 y hacemos ping



```
Actividades Terminal jue 10:22
abraham@abraham-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
To run a command as administrator (user "root"), use "sudo <command>".
See "man sudo_root" for details.
abraham@abraham-VirtualBox:~$ telnet 172.16.1.20
Trying 172.16.1.20...
Connected to 172.16.1.20.
Escape character is '^J'.

User Access Verification

Username: cisco
Password:
iosv-1#ping 172.16.1.21

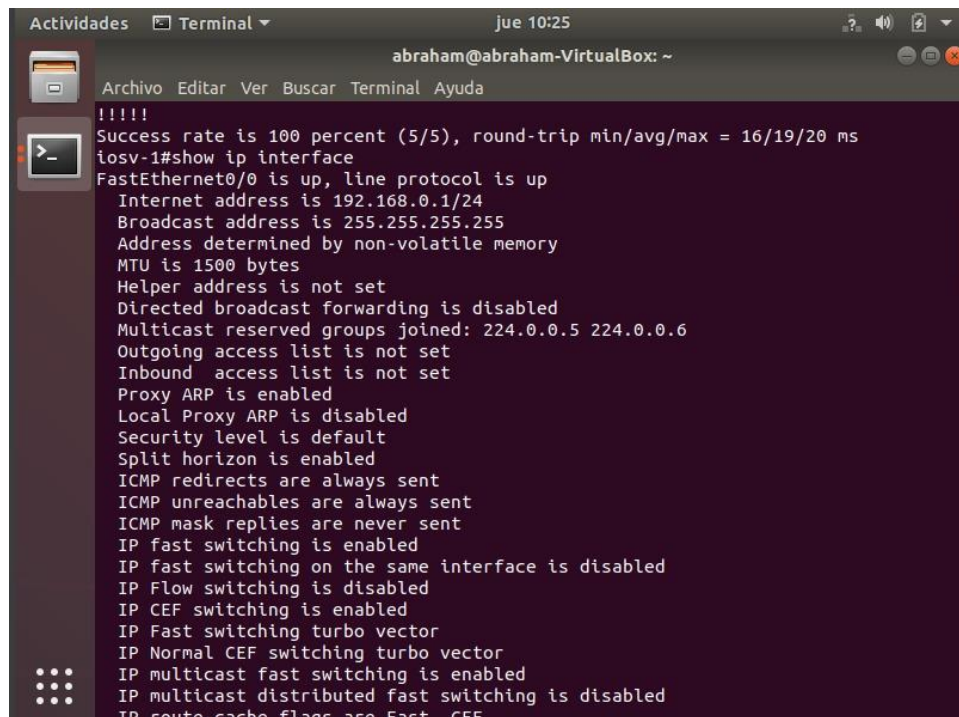
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 8/10/12 ms
iosv-1#Connection closed by foreign host.
abraham@abraham-VirtualBox:~$ telnet 172.16.1.20
Trying 172.16.1.20...
Connected to 172.16.1.20.
Escape character is '^J'.

User Access Verification

Username: cisco
```

Ilustración 14. Conexión de la máquina virtual con el router 1 desde la consola de la máquina virtual

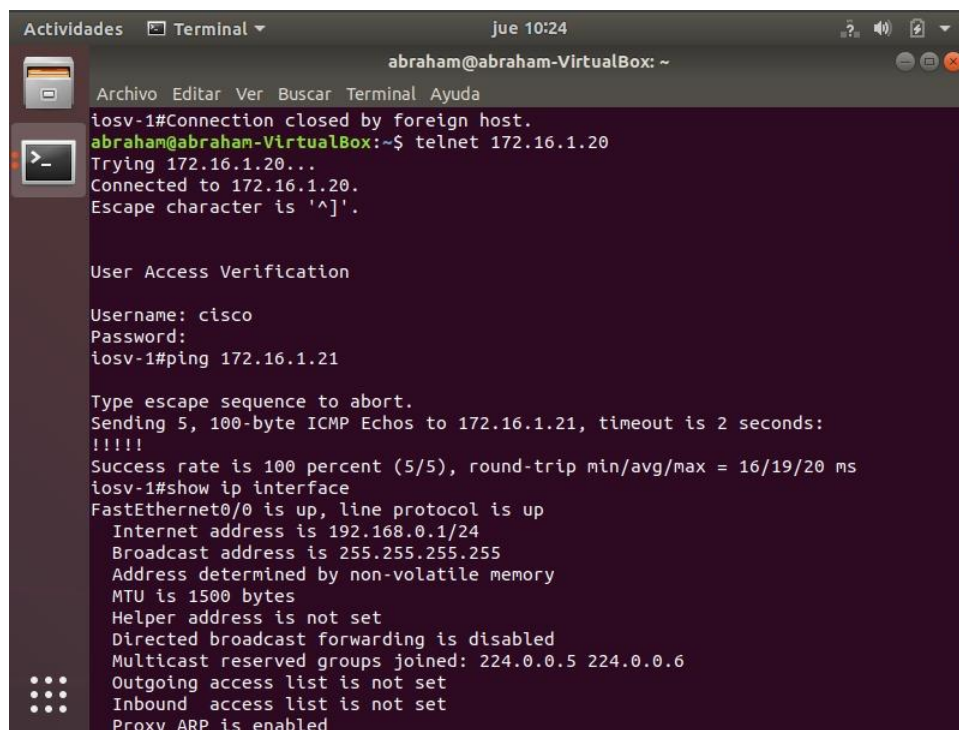
Ejecutamos el comando “show ip router” al router 1 desde la máquina virtual



```
Actividades Terminal Jue 10:25
abraham@abraham-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/20 ms
iosv-1#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
  Local Proxy ARP is disabled
  Security level is default
  Split horizon is enabled
  ICMP redirects are always sent
  ICMP unreachable are always sent
  ICMP mask replies are never sent
  IP fast switching is enabled
  IP fast switching on the same interface is disabled
  IP Flow switching is disabled
  IP CEF switching is enabled
  IP Fast switching turbo vector
  IP Normal CEF switching turbo vector
  IP multicast fast switching is enabled
  IP multicast distributed fast switching is disabled
  IP route-cache flags are Fast CEF
```

Ilustración 15. Comando “show ip router” en la consola de la máquina virtual para el router 1

En la misma consola desde el router 1 entramos al router 2



```
Actividades Terminal Jue 10:24
abraham@abraham-VirtualBox: ~
Archivo Editar Ver Buscar Terminal Ayuda
iosv-1#Connection closed by foreign host.
abraham@abraham-VirtualBox:~$ telnet 172.16.1.20
Trying 172.16.1.20...
Connected to 172.16.1.20.
Escape character is '^J'.

User Access Verification

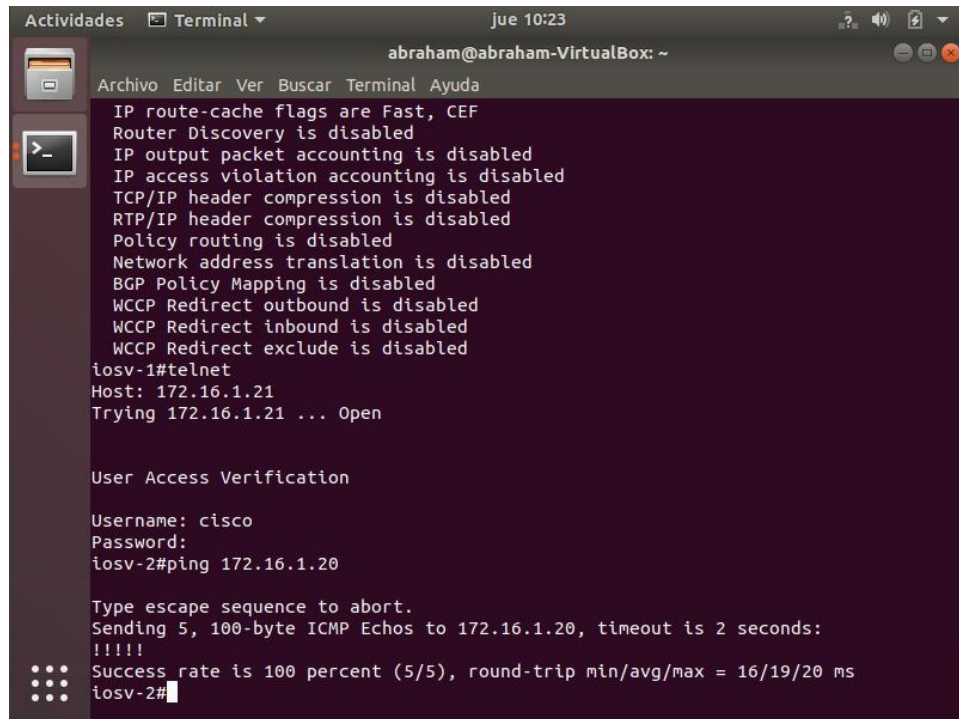
Username: cisco
Password:
iosv-1#ping 172.16.1.21

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.21, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/20 ms
iosv-1#show ip interface
FastEthernet0/0 is up, line protocol is up
  Internet address is 192.168.0.1/24
  Broadcast address is 255.255.255.255
  Address determined by non-volatile memory
  MTU is 1500 bytes
  Helper address is not set
  Directed broadcast forwarding is disabled
  Multicast reserved groups joined: 224.0.0.5 224.0.0.6
  Outgoing access list is not set
  Inbound access list is not set
  Proxy ARP is enabled
```

Ilustración 16. Conexión de la máquina virtual con el router 2 desde la consola de la máquina virtual

Ejecutamos el comando “show ip router” al router 2 desde la máquina virtual

Ahora hacemos ping al router 2



```
Abraham@Abraham-VirtualBox: ~
IP route-cache flags are Fast, CEF
Router Discovery is disabled
IP output packet accounting is disabled
IP access violation accounting is disabled
TCP/IP header compression is disabled
RTP/IP header compression is disabled
Policy routing is disabled
Network address translation is disabled
BGP Policy Mapping is disabled
WCCP Redirect outbound is disabled
WCCP Redirect inbound is disabled
WCCP Redirect exclude is disabled
iosv-1#telnet
Host: 172.16.1.21
Trying 172.16.1.21 ... Open

User Access Verification

Username: cisco
Password:
iosv-2#ping 172.16.1.20

Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 172.16.1.20, timeout is 2 seconds:
!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 16/19/20 ms
iosv-2#
```

Ilustración 17. Comando “show ip router” en la consola de la máquina virtual para el router 2

Vemos que todo fue correcto en la ejecución de la práctica.

Conclusiones

Meza Vargas Brandon David

La práctica de conectar una máquina virtual con una topología en GNS3 usando configuración de routers pexpect fue una actividad muy útil para aprender cómo funciona el enrutamiento y la comunicación en una red virtual.

Durante esta práctica, aprendí cómo configurar los routers en GNS3 con esta modificación que agrega pexpect, cómo conectarlos entre sí y cómo configurar la comunicación entre diferentes redes.

Además, al utilizar la herramienta pexpect, pude ver que se pueden automatizar algunos de los pasos de configuración, lo que les permite ahorrar tiempo y mejorar la eficiencia de su trabajo.

Romero Angeles Abraham

Esta práctica me sirvió mucho primeramente me enseñó a conectar una maquina virtual a la herramienta de virtual box, cosa que nunca había hecho y me pareció muy interesante, me enseñó la configuración de la IP de la maquina virtual y principalmente aprendí el procedimiento y configuración de los router pexpect y como al principio parece un poco complejo, pero si facilita bastante la comunicación y nos permite conectarnos con la máquina virtual y a una red virtual