Tecnológico de Monterrey

Ejercicio 10. Acceso a dispositivos de red mediante SSH

Topología física

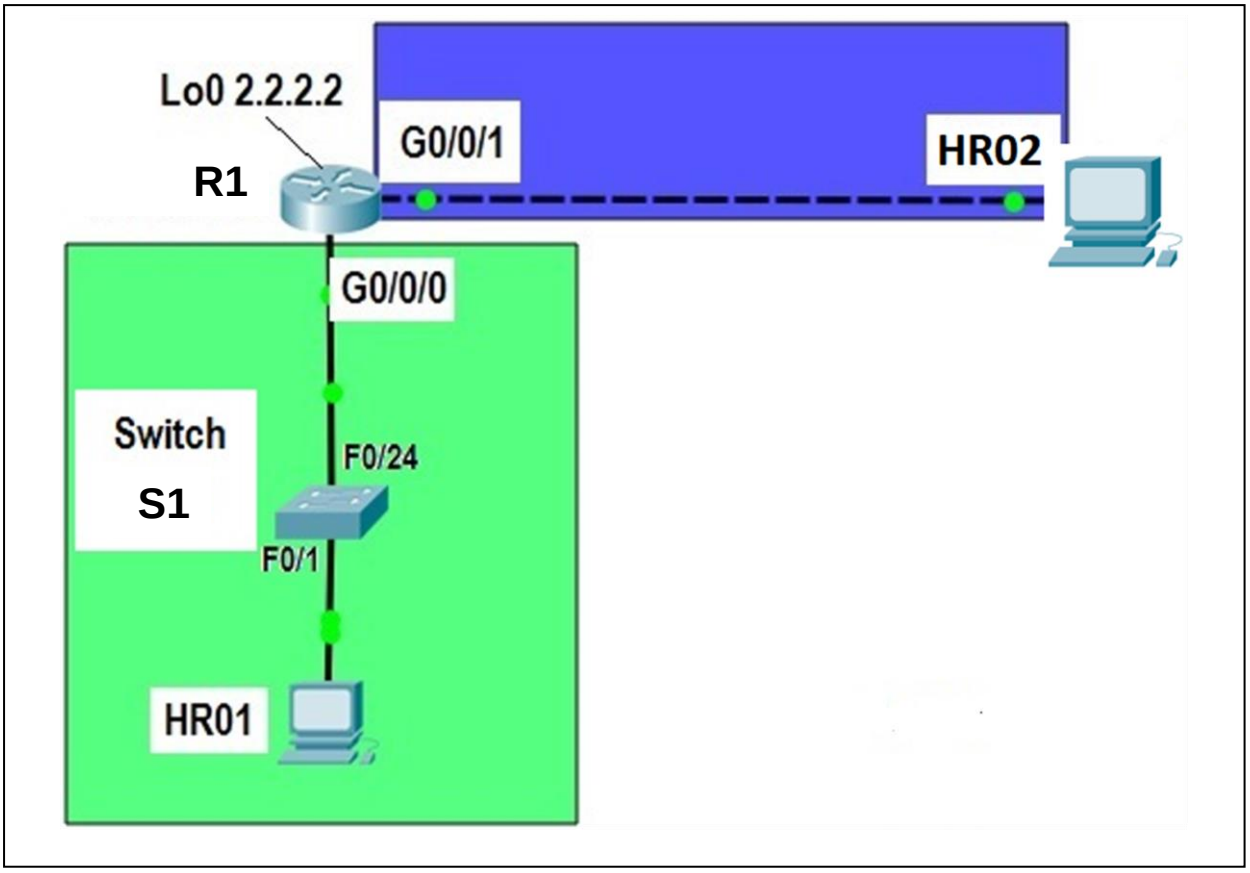

Tabla de direccionamiento

Dispositivo	Interface	Dirección IP	Máscara de subred	Default Gateway
Host **HR01**	**NIC**	172.16.0.35	255.255.255.128	172.16.0.62
Host **HR02**	**NIC**	172.16.0.242	255.255.255.252	172.16.0.241
R1	**G0/0/0**	172.16.0.62	255.255.255.128	N/A
	G0/0/1	172.16.0.241	255.255.255.252	N/A
	Lo0	2.2.2.2	255.255.255.0	N/A
S1	**VLAN 1**	172.16.0.33	255.255.255.128	172.16.0.62

Introducción

En el pasado, **Telnet** era el protocolo de red más común que se usaba para configurar dispositivos de red en forma remota. El protocolo **Telnet** no cifra la información entre el cliente y el servidor. Esto permite que un programa detector de redes intercepte contraseñas e información de configuración.

Shell seguro (SSH) es un protocolo de red que establece una conexión de emulación de terminal segura con un router u otro dispositivo de red. SSH cifra toda la información que atraviesa el enlace de red y proporciona autenticación de los equipos remotos. SSH está reemplazando rápidamente a Telnet como la herramienta de conexión remota preferida por los profesionales de red. SSH se utiliza con mayor frecuencia para conectarse a un dispositivo remoto y ejecutar comandos.

Para que el protocolo SSH funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En este ejercicio, deberá habilitar el servidor SSH en un router y luego conectarse a ese router desde una PC con un cliente SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP.

Parte 1. Configurar el router para el acceso por SSH

Usar el protocolo Telnet para conectarse a un dispositivo de red es un riesgo de seguridad, porque toda la información se transmite en formato de texto no cifrado. El protocolo SSH cifra los datos de sesión y ofrece autenticación del dispositivo, por lo que se recomienda usar SSH para conexiones remotas. En la parte 1, configurará el router para que acepte conexiones SSH por las líneas VTY.

1. Configurar la autenticación del dispositivo.

El nombre y el dominio del dispositivo se usan como parte de la clave de cifrado cuando esta se genera. Por lo tanto, estos nombres deben introducirse antes de emitir el comando **crypto key**.

a. Configure el nombre del dispositivo.

```
RouterUM(config)# hostname R1
```

b. Configure el dominio para el dispositivo.

```
R1(config)# ip domain-name tec.com
```

2. Configurar el método de la clave de cifrado.

```
R1(config)# crypto key generate rsa
Type the value of 1024 as the answer to the question and press enter.
How many bits in the modulus [512]: 1024

The name for the keys will be: R1.ccna-lab.com

% The key modulus size is 1024 bits
% Generating 1024 bit RSA keys, keys will be non-exportable...
[OK] (elapsed time was 1 seconds)

R1(config)#
*Jan 28 21:09:29.867: %SSH-5-ENABLED: SSH 1.99 has been enabled
```

3. Configurar un nombre de usuario de la base de datos local.

```
R1(config)# username admin privilege 15 secret adminpass
```

Nota: el nivel de privilegio 15 otorga derechos de administrador al usuario.

4. Habilitar SSH en las líneas VTY.

c. Habilite Telnet y SSH en las líneas VTY entrantes mediante el comando **transport input**.

```
R1(config)# line vty 0 4
R1(config-line)# transport input ssh
```

5. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

```
R1(config-line)# login local
R1(config-line)# end
R1#
```

5. Guardar la configuración en ejecución en el archivo de configuración de inicio.

```
R1# copy running-config startup-config
Destination filename [startup-config]?
Building configuration...
[OK]
R1#
```

6. Establecer una conexión SSH con el router R1.

a. Acceda remotamente al **R1** desde la PC **HR01** con el comando **SSH**. Use el nombre de usuario **admin** y la contraseña **adminpass**. En la línea de comandos (**Desktop > Command Prompt**) de la PC **HR01**, inserta el siguiente comando:

ssh –l admin 172.16.0.62

Use el password adminpass

b. ¿Pudo conectarse remotamente? ____

Parte 2. Configurar el switch para el acceso por SSH

En la parte 2, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH desde la PC **HR01**.

1. Configurar el switch para que tenga conectividad de SSH.

Para configurar SSH en el switch, utilice los mismos comandos que usó para configurar SSH en el router.

a. Configure el nombre del dispositivo.

```
SUM(config)# hostname S1
```

b. Configure el dominio para el dispositivo.

```
S1(config)# ip domain-name tec.com
```

c. Configure el método de la clave de cifrado.

```
S1(config)# crypto key generate rsa
Type the value of 1024 as the answer to the question and press enter.
How many bits in the modulus [512]: 1024
```

d. Configure un nombre de usuario de la base de datos local.

```
S1(config)# username admin privilege 15 secret adminpass
```

e. Habilite Telnet y SSH en las líneas VTY.

```
S1(config)# line vty 0 15
S1(config-line)# transport input ssh
```

f. Cambie el método de inicio de sesión para utilizar la base de datos local para la verificación del usuario.

```
S1(config-line)# login local
S1(config-line)# end
```

2. Establecer una conexión SSH con el switch.

a. Acceda remotamente a la interfaz SV1 del switch **S1** desde la PC **HR01** con el comando SSH. En la línea de comandos (**Desktop > Command Prompt**) de la PC **HR01**, inserta el siguiente comando:

ssh –l admin 172.16.0.33

Use el password adminpass

b. ¿Pudo establecer una sesión de SSH con el switch? _____

3. Acceder a R1 mediante SSH desde S1.

a. Debe usar la opción **–l admin** cuando acceda a **R1** mediante SSH. De esta manera, podrá iniciar sesión como usuario **admin**. Cuando se le solicite, introduzca la contraseña **adminpass**.

```
S1# ssh -l admin 172.16.0.62
Password:
**********************************************
  Prohibido entrar sin autorización
**********************************************
R1#
```

b. Para finalizar la sesión de SSH en R1, escriba **exit** en el símbolo de sistema del router.

```
R1# exit
[Connection to 172.16.0.62 closed by foreign host]
S1#
```

4. Establecer una conexión SSH con el router R1 desde la PC remota HR02.

a. Acceda remotamente al **R1** desde la PC **HR02** con el comando **SSH**. Use el nombre de usuario **admin** y la contraseña **adminpass**. En la línea de comandos (**Desktop > Command Prompt**) de la PC **HR02**, inserta el siguiente comando:

ssh –l admin 172.16.0.62

Use el password adminpass

b. ¿Pudo conectarse remotamente? ____

5. Establecer una conexión SSH con el switch S1 desde la PC remota HR02.

a. Acceda remotamente a la interfaz SV1 del switch **S1** desde la PC **HR02** con el comando SSH. En la línea de comandos (**Desktop > Command Prompt**) de la PC **HR02**, inserta el siguiente comando:

ssh –l admin 172.16.0.33

Use el password adminpass

b. ¿Pudo conectarse remotamente? ____

Reflexión:

¿Cómo proporcionaría acceso a un dispositivo de red a varios usuarios, cada uno con un nombre de usuario diferente?

Se agregaría el nombre de usuario y la contraseña de cada usuario a la base de datos local mediante el comando username.

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)# username usuario1 privilege 1 secret userpass
R1(config)# username usuario2 privilege 1 secret userpass
```

Nota: Un nivel de privilegio de **15** otorga al usuario derechos de **administrador**.

La CLI del Cisco IOS tiene dos niveles de acceso a los comandos:

- **Modo EXEC de usuario (nivel de privilegio 1)**: proporciona los privilegios de usuario de modo EXEC más bajos y permite que solo estén disponibles los comandos del nivel de usuario en el prompt **router>**.
- **Modo EXEC privilegiado (nivel de privilegio 15)**: incluye todos los comandos de nivel de privilegiado en el prompt **router#**.