Práctica de laboratorio: acceso a dispositivos de red mediante SSH

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	N/D
S1	VLAN 1	192.168.1.11	255.255.255.0	192.168.1.1
PC-A	NIC	192.168.1.3	255.255.255.0	192.168.1.1

Objetivos

Parte 1: Configurar los parámetros básicos de los dispositivos

Parte 2: Configurar el router para el acceso por SSH

Parte 3: Configurar el switch para el acceso por SSH

Parte 4: Ejecutar SSH desde la CLI del switch

Aspectos básicos/situación

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. Sin embargo, también puede transferir archivos mediante los protocolos asociados de FTP seguro (SFTP) o de copia segura (SCP).

Para que el protocolo SSH funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En esta práctica de laboratorio, 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.

Nota: Los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR) Cisco 1941 con Cisco IOS versión 15.2(4)M3 (imagen universalk9). Los switches que se utilizan son Cisco Catalyst 2960s con Cisco IOS versión 15.0(2) (imagen lanbasek9). Se pueden utilizar otros routers, switches y otras versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados que se obtienen pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces de router al final de esta práctica de laboratorio para obtener los identificadores de interfaz correctos.

Nota: Asegúrese de que los routers y los switches se hayan borrado y no tengan configuraciones de inicio. Si no está seguro, consulte al instructor.

Recursos necesarios

- 1 router (Cisco 1941 con Cisco IOS versión 15.2(4)M3, imagen universal o similar)
- 1 switch (Cisco 2960 con Cisco IOS versión 15.0(2), imagen lanbasek9 o comparable)
- 1 PC (Windows 7 u 8 con un programa de emulación de terminal, como Tera Term, y Wireshark instalado)
- Cables de consola para configurar los dispositivos con Cisco IOS mediante los puertos de consola
- Cables Ethernet, como se muestra en la topología

Parte 1: Configurar los parámetros básicos de dispositivos

En la parte 1, establecerá la topología de la red y configurará los parámetros básicos, como las direcciones IP de las interfaces, el acceso de los dispositivos y las contraseñas del router.

Paso 1: Realice el cableado de red como se muestra en la topología.

Paso 2: Iniciar y volver a cargar el router y el switch.

Paso 3: Configurar el router.

a. Acceda al router mediante el puerto de consola y habilite el modo EXEC privilegiado.

b. Ingrese al modo de configuración.

c. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

d. Use **class** como la contraseña cifrada de EXEC privilegiado.

e. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

f. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

g. Cifre las contraseñas de texto sin formato.

h. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

i. Configure y active la interfaz G0/1 en el router utilizando la información de la tabla de direccionamiento.

j. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 4: Configure PC-A.

a. Configure PC-A con una dirección IP y una máscara de subred.

b. Configure un gateway predeterminado para PC-A.

Paso 5: Verificar la conectividad de la red.

Haga ping a R1 desde PC-A. Si el ping falla, solucione los problemas de la conexión.

Parte 2: 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 2, configurara el router para que acepte conexiones SSH por las líneas VTY.

Paso 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.

```
Router(config)# hostname R1
```

b. Configure el dominio para el dispositivo.

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

Paso 2: Configurar el método de la clave de cifrado.

```
R1(config)# crypto key generate rsa modulus 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
```

Paso 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.

Paso 4: Habilitar SSH en las líneas VTY.

a. 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 telnet ssh
```

b. 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#
```

Paso 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#
```

Paso 6: Establecer una conexión SSH con el router.

a. Inicie Tera Term desde PC-A.

b. Establezca una sesión de SSH con R1. Use el nombre de usuario **admin** y la contraseña **adminpass**. Debería poder establecer una sesión de SSH con R1.

Parte 3: Configurar el switch para el acceso por SSH

En la parte 3, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH utilizando Tera Term.

Paso 1: Configurar los parámetros básicos en el switch.

a. Acceda al switch mediante el puerto de consola y habilite el modo EXEC privilegiado.

b. Ingrese al modo de configuración.

c. Deshabilite la búsqueda DNS para evitar que el router intente traducir los comandos incorrectamente introducidos como si fueran nombres de host.

d. Use **class** como la contraseña cifrada de EXEC privilegiado.

e. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.

f. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.

g. Cifre las contraseñas de texto sin formato.

h. Cree un aviso que advierta a todo aquel que acceda al dispositivo que el acceso no autorizado está prohibido.

i. Configure y active la interfaz VLAN 1 en el switch de acuerdo con lo que figura en la tabla de direccionamiento.

j. Guarde la configuración en ejecución en el archivo de configuración de inicio.

Paso 2: Configurar el switch para que tenga conectividad de SSH.

A fin de configurar SSH para el switch, utilice los mismos comandos que usó para configurar SSH en el router en la parte 2.

a. Configure el nombre del dispositivo como se indica en la tabla de direccionamiento.

b. Configure el dominio para el dispositivo.

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


c. Configure el método de la clave de cifrado.

```
S1(config)# crypto key generate rsa modulus 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 telnet 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
```

Paso 3: Establecer una conexión SSH con el switch.

Inicie Tera Term desde PC-A y acceda a la interfaz SVI en S1 mediante SSH.

¿Puede establecer una sesión de SSH con el switch?

Parte 4: Ejecutar SSH desde la CLI del switch

El cliente SSH está incorporado en Cisco IOS y puede ejecutarse desde la CLI. En la parte 4, deberá ejecutar una conexión SSH con el router desde la CLI del switch.

Paso 1: Observar los parámetros disponibles para el cliente SSH de Cisco IOS.

Utilice el signo de interrogación (**?**) para mostrar las opciones de parámetros disponibles con el comando **ssh**.

```
S1# ssh ?
  -c    Select encryption algorithm
  -l    Log in using this user name
  -m    Select HMAC algorithm
  -o    Specify options
  -p    Connect to this port
  -v    Specify SSH Protocol Version
  -vrf  Specify vrf name
  WORD  IP address or hostname of a remote system
```

Paso 2: 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 192.168.1.1
Password:
**********************************************
  Warning: Unauthorized Access is Prohibited!
**********************************************

R1#
```


b. Puede volver a S1 sin cerrar la sesión de SSH con R1 presionando **Ctrl**+**Mayús**+**6**. Suelte las teclas **Ctrl**+**Mayús**+**6** y presione **x**. Aparece el símbolo del sistema del modo EXEC privilegiado del switch.

```
R1#
S1#
```

c. Para volver a la sesión de SSH en R1, presione Intro en una línea en blanco de la CLI. Es posible que deba presionar Intro por segunda vez para ver el símbolo del sistema de la CLI del router.

```
S1#
[Resuming connection 1 to 192.168.1.1 ... ]

R1#
```

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

```
R1# exit

[Connection to 192.168.1.1 closed by foreign host]
S1#
```

¿Qué versiones de SSH se admiten en la CLI?

Reflexión

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

Tabla de resumen de interfaces de router

Resumen de interfaces de router				
Modelo de router	**Interfaz Ethernet 1**	**Interfaz Ethernet 2**	**Interfaz serial 1**	**Interfaz serial 2**
1800	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
1900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2801	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/1/0 (S0/1/0)	Serial 0/1/1 (S0/1/1)
2811	Fast Ethernet 0/0 (F0/0)	Fast Ethernet 0/1 (F0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)
2900	Gigabit Ethernet 0/0 (G0/0)	Gigabit Ethernet 0/1 (G0/1)	Serial 0/0/0 (S0/0/0)	Serial 0/0/1 (S0/0/1)

Nota: Para conocer la configuración del router, observe las interfaces a fin de identificar el tipo de router y cuántas interfaces tiene. No existe una forma eficaz de confeccionar una lista de todas las combinaciones de configuraciones para cada clase de router. En esta tabla, se incluyen los identificadores para las posibles combinaciones de interfaces Ethernet y seriales en el dispositivo. En esta tabla, no se incluye ningún otro tipo de interfaz, si bien puede haber interfaces de otro tipo en un router determinado. La interfaz BRI ISDN es un ejemplo. La cadena entre paréntesis es la abreviatura legal que se puede utilizar en un comando de Cisco IOS para representar la interfaz.