Práctica de laboratorio: Acceso a dispositivos de red mediante SSH (versión para el instructor)

Nota para el instructor: el color de fuente rojo o las partes resaltadas en gris indican texto que aparece en la copia del instructor solamente.

Topología

Tabla de direccionamiento

Dispositivo	Interfaz	Dirección IP	Máscara de subred	Gateway predeterminado
R1	G0/1	192.168.1.1	255.255.255.0	No aplicable
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 parámetros básicos de los dispositivos

Parte 2: Configurar el router para el acceso por SSH

Parte 3: Examinar una sesión de Telnet con Wireshark

Parte 4: Examinar una sesión de SSH con Wireshark

Parte 5: Configurar el switch para el acceso por SSH

Parte 6: Ejecutar SSH desde la CLI del switch

Información básica/Situación

En el pasado, Telnet era el protocolo de red más común utilizado para configurar dispositivos de red de manera remota. Sin embargo, los protocolos como Telnet no autentican ni encriptan la información entre el cliente y el servidor. Esto permite que un programa detector de redes intercepte contraseñas y la información de configuración.

Shell seguro (SSH) es un protocolo de red que establece una conexión de emulación de terminal segura a un router u otro dispositivo de red. SSH encripta toda la información que atraviesa el enlace de red y proporciona autenticación de la computadora remota. 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 de transferencia segura de archivos (SFTP) o de copia segura (SCP) asociados.

Para que SSH funcione, los dispositivos de red que se comunican deben estar configurados para admitirlo. En esta práctica de laboratorio, habilitará el servidor SSH en un router y luego se conectará a ese router mediante una PC con un cliente SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP.

En esta práctica de laboratorio, configurará un router para que acepte conectividad de SSH y utilizará Wireshark para capturar y ver sesiones de Telnet y SSH. Esto demostrará la importancia de la encriptación con SSH. También se lo desafiará a que configure un switch para que tenga conectividad de SSH.

Nota: los routers que se utilizan en las prácticas de laboratorio de CCNA son routers de servicios integrados (ISR, Integrated Services Routers) 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 de lanbasek9). Pueden utilizarse otros routers, switches y versiones de Cisco IOS. Según el modelo y la versión de Cisco IOS, los comandos disponibles y los resultados obtenidos pueden diferir de los que se muestran en las prácticas de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra 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 con el instructor.

Nota para el instructor: consulte el Manual de prácticas de laboratorio para el instructor a fin de conocer los procedimientos para inicializar y volver a cargar los dispositivos.

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 similar)
- 1 PC (Windows 7, Vista o XP con Wireshark y programa de emulación de terminal — por ejemplo, Tera Term — instalados)
- Cables de consola para configurar los dispositivos 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 los parámetros básicos de configuración, como las direcciones IP de interfaz, el acceso al dispositivo y las contraseñas del router.

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

Paso 2: Inicialice y vuelva a cargar el router y el switch.

Paso 3: Configurar el router.

a. Acceda al router mediante el puerto de consola e ingrese al modo EXEC privilegiado.

b. Entre 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. Asigne **class** como la contraseña encriptada de EXEC privilegiado.

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

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

g. Encripte las contraseñas de texto no cifrado.

h. Cree un mensaje de aviso que advierta a todo el 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 contenida en la Tabla de direccionamiento.

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

Paso 4: Configurar la PC-A

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

b. Configure un gateway predeterminado para la PC-A.

Paso 5: Verificar la conectividad de la red.

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

Parte 2: Configurar el router para el acceso por SSH

Usar 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. SSH encripta los datos de sesión y proporciona autenticación del dispositivo, por lo que se recomienda SSH para las conexiones remotas. En la parte 2, configurará el router para que acepte conexiones SSH por las líneas VTY.

Paso 1: Configurar la autenticación del dispositivo

El nombre del dispositivo y el dominio se utilizan como parte de la clave de encriptación, cuando 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 encriptación

```
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 el nombre de usuario de una base de datos local

```
R1(config)# username admin privilege 15 secret adminpass
R1(config)#
*Feb  6 23:24:43.971: End->Password:QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
R1(config)#
```

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

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: Guarde 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#
```

Parte 3: Examinar una sesión de Telnet con Wireshark

En la parte 3, utilizará Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder al R1 mediante Telnet, se registrará y luego emitirá el comando show run en el router.

Nota: si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, debe instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html) y PuTTy (www.putty.org).

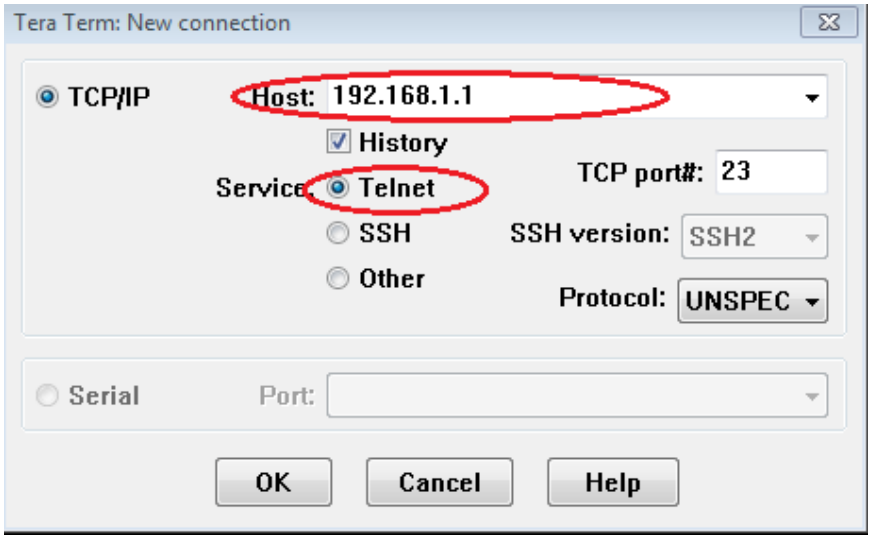
Nota: Telnet no está disponible de manera predeterminada mediante el símbolo del sistema de Windows 7. Para habilitar Telnet a fin de utilizarlo en la ventana del símbolo del sistema, haga clic en **Inicio** > **Panel de control** > **Programas** > **Programas y características** > **Activar o desactivar las características de Windows**. Haga clic en la casilla de verificación **Client Telnet** y, a continuación, haga clic en **Aceptar**.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

Nota: si no puede comenzar la captura en la interfaz LAN, necesitará abrir Wireshark mediante la opción **Run as Administrator** (Ejecutar como administrador).

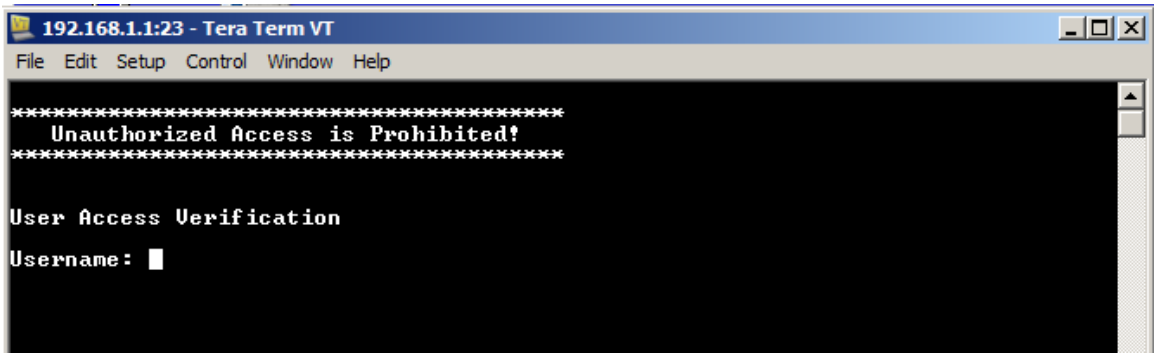
Paso 2: Iniciar una sesión de Telnet en el router

a. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, introduzca **192.168.1.1**.



¿Cuál es el puerto TCP predeterminado para las sesiones de Telnet? _____ Puerto 23

b. En la petición de entrada Username: (Nombre de usuario:), introduzca **admin**, y en la petición de entrada Password: (Contraseña:), introduzca **adminpass**. Estas peticiones de entrada se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando **login local**.



c. Emita el comando **show run**.

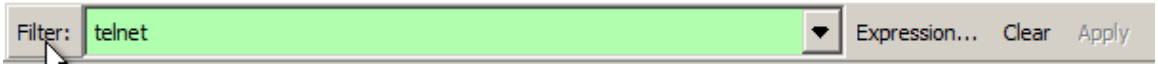
```
R1# show run
```

d. Introduzca **exit** para salir de la sesión de Telnet y de Tera Term.

```
R1# exit
```

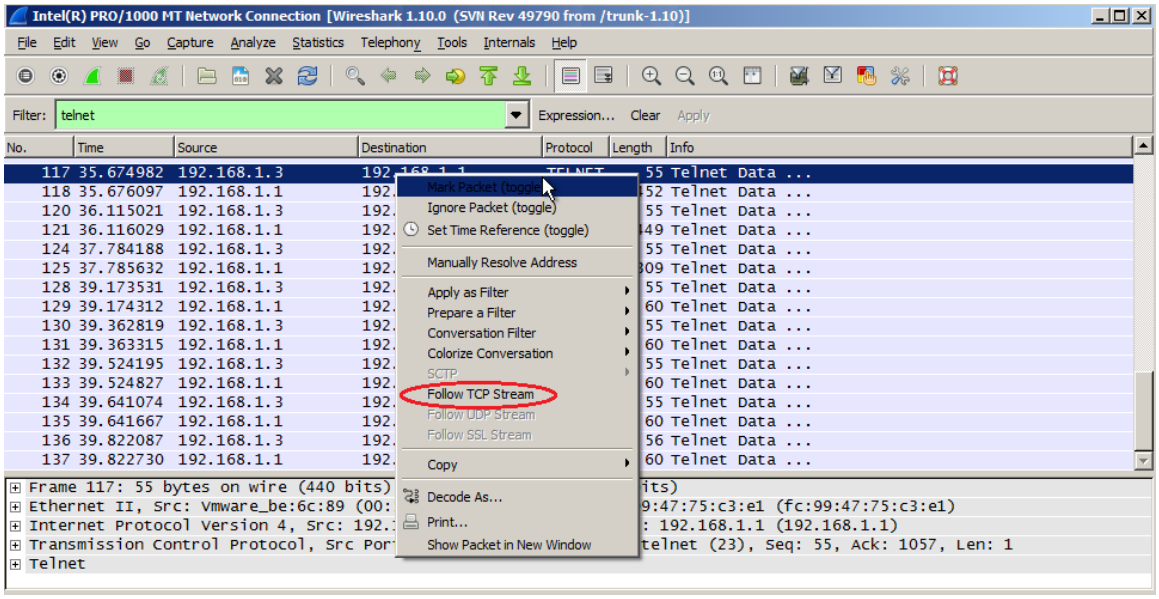
Paso 3: Detener la captura de Wireshark

Paso 4: Aplicar un filtro de Telnet a los datos de captura de Wireshark

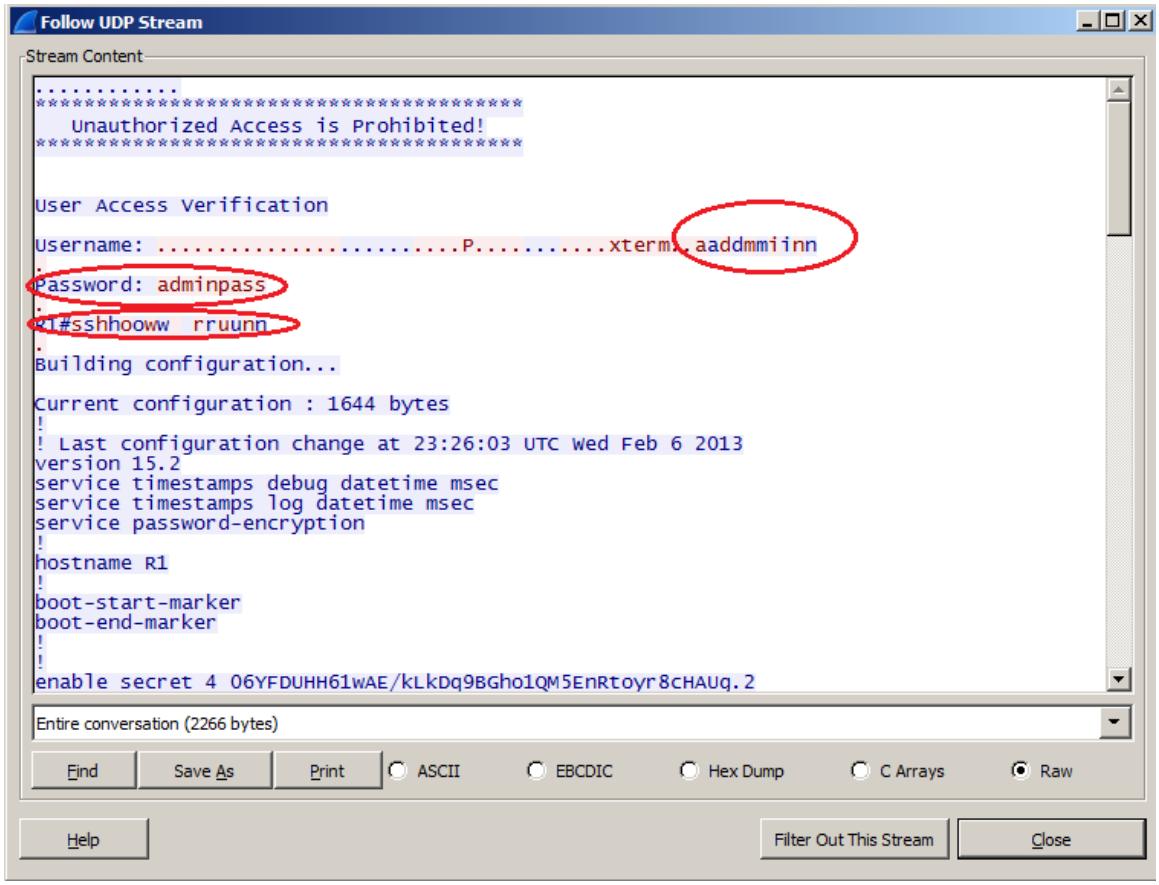


Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón secundario en una de las líneas **Telnet** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).



b. En la ventana Follow TCP Stream, se muestran los datos para su sesión de Telnet con el router. Toda la sesión, incluida la contraseña, se muestra como texto no cifrado. Observe que el nombre de usuario y el comando **show run** que introdujo se muestran con caracteres duplicados. Esto lo causa el ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.



c. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream**, haga clic en **Close** (Cerrar).

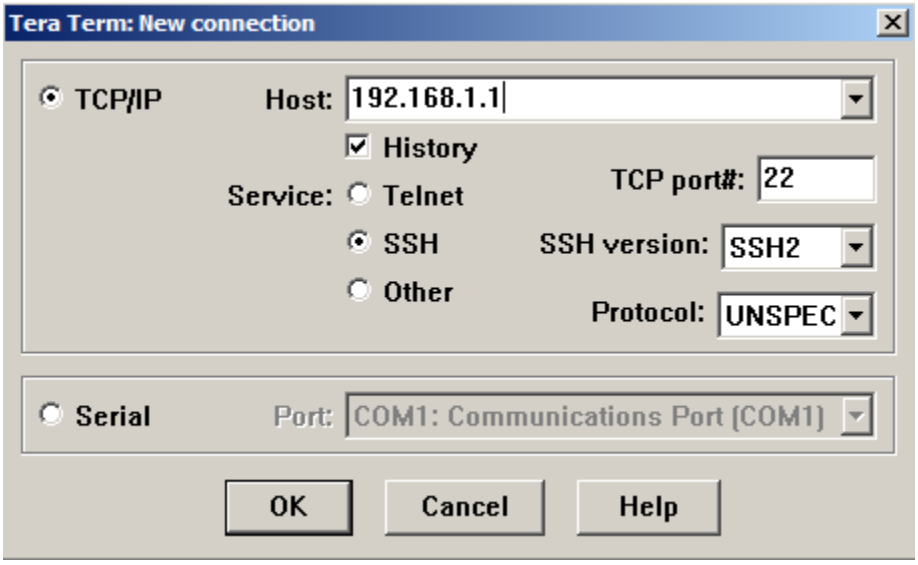
Parte 4: Examinar una sesión de SSH con Wireshark

En la parte 4, utilizará el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

Paso 1: Abrir Wireshark y comenzar a capturar los datos en la interfaz LAN.

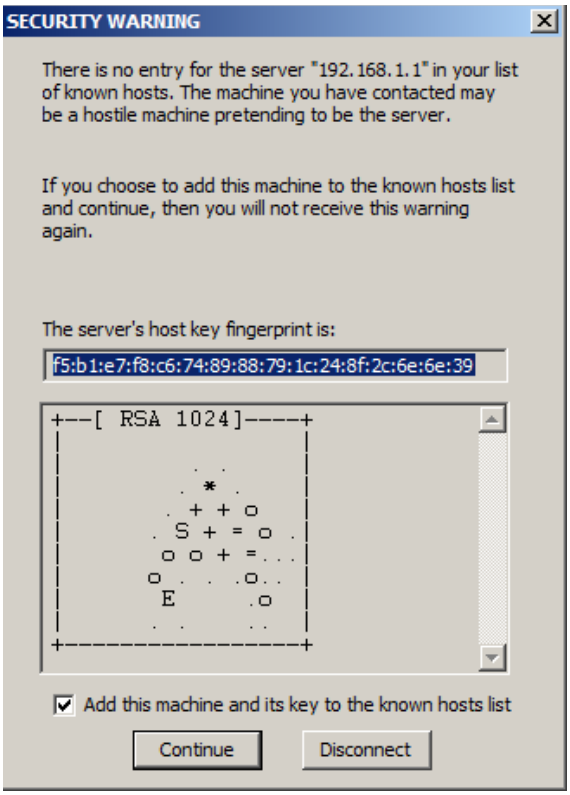
Paso 2: Iniciar una sesión de SSH en el router

a. Abra Tera Term e introduzca la dirección IP de la interfaz G0/1 del R1 en el campo Host: de la ventana Tera Term: New Connection (Tera Term: Conexión nueva). Asegúrese de que el botón de opción **SSH** esté seleccionado y, a continuación, haga clic en **OK** (Aceptar) para conectarse al router.

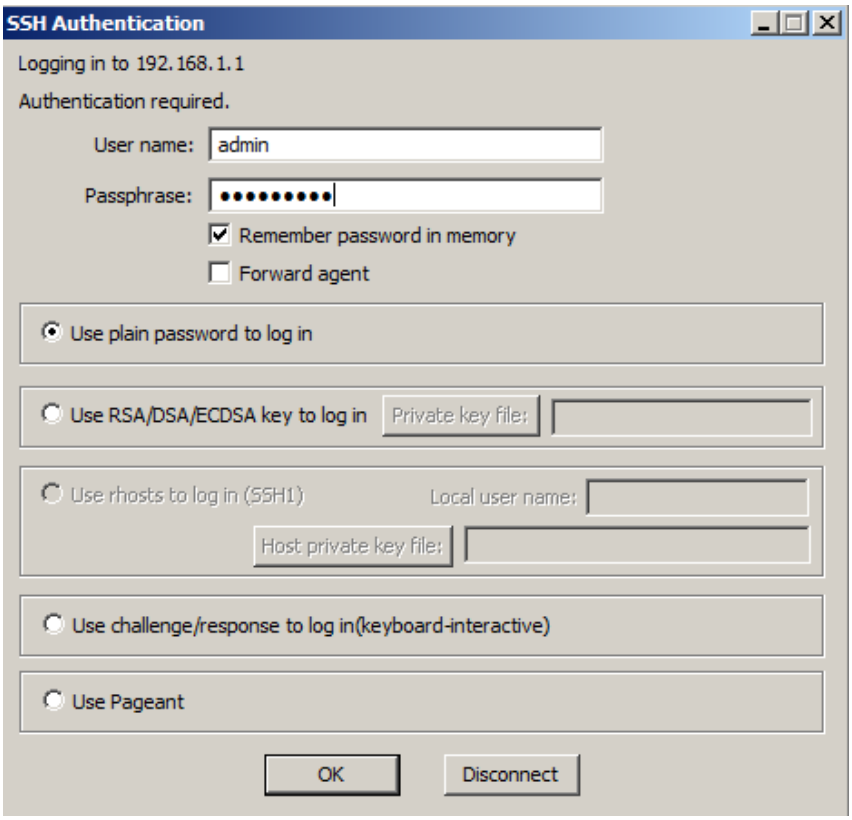


¿Cuál es el puerto TCP predeterminado que se utiliza para las sesiones de SSH? _____
Puerto 22

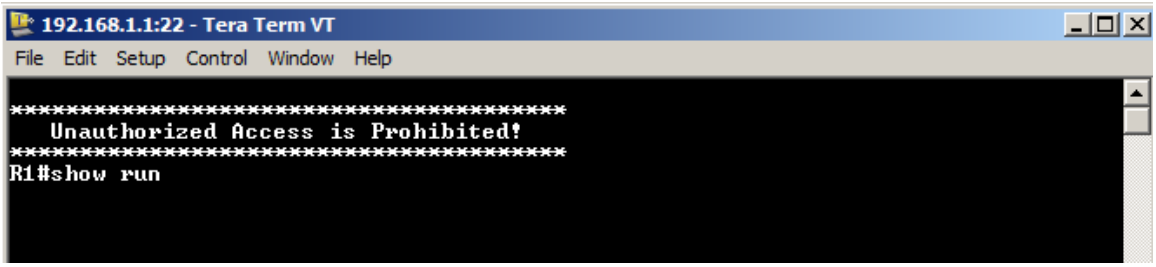
b. La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (ADVERTENCIA DE SEGURIDAD) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y, luego, haga clic en **Continue** (Continuar).



c. En la ventana de la autenticación de SSH, introduzca **admin** en User name (Nombre de usuario) y **adminpass** en Passphrase (Frase de contraseña). Haga clic en **OK** (Aceptar) para registrarse en el router.



d. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En la petición de entrada, emita el comando **show version**.



e. Salga de la sesión de SSH y de Tera Term emitiendo el comando **exit**.

```
R1# exit
```

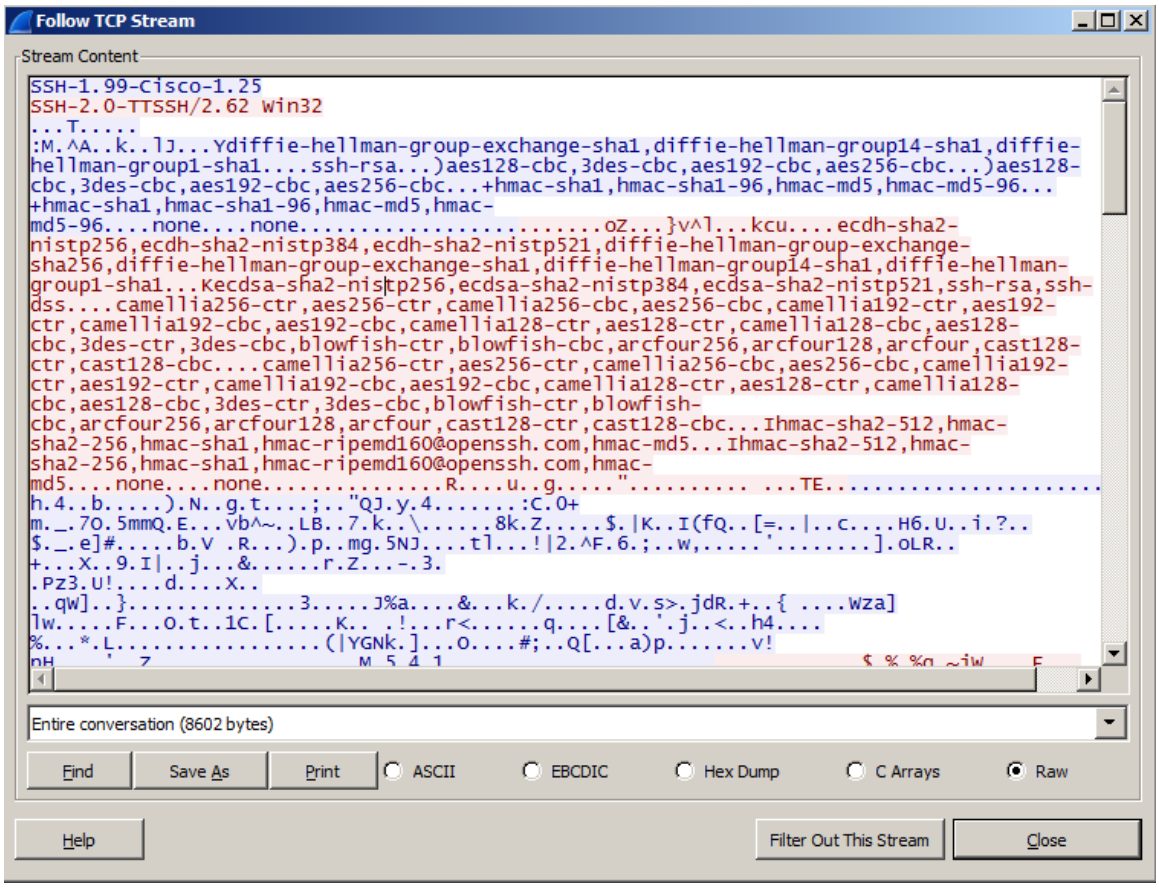
Paso 3: Detener la captura de Wireshark

Paso 4: Aplicar un filtro de SSH a los datos de captura de Wireshark

Paso 5: Utilizar la característica Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet

a. Haga clic con el botón secundario en una de las líneas **SSHv2** en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream** (Seguir stream de TCP).

b. Examine la ventana **Follow TCP Stream** de la sesión de SSH. Los datos se encriptaron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.



¿Por qué se prefiere SSH a Telnet para las conexiones remotas?

_____

_____

Las respuestas pueden variar. SSH lleva a cabo una autenticación con un dispositivo y le hace saber si es la primera vez que se conecta al dispositivo. También protege la sesión al encriptar todos los datos.

c. Después de analizar la sesión de SSH, haga clic en **Close** (Cerrar).

d. Cierre Wireshark.

Parte 5: Configurar el switch para el acceso por SSH

En la parte 5, configurará el switch en la topología para que se acepten conexiones SSH. Una vez configurado el switch, establezca una sesión de SSH en él utilizando Tera Term.

Paso 1: Configurar los parámetros básicos en el switch

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.

Paso 3: Establecer una conexión SSH al switch

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

Paso 4: Resuelva cualquier problema que se presente.

¿Puede establecer una sesión de SSH con el switch?

_____

Sí. SSH se puede configurar en un switch mediante los mismos comandos que se usaron en el router.

Parte 6: Ejecutar SSH desde la CLI del switch

El cliente de SSH está incorporado en Cisco IOS y puede ejecutarse desde la CLI. En la parte 6, ejecutará una conexión SSH al router desde la CLI del switch.

Paso 1: Ver los parámetros disponibles para el cliente de 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 al router R1 mediante SSH desde el S1

a. Cuando accede al R1 mediante SSH, debe utilizar la opción **–l admin**. De esta manera, podrá iniciar sesión como usuario **admin**. Cuando se le solicite, introduzca **adminpass** en el campo Password (contraseña).

```
S1# ssh -l admin 192.168.1.1
Password:
*********************************************
  Warning: Unauthorized Access is Prohibited!
*********************************************

R1#
```

b. Para volver al S1 sin cerrar la sesión de SSH para el R1, presione las teclas **Ctrl**+**Mayús**+**6.** Suelte las teclas **Ctrl**+**Mayús**+**6** y presione **x.** Debería ver la ventana de petición de entrada del modo EXEC privilegiado del switch.

```
R1#
S1#
```

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

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

R1#
```


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

```
R1# exit

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

¿Qué versiones de SSH se admiten en la CLI?

_____

_____

Las respuestas pueden variar, pero se puede determinar al introducir **ssh –v ?** en la línea de comandos. La versión 15.0(2) del IOS que se ejecuta en el switch 2960 admite SSH v1 y V2.

```
S1# ssh -v ?
  1  Protocol Version 1
  2  Protocol Version 2
```

Reflexión

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

_____

Las respuestas pueden variar. Se agregaría el nombre de usuario y la contraseña de cada usuario a la base de datos local mediante el comando username. También es posible utilizar un servidor RADIUS o TACACS, pero este tema aún no se analizó.

Tabla de resumen de interfaces del router

Resumen de interfaces del 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 hacer 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 los comandos de Cisco IOS para representar la interfaz.

Configuraciones de dispositivos, final

Router R1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname R1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
no aaa new-model
memory-size iomem 10
!
no ip domain lookup
ip domain name ccna-lab.com
ip cef
no ipv6 cef
multilink bundle-name authenticated
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
!
interface GigabitEthernet0/0
 no ip address
 shutdown
 duplex auto
 speed auto
!
interface GigabitEthernet0/1
 description Connection to S1-F0/5.
 ip address 192.168.1.1 255.255.255.0
 duplex auto
 speed auto
!
interface Serial0/0/0
 no ip address
 shutdown
 clock rate 2000000
!
interface Serial0/0/1
 no ip address
 shutdown
!
ip forward-protocol nd
!
no ip http server
```



```
no ip http secure-server
!
control-plane
!
!
banner motd ^C
**************************************
   Unauthorized Access is Prohibited!
**************************************
^C
!
line con 0
 password 7 00071A150754
 login
line aux 0
line 2
 no activation-character
 no exec
 transport preferred none
 transport input all
 transport output pad telnet rlogin lapb-ta mop udptn v120 ssh
 stopbits 1
line vty 0
 password 7 110A1016141D
 login local
 transport input telnet ssh
line vty 1 4
 login local
 transport input telnet ssh
!
scheduler allocate 20000 1000
!
end
```

Switch S1

```
service timestamps debug datetime msec
service timestamps log datetime msec
service password-encryption
!
hostname S1
!
boot-start-marker
boot-end-marker
!
enable secret 4 06YFDUHH61wAE/kLkDq9BGho1QM5EnRtoyr8cHAUg.2
!
username admin privilege 15 secret 4 QHjxdsVkjtoP7VxKIcPsLdTiMIvyLkyjT1HbmYxZigc
no aaa new-model
system mtu routing 1500
```



```
!
!
no ip domain-lookup
ip domain-name ccna-lab.com
!
spanning-tree mode pvst
spanning-tree extend system-id
!
vlan internal allocation policy ascending
!
interface FastEthernet0/1
!
interface FastEthernet0/2
!
interface FastEthernet0/3
!
interface FastEthernet0/4
!
interface FastEthernet0/5
!
interface FastEthernet0/6
!
interface FastEthernet0/7
!
interface FastEthernet0/8
!
interface FastEthernet0/9
!
interface FastEthernet0/10
!
interface FastEthernet0/11
!
interface FastEthernet0/12
!
interface FastEthernet0/13
!
interface FastEthernet0/14
!
interface FastEthernet0/15
!
interface FastEthernet0/16
!
interface FastEthernet0/17
!
interface FastEthernet0/18
!
interface FastEthernet0/19
!
interface FastEthernet0/20
```



```
!
interface FastEthernet0/21
!
interface FastEthernet0/22
!
interface FastEthernet0/23
!
interface FastEthernet0/24
!
interface GigabitEthernet0/1
!
interface GigabitEthernet0/2
!
interface Vlan1
 ip address 192.168.1.11 255.255.255.0
!
ip http server
ip http secure-server
!
!
banner motd ^C
**************************************
  Unauthorized Access is Prohibited!
**************************************
^C
!
line con 0
 password 7 060506324F41
 login
line vty 0 4
 password 7 060506324F41
 login local
 transport input telnet ssh
line vty 5 15
 password 7 00071A150754
 login local
 transport input telnet ssh
!
end
```

