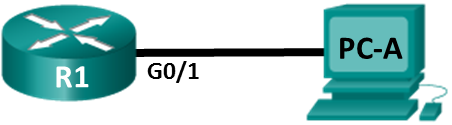
Actividad de laboratorio: examinar Telnet y SSH en Wireshark (Versión del instructor: actividad de laboratorio opcional)

**Nota del instructor**: los elementos destacados rojo o gris indican texto que aparece solo en la copia del instructor. Las actividades opcionales están pensadas para mejorar la comprensión o brindar más ejercicios prácticos .

1. Topología



1. Tabla de direccionamiento

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| El administrador | Interfaces | IP Address (Dirección IP) | Subnet Mask (Máscara de subred) | Gateway predeterminado |
| R1 | G0/1 | 192.168.1.1 | 255.255.255.0 | N/D |
| PC-A | NIC | 192.168.1.3 | 255.255.255.0 | 192.168.1.1 |

1. Objetivos

Parte 1: configurar los dispositivos para el acceso por SSH

Parte 2: examinar una sesión de Telnet con Wireshark

Parte 3: examinar una sesión de SSH con Wireshark

1. Aspectos básicos/situación

En esta actividad de laboratorio, deberá configurar un router para que acepte la conectividad de SSH y usará Wireshark para capturar y ver las sesiones de Telnet y SSH. Esto demostrará la importancia del cifrado con SSH.

**Nota**: los routers que se utilizan en las actividades 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 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 actividades de laboratorio. Consulte la tabla Resumen de interfaces del router que se encuentra al final de esta práctica de laboratorio para conocer 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.

**Nota del instructor**: consulte el Manual de actividades de laboratorio del instructor para conocer los procedimientos para iniciar y volver a cargar los dispositivos.

1. Recursos necesarios

* Un router (Cisco 1941 con Cisco IOS, versión 15.2(4)M3, imagen universal o similar)
* Una PC (Windows 7 u 8, Vista o XP con Wireshark y programa de emulación de terminal —como Tera Term— instalados)
* Cables de consola para configurar los dispositivos Cisco IOS mediante los puertos de la consola
* Cables Ethernet, como se muestra en la topología

1. Configurar los dispositivos para el acceso por SSH

En la parte 1, establecerá la topología de la red y configurará los ajustes básicos, como las direcciones IP de la interfaz, el acceso al dispositivo y las contraseñas del router.

* 1. Realice el cableado de red tal como se muestra en la topología.
  2. Inicie y vuelva a cargar el router.
  3. Configure los ajustes básicos en el router.
     1. Acceda al router mediante el puerto de la consola e ingrese al modo EXEC privilegiado.
     2. Entre al modo de configuración.
     3. Configure el nombre del dispositivo como se indica en la tabla de direccionamiento.
     4. Inhabilite la búsqueda DNS para evitar que el router intente traducir los comandos mal introducidos como si fueran nombres de host.
     5. Asigne **class** como la contraseña cifrada de EXEC privilegiado.
     6. Asigne **cisco** como la contraseña de la consola y habilite el inicio de sesión.
     7. Asigne **cisco** como la contraseña de VTY y habilite el inicio de sesión.
     8. Encripte las contraseñas de texto no cifrado.
     9. Cree un banner que advierta a todo el que acceda al dispositivo que el acceso no autorizado está prohibido.
     10. Configure y active la interfaz G0/1 utilizando la información de la tabla de direccionamiento.
  4. Configure R1 para el acceso por SSH.
     1. Configure el dominio para el dispositivo.

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

* + 1. Configure el método de cifrado de clave.

R1(config)# **crypto key generate rsa modulus 1024**

* + 1. Configure un nombre de usuario de la base de datos local.

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

* + 1. Habilite Telnet y SSH en las líneas VTY.

R1(config)# **line vty 0 4**

R1(config-line)# **transport input telnet ssh**

* + 1. 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**

* 1. Guarde la configuración en ejecución en el archivo de configuración de inicio.
  2. Configure PC-A.
     1. Configure PC-A con una dirección IP y una máscara de subred.
     2. Configure una puerta de enlace predeterminada para PC-A.
  3. Verificar la conectividad de la red

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

1. Examinar una sesión de Telnet con Wireshark

En la parte 2, deberá usar Wireshark para capturar y ver los datos transmitidos de una sesión de Telnet en el router. Utilizará Tera Term para acceder a R1 mediante Telnet, se registrará y luego emitirá el comando **show run** en el router.

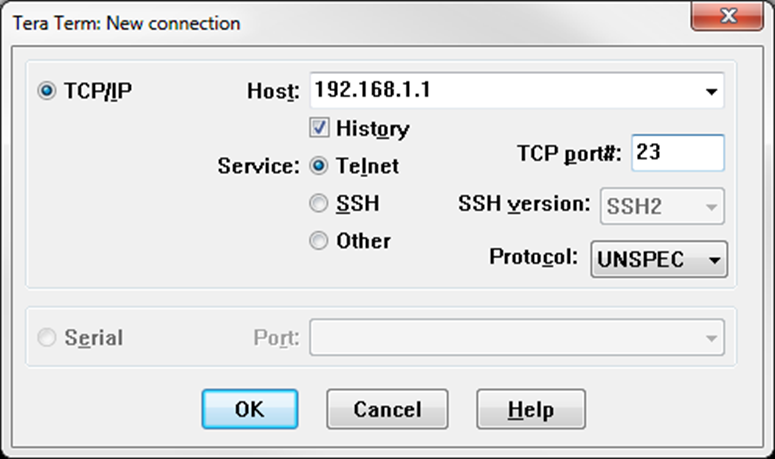
**Nota**: si no tiene un paquete de software de cliente Telnet/SSH instalado en la PC, deberá instalarlo antes de continuar. Dos paquetes populares de software gratuito de Telnet/SSH son Tera Term (<http://download.cnet.com/Tera-Term/3000-20432_4-75766675.html>) y PuTTY ([www.putty.org](http://www.putty.org/)).

**Nota**: Telnet no está disponible desde el símbolo del sistema enWindows 7, de manera predeterminada. Para habilitar Telnet para usarlo en la ventana de símbolo del sistema, haga clic en **Start** (Comenzar) > **Control Panel** (Panel de control) > **Programs** (Programas) > **Programs and Features** (Programas y funciones) > **Turn Windows features on or off** (Activar o desactivar las funciones de Windows). Haga clic en la casilla de verificación **Telnet Client** (Cliente Telnet) y luego haga clic en **OK** (Aceptar).

* 1. Capture los datos.
     1. Abra Wireshark.
     2. Comience a capturar los datos en la interfaz de LAN.

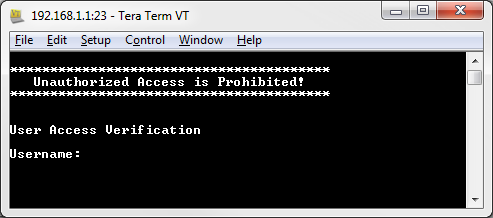
**Nota**: si no puede comenzar la captura en la interfaz LAN, deberá abrir Wireshark con la opción **Run as Administrator** (Ejecutar como administrador).

* 1. Inicie una sesión de Telnet en el router.
     1. Abra Tera Term y seleccione el botón de opción **Telnet** del campo Service (Servicio) y, en el campo Host, ingrese **192.168.1.1**.



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

* + 1. En la petición Username: (Nombre de usuario:), ingrese **admin** y en la petición Password: (Contraseña:), ingrese **adminpass**. Estas peticiones se generan porque configuró las líneas VTY para que utilicen la base de datos local con el comando **login local**.



* + 1. Emita el comando **show run**.

R1# **show run**

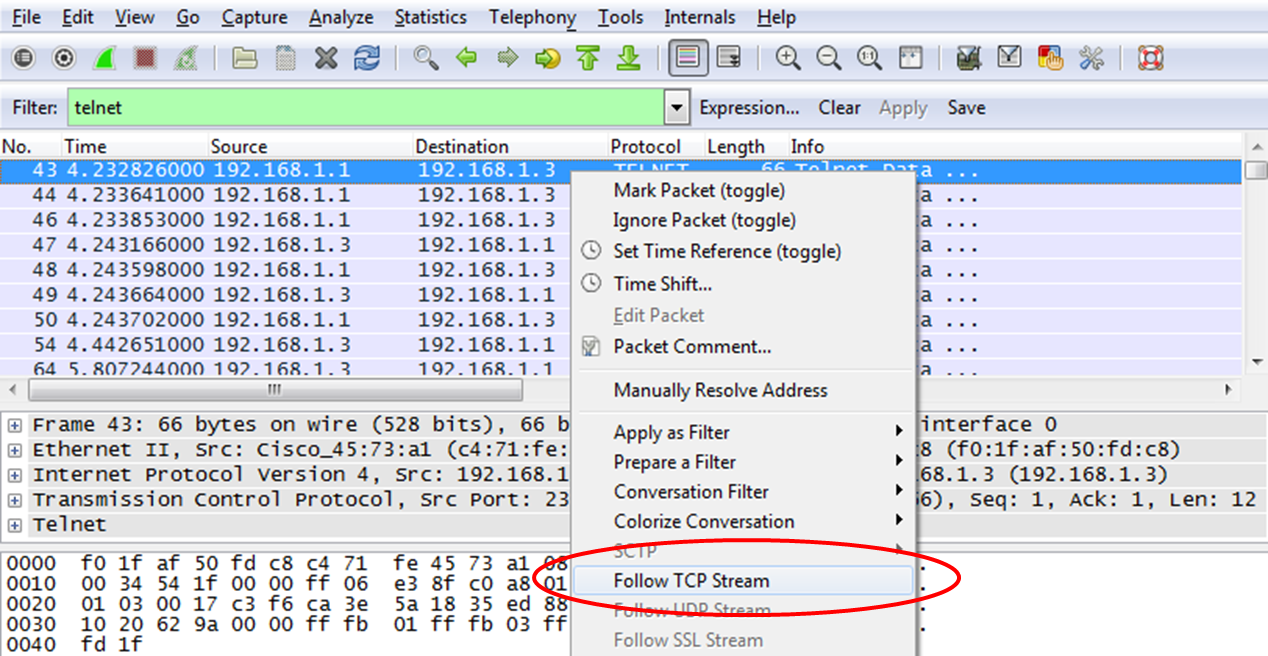
* + 1. Ingrese **exit** (Salir) para cerrar la sesión de Telnet y Tera Term.

R1# **exit**

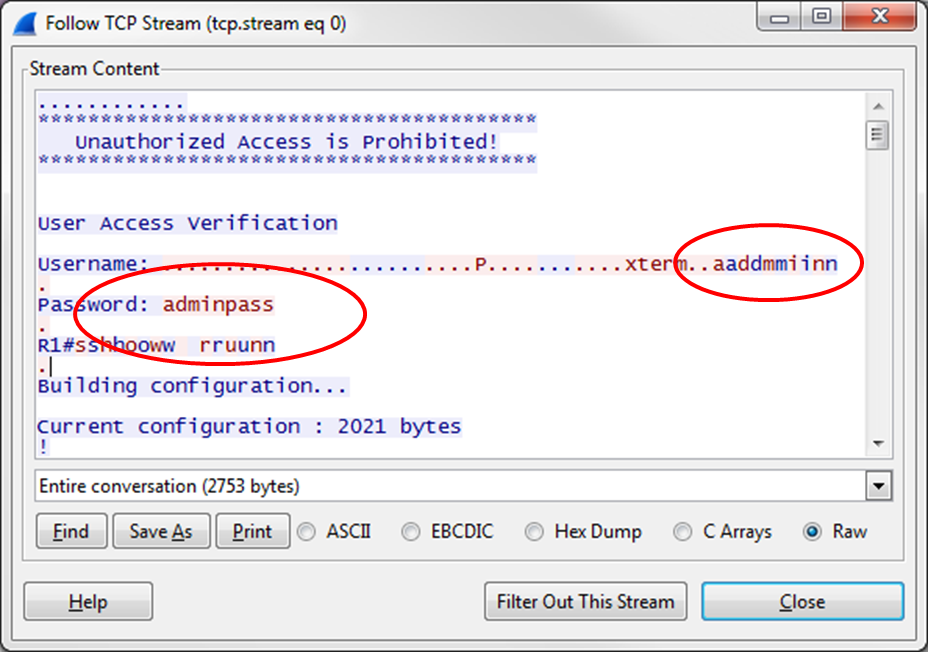
* 1. Detenga la captura Wireshark.
  2. Aplique un filtro de Telnet a los datos de captura de Wireshark.



* 1. Utilice la función Follow TCP Stream (Seguir stream de TCP) en Wireshark para ver la sesión de Telnet.
     1. Haga clic con el botón derecho en una de las líneas **Telnet** y en la sección **Packet list** (Lista de paquetes) de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream**.



* + 1. En la ventana Follow TCP Stream, se muestran los datos para su sesión de Telnet con el router. Toda la sesión y la contraseña se muestran como texto no cifrado. Observe que el nombre de usuario y el comando **show run** que ingresó aparecen con caracteres duplicados. Esto se debe al ajuste de eco en Telnet para permitirle ver los caracteres que escribe en la pantalla.

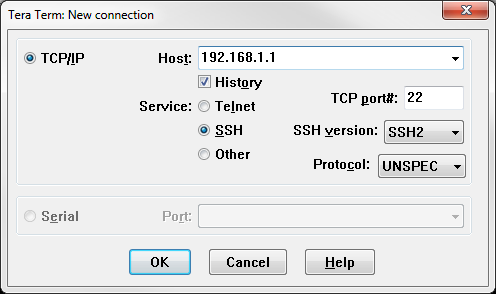


* + 1. Cuando termine de revisar la sesión de Telnet en la ventana **Follow TCP Stream**, haga clic en **Close** (Cerrar).

1. Examinar una sesión de SSH con Wireshark

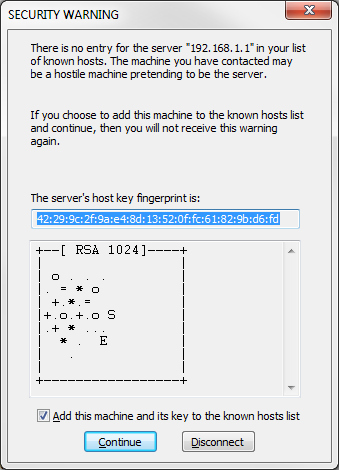
En la parte 4, deberá usar el software Tera Term para establecer una sesión de SSH con el router. Se usará Wireshark para capturar y ver los datos de esta sesión de SSH.

* 1. Abra Wireshark y comience a capturar los datos en la interfaz LAN.
  2. Inicie una sesión de SSH en el router.
     1. Abra Tera Term e ingrese la dirección IP de la interfaz G0/1 de 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 haga clic en **OK** para conectarse al router.

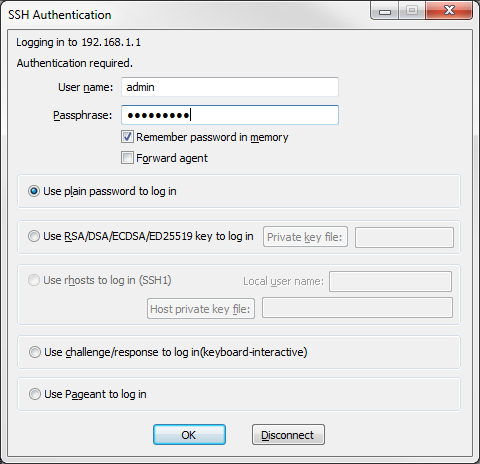


¿Cuál es el puerto TCP predeterminado que se usa para las sesiones de SSH? \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ Puerto 22

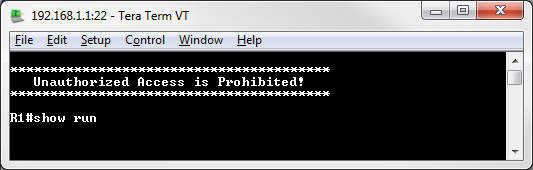
* + 1. La primera vez que establece una sesión de SSH con un dispositivo, se genera una **SECURITY WARNING** (Advertencia de seguridad) para comunicarle que no se conectó a ese dispositivo anteriormente. Este mensaje es parte del proceso de autenticación. Lea la advertencia de seguridad y luego haga clic en **Continue** (Continuar).



* + 1. En la ventana de la autenticación de SSH, ingrese **admin** en username y **adminpass** en passphrase (Frase de contraseña). Haga clic en **OK** para registrarse en el router.



* + 1. Estableció una sesión de SSH en el router. El software Tera Term parece muy similar a una ventana de comandos. En el símbolo del sistema, emita el comando **show run**.



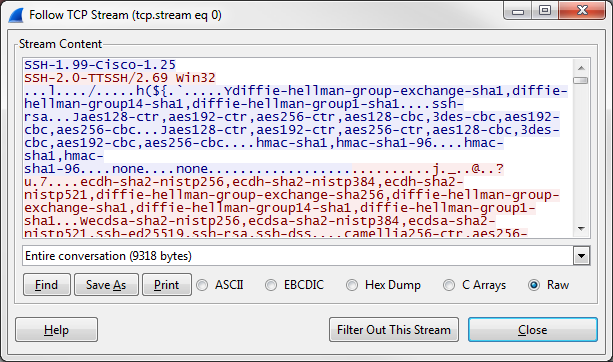
* + 1. Salga de la sesión de SSH emitiendo el comando **exit**.

R1# **exit**

* 1. Detenga la captura Wireshark.
  2. Aplique un filtro de SSH a los datos de captura de Wireshark.



* 1. Utilice la función Follow TCP Stream en Wireshark para ver la sesión de SSH.
     1. Haga clic con el botón derecho en una de las líneas **SSHv2** y en la sección **Packet list** de Wireshark y, en la lista desplegable, seleccione **Follow TCP Stream**.
     2. Examine la ventana **Follow TCP Stream** en la sesión de SSH. Los datos se cifraron y son ilegibles. Compare los datos de la sesión de SSH con los datos de la sesión de Telnet.



¿Por qué se prefiere SSH en lugar de Telnet para las conexiones remotas?

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar.

Similar a Telnet, SSH se usa para acceder a comandos y ejecutarlos en un sistema remoto. Sin embargo, el protocolo SSH permite a los usuarios comunicarse de manera segura con un sistema remoto al cifrar las comunicaciones. Esto evita que se capten datos confidenciales durante la transmisión, como nombres de usuario y contraseñas.

Al usar un cifrado de claves públicas para respaldar la comunicación entre computadoras remotas, SSH elimina la necesidad de intercambiar claves públicas iniciales entre los participantes de la comunicación. Con SSH, la clave privada nunca se envía, ya que usa un par de claves (una pública y una privada) para el cifrado. Los mensajes cifrados con una clave pública solo pueden descifrarse con la clave privada correspondiente. Dado que la llave privada nunca abandona a los terminales, el sistema es inherentemente seguro.

Cuando un usuario establece una conexión SSH por primera vez, el programa del cliente SSH intercambia las claves públicas. El usuario confía en la seguridad de la red durante el intercambio de clave. Cuando el usuario hace clic en Continue (Continuar) en el cliente SSH, está aceptando el acceso del sistema remoto a la lista de hosts conocidos.

* + 1. Luego de haber examinado su sesión SSH, haga clic en **Close**.
    2. Cierre Wireshark.

1. Reflexión

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

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Las respuestas pueden variar. Agregaría cada nombre de usuario y la contraseña a la base de datos usando el comando username. También se puede agregar un servidor RADIUS o TACACS, pero aún no se abordó este tema.

1. Tabla de resumen de interfaces del router

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Resumen de la interfaz 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 para 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, aunque 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 los comandos de Cisco IOS para representar la interfaz. | | | | |

1. Configuración de dispositivo: final
2. 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