

Práctica de laboratorio 8.3.3b Configuración de un router remoto mediante SSH



Objetivos

- Utilizar SDM para configurar un router para que acepte las conexiones SSH.
- Configurar el software de cliente SSH en una PC.
- Establecer una conexión a un ISR de Cisco usando SSH, versión 2.
- Verificar la configuración en ejecución existente.
- Configurar un router sin SDM para SSH mediante la CLI del IOS de Cisco.

Información básica / Preparación

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

Shell seguro (SSH, Secure Shell) 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 es más comúnmente utilizado para conectarse a una máquina remota y ejecutar comandos. Sin embargo, también puede transferir archivos mediante los protocolos SFTP o SCP asociados.

Para que SSH funcione, los dispositivos de red que se comunican deben admitirlo. En esta práctica de laboratorio, usted podrá habilitar el servidor SSH en un router y luego conectarse a ese router mediante una PC con un cliente SSH instalado. En una red local, la conexión generalmente se realiza utilizando Ethernet e IP. Los dispositivos de red conectados a través de otros tipos de enlaces, como serial, también pueden ser administrados mediante SSH, siempre que admitan IP. Al igual que Telnet, SSH es un protocolo de Internet dentro de banda basado en TCP/IP.

Puede utilizar los comandos SDM de Cisco o la CLI del IOS de Cisco para configurar SSH en el router. El ISR Cisco 1841 admite las versiones 1 y 2 de SSH. Se prefiere la versión 2. El cliente SSH utilizado en esta práctica de laboratorio es PuTTY y puede descargarse de manera gratuita. Si está trabajando con un router que no posee SDM instalado, utilice los comandos CLI de IOS de Cisco para configurar SSH. Las instrucciones se encuentran en el Paso 2 de esta práctica de laboratorio. Para realizar la configuración básica de router, consulte la práctica de laboratorio 5.3.5, "Configuración de parámetros básicos del router con la CLI de IOS."

El SDM Cisco es admitido por una amplia variedad de routers Cisco y versiones del software IOS de Cisco. Muchos de los routers más nuevos de Cisco vienen con SDM preinstalado. Esta práctica de laboratorio usa un router Cisco 184, que cuenta con SDM (y SDM Express) preinstalado. Puede utilizar otro modelo de router que admita SDM. Si el router no posee SDM instalado, puede descargar gratuitamente la última versión desde <http://www.cisco.com/pcgi-bin/tablebuild.pl/sdm>. Desde esta página Web también puede ver o descargar "Descargar e instalar el Administrador de routers y dispositivos de seguridad Cisco." Este documento contiene instrucciones y requerimientos del sistema para instalar SDM.

Nota: Si está utilizando SDM para configurar SSH, antes de realizar esta práctica, debe completar la práctica de laboratorio 5.2.3, "Configuración de un ISR con SDM Express" en el router que desea utilizar. Esta práctica de laboratorio supone que el router se configuró anteriormente con los valores básicos.

Nota: Si se elimina startup-config en un router SDM, SDM ya no aparecerá de manera predeterminada cuando se reinicie el router. En este caso, es necesario construir una configuración básica del router mediante los comandos IOS de Cisco. Consulte el procedimiento que aparece al final de esta práctica de laboratorio o comuníquese con su instructor.

Recursos requeridos

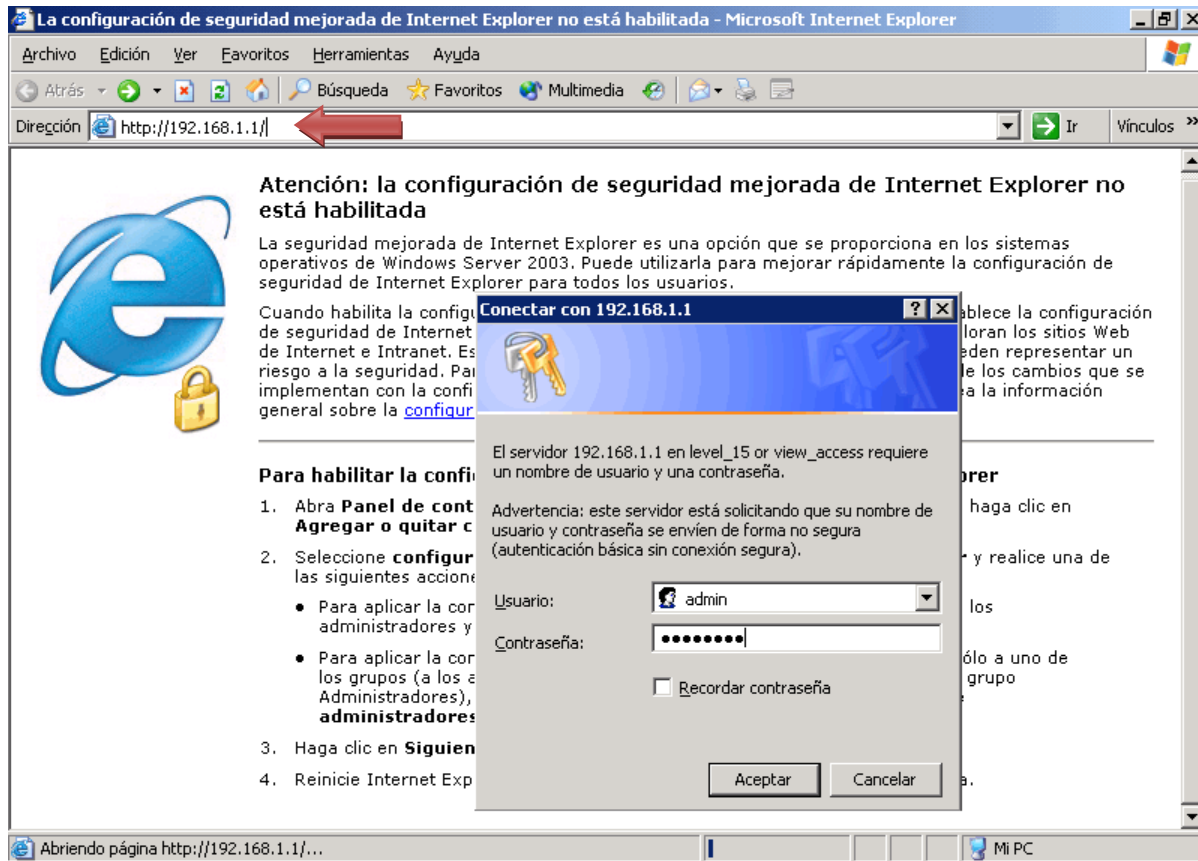
Se necesitan los siguientes recursos:

- Router ISR Cisco 1841 con la versión 2.4 de SDM instalada y con la configuración básica completa
- (Opcional) Otro modelo de router Cisco con SDM instalado
- (Opcional) Otro modelo de router Cisco sin SDM instalado (versión 12.2 del software IOS de Cisco o posterior; debe admitir SSH)
- Computadora con Windows XP con Internet Explorer 5.5 o versión posterior y Sun Java Runtime Environment (JRE) versión 1.4.2_05 o posterior (o Java Virtual Machine (JVM) 5.0.0.3810)
- Última versión de cliente putty.exe instalada en la PC y con acceso en el escritorio
- Cable de conexión directa o conexión cruzada Ethernet categoría 5 (para SDM y SSH)
- (Opcional) Cable de consola: si el router debe ser configurado mediante la CLI
- Acceso al indicador de comando de la PC
- Acceso a la configuración TCP/IP de red de la PC

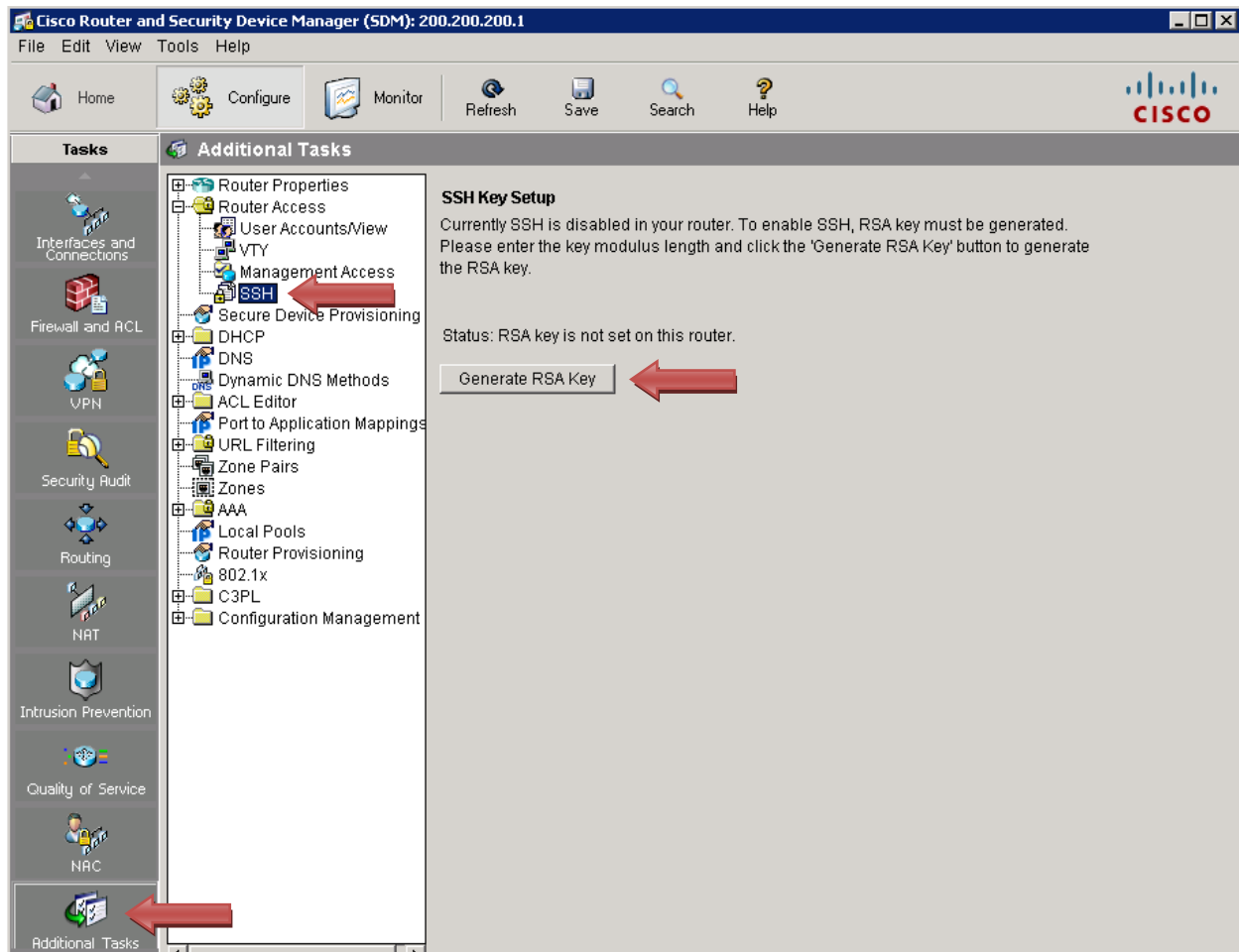
Paso 1: Utilizar SDM para configurar el router para que acepte las conexiones SSH.

Nota: Si está configurando un router que no posee SDM instalado, lea detenidamente el Paso 1 para ver cómo se configura SSH como una tarea separada cuando se utiliza SDM y luego diríjase al Paso 2.

- Conéctese a la interfaz Fa0/0 del router. Abra el explorador Web y conéctese a `http://192.168.1.1`. Cuando se le solicite, ingrese **admin** para el nombre de usuario y **cisco123** para la contraseña. Haga clic en **Aceptar**. Se carga SDM Cisco.

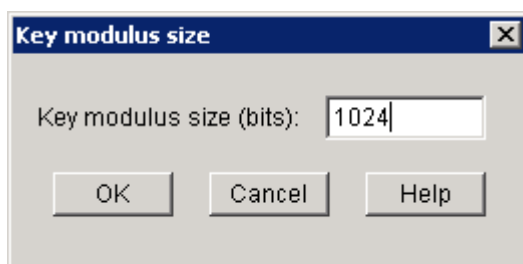


- b. Haga clic en el botón **Configure (Configurar)** en la barra de herramientas. En el panel de tareas, haga clic en **Additional Tasks (Tareas adicionales)**. En el panel de Tareas adicionales, expanda **Router Access (Acceso al router)** y haga clic en la tarea **SSH**. Luego haga clic en el botón **Generate RSA Key (Generar la clave RSA)**.

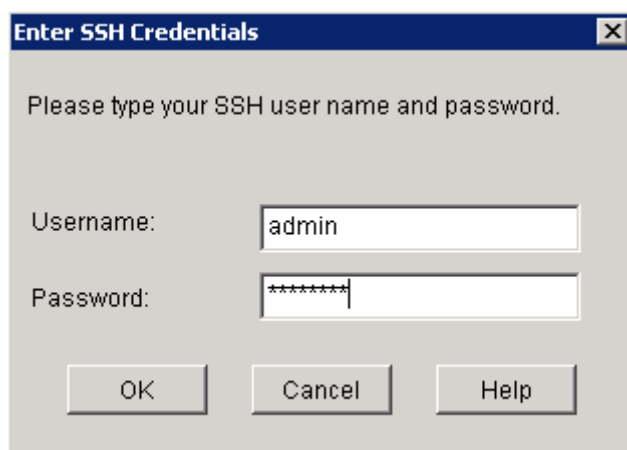


Nota: Si el mensaje **SSH Key Setup (Configuración de clave SSH)** dice: “Currently SSH is disabled in your router” (“SSH está deshabilitado en el router”) y en **Estado (Status)** “RSA key is not set on this router” (“La clave RSA no está configurada en este router”), probablemente sea porque usted completó la Práctica de laboratorio 5.2.3, “Configuración de un ISR con SDM Express.” En esa práctica de laboratorio, cuando configuró la seguridad, uno de los parámetros recomendados de seguridad habilitado de manera predeterminada es “Mejorar la seguridad en este router.” Si este cuadro está marcado, configura automáticamente SSH para el acceso al router, establece el mensaje para advertir sobre intrusos, aplica la longitud mínima de contraseña y restringe la cantidad de intentos de inicio de sesión no exitosos.

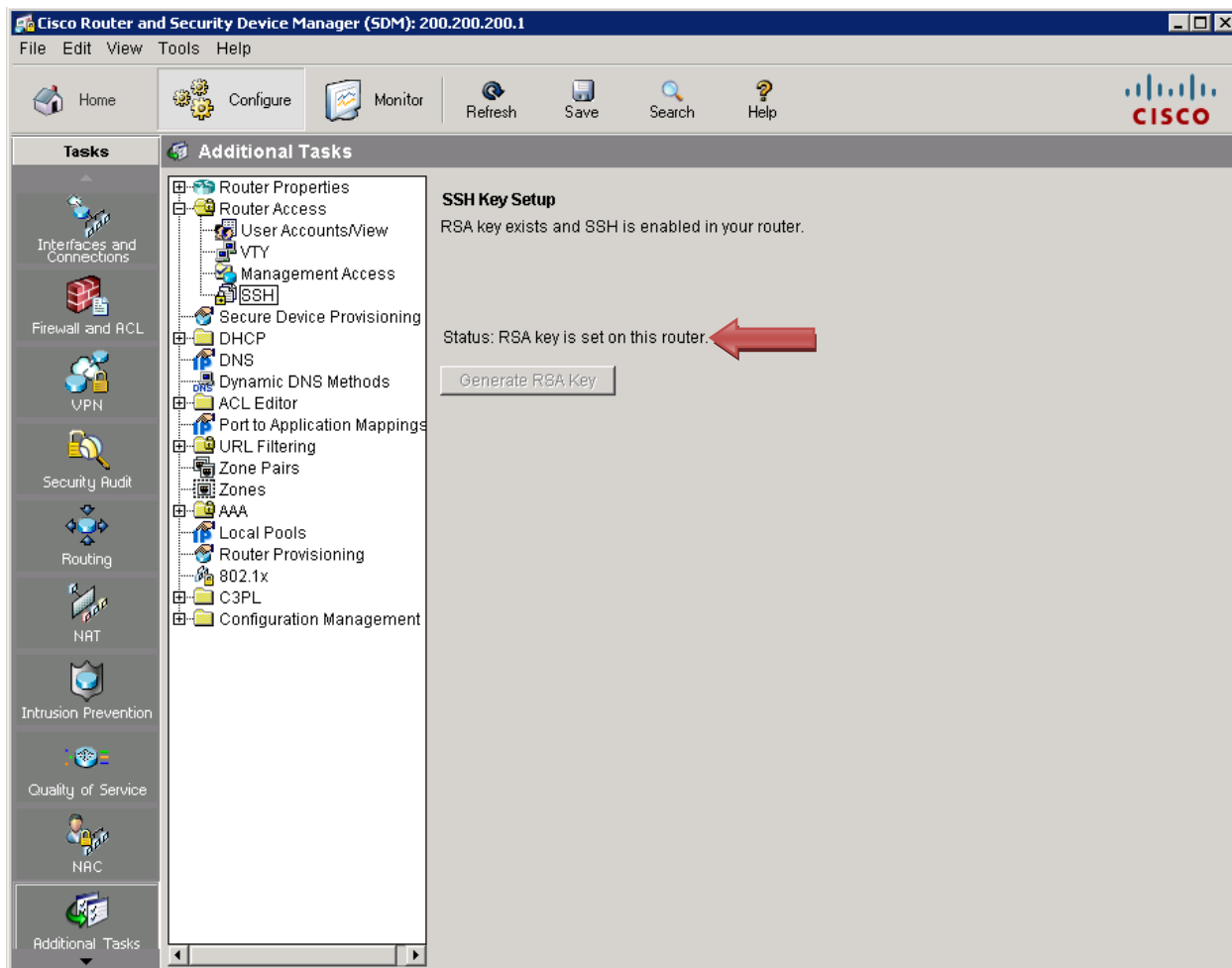
- c. En el cuadro de diálogo del **Key modulus size (Tamaño del módulo de la clave)**, ingrese un tamaño de clave de 1024 bits. Haga clic en **OK (Aceptar)**.



- d. En el cuadro de diálogo **Enter SSH Credentials (Ingresar las credenciales SSH)**, ingrese **admin** para el nombre de usuario y **cisco123** para la contraseña. Haga clic en **OK**.



- e. Observe que la clave RSA se encuentra ahora configurada en el router.



- f. En el panel de Tareas adicionales, haga clic en la opción **VTY**. Seleccione **Input Protocols Allowed** (Protocolos de entrada permitidos) y luego haga clic en el botón **Edit** (Editar).

The screenshot shows the Cisco Router and Security Device Manager (SDM) interface. The left sidebar contains a 'Tasks' pane with 'Additional Tasks' expanded, showing a tree structure where 'VTY' is selected. The main panel displays the 'VTYs' configuration page. It features a table with two sections for Line Ranges 0-4 and 5-15. The 'Input Protocols Allowed' row in the 5-15 range is highlighted. A red arrow points to the 'Edit...' button in the top right corner of the VTYs panel.

Item Name	Item Value
Line Range	0-4
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None
Line Range	5-15
Input Protocols Allowed	telnet
Output Protocols Allowed	None
EXEC timeout	10
Inbound Access-class	None
Outbound Access-class	None

- g. Marque el casillero **SSH** para el Protocolo de entrada y luego haga clic en **OK**.

Edit VTY Lines

Line Range

Lines: 5 -- 15

Time out: 10 minutes

Input Protocol

☒ Telnet ☒ SSH

Output Protocol

☐ Telnet ☐ SSH

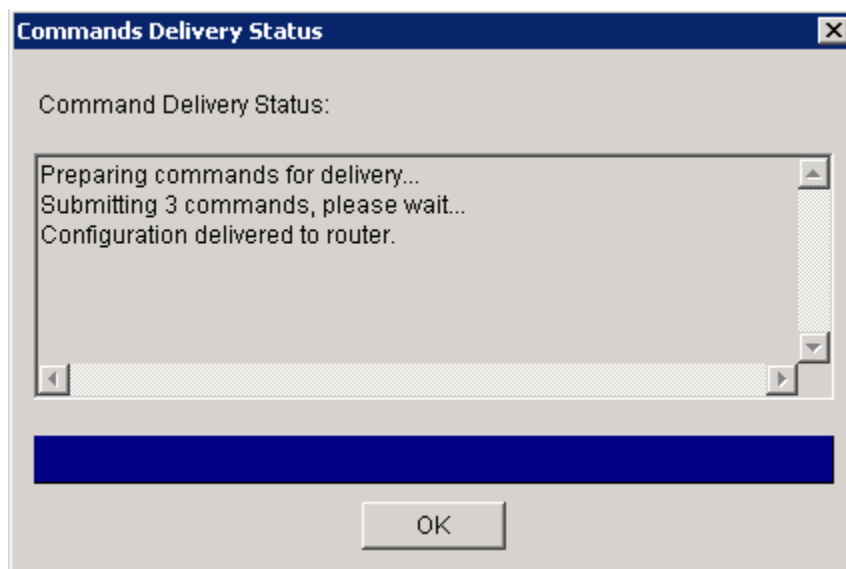
Access Rule

Inbound: [] ...

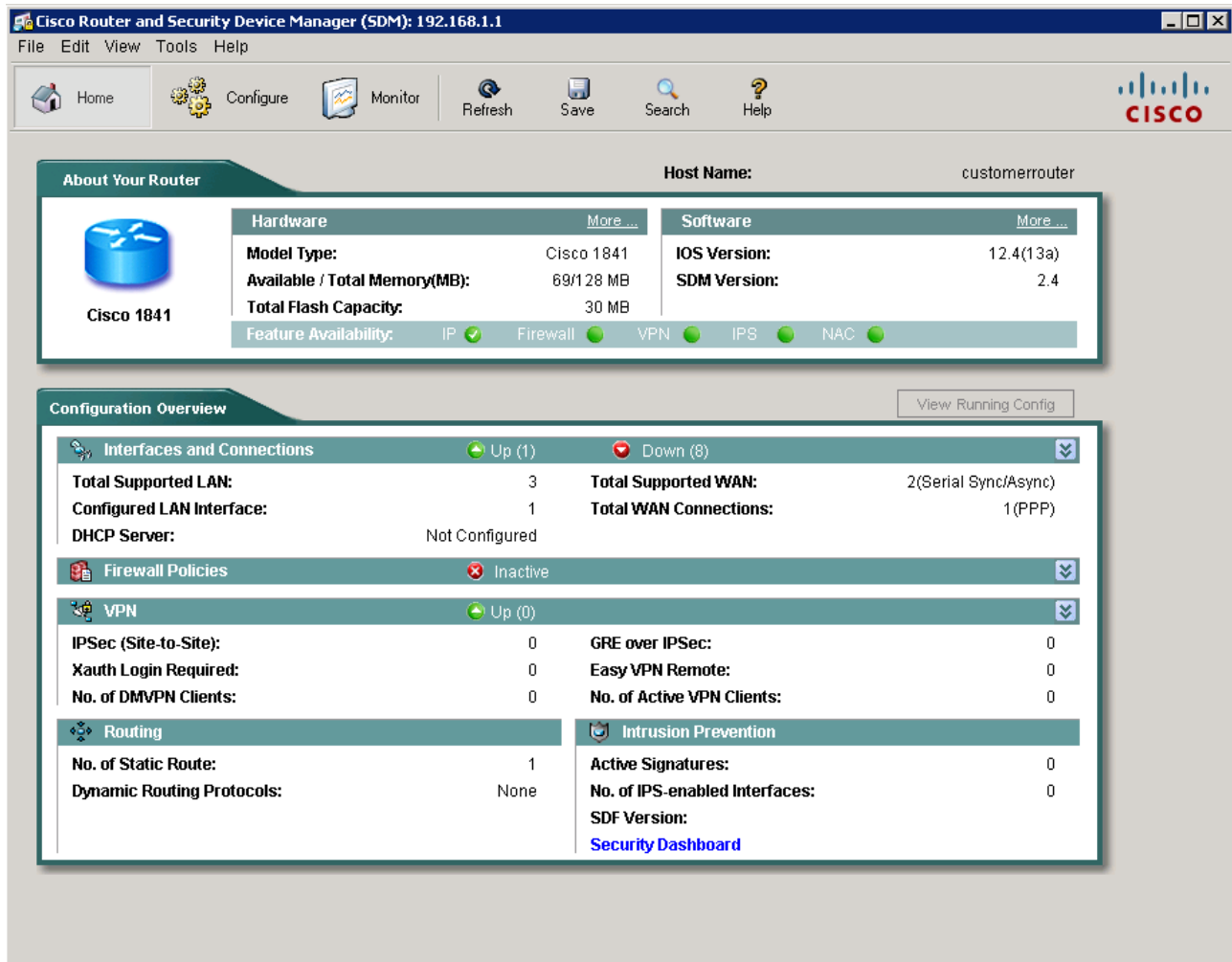
Outbound: [] ...

OK Cancel Help

- h. Cuando se abra la ventana de **Commands Delivery Status (Estado de entrega de comandos)**, haga clic en **OK**.



- i. Cierre el SDM Cisco al hacer clic en **X** en la esquina superior derecha de la ventana.



- j. Haga clic en **Yes (Si)** para confirmar que desea cerrar SDM y vaya al Paso 3. (El Paso 2 le enseña cómo configurar SSH en un router sin SDM).

Paso 2: (OPCIONAL) Configurar SSH en un router que no sea SDM.

Nota: Si está configurando un router para SSH que ya tiene SDM instalado, puede saltar el Paso 2 e ir directamente al Paso 3.

- a. Conecte el puerto de consola del router con una PC y el programa HyperTerminal, tal como se describe en la Práctica de laboratorio 5.1.3, "Conexión de un router de servicios integrados".
- b. Conéctese al router. Desde la petición de entrada en el modo EXEC privilegiado, ingrese los comandos CLI del IOS de Cisco como se muestra a continuación. Estos comandos no incluyen todas las contraseñas que deben ser establecidas. Consulte la Práctica de laboratorio 5.3.5, "Configuración de parámetros básicos del router con la CLI del IOS," para ver las instrucciones, para obtener los valores de configuración.

Nota: El router debe estar ejecutando la versión 12.2 del software IOS de Cisco o posterior. En este ejemplo, el router es un modelo Cisco 2620XM con la versión 12.2(7r) del software IOS de Cisco.

- c. Configure la información básica del router y de la interfaz.

```
Router#config terminal
Router(config)#hostname CustomerRouter
CustomerRouter(config)#ip domain-name customer.com
CustomerRouter(config)#username admin privilege 15 password 0 cisco123
CustomerRouter(config)#interface FastEthernet 0/0
CustomerRouter(config-if)#ip address 192.168.1.1 255.255.255.0
CustomerRouter(config-if)#no shutdown
CustomerRouter(config-if)#exit
```

- d. Configure las líneas de terminal vty remotas entrantes para aceptar Telnet y SSH.

```
CustomerRouter(config)#line vty 0 4
CustomerRouter(config-line)#privilege level 15
CustomerRouter(config-line)#login local
CustomerRouter(config-line)#transport input telnet ssh
CustomerRouter(config-line)#exit
```

- e. Genere el par de claves de encriptación RSA para que el router lo utilice para autenticación y encriptación de los datos SSH que se están transmitiendo. Ingrese **768** para la cantidad de bits del módulo. De manera predeterminada, es 512.

```
CustomerRouter(config)#crypto key generate rsa
```

```
How many bits in the modulus [512] 768
```

```
CustomerRouter(config)#exit
```

- f. Verifique que SSH haya sido habilitado y la versión que se está utilizando.

```
CustomerRouter#show ip ssh
```

- g. Complete la siguiente información según el resultado del comando **show ip ssh**.

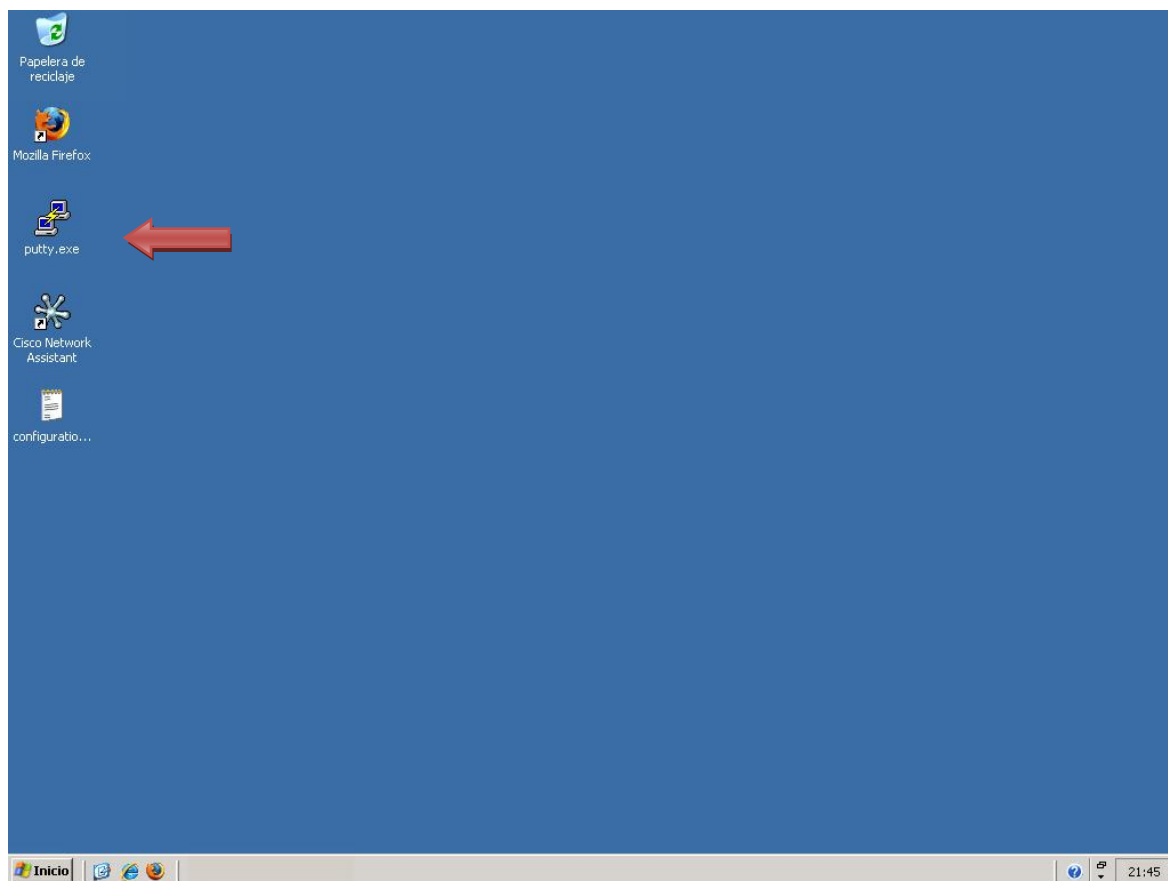
```
Versión SSH habilitada_____
Expiración de autenticación_____
Reintentos de autenticación_____
```

- h. Guarde la configuración en ejecución en la configuración de inicio.

```
CustomerRouter#copy running-config startup-config
```

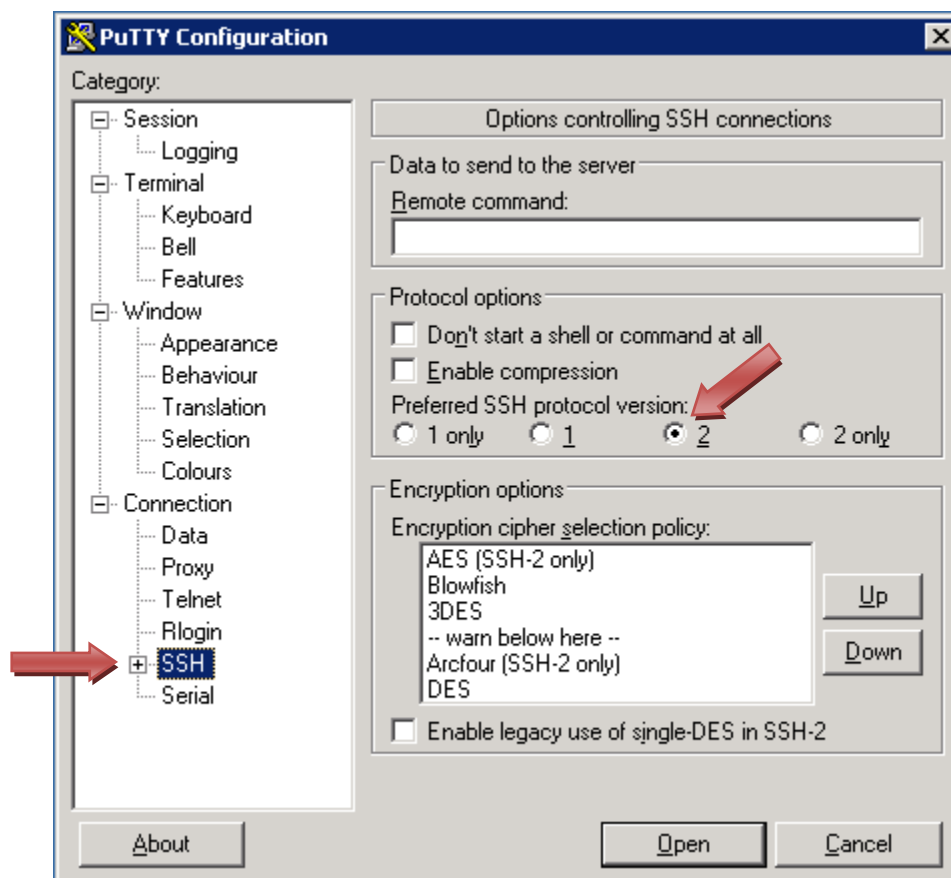
Paso 3: Configurar el cliente SSH y conectar la PC al ISR.

- a. Descargue putty.exe y ubique la aplicación en el escritorio. Inicie PuTTY al hacer doble clic en el ícono putty.exe.

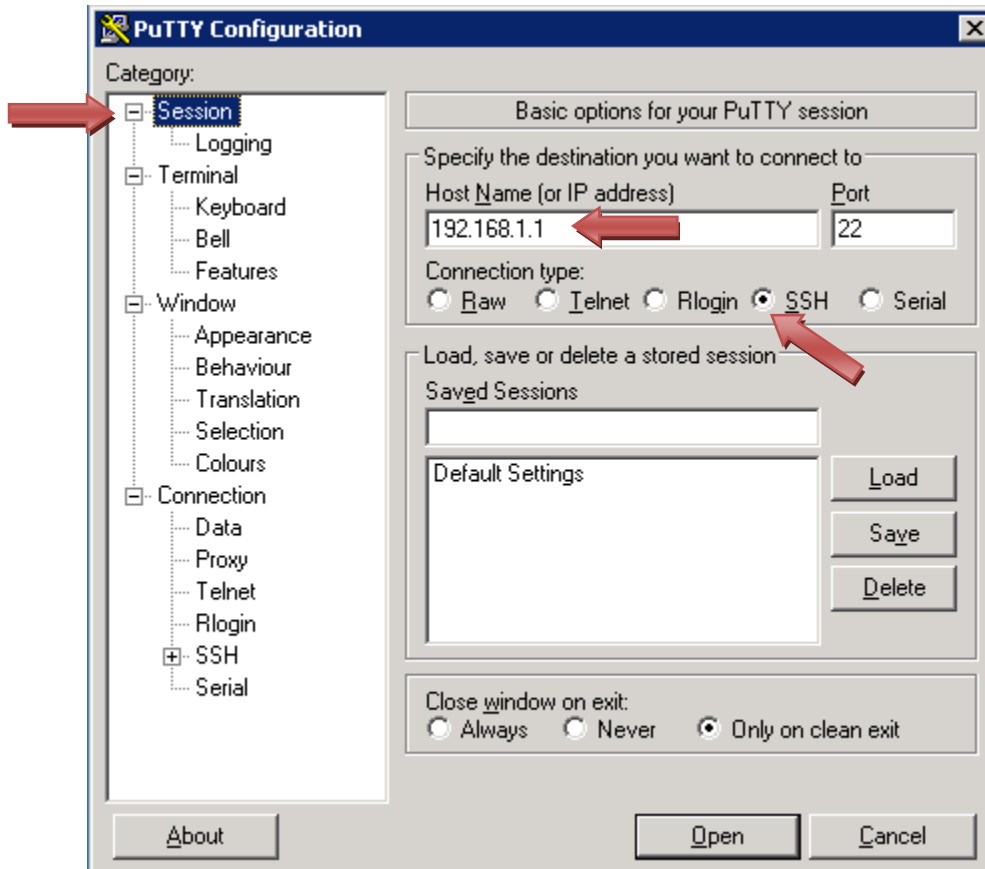


- b. En el panel Categoría, haga clic en **SSH**. Verifique que la versión preferida de protocolo SSH esté establecida en **2**.

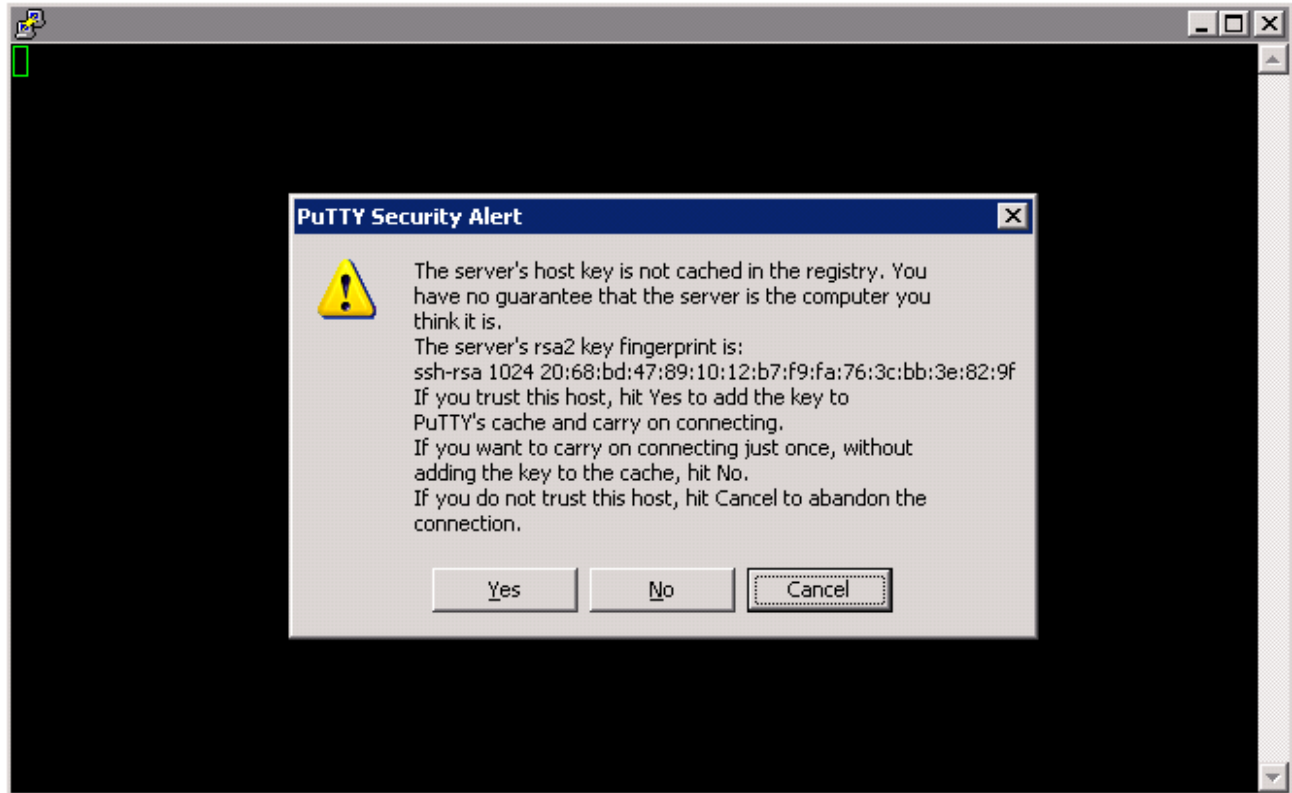
Nota: El cliente Putty igual se conecta incluso si el servidor SSH está ejecutando la versión 1 de SSH.



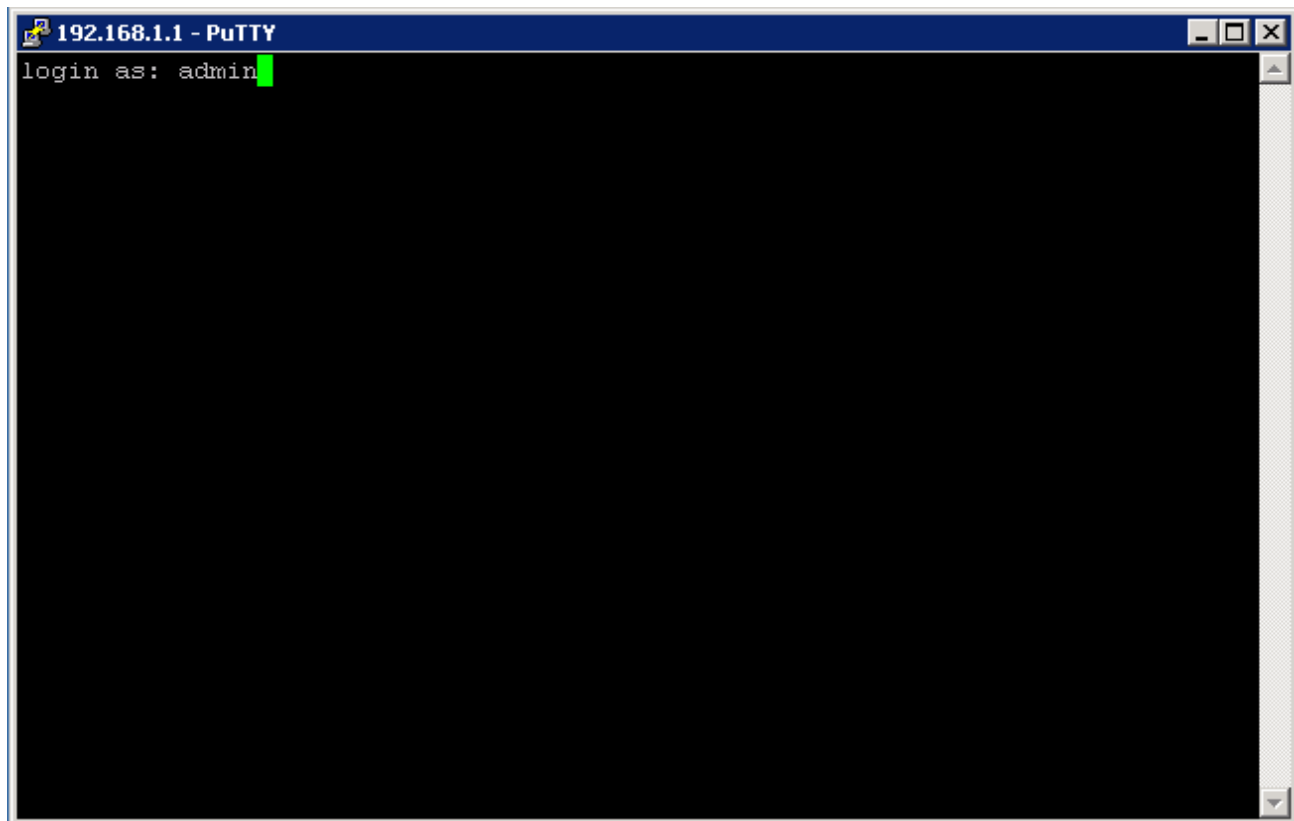
- c. En el panel Categoría, haga clic en **Session (Sesión)**. Ingrese la dirección IP de la interfaz LAN del router, que es 192.168.1.1. Verifique que se seleccione SSH para el tipo de conexión. Haga clic en **Open (Abrir)**.



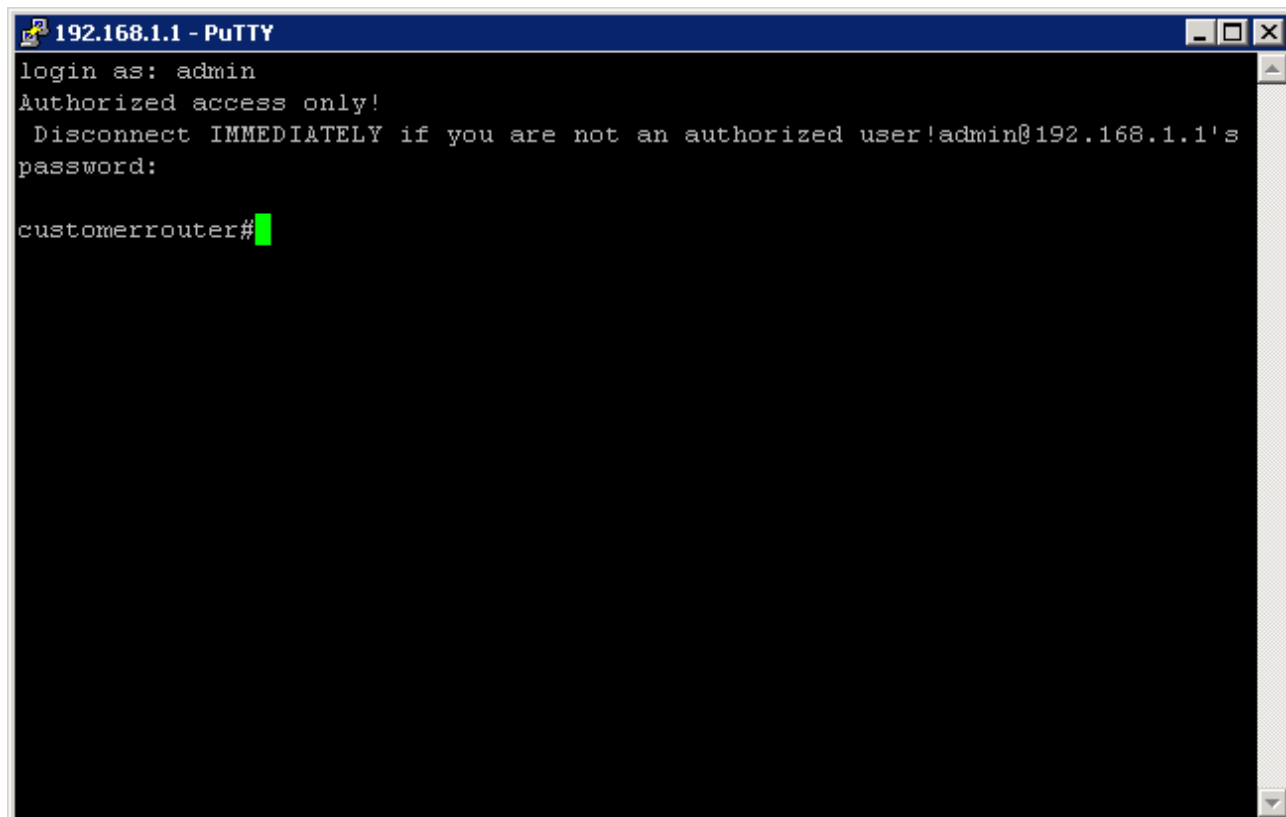
- d. La primera vez que se realiza una conexión a SSH en el ISR Cisco 1841 mediante un cliente SSH, se guarda en caché una clave de conexión en el registro local de la máquina. En la ventana de alerta de seguridad PuTTY, haga clic en **Sí (Yes)** para continuar.



- e. En el indicador de conexión, escriba el nombre de usuario del administrador, **admin**, y presione **Enter**.



- f. En el indicador de contraseña, escriba la contraseña del administrador, **cisco123** y presione **Enter**.



The image shows a PuTTY terminal window titled "192.168.1.1 - PuTTY". The terminal output is as follows:

```
login as: admin
Authorized access only!
Disconnect IMMEDIATELY if you are not an authorized user!admin@192.168.1.1's
password:
customerrouter#
```

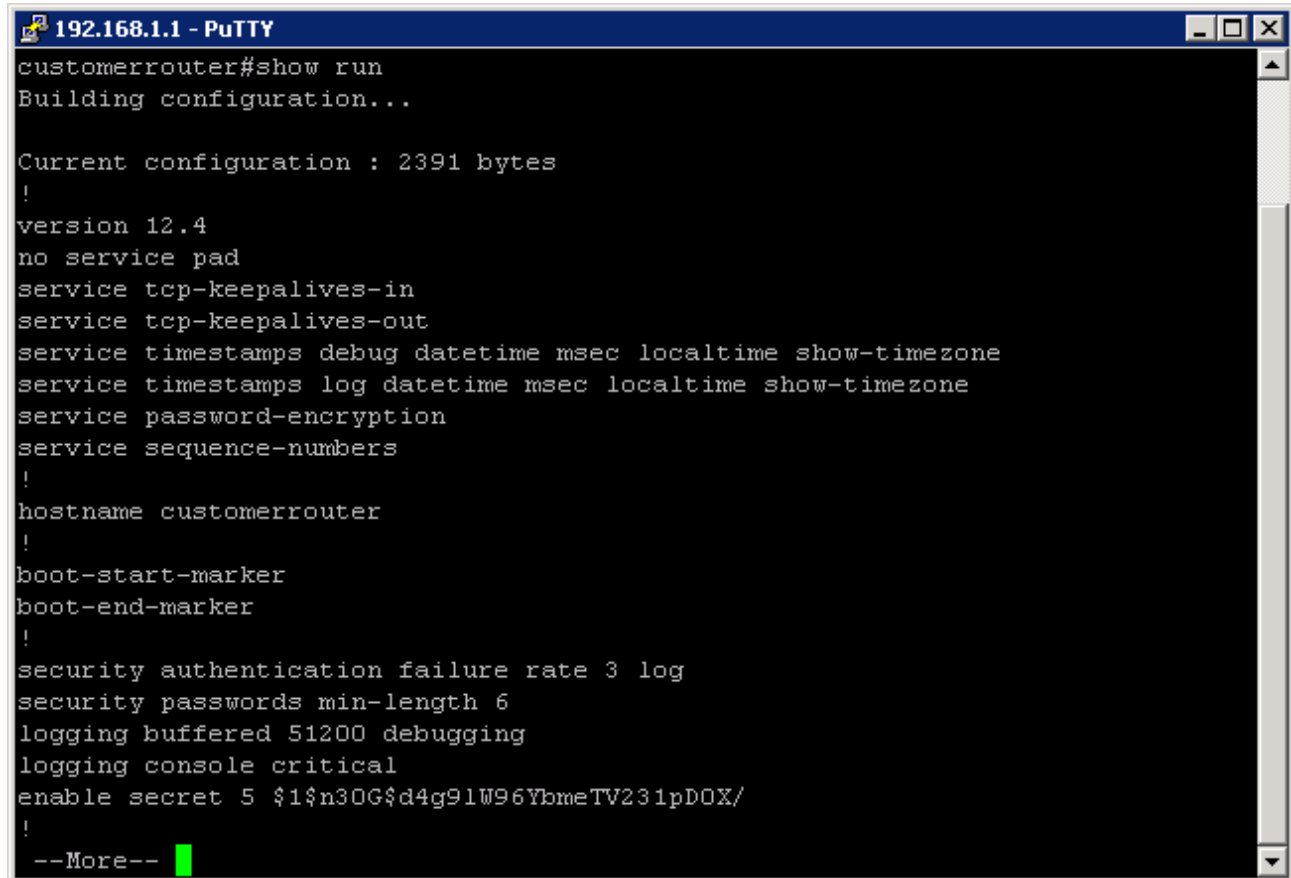
The prompt "customerrouter#" is followed by a green cursor.

Paso 4: Verificar la configuración del ISR Cisco 1841.

- a. Para verificar la configuración del router, escriba **show run** en la petición de entrada del modo privilegiado y presione **Enter**.

Nota: No es necesario cambiar del modo de usuario al modo privilegiado si está usando SDM porque el modo privilegiado es el modo predeterminado.

- b. Presione la **barra espaciadora** para desplazarse por la configuración actual del router.

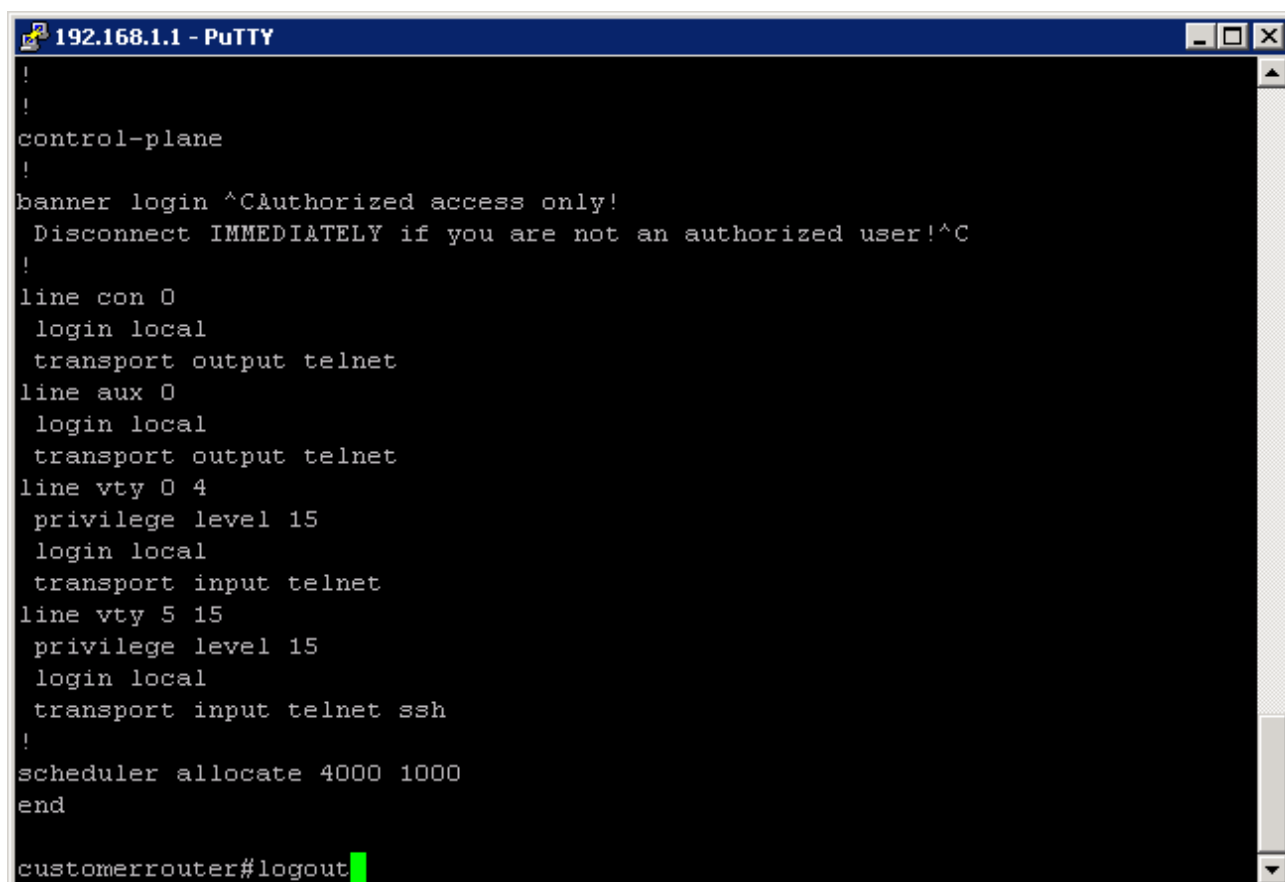


```
192.168.1.1 - PuTTY
customerrouter#show run
Building configuration...

Current configuration : 2391 bytes
!
version 12.4
no service pad
service tcp-keepalives-in
service tcp-keepalives-out
service timestamps debug datetime msec localtime show-timezone
service timestamps log datetime msec localtime show-timezone
service password-encryption
service sequence-numbers
!
hostname customerrouter
!
boot-start-marker
boot-end-marker
!
security authentication failure rate 3 log
security passwords min-length 6
logging buffered 51200 debugging
logging console critical
enable secret 5 $1$n30G$d4g91W96YbmeTV231pDOX/
!
--More--
```

Paso 5: Desconectarse del ISR Cisco 1841.

Para desconectarse del router cuando finalice de verificar la configuración, escriba **logout** en la petición de entrada del modo privilegiado y luego presione **Enter**.



```
192.168.1.1 - PuTTY
!
!
control-plane
!
banner login ^CAuthorized access only!
  Disconnect IMMEDIATELY if you are not an authorized user!^C
!
line con 0
  login local
  transport output telnet
line aux 0
  login local
  transport output telnet
line vty 0 4
  privilege level 15
  login local
  transport input telnet
line vty 5 15
  privilege level 15
  login local
  transport input telnet ssh
!
scheduler allocate 4000 1000
end
customerrouter#logout
```

Paso 6: Reflexión

- a. Al comparar Telnet y SSH, ¿cuáles son las ventajas y las desventajas de cada uno?

- b. ¿Cuál es el puerto predeterminado para SSH? _____ ¿Cuál es el puerto predeterminado para Telnet? _____
- c. ¿Qué versión del software IOS de Cisco IOS apareció en running-config?

Configuración básica del IOS de Cisco para activar SDM

Si se elimina startup config en un router SDM, SDM ya no aparecerá de manera predeterminada cuando se reinicie el router. Entonces es necesario establecer una configuración básica tal como se muestra a continuación. La Guía de inicio rápido de SDM contiene más detalles sobre la configuración y el uso de SDM

http://www.cisco.com/en/US/products/sw/secursw/ps5318/products_quick_start09186a0080511c89.html#wp44788

1) Establezca la dirección IP Fa0/0 del router. (Ésta es la interfaz a la que se conecta una PC para usar un explorador para activar el SDM. Se debe establecer la dirección IP de la PC en 10.10.10.2 255.255.255.248).

Nota: Un router SDM que no sea el 1841 puede requerir conexión a un puerto diferente para acceder a SDM.

```
Router(config)#interface Fa0/0  
Router(config-if)#ip address 10.10.10.1 255.255.255.248  
Router(config-if)#no shutdown
```

2) Habilite el servidor HTTP y HTTPS del router.

```
Router(config)#ip http server  
Router(config)#ip http secure-server  
Router(config)#ip http authentication local
```

3) Cree una cuenta de usuario con nivel 15 de privilegio (habilitar privilegios). Reemplace username y password con el nombre de usuario y la contraseña que desea configurar

```
Router(config)#username <username> privilege 15 password 0 <password>
```

4) Configure el SSH y Telnet para el inicio de sesión local y el nivel de privilegio 15.

```
Router(config)#line vty 0 4  
Router(config-line)#privilege level 15  
Router(config-line)#login local  
Router(config-line)#transport input telnet  
Router(config-line)#transport input telnet ssh  
Router(config-line)#exit
```