Habilitación del Secure Shell (SSH) en un punto de acceso

Contenido

Introducción

Este documento explica cómo configurar un punto de acceso (AP) para habilitar el acceso basado en Secure Shell (SSH).

prerrequisitos

Requisitos

Asegúrese de cumplir estos requisitos antes de intentar esta configuración:

- Conocimiento de cómo configurar el Cisco Aironet AP
- Conocimiento básico de SSH y de los conceptos relacionados de la Seguridad

Componentes Utilizados

La información que contiene este documento se basa en las siguientes versiones de software y hardware.

- 1200 Series AP del Aironet que funcionan con el Software Release 12.3(8)JEB de Cisco IOS®
- PC o laptop con la utilidad del cliente SSH

Note: Este documento utiliza la utilidad del cliente SSH para verificar la configuración. Usted puede utilizar cualquier utilidad de cliente de tercera persona para iniciar sesión al AP con el uso de SSH.

La información que contiene este documento se creó a partir de los dispositivos en un ambiente de laboratorio específico. Todos los dispositivos que se utilizan en este documento se pusieron en funcionamiento con una configuración verificada (predeterminada). Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener cualquier comando.

Convenciones

Consulte Convenciones de Consejos TécnicosCisco para obtener más información sobre las convenciones del documento.

Acceder el comando line interface(cli) en el Aironet AP

Usted puede utilizar ninguno de estos métodos para acceder el comando line interface(cli) en el Aironet AP:

- El puerto de la consola
- Telnet
- SSH

Si el AP tiene un puerto de la consola y usted tiene acceso físico al AP, usted puede utilizar el puerto de la consola para iniciar sesión al AP y cambiar la configuración en caso necesario. Para la información sobre cómo utilizar el puerto de la consola para iniciar sesión al AP, refiera a *conexión con las 1200 Series que los Puntos de acceso localmente* seccionan del documento que configura el Punto de acceso por primera vez.

Si usted puede acceder solamente el AP con los Ethernetes, utilice el Telnet Protocol o el protocolo SSH para iniciar sesión al AP.

El puerto 23 de las aplicaciones del Telnet Protocol para la comunicación. Telnet transmite y recibe los datos en el texto claro. Porque la comunicación de datos sucede en el texto claro, un hacker puede comprometer fácilmente las contraseñas y acceder el AP. El RFC 854 define Telnet y amplía Telnet con las opciones por muchos otros RFC.

SSH es una aplicación y un protocolo que proporciona un reemplazo seguro a las r-herramientas de Berkley. SSH es un protocolo que proporciona un seguro, conexión remota a una capa 2 o un dispositivo de la capa 3. Hay dos versiones de SSH: SSH versión 1 y SSH versión 2. Este soportes para la versión de software ambos SSH versión. Si usted no especifica el número de la versión, el AP omite la versión 2.

SSH proporciona más Seguridad para las conexiones remotas que Telnet proporcionando a la encripción fuerte cuando se autentica un dispositivo. Este cifrado es una ventaja sobre una sesión telnet, en quien la comunicación sucede en el texto claro. Para más información sobre SSH, refiera al Secure Shell (SSH) FAQ. La característica de SSH tiene un servidor SSH y un cliente integrado de SSH. Los soportes de cliente estos métodos de autenticación de usuario:

- RADIUS (para más información, refiera al acceso del Punto de acceso que controla con la sección RADIUS)
- Autenticación local y autorización (para más información, refiera a configurar el Punto de

acceso para la sección de la autenticación local y de la autorización)

Para más información sobre SSH, refiera a la parte 5, *"otras funciones de seguridad"* en la *guía de configuración de la Seguridad de Cisco IOS para el Release12.3.*

Note: La característica de SSH en esta versión de software no soporta la seguridad IP (IPSec).

Usted puede configurar los AP para SSH con el uso del CLI o del GUI. Este documento explica ambos métodos de configuración.

Configurar

Configuración de CLI

En esta sección, le presentan con la información para configurar las características descritas en este documento con el uso del CLI.

Instrucciones Paso a Paso

Para habilitar SSH-basó el acceso en el AP, usted primero debe configurar el AP como servidor SSH. Siga los siguientes pasos para configurar a un servidor SSH en el AP del CLI:

1. Configure un nombre del host y un Domain Name para el AP.
   ```
   AP#configure terminal
   !--- Enter global configuration mode on the AP. AP<config>#hostname Test
   !--- This example uses "Test" as the AP host name. Test<config>#ip domain name abc.com
   !--- This command configures the AP with the domain name "abc.com".
   ```
2. Genere una clave del Rivest, del Shamir, y del Adelman (RSA) para su AP.La generación de una clave RSA habilita SSH en el AP. Publique este comando en el modo de configuración global:
   ```
   Test<config>#crypto key generate rsa rsa_key_size
   !--- This generates an RSA key and enables the SSH server.
   ```
   Note: El tamaño de clave mínimo recomendado RSA es 1024.
3. Autenticación de usuario de la configuración en el AP.En el AP, usted puede configurar la autenticación de usuario para utilizar la lista local o una autenticación externa, una autorización, y un servidor de las estadísticas (AAA). Este ejemplo utiliza una lista localmente generada para autenticar a los usuarios:
   ```
   Test<config>#aaa new-model
   !--- Enable AAA authentication. Test<config>#aaa authentication login default local none
   !--- Use the local database in order to authenticate users. Test<config>#username Test
   password Test123
   !--- Configure a user with the name "Test". Test<config>#username ABC password xyz123
   !--- Configure a second user with the name "ABC".
   ```
   Esta configuración configura el AP para realizar la autenticación basada en el usuario con el uso de una base de datos local que se configure en el AP. El ejemplo configura a dos usuarios en la base de datos local, "prueba" y "ABC".
4. Configure los parámetros de SSH.
   ```
   Test<config>#ip ssh {[timeout seconds] | [authentication-retries integer]}
   !--- Configure the SSH control variables on the AP.
   ```
   Note: Usted puede especificar el descanso en los segundos, pero no excede 120 segundos. El valor por defecto es 120. Esta configuración aplica a SSH la fase de negociación. Usted puede también especificar el número de recomprobaciones de la autenticación, pero no

excede cinco recomprobaciones de la autenticación. El valor por defecto es tres.

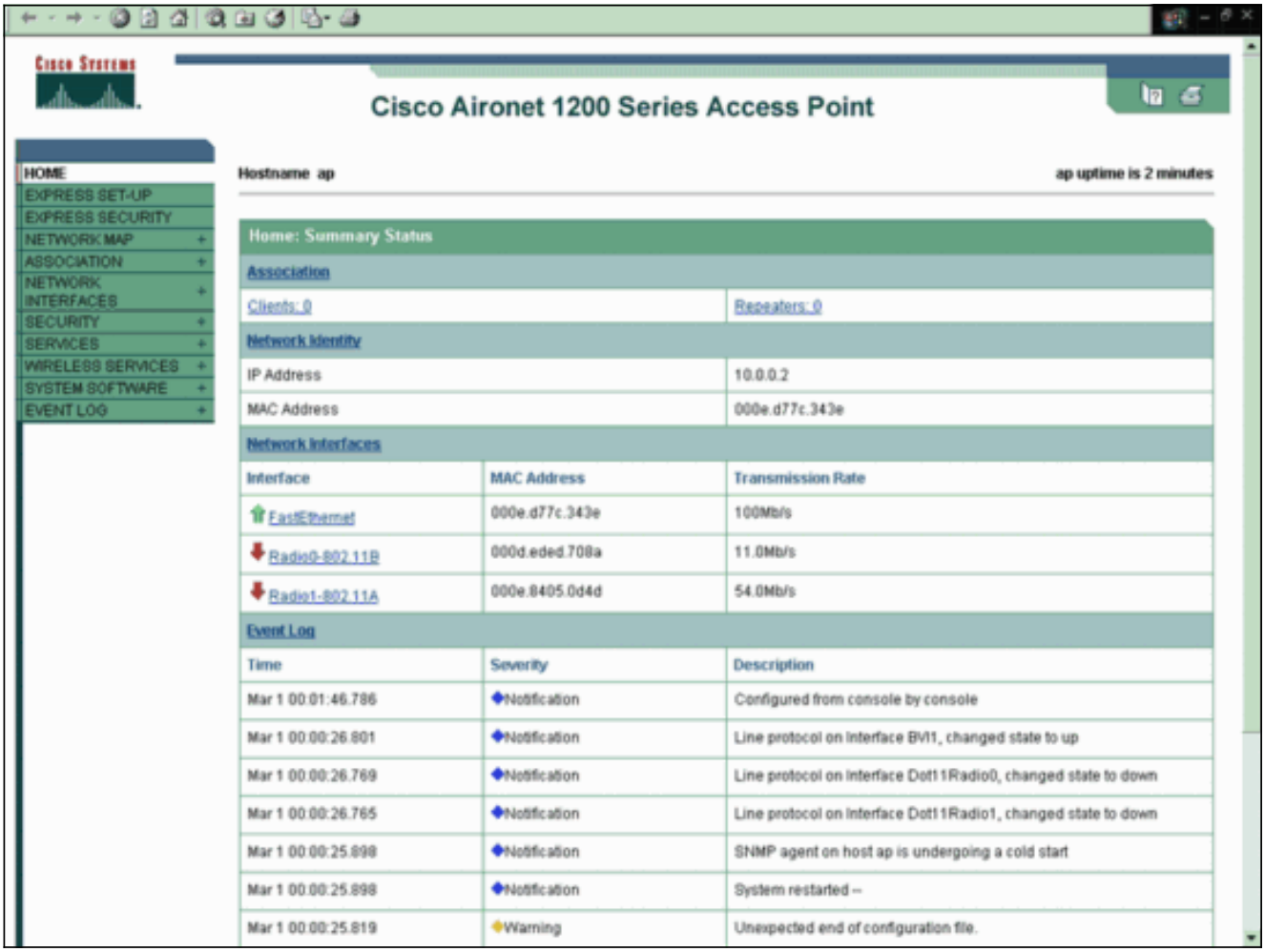
Configuración de la interfaz gráfica para el usuario

Usted puede también utilizar el GUI para habilitar el acceso SSH-basado en el AP.

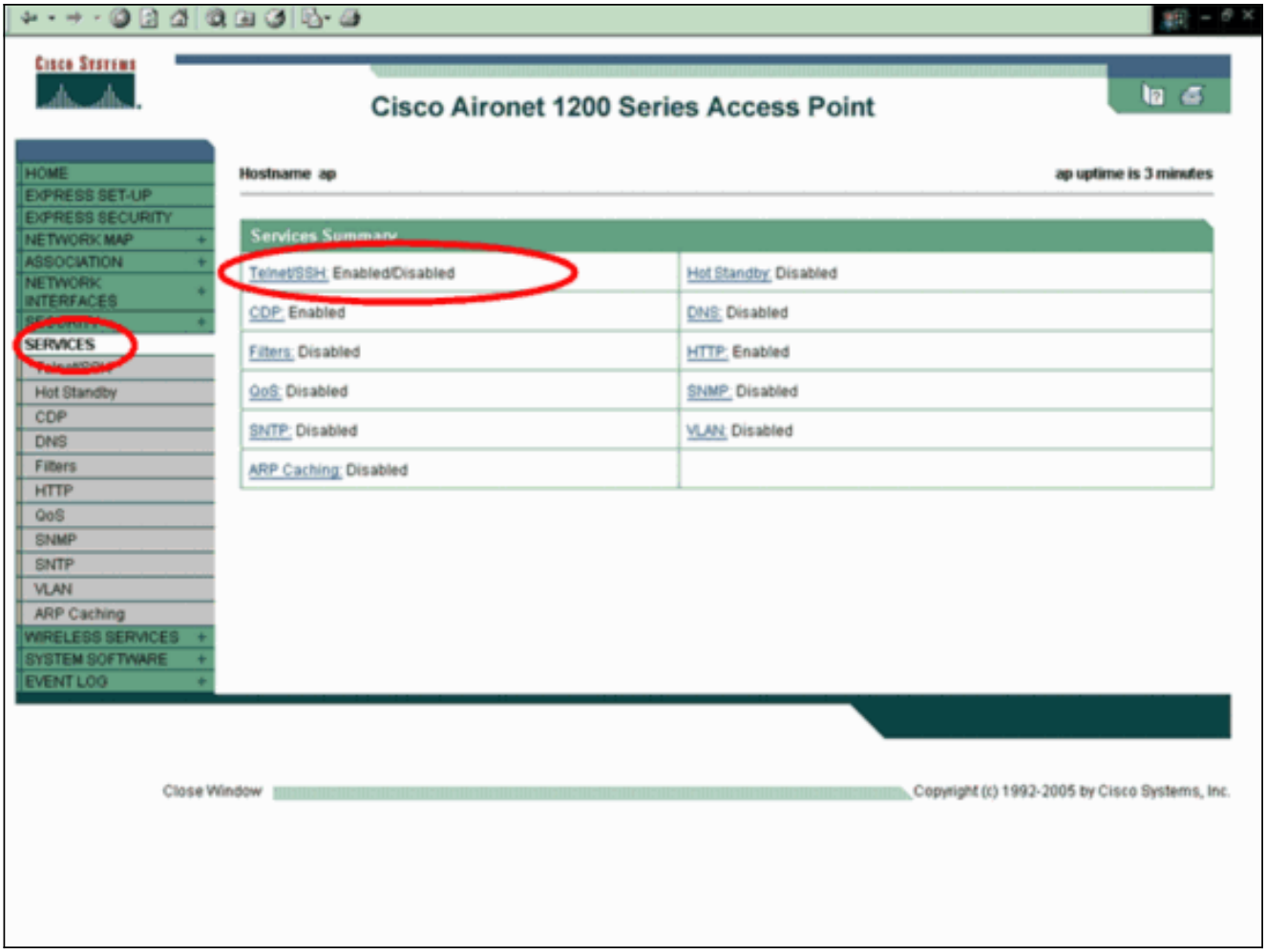
Instrucciones Paso a Paso

Complete estos pasos:

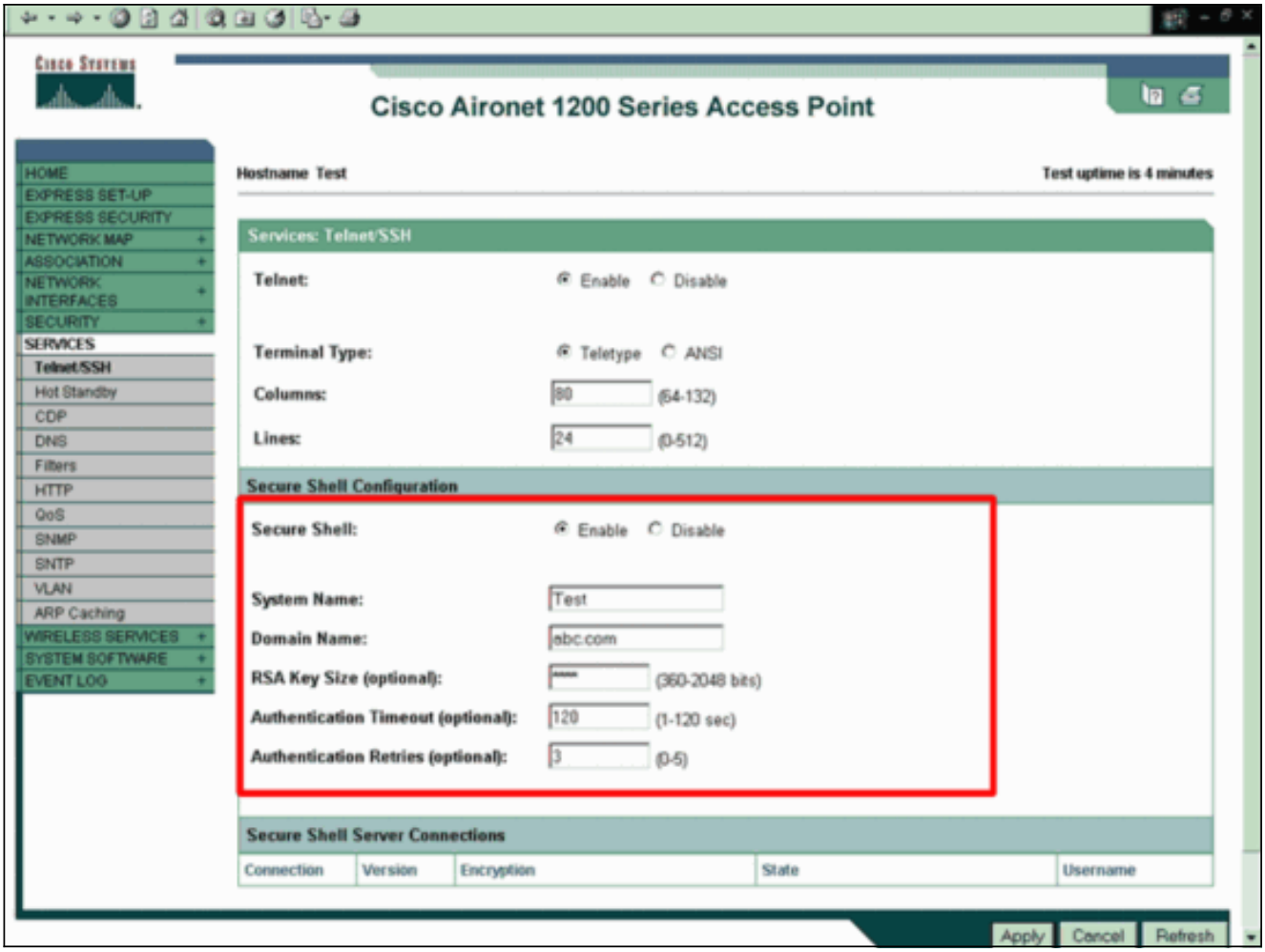
1. Inicie sesión al AP a través del navegador.Las visualizaciones de la ventana del estado resumido.



2. **Servicios del** tecleo en el menú a la izquierda.Las visualizaciones de la ventana de resumen de los
servicios.



3. Haga clic el **telnet/SSH** para habilitar y configurar los parámetros del telnet/SSH.Los servicios: Visualizaciones de la ventana del telnet/SSH. Navegue hacia abajo a la área de configuración del Secure Shell. El tecleo **habilita** al lado del Secure Shell, y ingresa los parámetros de SSH mientras que este ejemplo muestra:Este ejemplo utiliza estos parámetros:Nombre del sistema: PruebaDomain Name: abc.comTamaño de clave RSA: 1024Descanso de la autenticación: 120Retries de la autenticación:
   3



4. Haga clic en **Aply** para guardar los cambios.

Verificación

Use esta sección para confirmar que su configuración funciona correctamente.

La herramienta Output Interpreter Tool (clientes registrados solamente) (OIT) soporta ciertos comandos show. Utilice la OIT para ver un análisis del resultado del comando show.

- **muestre el ssh del IP** — Le verifica si SSH se habilita en el AP y permite para marcar la versión de SSH que se ejecuta en el AP. Esta salida proporciona un

```
Test#show ip ssh
SSH Enabled - version 1.99
Authentication timeout: 120 secs; Authentication retries: 3
```

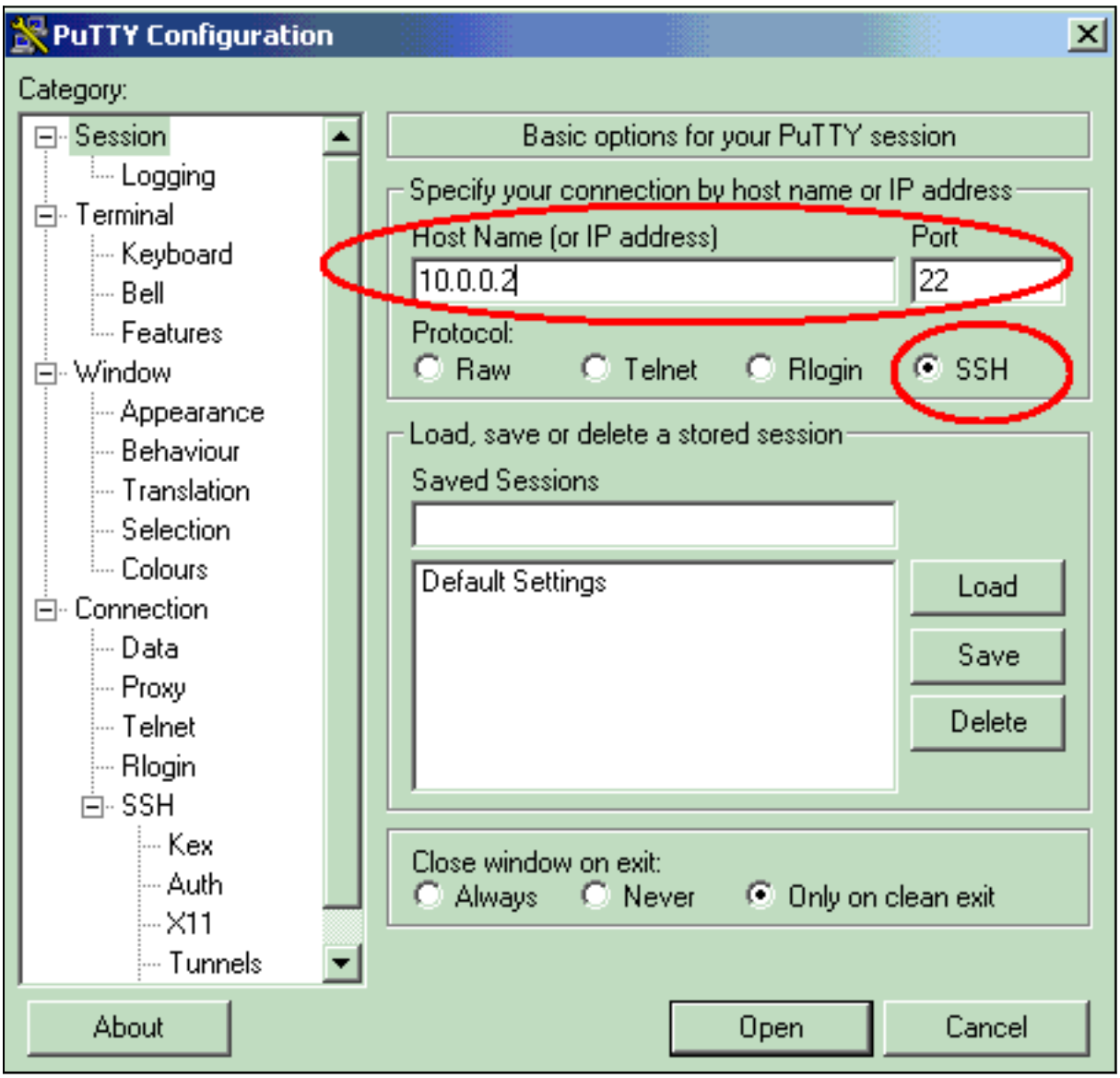
ejemplo:

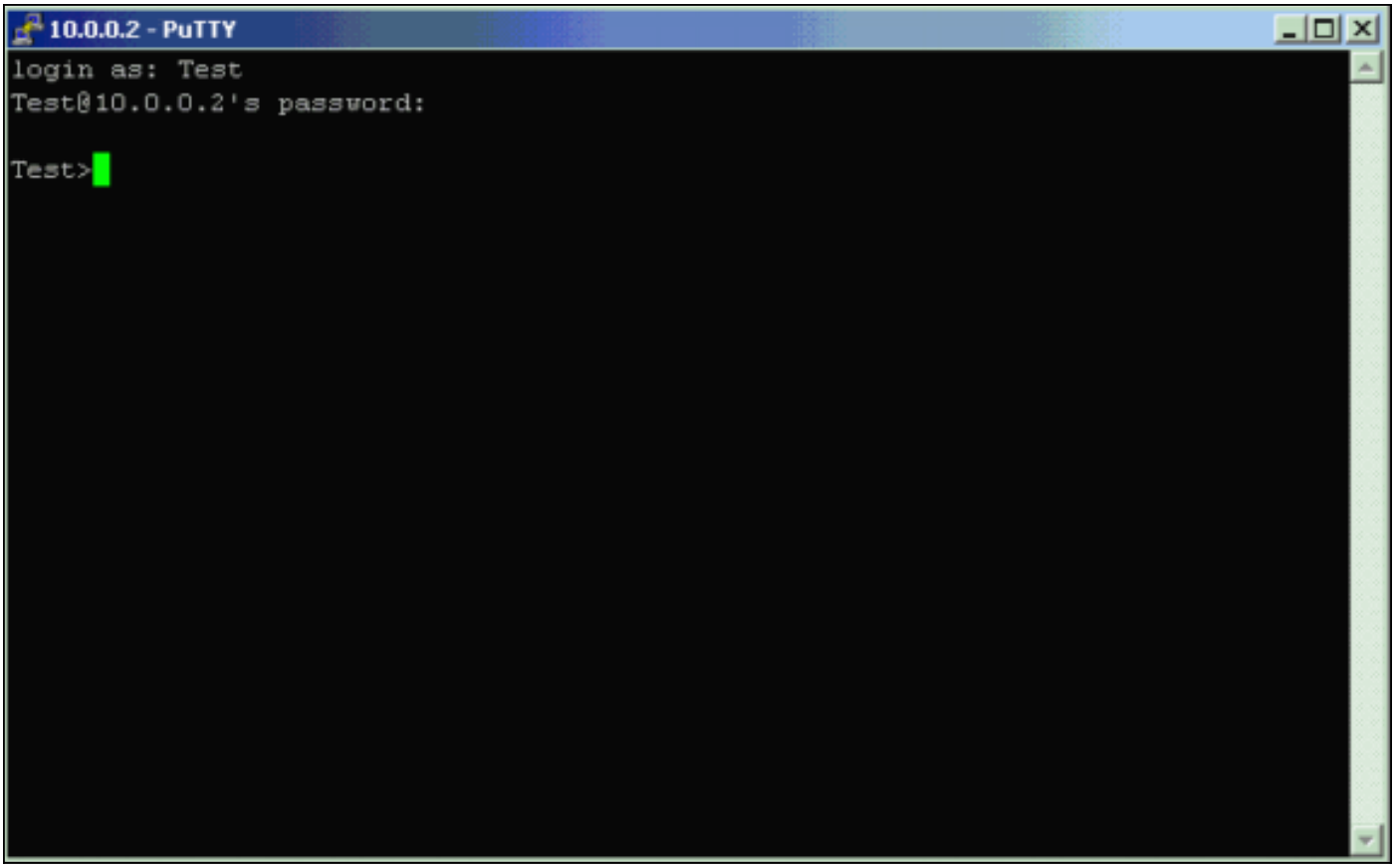
- **ssh de la demostración** — Le permite para ver el estatus de sus conexiones del servidor SSH. Esta salida proporciona un

```
Test#show ssh
Connection Version Mode Encryption  Hmac          State          Username
0          2.0     IN   aes256-cbc  hmac-sha1    Session started    ABC
0          2.0     OUT  aes256-cbc  hmac-sha1    Session started    ABC
```

ejemplo:

Ahora, inicie una conexión con un PC que los funcionamientos de tercera persona Software SSH y después hagan una tentativa de iniciar sesión al AP. Esta verificación utiliza la dirección IP AP, 10.0.0.2. Porque usted ha configurado la prueba del Nombre de usuario, utilice este nombre para acceder el AP con SSH:





Troubleshooting

Use esta sección para resolver problemas de configuración.

Si sus comandos de configuración SSH se rechazan como comandos ilegales, usted no ha generado con éxito un par clave RSA para su AP. Refiera a la sección de los *consejos de Troubleshooting de la* configuración de Secure Shell del documento para una lista de razones posibles de este problema.

Inhabilite SSH

Para inhabilitar SSH en un AP, usted debe borrar el par RSA que se genera en el AP. Para borrar los pares RSA, publique el **comando crypto key zeroize rsa** en el modo de configuración global. Cuando usted borra el par clave RSA, usted inhabilita automáticamente al servidor SSH. Esta salida proporciona un ejemplo:

```
Test(config)#crypto key zeroize rsa
% All RSA keys will be removed.
% All router certs issued using these keys will also be removed.
Do you really want to remove these keys? [yes/no]: yes
```

Información Relacionada

- Configuración de Secure Shell

- Configuración de Punto de Acceso por Primera Vez
- Página de soporte del Secure Shell (SSH)
- Página de Soporte de Red Inalámbrica
- Soporte Técnico y Documentación - Cisco Systems