**Configuración de SSH**

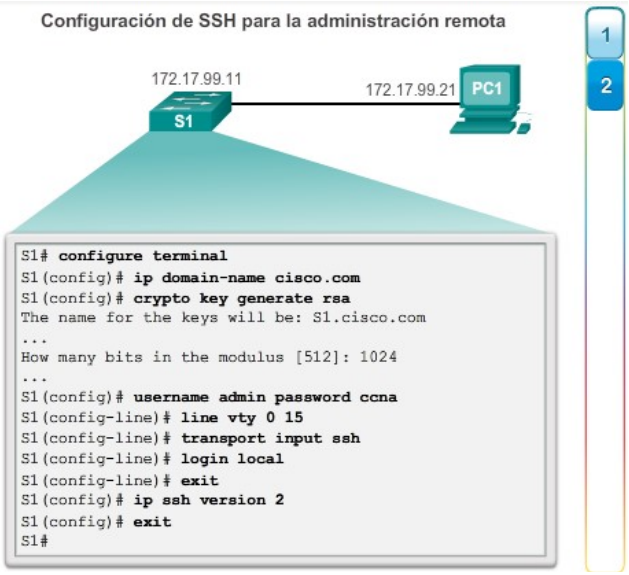
Antes de configurar SSH, el switch debe tener configurado, como mínimo, un nombre de host único y los parámetros correctos de conectividad de red.

**Paso 1. Verificar la compatibilidad con SSH**

Use el comando **show ip ssh** para verificar que el switch admita SSH. Si el switch no ejecuta un IOS que admita características criptográficas, este comando no se reconoce.

**Paso 2. Configurar el dominio IP**

Configure el nombre de dominio IP de la red mediante el comando **ip domain-name** *nombre-de-dominio* del modo de configuración global. En la figura 1, el valor de *nombre-de-dominio* es **cisco.com**.




**Paso 3. Generar pares de claves RSA**

No todas las versiones del IOS utilizan la versión 2 de SSH de manera predeterminada, y la versión 1 de SSH tiene fallas de seguridad conocidas. Para configurar la versión 2 de SSH, emita el comando **ip ssh version 2** del modo de configuración global. La creación de un par de claves RSA habilita SSH automáticamente. Use el comando **crypto key generate rsa** del modo de configuración global para habilitar el servidor SSH en el switch y generar un par de claves RSA. Al crear claves RSA, se solicita al administrador que introduzca una longitud de módulo. Cisco recomienda un tamaño de módulo mínimo de 1024 bits (consulte la configuración de muestra en la figura 1). Una longitud de módulo mayor es más segura, pero se tarda más en generarlo y utilizarlo.

**Nota:** para eliminar el par de claves RSA, use el comando **crypto key zeroize rsa** del modo de configuración global. Después de eliminarse el par de claves RSA, el servidor SSH se deshabilita automáticamente.

**Paso 4. Configurar la autenticación de usuario**

El servidor SSH puede autenticar a los usuarios localmente o con un servidor de autenticación. Para usar el método de autenticación local, cree un nombre de usuario y una contraseña con el comando del modo de configuración global **username** *nombre-de-usuario* **secret** *contraseña*. En el ejemplo, se asignó la contraseña **ccna** al usuario **admin**.

**Paso 5. Configurar las líneas vty**

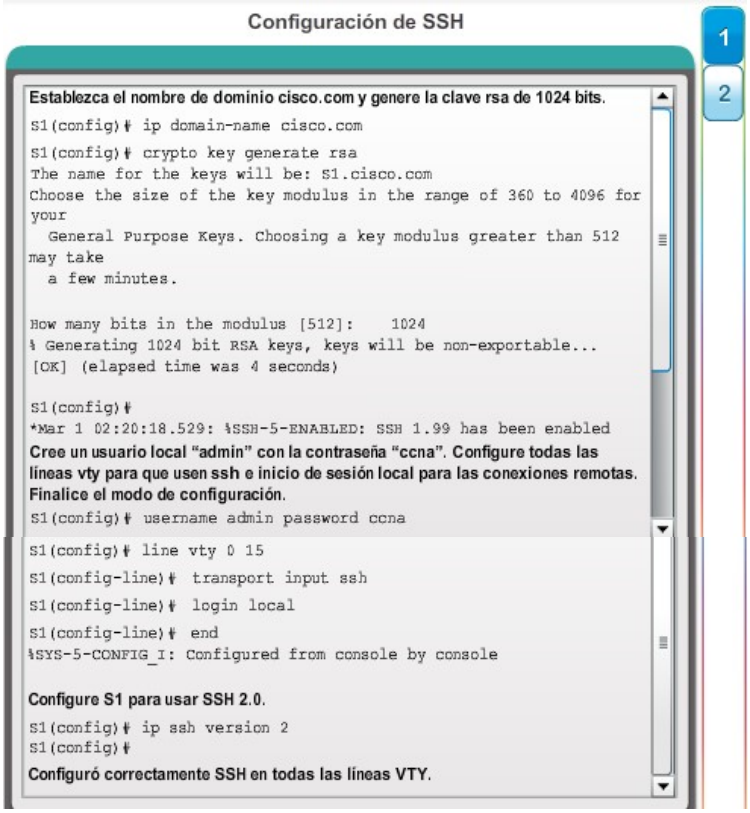
Habilite el protocolo SSH en las líneas vty mediante el comando **transport input ssh** del modo de configuración de línea. El switch Catalyst 2960 tiene líneas vty que van de 0 a 15. Esta configuración evita las conexiones que no son SSH (como Telnet) y limita al switch a que acepte solo las conexiones SSH. Use el comando **line vty** del modo de configuración global y, luego, el comando **login local** del modo de configuración de línea para requerir la

autenticación local de las conexiones SSH mediante la base de datos de nombres de usuarios locales.

**Paso 6. Habilitar la versión 2 de SSH.**

De manera predeterminada, SSH admite las versiones 1 y 2. Si se admiten ambas versiones, en el resultado de **show ip ssh** se muestra que se admite la versión 1.99. La versión 1 tiene vulnerabilidades conocidas. Por esta razón, se recomienda habilitar únicamente la versión 2. Habilite la versión de SSH mediante el comando de configuración global **ip ssh version 2**.

Use el verificador de sintaxis de la figura 2 para configurar SSH en el switch S1.




## 2.2.1.3 Verificación de SSH

En las computadoras, se usa un cliente SSH, como PuTTY, para conectarse a un servidor SSH. Para los ejemplos de las figuras 1 a 3, se configuró lo siguiente:

- Se habilitó SSH en el switch S1.
- Interfaz VLAN 99 (SVI) con la dirección IP 172.17.99.11 en el switch S1.
- PC1 con la dirección IP 172.17.99.21.

En la figura 1, la computadora inicia una conexión SSH a la dirección IP de la VLAN SVI de S1.

En la figura 2, se solicita al usuario que introduzca un nombre de usuario y una contraseña. Con la configuración del ejemplo anterior, se introduce el nombre de usuario **admin** y la contraseña **ccna**. Después de introducir la combinación correcta, el usuario se conecta a la CLI del switch Catalyst 2960 mediante SSH.

Para mostrar los datos de la versión y de configuración de SSH en el dispositivo que configuró como servidor SSH, use el comando **show ip ssh**. En el ejemplo, se habilitó la versión 2 de SSH. Para revisar las conexiones SSH al dispositivo, use el comando **show ssh** (consulte la figura 3).

**Configuración de los parámetros de conexión de cliente SSH PuTTY**


**Conexión de SSH para la administración remota**


**Verificación del estado y la configuración de SSH**