Cómo Configurar SSH en Switches Catalyst que Ejecutan CatOS

Contenido

Introducción

En este documento se proporcionan instrucciones paso a paso para configurar Secure Shell (SSH) Versión 1 en switches Catalyst que ejecutan Catalyst OS (CatOS). La versión probada es cat6000-supk9.6-1-1c.bin.

Prerequisites

Requirements

Esta tabla muestra el estado del soporte de SSH en los switches. Los usuarios registrados pueden acceder a estas imágenes de software visitando el Centro de Software.

CatOS SSH	
Dispositivo	Compatibilidad con SSH

Cat 4000/4500/2948G/2980G (CatOS)	Imágenes K9 a partir de 6.1
Cat 5000/5500 (CatOS)	Imágenes K9 a partir de 6.1
Cat 6000/6500 (CatOS)	Imágenes K9 a partir de 6.1
IOS SSH	
Dispositivo	**Compatibilidad con SSH**
Cat 2950*	12.1(12c)EA1 y posteriores
Cat 3550*	12.1(11)EA1 y posteriores
Cat 4000/4500 (software Cisco IOS integrado)*	12.1(13)EW y posteriores **
Cat 6000/5500 (software Cisco IOS integrado)*	12.1(11b)E y posteriores
Cat 8540/8510	12.1(12c)EY y posteriores, 12.1(14)E1 y posteriores
Sin SSH	
Dispositivo	**Compatibilidad con SSH**
CAT 1900	no
CAT 2800	no
Cat 2948G-L3	no
Cat 2900XL	no
Cat 3500XL	no
Cat 4840G-L3	no
Cat 4908G-L3	no

* La configuración se trata en Configuración de Secure Shell en Routers y Switches que Ejecutan Cisco IOS.

** No hay soporte para SSH en el tren 12.1E para Catalyst 4000 que ejecuta Integrated Cisco IOS Software.

Consulte Encryption Software Export Distribution Authorization Form para solicitar 3DES.

Este documento asume que la autenticación funciona antes de la implementación de SSH (a través de la contraseña Telnet, TACACS+) o RADIUS. SSH con Kerberos no se soporta antes de la implementación de SSH.

Componentes Utilizados

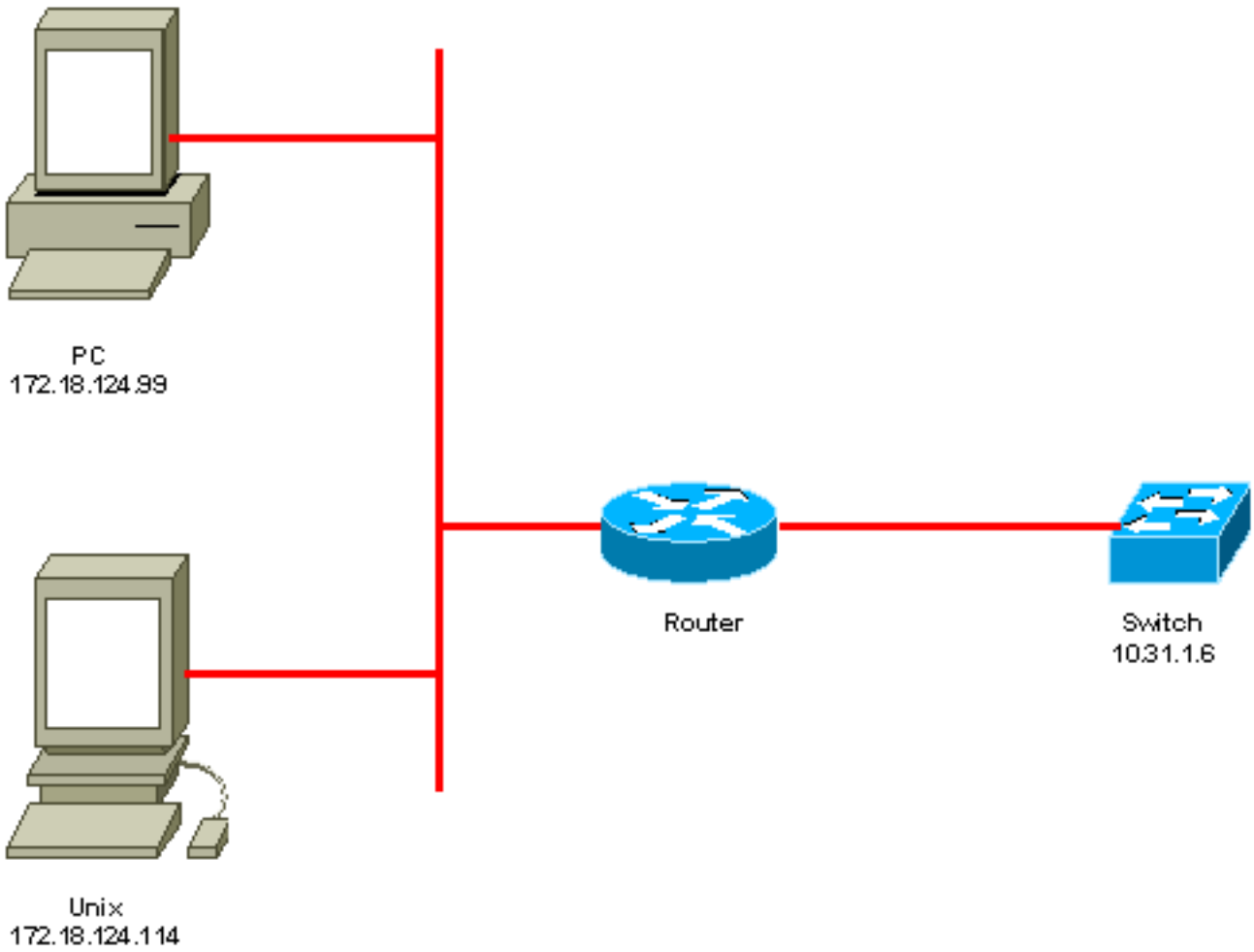
Este documento aborda solamente las series Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500, Catalyst 5000/5500 y Catalyst 6000/6500 que ejecutan la imagen CatOS K9. Para obtener más detalles, consulte la sección Requisitos de este documento.

La información que se presenta en este documento se originó a partir de dispositivos dentro de un ambiente de laboratorio específico. All of the devices used in this document started with a cleared (default) configuration. Si la red está funcionando, asegúrese de haber comprendido el impacto que puede tener un comando antes de ejecutarlo.

Convenciones

Para obtener más información sobre las convenciones del documento, consulte Convenciones de Consejos Técnicos de Cisco.

Diagrama de la red



Configuración del switch

```
!--- Generate and verify RSA key. sec-cat6000> (enable) set crypto key rsa 1024
Generating RSA keys..... [OK]
sec-cat6000> (enable) ssh_key_process: host/server key size: 1024/768
 !--- Display the RSA key. sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
!--- Restrict which host/subnets are allowed to use SSH to the switch. !--- Note: If you do not
do this, the switch will display the message !--- "WARNING!! IP permit list has no entries!"
sec-cat6000> set ip permit 172.18.124.0 255.255.255.0
172.18.124.0 with mask 255.255.255.0 added to IP permit list.
```

```
!--- Turn on SSH. sec-cat6000> (enable) set ip permit enable ssh
SSH permit list enabled.
!--- Verity SSH permit list. sec-cat6000> (enable) show ip permit
Telnet permit list disabled.
Ssh permit list enabled.
Snmp permit list disabled.
Permit List Mask Access-Type
---------------- --------------- -------------
172.18.124.0 255.255.255.0 telnet ssh snmp

Denied IP Address Last Accessed Time Type
---------------- ----------------- ------
```

Inhabilitación de SSH

En algunas situaciones puede ser necesario inhabilitar SSH en el switch. Debe verificar si SSH está configurado en el switch y, si es así, inhabilitarlo.

Para verificar si se ha configurado SSH en el switch, ejecute el comando **show crypto key**. Si el resultado muestra la clave RSA, entonces se ha configurado y habilitado SSH en el switch. Aquí se muestra un ejemplo.

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
199668201930132947097826805906337821547938540549819306165 1
```

Para quitar la clave crypto, ejecute el comando **clear crypto key rsa** para inhabilitar SSH en el switch. Aquí se muestra un ejemplo.

```
sec-cat6000> (enable) clear crypto key rsa
Do you really want to clear RSA keys (y/n) [n]? y
RSA keys has been cleared.
sec-cat6000> (enable)
```

depuración en el Catalyst

Para activar los debugs, ejecute el comando **set trace ssh 4**.

Para desactivar los debugs, ejecute el comando **set trace ssh 0**.

Ejemplos de una buena conexión del comando debug

Solaris en Catalyst, Norma del encripción de datos triple (3DES), contraseña Telnet

Solaris

```
rtp-evergreen# ssh -c 3des -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
```

```
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes
Host '10.31.1.6' added to the list of known hosts.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
root@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x8298a494, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: root
debug: Trying Local Login
Password authentication for root accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

PC a Catalyst, 3DES, contraseña de Telnet

Catalyst

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: des
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
Password authentication for accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 37
```

```
Unknown packet type received after authentication: 37
debug: ssh received packet type: 12
debug: ssh89: starting exec shell
debug: Entering interactive session.
```

Autenticación de Solaris a Catalyst, 3DES y Autenticación, Autorización y Contabilidad (AAA)

Solaris

```
Solaris with aaa on:
rtp-evergreen# ssh -c 3des -l abcde123 -v 10.31.1.6
SSH Version 1.2.26 [sparc-sun-solaris2.5.1], protocol version 1.5.
Compiled with RSAREF.
rtp-evergreen: Reading configuration data /opt/CISssh/etc/ssh_config
rtp-evergreen: ssh_connect: getuid 0 geteuid 0 anon 0
rtp-evergreen: Allocated local port 1023.
rtp-evergreen: Connecting to 10.31.1.6 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5, remote software version 1.2.26
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits) and host key (1024 bits).
rtp-evergreen: Host '10.31.1.6' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: 3des
rtp-evergreen: Sent encrypted session key.
rtp-evergreen: Installing crc compensation attack detector.
rtp-evergreen: Received encrypted confirmation.
rtp-evergreen: Doing password authentication.
abcde123@10.31.1.6's password:
rtp-evergreen: Requesting pty.
rtp-evergreen: Failed to get local xauth data.
rtp-evergreen: Requesting X11 forwarding with authentication spoofing.
Warning: Remote host denied X11 forwarding, perhaps xauth program
   could not be run on the server side.
rtp-evergreen: Requesting shell.
rtp-evergreen: Entering interactive session.

Cisco Systems Console

sec-cat6000>
```

Catalyst

```
sec-cat6000> (enable) debug: _proc->tty = 0x82a07714, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: abcde123
debug: Trying TACACS+ Login
Password authentication for abcde123 accepted.
debug: ssh received packet type: 10
debug: ssh received packet type: 34
Unknown packet type received after authentication: 34
debug: ssh received packet type: 12
debug: ssh88: starting exec shell
debug: Entering interactive session.
```

Ejemplos de lo que puede salir mal con el comando debug

Depuración de Catalyst con intentos del cliente por utilizar Cifrado Blowfish [no admitido]

```
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: blowfish
cipher_set_key: unknown cipher: 6
debug: Calling cleanup
```

Depuración de Catalyst con contraseña de Telnet incorrecta

```
debug: _proc->tty = 0x82897414, socket_index = 4
debug: version: SSH-1.5-1.2.26
debug: Client protocol version 1.5; client software version W1.0
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user:
debug: Trying Local Login
debug: Password authentication for failed.
```

Depuración de Catalyst con autenticación AAA incorrecta

```
cat6000> (enable) debug: _proc->tty = 0x829abd94, socket_index = 3
debug: version: SSH-1.5-1.2.26

debug: Client protocol version 1.5; client software version 1.2.26
debug: Sent 768 bit public key and 1024 bit host key.
debug: Encryption type: 3des
debug: Received session key; encryption turned on.
debug: ssh login by user: junkuser
debug: Trying TACACS+ Login
debug: Password authentication for junkuser failed.
SSH connection closed by remote host.
debug: Calling cleanup
```

Troubleshoot

Esta sección trata sobre diferentes escenarios de troubleshooting relacionados con la configuración SSH en los switches Cisco.

No se puede conectar al switch a través de SSH

Problema:

No se puede conectar al switch mediante SSH.

El comando **debug ip ssh** muestra este resultado:

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

Solución:

Este problema ocurre por cualquiera de estas razones:

- Las nuevas conexiones SSH fallan después de cambiar el nombre de host.
- SSH configurado con claves no etiquetadas (que tienen el FQDN del router).

Las soluciones alternativas para este problema son:

- Si el hostname fue cambiado y SSH ya no funciona, entonces ponga a cero la nueva clave y cree otra nueva clave con la etiqueta adecuada.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- No utilice claves RSA anónimas (denominadas así por el FQDN del switch). En su lugar, utilice claves etiquetadas.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

Para resolver este problema para siempre, actualice el software IOS a cualquiera de las versiones en las que se corrija este problema.

Se ha introducido un error sobre este problema. Para obtener más información, consulte la identificación de error de Cisco CSCtc41114 (**sólo para clientes registrados**) .

Información Relacionada

- Página de soporte de SSH
- Configuración de Secure Shell en Routers y Switches que ejecutan Cisco IOS
- Herramienta para errores de funcionamiento
- Soporte Técnico - Cisco Systems

Acerca de esta traducción
Cisco ha traducido este documento combinando la traducción automática y los recursos humanos a fin de ofrecer a nuestros usuarios en todo el mundo contenido en su propio idioma.

Tenga en cuenta que incluso la mejor traducción automática podría no ser tan precisa como la proporcionada por un traductor profesional.

Cisco Systems, Inc. no asume ninguna responsabilidad por la precisión de estas traducciones y recomienda remitirse siempre al documento original escrito en inglés (insertar vínculo URL).