

How to Configure SSH on Catalyst Switches Running CatOS

Document ID: 13881

Introduction

Prerequisites

- Requirements

- Components Used

- Conventions

Network Diagram

Switch Configuration

Disabling SSH

debug in the Catalyst

debug Command Examples of a Good Connection

- Solaris to Catalyst, Triple Data Encryption Standard (3DES), Telnet Password

- PC to Catalyst, 3DES, Telnet Password

- Solaris to Catalyst, 3DES, Authentication, Authorization, and Accounting (AAA)

- Authentication

debug Command Examples of What Can Go Wrong

- Catalyst debug with Client Attempting [unsupported] Blowfish Cipher

- Catalyst debug with Bad Telnet Password

- Catalyst debug with Bad AAA Authentication

Related Information

Introduction

This document gives step-by-step instructions to configure Secure Shell (SSH) Version 1 on Catalyst switches running Catalyst OS (CatOS). The version tested is cat6000-supk9.6-1-1c.bin.

Prerequisites

Requirements

This table shows the status of SSH support in the switches. Registered users can access these software images by visiting the Software Center (registered customers only).

CatOS SSH	
Device	SSH Support
Cat 4000/4500/2948G/2980G (CatOS)	K9 images as of 6.1
Cat 5000/5500 (CatOS)	K9 images as of 6.1
Cat 6000/6500 (CatOS)	K9 images as of 6.1
IOS SSH	
Device	SSH Support
Cat 2950*	12.1(12c)EA1 and later

Cat 3550*	12.1(11)EA1 and later
Cat 4000/4500 (Integrated Cisco IOS Software)*	12.1(13)EW and later **
Cat 6000/5500 (Integrated Cisco IOS Software)*	12.1(11b)E and later
Cat 8540/8510	12.1(12c)EY and later, 12.1(14)E1 and later
No SSH	
Device	SSH Support
Cat 1900	no
Cat 2800	no
Cat 2948G-L3	no
Cat 2900XL	no
Cat 3500XL	no
Cat 4840G-L3	no
Cat 4908G-L3	no

* Configuration is covered in Configuring Secure Shell on Cisco IOS Routers.

** There is no support for SSH in 12.1E train for Catalyst 4000 running Integrated Cisco IOS Software.

Refer to Encryption Software Export Distribution Authorization Form in order to apply for 3DES.

This document assumes that authentication works prior to implementation of SSH (through the Telnet password, TACACS+) or RADIUS. SSH with Kerberos is not supported prior to the implementation of SSH.

Components Used

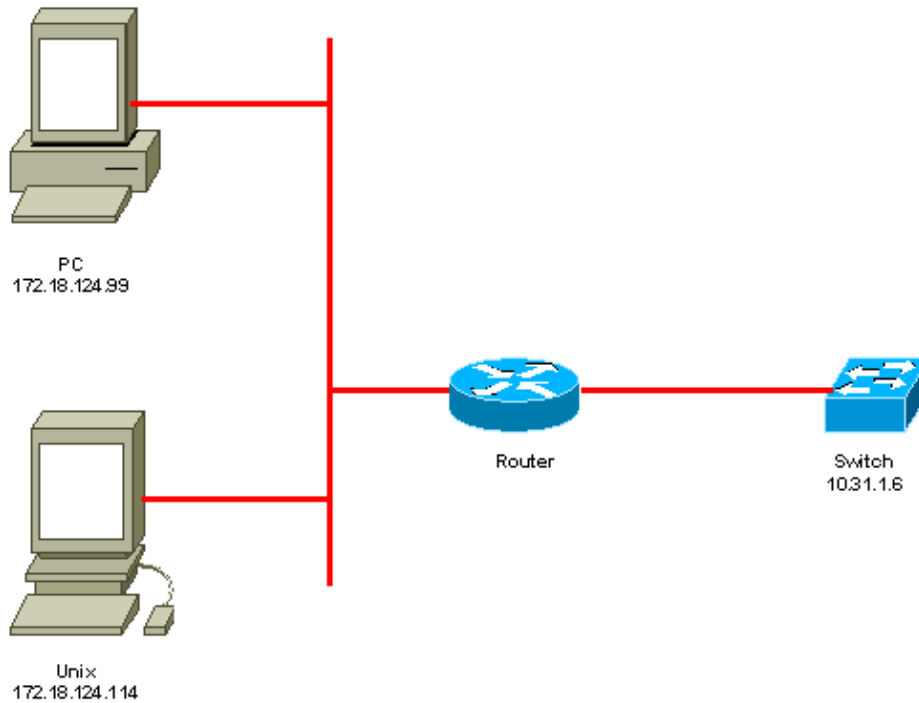
This document addresses only the Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500 series, Catalyst 5000/5500 series, and Catalyst 6000/6500 series running the CatOS K9 image. For more details, refer to the Requirements section of this document.

The information presented in this document was created from devices in a specific lab environment. All of the devices used in this document started with a cleared (default) configuration. If you are working in a live network, ensure that you understand the potential impact of any command before using it.

Conventions

For more information on document conventions, see the Cisco Technical Tips Conventions.

Network Diagram



Switch Configuration

!--- 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
1996682019301329470978268059063378215479385405498193061651
```

*!--- 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
-----

```

Disabling SSH

In some situations it may be necessary to disable SSH on the switch. You must verify whether SSH is configured on the switch and if so, disable it.

To verify if SSH has been configured on the switch, issue the **show crypto key** command. If the output displays the RSA key, then SSH has been configured and enabled on the switch. An example is shown here.

```

sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
577332853671704785709850606634768746869716963940352440620678575338701550888525
699691478330537840066956987610207810959498648179965330018010844785863472773067
697185256418386243001881008830561241137381692820078674376058275573133448529332
1996682019301329470978268059063378215479385405498193061651

```

To remove the crypto key, issue the **clear crypto key rsa** command to disable SSH on the switch. An example is shown here.

```

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)

```

debug in the Catalyst

To turn on debugs, issue the **set trace ssh 4** command.

To turn off debugs, issue the **set trace ssh 0** command.

debug Command Examples of a Good Connection

Solaris to Catalyst, Triple Data Encryption Standard (3DES), Telnet Password

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 to Catalyst, 3DES, Telnet Password

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.

```

Solaris to Catalyst, 3DES, Authentication, Authorization, and Accounting (AAA) Authentication

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.
abcdel23@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: abcdel23
debug: Trying TACACS+ Login
Password authentication for abcdel23 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.
```

debug Command Examples of What Can Go Wrong

Catalyst debug with Client Attempting [unsupported] Blowfish Cipher

```
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
```

Catalyst debug with Bad Telnet Password

```
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.
```

Catalyst debug with Bad AAA Authentication

```
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
```

Related Information

- [SSH Support Page](#)
- [Configuring Secure Shell on Cisco IOS Routers](#)
- [Bug Toolkit – Find bugs related to SSH on Catalyst switches running CatOS](#)
- [Technical Support – Cisco Systems](#)

[Contacts & Feedback](#) | [Help](#) | [Site Map](#)

© 2008 – 2009 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

Updated: Jan 19, 2006

Document ID: 13881
