

# Configuring Secure Shell on Routers and Switches Running Cisco IOS

Document ID: 4145

## Contents

### Introduction

#### Prerequisites

- Requirements
- Components Used
- Conventions

#### SSH v1 vs. SSH v2

#### Network Diagram

#### Test Authentication

- Authentication Test without SSH
- Authentication Test with SSH

#### Optional Configuration Settings

- Prevent Non-SSH Connections
- Set Up an IOS Router or Switch as SSH Client
- Setup an IOS Router as an SSH server that performs RSA based User Authentication
- Add SSH Terminal-Line Access
- Restrict SSH access to a subnet
- Configure the SSH Version
- Variations on banner Command Output
- Unable to Display the Login Banner

#### debug and show Commands

#### Sample Debug Output

- Router Debug
- Server Debug

#### What can go Wrong

- SSH From an SSH Client Not Compiled with Data Encryption Standard (DES)
- Bad Password
- SSH Client Sends Unsupported (Blowfish) Cipher
- Getting the "%SSH-3-PRIVATEKEY: Unable to retrieve RSA private key for" Error

#### Troubleshooting Tips

#### Related Information

## Introduction

Secure Shell (SSH) is a protocol which provides a secure remote access connection to network devices. Communication between the client and server is encrypted in both SSH version 1 and SSH version 2. Implement SSH version 2 when possible because it uses a more enhanced security encryption algorithm.

This document discusses how to configure and debug SSH on Cisco routers or switches that run a version of Cisco IOS<sup>®</sup> Software that supports SSH. This document contains more information on specific versions and software images.

## Prerequisites

## Requirements

The Cisco IOS image used must be a **k9(crypto)** image in order to support SSH. For example **c3750e-universalk9-tar.122-35.SE5.tar** is a k9 (crypto) image.

## Components Used

The information in this document is based on Cisco IOS 3600 Software (C3640-IK9S-M), Release 12.2(2)T1.

SSH was introduced into these Cisco IOS platforms and images:

- SSH Version 1.0 (SSH v1) server was introduced in some Cisco IOS platforms and images that start in Cisco IOS Software Release 12.0.5.S.
- SSH client was introduced in some Cisco IOS platforms and images starting in Cisco IOS Software Release 12.1.3.T.
- SSH terminal-line access (also known as reverse-Telnet) was introduced in some Cisco IOS platforms and images starting in Cisco IOS Software Release 12.2.2.T.
- SSH Version 2.0 (SSH v2) support was introduced in some Cisco IOS platforms and images starting in Cisco IOS Software Release 12.1(19)E.
- Refer to *How to Configure SSH on Catalyst Switches Running CatOS* for more information on SSH support in the switches.

Refer to the Software Advisor (registered customers only) for a complete list of feature sets supported in different Cisco IOS Software releases and on different platforms.

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 in a live network, make sure that you understand the potential impact of any command before you use it.

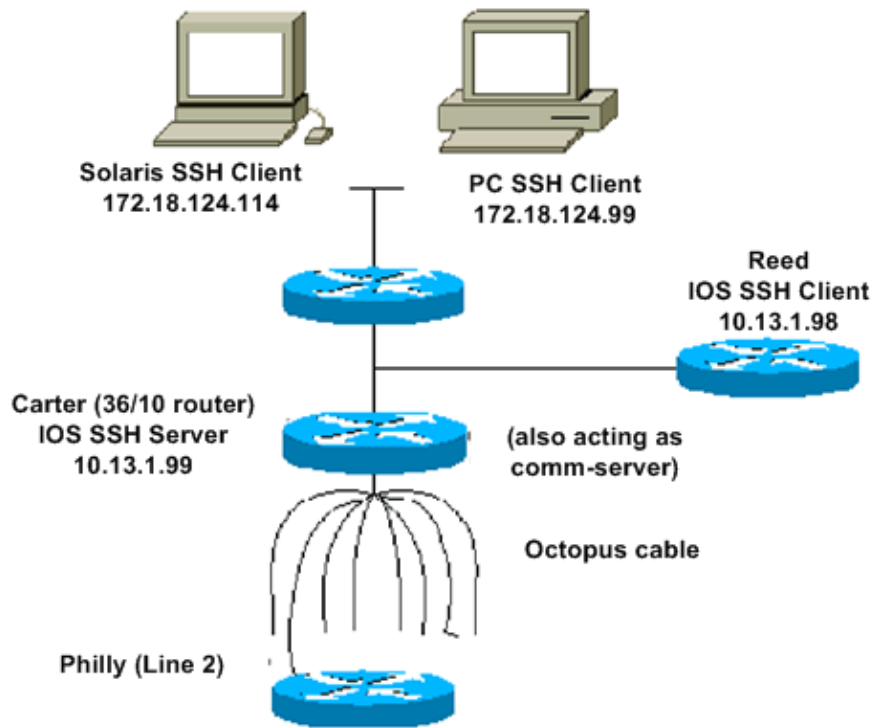
## Conventions

Refer to Cisco Technical Tips Conventions for more information on document conventions.

## SSH v1 vs. SSH v2

Use the Cisco Software Advisor (registered customers only) in order to help you find the version of code with appropriate support for either SSH v1 or SSH v2.

## Network Diagram



## Test Authentication

### Authentication Test without SSH

First test the authentication without SSH to make sure that authentication works with the router Carter before you add SSH. Authentication can be with a local username and password or with an authentication, authorization, and accounting (AAA) server that runs TACACS+ or RADIUS. (Authentication through the line password is not possible with SSH.) This example shows local authentication, which lets you Telnet into the router with username "cisco" and password "cisco."

*!--- The **aaa new-model** command causes the local username and password on the router to be used in the absence of other AAA statements.*

```
aaa new-model
username cisco password 0 cisco
line vty 0 4
transport input telnet
```

*!--- Instead of **aaa new-model**, you can use the **login local** command.*

### Authentication Test with SSH

In order to test authentication with SSH, you have to add to the previous statements in order to enable SSH on Carter and test SSH from the PC and UNIX stations.

```
ip domain-name rtp.cisco.com
```

*!--- Generate an SSH key to be used with SSH.*

```
crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2
```

At this point, the **show crypto key mypubkey rsa** command must show the generated key. After you add the SSH configuration, test your ability to access the router from the PC and UNIX station. If this does not work, see the debug section of this document.

## Optional Configuration Settings

### Prevent Non-SSH Connections

If you want to prevent non-SSH connections, add the **transport input ssh** command under the lines to limit the router to SSH connections only. Straight (non-SSH) Telnets are refused.

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

Test to make sure that non-SSH users cannot Telnet to the router Carter.

### Set Up an IOS Router or Switch as SSH Client

There are four steps required to enable SSH support on a Cisco IOS router:

1. Configure the **hostname** command.
2. Configure the DNS domain.
3. Generate the SSH key to be used.
4. Enable SSH transport support for the virtual type terminal (vty).

If you want to have one device act as an SSH client to the other, you can add SSH to a second device called Reed. These devices are then in a client-server arrangement, where Carter acts as the server, and Reed acts as the client. The Cisco IOS SSH client configuration on Reed is the same as required for the SSH server configuration on Carter.

```
!--- Step 1: Configure the hostname if you have not previously done so.

hostname carter

!--- The aaa new-model command causes the local username and password on the router
!--- to be used in the absence of other AAA statements.

aaa new-model
username cisco password 0 cisco

!--- Step 2: Configure the DNS domain of the router.

ip domain-name rtp.cisco.com

!--- Step 3: Generate an SSH key to be used with SSH.

crypto key generate rsa
ip ssh time-out 60
ip ssh authentication-retries 2

!--- Step 4: By default the vtys' transport is Telnet. In this case,
!--- Telnet is disabled and only SSH is supported.

line vty 0 4
transport input SSH
```

*!--- Instead of `aaa new-model`, you can use the `login local` command.*

Issue this command to SSH from the Cisco IOS SSH client (Reed) to the Cisco IOS SSH server (Carter) in order to test this:

- SSH v1:

```
ssh -l cisco -c 3des 10.13.1.99
```

- SSH v2:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -l cisco 10.31.1.99
```

## Setup an IOS Router as an SSH server that performs RSA based User Authentication

Complete these steps in order to configure the SSH server to perform RSA based authentication.

1. Specify the Host name.

```
Router(config)#hostname <host name>
```

2. Define a default domain name.

```
Router(config)#ip domain-name <Domain Name>
```

3. Generate RSA key pairs.

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

4. Configure SSH–RSA keys for user and server authentication.

```
Router(config)#ip ssh pubkey-chain
```

5. Configure the SSH username.

```
Router(conf-ssh-pubkey)#username <user name>
```

6. Specify the RSA public key of the remote peer.

```
Router(conf-ssh-pubkey-user)#key-string
```

7. Specify the SSH key type and version. (optional)

```
Router(conf-ssh-pubkey-data)#key-hash ssh-rsa <key ID>
```

8. Exit the current mode and return to privileged EXEC mode.

```
Router(conf-ssh-pubkey-data)#end
```

**Note:** Refer to Secure Shell Version 2 Support for more information.

## Add SSH Terminal–Line Access

If you need outbound SSH terminal–line authentication, you can configure and test SSH for outbound reverse Telnets through Carter, which acts as a comm server to Philly.

```
ip ssh port 2001 rotary 1
line 1 16
  no exec
  rotary 1
  transport input ssh
  exec-timeout 0 0
```

```
modem In Out
Stopbits 1
```

If Philly is attached to Carter's port 2, then you can configure SSH to Philly through Carter from Reed with the help of this command:

- SSH v1:

```
ssh -c 3des -p 2002 10.13.1.99
```

- SSH v2:

```
ssh -v 2 -c aes256-cbc -m hmac-sha1-160 -p 2002 10.31.1.99
```

You can use this command from Solaris:

```
ssh -c 3des -p 2002 -x -v 10.13.1.99
```

## Restrict SSH access to a subnet

You need to limit SSH connectivity to a specific subnetwork where all other SSH attempts from IPs outside the subnetwork should be dropped.

You can use these steps to accomplish the same:

1. Define an access-list that permits the traffic from that specific subnetwork.
2. Restrict access to the VTY line interface with an access-class.

This is an example configuration. In this example only SSH access to the 10.10.10.0 255.255.255.0 subnet is permitted, any other is denied access.

```
Router(config)#access-list 23 permit 10.10.10.0 0.0.0.255
Router(config)#line vty 5 15
Router(config-line)#transport input ssh
Router(config-line)#access-class 23 in
Router(config-line)#exit
```

**Note:** The same procedure to lock down the SSH access is also applicable on switch platforms.

## Configure the SSH Version

Configure SSH v1:

```
carter(config)#ip ssh version 1
```

Configure SSH v2:

```
carter(config)#ip ssh version 2
```

Configure SSH v1 and v2:

```
carter(config)#no ip ssh version
```

**Note:** You receive this error message when you use SSHv1:

```
%SCHED-3-THRASHING: Process thrashing on watched message event.
```

**Note:** Cisco bug ID CSCsu51740 (registered customers only) is filed for this issue. Workaround is to configure SSHv2.

## Variations on banner Command Output

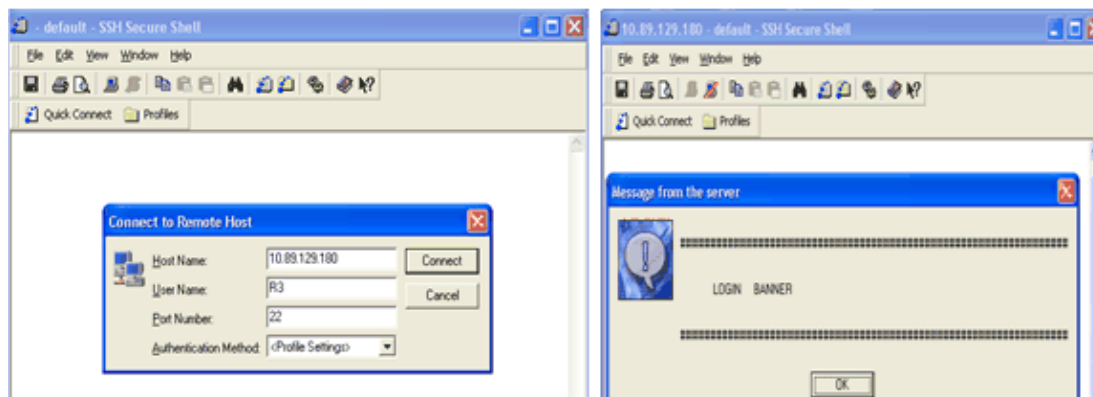
The **banner** command output varies between the Telnet and different versions of SSH connections. This table illustrates how different **banner** command options work with various types of connections.

Banner Command Option	Telnet	SSH v1 only	SSH v1 and v2	SSH v2 only
<b>banner login</b>	Displayed <b>before</b> logging into the device.	Not displayed.	Displayed <b>before</b> logging into the device.	Displayed <b>before</b> logging into the device.
<b>banner motd</b>	Displayed <b>before</b> logging into the device.	Displayed <b>after</b> logging into the device.	Displayed <b>after</b> logging into the device.	Displayed <b>after</b> logging into the device.
<b>banner exec</b>	Displayed <b>after</b> logging into the device.	Displayed <b>after</b> logging into the device.	Displayed <b>after</b> logging into the device.	Displayed <b>after</b> logging into the device.

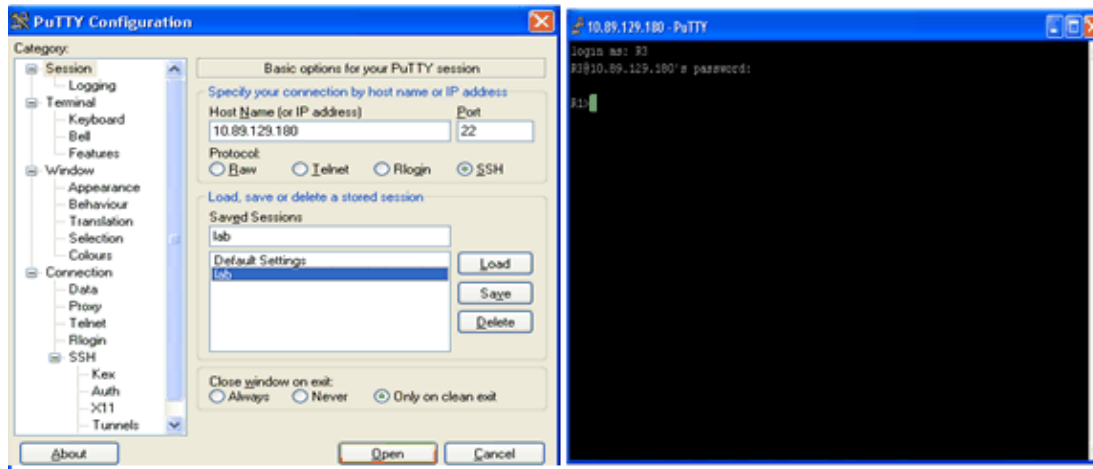
## Unable to Display the Login Banner

SSH version 2 supports the login banner. The login banner is displayed if the SSH client sends the username when it initiates the SSH session with the Cisco router. For example, when the Secure Shell ssh client is used, the login banner is displayed. When the PuTTY ssh client is used, the login banner is not displayed. This is because Secure Shell sends the username by default and PuTTY does not send the username by default.

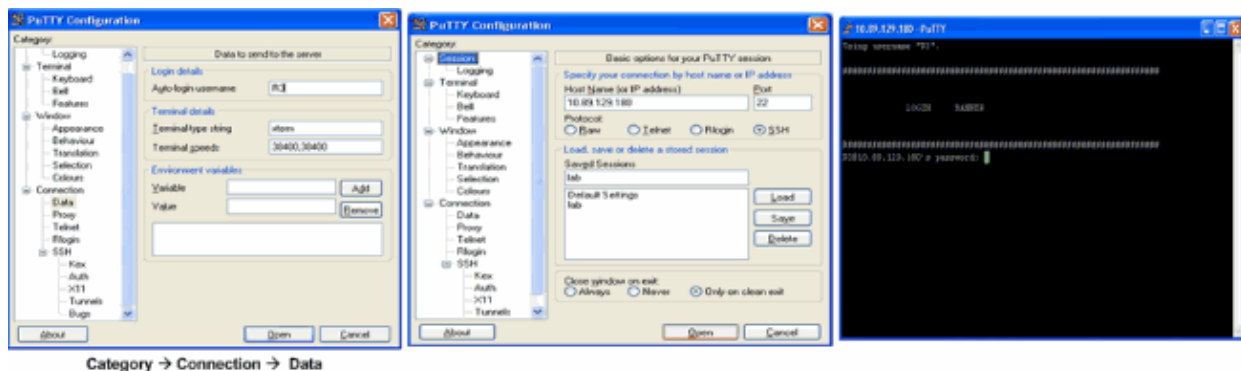
The Secure Shell client needs the username to initiate the connection to the SSH enabled device. The Connect button is not enabled if you do not enter the host name and username. This screenshot shows that the login banner is displayed when Secure Shell connects to the router. Then, the login banner password prompt displays.



The PuTTY client does not require the username to initiate the SSH connection to the router. This screenshot shows that the PuTTY client connects to the router and prompts for the username and password. It does not display the login banner.



This screen shot shows that the login banner is displayed when PuTTY is configured to send the username to the router.



## debug and show Commands

Before you issue the **debug** commands described and illustrated here, refer to Important Information on Debug Commands. Certain **show** commands are supported by the Output Interpreter Tool (registered customers only) , which allows you to view an analysis of **show** command output.

- **debug ip ssh** Displays debug messages for SSH.
- **show ssh** Displays the status of SSH server connections.

```

carter#show ssh
      Connection      Version Encryption      State      Username
      0                1.5      DES              Session started      cisco
  
```

- **show ip ssh** Displays the version and configuration data for SSH.

### ◆ Version 1 Connection and no Version 2

```

carter#show ip ssh
      SSH Enabled - version 1.5
      Authentication timeout: 60 secs; Authentication retries: 2
  
```

### ◆ Version 2 Connection and no Version 1

```

carter#show ip ssh
  
```

```
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

### ◆ Version 1 and Version 2 Connections

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

## Sample Debug Output

### Router Debug

**Note:** Some of this good debug output is wrapped to multiple lines because of spatial considerations.

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-1.5-1.2.26
00:23:20: SSH0: SSH_MSG_PUBLIC_KEY msg
00:23:21: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH: RSA decrypt started
00:23:21: SSH: RSA decrypt finished
00:23:21: SSH0: sending encryption confirmation
00:23:21: SSH0: keys exchanged and encryption on
00:23:21: SSH0: SSH_CMSG_USER message received
00:23:21: SSH0: authentication request for userid cisco
00:23:21: SSH0: SSH_MSG_FAILURE message sent
00:23:23: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:23:23: SSH0: authentication successful for cisco
00:23:23: SSH0: requesting TTY
00:23:23: SSH0: setting TTY - requested: length 24, width 80; set:
length 24, width 80
00:23:23: SSH0: invalid request - 0x22
00:23:23: SSH0: SSH_CMSG_EXEC_SHELL message received
00:23:23: SSH0: starting shell for vty
```

### Server Debug

**Note:** This output was captured on a Solaris machine.

```
rtp-evergreen.rtp.cisco.com#ssh -c 3des -l cisco -v 10.31.1.99
rtp-evergreen# /opt/CISssh/bin/ssh -c 3des -l cisco -v 10.13.1.99
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 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5,
remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' 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.
```

```
cisco@10.13.1.99'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.
```

## What can go Wrong

These sections have sample debug output from several incorrect configurations.

## SSH From an SSH Client Not Compiled with Data Encryption Standard (DES)

### Solaris Debug

```
rtp-evergreen#/opt/CISssh/bin/ssh -c des -l cisco -v 10.13.1.99
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 10.13.1.99 port 22.
rtp-evergreen: Connection established.
rtp-evergreen: Remote protocol version 1.5,
remote software version Cisco-1.25
rtp-evergreen: Waiting for server public key.
rtp-evergreen: Received server public key (768 bits)
and host key (512 bits).
rtp-evergreen: Host '10.13.1.99' is known and matches the host key.
rtp-evergreen: Initializing random; seed file //.ssh/random_seed
rtp-evergreen: Encryption type: des
rtp-evergreen: Sent encrypted session key.
cipher_set_key: unknown cipher: 2
```

### Router Debug

```
00:24:41: SSH0: Session terminated normally
00:24:55: SSH0: starting SSH control process
00:24:55: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:24:55: SSH0: protocol version id is - SSH-1.5-1.2.26
00:24:55: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:24:55: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:24:55: SSH: RSA decrypt started
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH: RSA decrypt started
00:24:56: SSH: RSA decrypt finished
00:24:56: SSH0: sending encryption confirmation
00:24:56: SSH0: Session disconnected - error 0x07
```

## Bad Password

### Router Debug

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-1.5-1.2.26
00:26:52: SSH0: SSH_SMSG_PUBLIC_KEY msg
00:26:52: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
```

```
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH: RSA decrypt started
00:26:52: SSH: RSA decrypt finished
00:26:52: SSH0: sending encryption confirmation
00:26:52: SSH0: keys exchanged and encryption on
00:26:52: SSH0: SSH_CMSG_USER message received
00:26:52: SSH0: authentication request for userid cisco
00:26:52: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: SSH_CMSG_AUTH_PASSWORD message received
00:26:54: SSH0: password authentication failed for cisco
00:26:54: SSH0: SSH_MSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

## SSH Client Sends Unsupported (Blowfish) Cipher

### Router Debug

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-1.5-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-1.5-W1.0
00:39:26: SSH0: SSH_MSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

## Getting the "%SSH-3-PRIVATEKEY: Unable to retrieve RSA private key for" Error

If you receive this error message, it may be caused due to any change in the domain name or host name. In order to resolve this, try these workarounds.

- Zeroize the RSA keys and re-generate the keys.

```
crypto key zeroize rsa label key_name
crypto key generate rsa label key_name modulus key_size
```

- If the previous workaround does not work, try these steps:

1. Zeroize all RSA keys.
2. Reload the device.
3. Create new labeled keys for SSH.

Cisco bug ID CSCsa83601 (registered customers only) has been filed to address this behaviour.

## Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated a RSA key pair for your router. Make sure you have specified a host name and domain. Then use the **crypto key generate rsa** command to generate an RSA key pair and enable the SSH server.
- When you configure the RSA key pair, you might encounter these error messages:

- 1.No hostname specified

You must configure a host name for the router using the **hostname** global configuration command.

- 2.No domain specified

You must configure a host domain for the router using the **ip domain-name** global configuration command.

- The number of allowable SSH connections is limited to the maximum number of vty configured for the router. Each SSH connection uses a vty resource.
- SSH uses either local security or the security protocol that is configured through AAA on your router for user authentication. When you configure AAA, you must ensure that the console is not running under AAA by applying a keyword in the global configuration mode to disable AAA on the console.
- No SSH server connections running.

```
carter#show ssh

%No SSHv2 server connections running.
%No SSHv1 server connections running.
```

This output suggests that the SSH server is disabled or not enabled properly. If you have already configured SSH, it is recommended that you reconfigure the SSH server in the device. Complete these steps in order to reconfigure SSH server on the device.

1. Delete the RSA key pair. After the RSA key pair is deleted, the SSH server is automatically disabled.

```
carter(config)#crypto key zeroize rsa
```

**Note:** It is important to generate a key-pair with at least 768 as bit size when you enable SSH v2.



**Caution:** This command cannot be undone after you save your configuration, and after

RSA keys have been deleted, you cannot use certificates or the CA or participate in certificate exchanges with other IP Security (IPSec) peers unless you reconfigure CA interoperability by regenerating RSA keys, getting the CA's certificate, and requesting your own certificate again. Refer to `crypto key zeroize rsa` – Cisco IOS Security Command Reference, Release 12.3 for more information on this command.

2. Reconfigure the hostname and domain name of the device.

```
carter(config)#hostname hostname

carter(config)#ip domain-name domainname
```

3. Generate an RSA key pair for your router, which automatically enables SSH.

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

Refer to `crypto key generate rsa` – Cisco IOS Security Command Reference, Release 12.3 for more information on the usage of this command.

**Note:** You can receive the SSH2 0: Unexpected mesg type received error message due to a packet received that is not understandable by the router. Increase the key length while you generate rsa keys for ssh in order to resolve this issue.

4. Configure SSH server. In order to enable and configure a Cisco router/switch for SSH server, you can configure SSH parameters. If you do not configure SSH parameters, the default values are used.

**ip ssh** {[*timeout seconds*] | [*authentication-retries integer*]}

```
carter(config)# ip ssh
```

Refer to `ip ssh` – Cisco IOS Security Command Reference, Release 12.3 for more information on the usage of this command.

## Related Information

- [How to Configure SSH on Catalyst Switches Running CatOS](#)
  - [Secure Shell Version 2 Support](#)
  - [SSH Product Support Page](#)
  - [Technical Support & Documentation – Cisco Systems](#)
- 

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

© 2010 – 2011 Cisco Systems, Inc. All rights reserved. [Terms & Conditions](#) | [Privacy Statement](#) | [Cookie Policy](#) | [Trademarks of Cisco Systems, Inc.](#)

---

Updated: Jun 28, 2007

Document ID: 4145

---