

在路由器和交换机上配置 SSH

目录

[简介](#)

[先决条件](#)

[要求](#)

[使用的组件](#)

[规则](#)

[SSH v2网络图](#)

[测试身份验证](#)

[不使用 SSH 时的身份验证测试](#)

[使用 SSH 时的身份验证测试](#)

[可选配置集](#)

[阻止非 SSH 连接](#)

[设置 IOS 路由器或交换机作为 SSH 客户端](#)

[将IOS路由器设置为执行基于RSA的用户身份验证的SSH服务器](#)

[添加 SSH 终端线路接入](#)

[限制对子网的SSH访问](#)

[配置SSH第2版](#)

[banner 命令输出的变化](#)

[Banner命令选项](#)

[Telnet](#)

[SSH v2](#)

[无法显示LoginBanner](#)

[debug 和 show 命令](#)

[调试输出示例](#)

[路由器调试](#)

[服务器调试](#)

[配置不正确](#)

[来自 SSH 客户端的 SSH 不是使用数据加密标准 \(DES\) 编译的](#)

[错误密码](#)

[路由器调试](#)

[SSH 客户端发送不支持的 \(Blowfish\) 密码](#)

[路由器调试](#)

[获取"%SSH-3-PRIVATEKEY : 无法检索RSA私钥"错误](#)

[技巧](#)

[相关信息](#)

简介

本文档介绍如何在运行 Cisco IOS® 软件的思科路由器或交换机上配置和调试安全外壳 (SSH)。

先决条件

要求

使用的Cisco IOS映像必须是k9 (加密) 映像才能支持SSH。例如 , c3750e-universalk9-tar.122-35.SE5.tar是一个k9 (加密) 映像。

使用的组件

本文档中的信息基于 Cisco IOS 3600 软件 (C3640-IK9S-M) 版本 12.2(2)T1。

SSH被引入到以下Cisco IOS平台和映像中：

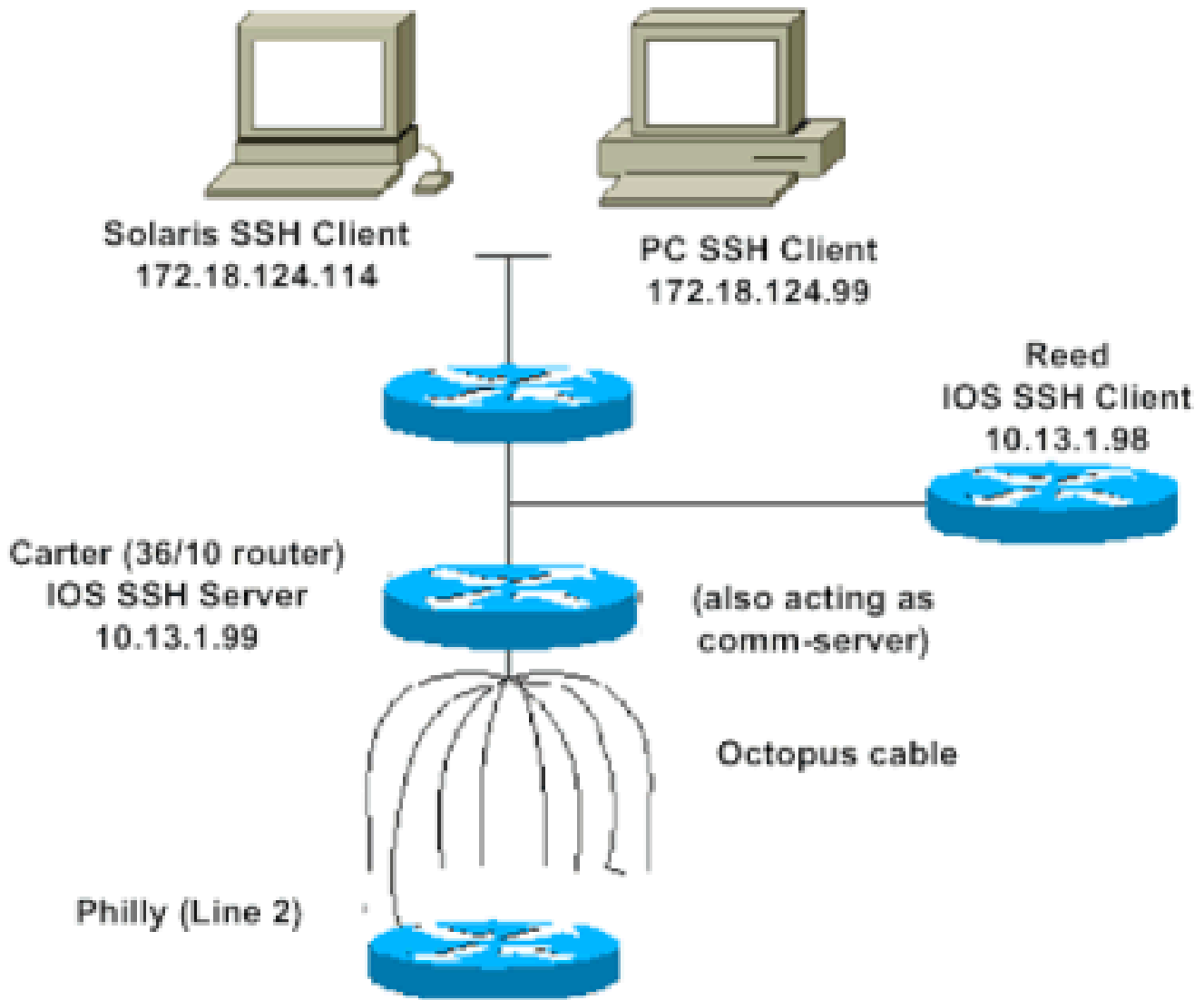
- 从Cisco IOS软件版本12.2.2.T开始，Cisco IOS平台和映像中引入了SSH终端行访问 (也称为反向Telnet) 。
- 从Cisco IOS软件版本12.1(19)E开始，Cisco IOS平台和映像中引入了SSH 2.0版(SSH v2)支持。

本文档中的信息都是基于特定实验室环境中的设备编写的。本文档中使用的所有设备最初均采用原始 (默认) 配置。如果您的网络处于活动状态，请确保您了解所有命令的潜在影响。

规则

有关详细信息，请参阅[Cisco技术提示规则](#)。


SSH v2网络图



测试身份验证

不使用 SSH 时的身份验证测试

首先在不使用 SSH 的情况下测试身份验证，以确保在您添加 SSH 之前，路由器 Carter 的身份验证工作正常。身份验证可以使用本地用户名和密码，也可以使用运行TACACS+或RADIUS的身份验证、授权和记帐(AAA)服务器。（使用SSH无法通过线路密码进行身份验证。）此示例显示本地身份验证，它允许使用用户名cisco和密码cisco通过Telnet连接到路由器。

 注意：在本文档中，vty用于指示虚拟终端类型。

!--- The aaa new-model command causes the local username and password on the router to be used in the a

```
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.

使用 SSH 时的身份验证测试

要使用SSH测试身份验证，您必须添加之前的语句以便在Carter上启用SSH，并从PC和UNIX工作站测试SSH。

```
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
```

此时，show crypto key mypubkey rsa命令必须显示生成的密钥。在添加 SSH 配置后，请测试从 PC 和 UNIX 工作站访问路由器的能力。

可选配置集

阻止非 SSH 连接

如果要阻止非 SSH 连接，请在语句行的下面添加 transport input ssh 命令，将路由器限制为只能使用 SSH 连接。直接 (非 SSH) Telnet 将被拒绝。

```
line vty 0 4

!--- Prevent non-SSH Telnets.

transport input ssh
```

进行测试，确保非SSH用户无法通过Telnet连接到路由器Carter。

设置 IOS 路由器或交换机作为 SSH 客户端

在Cisco IOS路由器上启用SSH支持需要四个步骤：

1. 配置hostname命令。
2. 配置DNS域。
3. 生成SSH密钥。
4. 为vty启用SSH传输支持。

如果要让一台设备充当另一台设备的 SSH 客户端，可以在称为 Reed 的第二台设备上添加 SSH。

将这些设备置于客户端-服务器布局中，其中Carter充当服务器，Reed充当客户端。Reed上的Cisco IOS SSH客户端配置与Carter上的SSH服务器配置所需的配置相同。

!--- 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 a

```
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 vty transport is Telnet. In this case, Telnet is disabled and only SSH is s

```
line vty 0 4  
transport input ssh
```

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

从Cisco IOS SSH客户端(Reed)向Cisco IOS SSH服务器(Carter)发出以下命令以测试这一点：

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

将IOS路由器设置为执行基于RSA的用户身份验证的SSH服务器

完成以下步骤，将SSH服务器配置为执行基于RSA的身份验证。

1. 指定主机名。

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

2. 定义默认域名。

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

3. 生成RSA密钥对

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

4. 为用户和服务器身份验证配置SSH-RSA密钥。

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

5. 配置SSH用户名。

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

6. 指定远程对等设备的RSA公钥。

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

7. 指定SSH密钥类型和版本。(此步骤是可选的。)

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

8. 退出当前模式并返回特权EXEC模式。

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

添加 SSH 终端线路接入

如果需要出站 SSH 终端线路身份验证，可以配置并测试通过 Carter (充当 Philly 的通信服务器) 进行出站反向 Telnet 的 SSH。

```
ip ssh port 2001 rotary 1
```

```
line 1 16
  no exec
  rotary 1
  transport input ssh
  exec-timeout 0 0
  modem InOut
  stopbits 1
```

如果Philly连接到Carter端口2，则可以使用以下命令配置从Reed通过Carter到Philly的SSH：

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

在 Solaris 上，可以使用以下命令：

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

限制对子网的SSH访问


您需要限制到特定子网的SSH连接，在该子网中会丢弃来自该子网外部IP的所有其他SSH尝试。

可以使用以下步骤执行相同的操作：

1. 定义允许来自该特定子网的数据流的访问列表。
2. 使用`access-class`限制对VTY线路接口的访问。

这是配置示例。在本示例中，仅允许通过SSH访问10.10.10.0 255.255.255.0子网，而拒绝任何其他访问。

```
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
```

 注意：锁定SSH访问的同一过程也用于交换机平台。

配置SSH第2版

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

banner 命令输出的变化

使用 Telnet 和不同版本的 SSH 连接时，banner 命令的输出会有所不同。下表说明了不同的 banner 命令选项如何处理各种类型的连接。

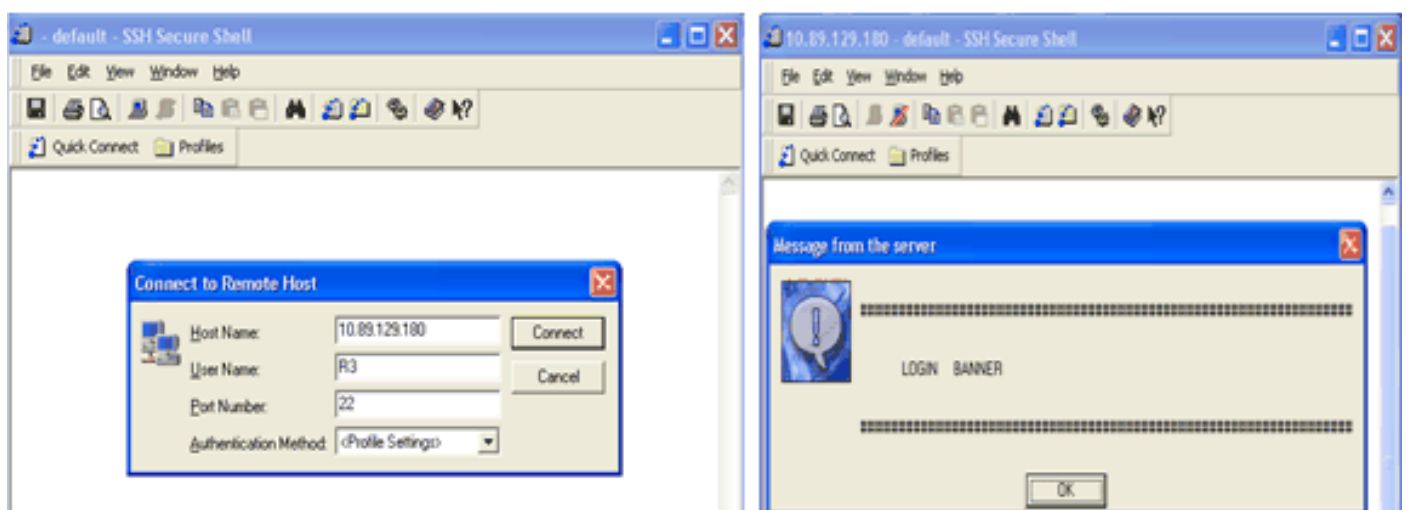
Banner命令选项	Telnet	SSH v2
横幅日志	在登录设备之前显示。	在登录设备之前显示。
banner motd	在登录设备之前显示。	登录设备后显示。
banner exec	登录设备后显示。	登录设备后显示。

 注意：不再建议使用SSH第1版。

无法显示登录标语

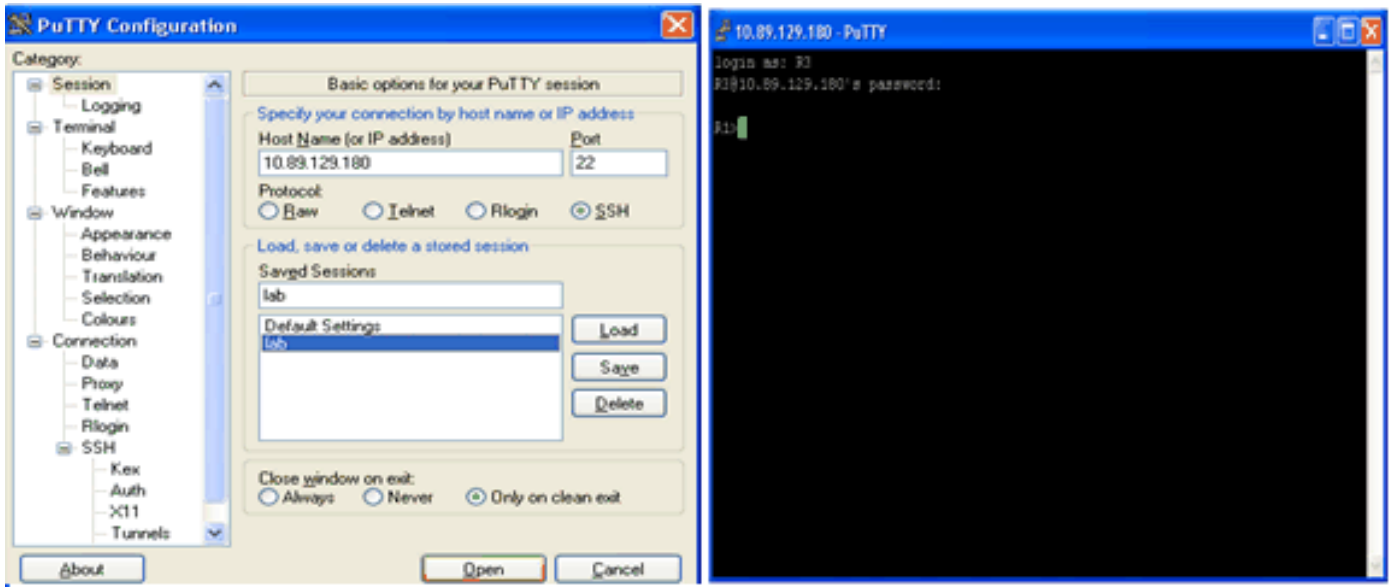
SSH第2版支持登录标语。当它启动与Cisco路由器的SSH会话时，如果SSH客户端发送用户名，则会显示登录提示。例如，使用安全外壳ssh客户端时，会显示登录标语。使用PuTTY ssh客户端时，不显示登录标语。这是因为SSH默认发送用户名，而PuTTY默认不发送用户名。

SSH客户端需要用户名来启动与启用了SSH的设备的连接。如果不输入主机名和用户名，则不会启用 Connect 按钮。此屏幕图像显示SSH连接到路由器时显示的登录标语。然后，标语会提示输入密码。



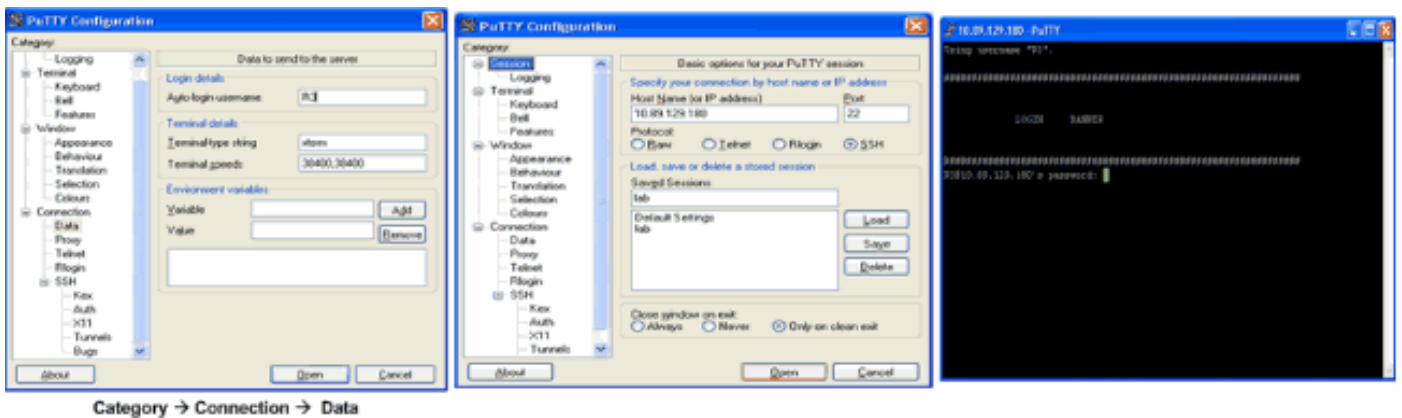
提示输入密码的横幅

PuTTY 客户端不需要用户名来发起到路由器的 SSH 连接。此屏幕图像显示PuTTY客户端连接到路由器并提示输入用户名和密码。它不显示登录标语。



到路由器的SSH连接

此屏幕截图显示当PuTTY配置为将用户名发送到路由器时显示的登录标语。



Category → Connection → Data

将用户名发送到路由器

debug 和 show 命令

在发出此处介绍的debug命令之前，请参阅[有关Debug命令的重要信息](#)。[输出解释器工具](#)（仅注册到客户）支持某些show命令（只注册到客户），通过该工具可查看对show命令输出的分析。

- debug ip ssh —显示SSH的调试消息。
- show ssh —显示SSH服务器连接的状态。

carter#show ssh

Connection	Version	Encryption	State	Username
0	2.0	DES	Session started	cisco

- show ip ssh —显示SSH的版本和配置数据。

```
carter#show ip ssh
SSH Enabled - version 2.0
Authentication timeout: 120 secs; Authentication retries: 3
```

调试输出示例

路由器调试

```
00:23:20: SSH0: starting SSH control process
00:23:20: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:23:20: SSH0: protocol version id is - SSH-2.0-1.2.26
00:23:20: SSH0: SSH_SMSG_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_SMSG_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
```

服务器调试

 注意：这是Solaris计算机输出。

```
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 2.0,
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.
```

配置不正确

以下部分列出了几种不正确的配置导致的调试输出示例。

来自 SSH 客户端的 SSH 不是使用数据加密标准 (DES) 编译的

错误密码

路由器调试

```
00:26:51: SSH0: starting SSH control process
00:26:51: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:26:52: SSH0: protocol version id is - SSH-2.0-1.2.26
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_SMSG_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_SMSG_FAILURE message sent
00:26:54: SSH0: authentication failed for cisco (code=7)
00:26:54: SSH0: Session disconnected - error 0x07
```

SSH 客户端发送不支持的 (Blowfish) 密码

路由器调试

```
00:39:26: SSH0: starting SSH control process
00:39:26: SSH0: sent protocol version id SSH-2.0-Cisco-1.25
00:39:26: SSH0: protocol version id is - SSH-2.0-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
```

获取“%SSH-3-PRIVATEKEY：无法检索RSA私钥”错误

域名或主机名的更改可能会触发此错误消息。使用以下解决方法：

- 将RSA密钥归零，然后重新生成密钥。

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

- 如果之前的解决方法不起作用，请尝试以下步骤：
 1. 将所有RSA密钥归零。
 2. 重新启动设备。
 3. 为SSH创建新的已标记密钥。

技巧

- 如果 SSH 配置命令被作为非法命令拒绝，则说明您没有成功地为路由器生成 RSA 密钥对。确保已指定主机名和域。然后，使用crypto key generate rsa命令生成RSA密钥对并启用SSH服务器。
- 配置RSA密钥对时，可能会收到以下错误消息：
 1. No hostname specified.
要配置路由器的主机名，必须使用hostname全局配置命令。
 2. No domain specified.
必须使用ip domain-name全局配置命令配置路由器的主机域。
- 允许的SSH连接数限制为路由器配置 vty 的最大连接数。每个SSH连接使用一个 vty 资源。

使用本地安全性或通过路由器上的AAA配置的安全协议进行用户身份验证。配置AAA时，必须确保控制台不在AAA下运行。在全局配置模式下应用关键字可禁用控制台上的AAA。

-

No SSH server connections running:

```
carter#show ssh %No SSHv2 server connections running.
```

此输出表明 SSH 服务器被禁用或未正确启用。如果已经配置了 SSH，建议您在设备中重新配置 SSH 服务器。要重新配置设备上的 SSH 服务器，请完成以下步骤。

- 删除RSA密钥对。删除RSA密钥对后，SSH服务器将自动禁用。

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



注意：启用SSH v2时，生成比特大小至少为768的密钥对非常重要。



注意：保存配置后，此命令无法撤消。此外，删除RSA密钥后，除非重新生成RSA密钥以重新配置CA互操作性、获取CA证书并再次请求您自己的证书，否则您不能使用证书或CA或其他IP安全(IPSec)对等体进行证书交换。

2. 重新配置设备的主机名和域名。


```
carter(config)#hostname hostname
```

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

3. 为路由器生成RSA密钥对。这将自动启用SSH。

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

 **注意：**有关此命令用法的详细信息，请参阅[crypto key generate rsa - Cisco IOS安全命令参考12.3版](#)。

 **注意：**您可能会收到SSH2 0: Unexpected mesg type received错误消息，因为路由器无法理解接收到的数据包。要解决此问题，请在生成用于 SSH 的 RSA 密钥时增加密钥长度。

4. 配置SSH服务器。

5. 要为SSH服务器启用和配置Cisco路由器/交换机，您必须配置SSH参数。如果不配置 SSH 参数，将使用默认值。

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

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

相关信息

- [SSH 产品支持页面](#)

关于此翻译

思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。