# Konfigurieren von Secure Shell auf Routern und Switches mit Cisco IOS

## Inhalt



## Einleitung

Das Protokoll Secure Shell (SSH) ermöglicht sicheren Remotezugriff auf Netzwerkgeräte. Die Kommunikation zwischen Client und Server wird sowohl in SSH Version 1 als auch in SSH Version 2 verschlüsselt. Wenn möglich sollten Sie SSH-Version 2 implementieren, da ein erweiterter Verschlüsselungsalgorithmus verwendet wird.

In diesem Dokument finden Sie eine Beschreibung der SSH-Konfiguration und der SSH-Fehlersuche auf Cisco Routern und Switches mit einer Version der Cisco IOS®-Software, die SSH

unterstützt. Das Dokument enthält zudem detailliertere Informationen zu den einzelnen Versionen und Software-Images.

# Voraussetzungen

## Anforderungen

Voraussetzung für SSH-Unterstützung ist die Verwendung eines Cisco IOS-Image des Typs **k9(crypto). c3750e-universalk9-tar.122-35.SE5.tar ist beispielsweise ein Image des Typs "k9(crypto)".**

## Verwendete Komponenten

Die Informationen in diesem Dokument beziehen sich auf die Cisco IOS 3600-Software (C3640-IK9S-M), Version 12.2(2)T1.

SSH wurde in die folgenden Cisco IOS-Plattformen und -Images integriert:

Ein SSHv1-Server ist in einigen Cisco IOS-Plattformen und -Images ab Version 12.0.5.S der Cisco IOS-Software verfügbar.

Ein SSH-Client ist in einigen Cisco IOS-Plattformen und -Images ab Version 12.1.3.T der Cisco IOS-Software verfügbar.

SSH-Terminalzugriff (auch Reverse-Telnet genannt) ist in einigen Cisco IOS-Plattformen und -Images ab Version 12.2.2.T der Cisco IOS-Software verfügbar.

Unterstützung für Version 2.0 von SSH (SSHv2) ist in einigen Cisco IOS-Plattformen und -Images ab Version 12.1(19)E der Cisco IOS-Software verfügbar.

Weitere Informationen zur SSH-Unterstützung auf Catalyst-Switches finden Sie unter How to Configure SSH on Catalyst Switches Running CatOS (SSH-Konfiguration auf Catalyst-Switches mit CatOS).

Eine vollständige Liste aller unterstützten Funktionssätze aufgeschlüsselt nach Plattform und Version der Cisco IOS-Software finden Sie in Software Advisor (nur registrierte Kunden).

Die Informationen in diesem Dokument beziehen sich auf Geräte in einer speziell eingerichteten Testumgebung. Alle Geräte, die in diesem Dokument benutzt wurden, begannen mit einer gelöschten (Nichterfüllungs) Konfiguration. Wenn Ihr Netzwerk in der Produktionsumgebung eingesetzt wird, müssen Sie sich bei jedem Befehl zunächst dessen potenzielle Auswirkungen vor Augen führen.

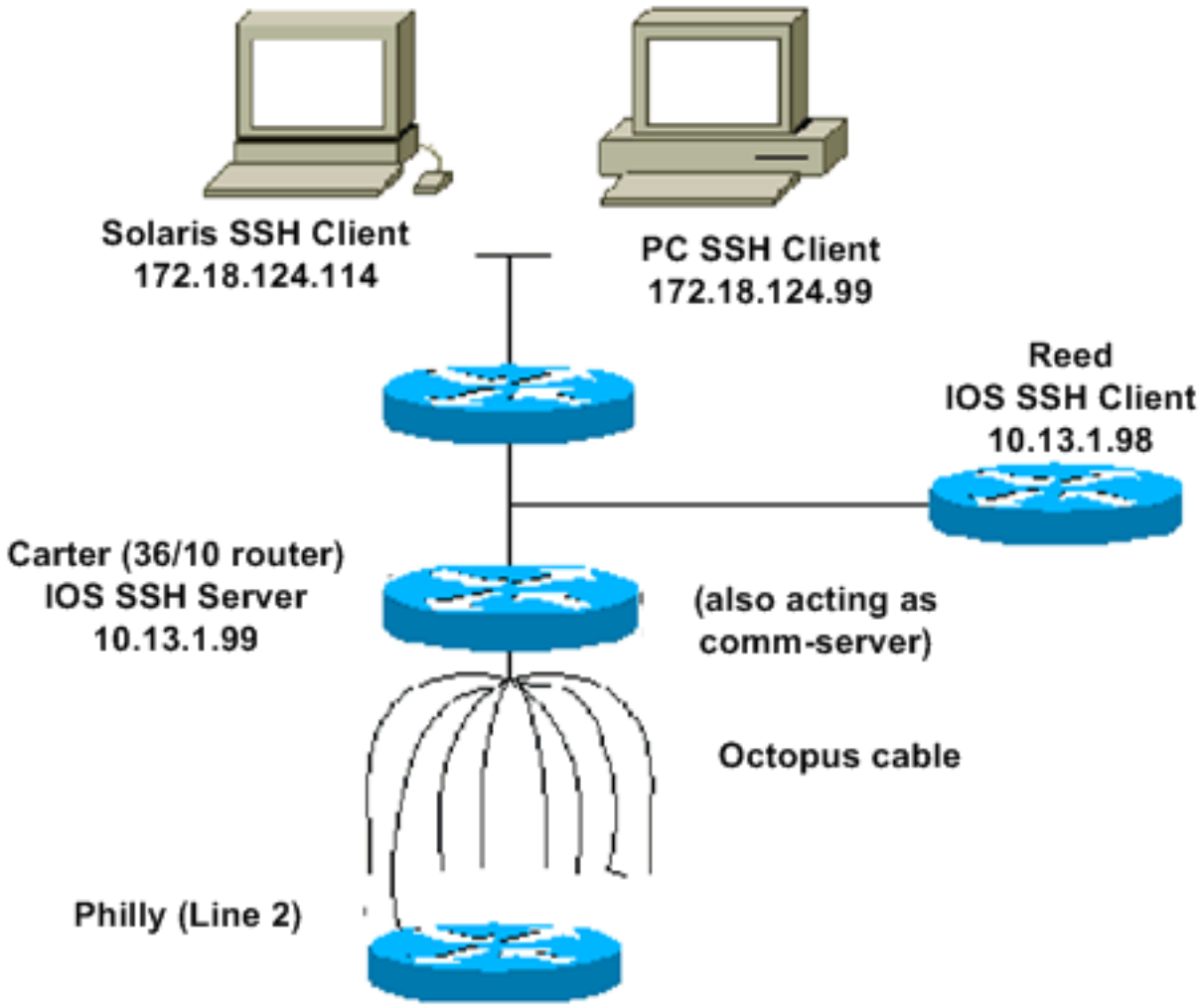
## Konventionen

Weitere Informationen zu Dokumentkonventionen finden Sie unter Cisco Technical Tips Conventions (Technische Tipps von Cisco zu Konventionen).

# SSHv1 oder SSHv2

Nutzen Sie Cisco Software Advisor (nur registrierte Kunden), um die Codeversion zu finden, die die gewünschte SSH-Version unterstützt (SSHv1 oder SSHv2).

# Netzwerkdiagramm




# Testen der Authentifizierung

## Authentifizierungstest ohne SSH

Führen Sie vor der Implementierung von SSH zunächst einen Authentifizierungstest ohne SSH durch, um sicherzustellen, dass eine Authentifizierung beim Router "Carter" möglich ist. Die Authentifizierung kann über einen lokalen Benutzernamen mit zugehörigem Kennwort oder über einen AAA-Server (Authentication, Authorization and Accounting) mit TACACs+ oder RADIUS erfolgen. (Eine Authentifizierung über das Line-Kennwort wird von SSH nicht unterstützt.) Das Beispiel unten zeigt eine lokale Authentifizierung, bei der mit dem Benutzernamen "cisco" und dem Kennwort "cisco" eine Telnet-Verbindung zum Router hergestellt werden kann.

```
!--- 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.
```

## Authentifizierungstest mit SSH

Für einen Authentifizierungstest mit SSH müssen Sie die im obigen Beispiel verwendeten Anweisungen so ergänzen, dass SSH auf "Carter" aktiviert wird. Anschließend müssen Sie die SSH-Verbindung vom PC und vom UNIX-System testen.

```
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
```

An diesem Punkt muss der Befehl **show crypto key mypubkey rsa den generierten Schlüssel zurückgeben.** Nachdem Sie die SSH-Konfiguration hinzugefügt haben, müssen Sie testen, ob der PC und das UNIX-System Zugriff auf den Router haben. Wenn der Zugriff nicht funktioniert: Lesen Sie den Abschnitt zum Thema Fehlersuche in diesem Dokument.

# Optionale Konfigurationseinstellungen

## Unterbinden von nicht SSH-basierten Verbindungen

Sollen nicht SSH-basierte Verbindungen unterbunden werden, müssen Sie den Befehl **transport input ssh unter den Zeilen hinzufügen. Damit wird der Router ausschließlich auf SSH-Verbindungen beschränkt.** Direkte (nicht SSH-basierte) Telnet-Verbindungen werden abgelehnt.

```
line vty 0 4
!--- Prevent non-SSH Telnets. transport input ssh
```

Vergewissern Sie sich durch einen Test, dass nicht SSH-basierte Benutzer keine Telnet-Verbindung zum Router "Carter" herstellen können.

## Einrichten eines IOS-Routers oder -Switches als SSH-Client

Zur Aktivierung der SSH-Unterstützung auf einem Cisco IOS-Router sind vier Schritte erforderlich:

Konfigurieren Sie den Befehl **hostname.**

Konfigurieren Sie die DNS-Domäne.

Generieren Sie den zu verwendenden SSH-Schlüssel.

Aktivieren Sie die Unterstützung für SSH-Übertragungen auf den virtuellen Terminals (VTYs).

Soll ein anderes Gerät als SSH-Client für den Router fungieren, können Sie SSH auf einem zweiten Gerät namens "Reed" implementieren. Die beiden Geräte befinden sich dann in einer Client-Server-Konfiguration, in der "Carter" der Server und "Reed" der Client ist. Zur Konfiguration des SSH-Client in Cisco IOS auf "Reed" gehen Sie genauso vor wie zur Konfiguration des SSH-Servers auf "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.
```

Führen Sie als Test den folgenden Befehl aus, um eine SSH-Verbindung vom Cisco IOS-SSH-Client (Reed) zum Cisco IOS-SSH-Server (Carter) zu öffnen:

SSHv1:

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

SSHv2:

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

## Einrichten eines IOS-Routers als SSH-Server mit RSA-basierter Benutzerauthentifizierung

Gehen Sie wie folgt vor, um den SSH-Server so zu konfigurieren, dass eine RSA-basierte Authentifizierung durchgeführt wird:

Geben Sie den Host-Namen an.

```
Router(config)#hostname
```

Legen Sie einen Standard-Domänennamen fest.

```
Router(config)#ip domain-name
```

Generieren Sie RSA-Schlüsselpaare.

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

Konfigurieren Sie die SSH-RSA-Schlüssel für die Benutzerauthentifizierung und die Serverauthentifizierung.

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

Konfigurieren Sie den SSH-Benutzernamen.

```
Router(conf-ssh-pubkey)#username
```

Geben Sie den öffentlichen RSA-Schlüssel des Remote-Peer an.

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

Geben Sie Typ und Version des SSH-Schlüssels an. (optional)

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

Beenden Sie den aktuellen Modus, und wechseln Sie zurück in den privilegierten EXEC-Modus.

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

**Hinweis:** Weitere Informationen finden Sie unter Secure Shell Version 2 Support.

## Hinzufügen von SSH-Terminalzugriff

Muss eine ausgehende Authentifizierung über ein SSH-Terminal eingerichtet werden, können Sie SSH für ausgehende Reverse-Telnet-Verbindungen über das Gerät "Carter" konfigurieren, das als Kommunikationsserver für das Gerät "Philly" fungiert. Testen Sie die Funktion anschließend.

```
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
```

Wenn "Philly" an Port 2 von "Carter" angebunden ist, können Sie mit dem folgenden Befehl eine SSH-Verbindung von "Reed" über "Carter" zu "Philly" konfigurieren:

SSHv1:

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

SSHv2:

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

Unter Solaris können Sie diesen Befehl verwenden:

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

## Beschränken des SSH-Zugriffs auf ein Subnetz

Nehmen wir an, Sie müssen SSH-Netzwerkverbindungen auf ein bestimmtes Subnetzwerk beschränken. Dabei sollen alle übrigen SSH-Verbindungsversuche von IP-Adressen außerhalb des Subnetzwerks verworfen werden.

Um eine solche Konfiguration einzurichten, können Sie wie folgt vorgehen:

1. Definieren Sie eine Zugriffsliste, die den Datenverkehr aus dem betreffenden Subnetzwerk zulässt.

2. Beschränken Sie mithilfe von `access-class` den Zugriff auf die VTY-Schnittstelle.

Unten sehen Sie eine Beispielkonfiguration. In diesem Beispiel werden ausschließlich SSH-Zugriffe auf das Subnetz "10.10.10.0 255.255.255.0" zugelassen. Alle anderen Zugriffsversuche werden abgelehnt.

```
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
```

**Hinweis:** Das gleiche Verfahren zum Sperren des SSH-Zugriffs gilt auch für Switch-Plattformen.

## Konfigurieren der SSH-Version

Konfigurieren von SSHv1:

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

Konfigurieren von SSHv2:

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

Konfigurieren von SSHv1 und SSHv2:

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

**Hinweis:** Sie erhalten diese Fehlermeldung, wenn Sie SSHv1 verwenden:

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

**Hinweis:** Cisco Bug ID CSCsu51740 (nur registrierte Kunden) wurde für dieses Problem abgelegt. Konfigurieren Sie SSHv2, um das Problem zu umgehen.

## Ausgabevariationen beim Befehl "banner"

Die Ausgabe des Befehls**banner variiert jeweils bei Telnet-Verbindungen und den verschiedenen**

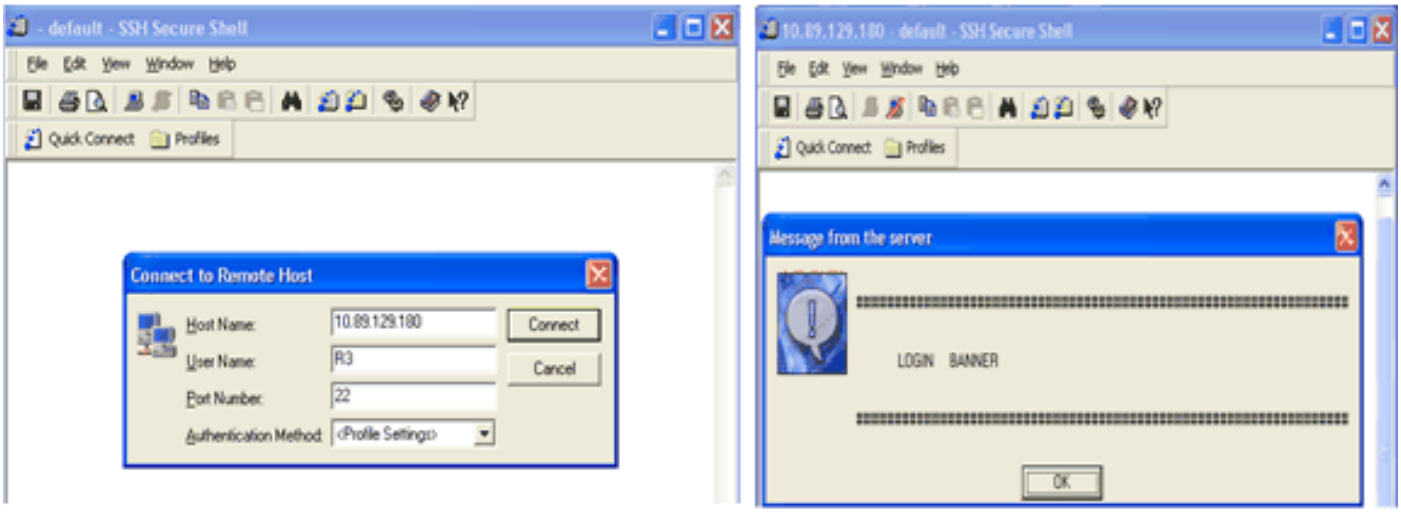
**Arten von SSH-Verbindungen.** In der Tabelle unten ist die Funktionsweise der Optionen des Befehls **banner bei Verwendung der einzelnen Verbindungstypen erläutert.**

| Option des Befehls "banner" | Telnet | Nur SSHv1 | SSHv1 und SSHv2 | Nur SSHv2 |
|---|---|---|---|---|
| banner login | Wird vor der Anmeldung beim Gerät angezeigt. | Wird nicht angezeigt. | Wird vor der Anmeldung beim Gerät angezeigt. | Wird vor der Anmeldung beim Gerät angezeigt. |
| banner motd | Wird vor der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. |
| banner exec | Wird nach der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. | Wird nach der Anmeldung beim Gerät angezeigt. |

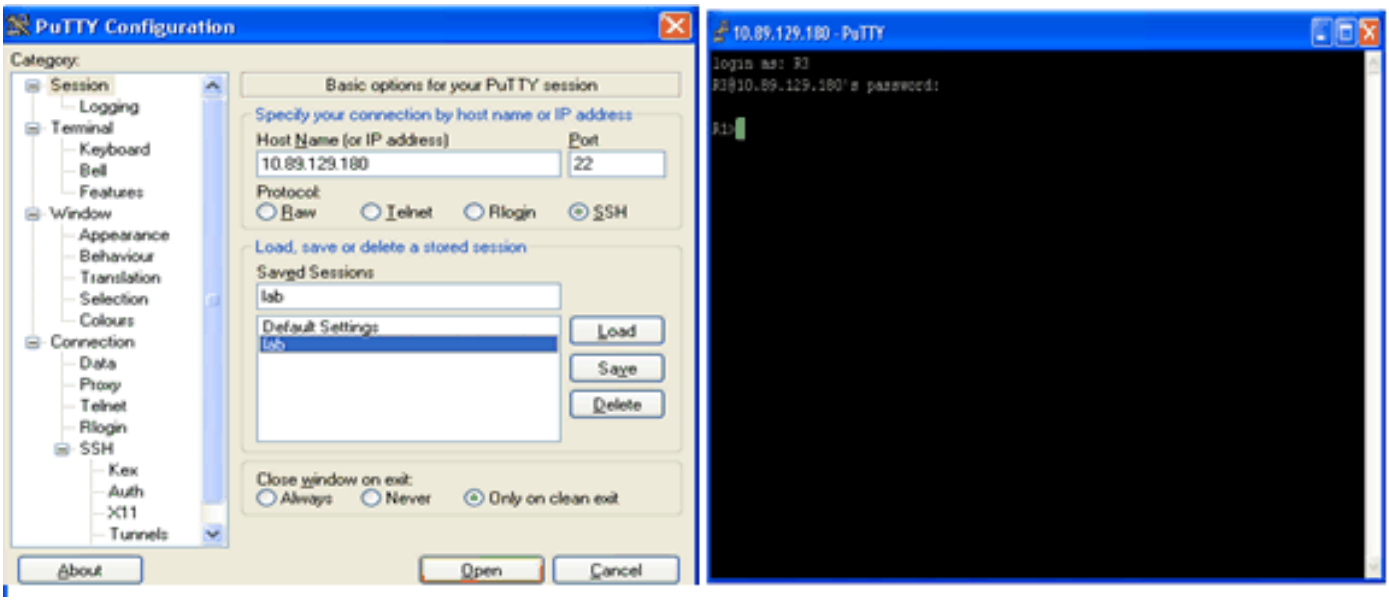
## Anmeldebanner kann nicht angezeigt werden

SSHv2 unterstützt das Anmeldebanner. Das Anmeldebanner wird angezeigt, sobald der SSH-Client bei der Initiierung der SSH-Sitzung mit dem Cisco Router den Benutzernamen sendet. Beispielsweise wird das Anmeldebanner angezeigt, wenn der Secure Shell-SSH-Client verwendet wird. Wird der PuTTY-SSH-Client verwendet, wird das Anmeldebanner nicht angezeigt. Dies liegt daran, dass Secure Shell den Benutzernamen standardmäßig sendet, PuTTY jedoch nicht.

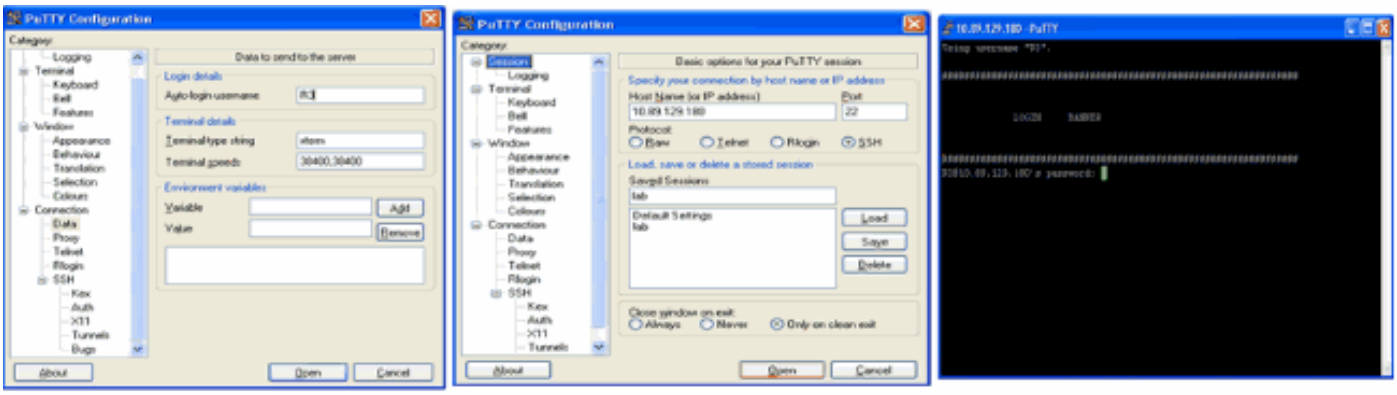
Der Secure Shell-Client benötigt den Benutzernamen, um die Verbindung zum SSH-fähigen Gerät zu initiieren. Die Schaltfläche "Connect" wird erst aktiviert, wenn Sie den Host-Namen und den Benutzernamen eingeben. Im Screenshot unten sehen Sie das Anmeldebanner, das angezeigt wird, wenn sich Secure Shell mit dem Router verbindet. Anschließend wird im Anmeldebanner die Aufforderung zur Kennworteingabe angezeigt.




Der PuTTY-Client benötigt keinen Benutzernamen, um die SSH-Verbindung zum Router zu initiieren. Im Screenshot unten sehen Sie, wie sich der PuTTY-Client mit dem Router verbindet und zur Eingabe des Benutzernamens und des Kennworts auffordert. Das Anmeldebanner wird nicht angezeigt.




Im Screenshot unten sehen Sie, dass das Anmeldebanner angezeigt wird, wenn PuTTY so konfiguriert ist, dass der Benutzername an den Router gesendet wird.



Category → Connection → Data

## Befehle "debug" und "show"

Lesen Sie sich das Dokument Important Information on Debug Commands (Wichtige Informationen zu Debug-Befehlen) durch, bevor Sie die hier beschriebenen Befehle des Typs **debug ausführen.** Einige Befehle des Typs **show werden vom Tool** Output Interpreter unterstützt (nur für registrierte Kunden), mit dem sich Analysen der Ausgabe von Befehlen des Typs **show abrufen lassen.**

**debug ip ssh: Zeigt Fehlersuchemeldungen für SSH an.**

**show ssh: Zeigt den Status von SSH-Serververbindungen an.**

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

**show ip ssh: Zeigt Versions- und Konfigurationsdaten zu SSH an.**

**v1-Verbindungen, aber keine v2-Verbindungen**

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

**v2-Verbindungen, aber keine v1-Verbindungen**

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

**v1-Verbindungen und v2-Verbindungen**

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

# Beispielausgabe einer Fehlersuche

## Router-Fehlersuche

**Hinweis:** Ein Teil dieser guten Debugausgabe wird aus räumlichen Gründen in mehrere Zeilen eingeschlossen.

```
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_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
```

## Server-Fehlersuche

**Hinweis:** Diese Ausgabe wurde auf einem Solaris-Computer erfasst.

```
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.
```

# Mögliche Probleme

In diesen Abschnitten finden Sie Beispielausgaben der Fehlersuche bei verschiedenen fehlerhaften Konfigurationen.

## SSH-Datenverkehr vom SSH-Client wird nicht mit DES (Data Encryption Standard) kompiliert

### Solaris-Fehlersuche

```
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-Fehlersuche

```
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
```

## Ungültiges Kennwort

### Router-Fehlersuche

```
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_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-Client sendet nicht unterstützte Chiffre (Blowfish)

#### Router-Fehlersuche

```
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_SMSG_PUBLIC_KEY msg
00:39:26: SSH0: SSH_CMSG_SESSION_KEY msg - length 112, type 0x03
00:39:26: SSH0: Session disconnected - error 0x20
```

### Fehler "%SSH-3-PRIVATEKEY: Unable to retrieve RSA private key for"

Wenn diese Fehlermeldung angezeigt wird, wurden möglicherweise der Domänenname oder der Host-Name geändert. Versuchen Sie die nachfolgend beschriebenen Problemumgehungen, um den Fehler zu beheben.

Nullen Sie die RSA-Schlüssel, und generieren Sie die Schlüssel neu.

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

Falls die oben genannte Problemumgehung nicht funktioniert, versuchen Sie Folgendes:

Nullen Sie alle RSA-Schlüssel.

Laden Sie das Gerät neu.

Erstellen Sie neue benannte Schlüssel für SSH.

Dieses Verhalten wurde als Cisco Bug CSCsa83601 gemeldet (nur für registrierte Kunden).

## Tipps zur Fehlerbehebung

Werden Ihre SSH-Konfigurationsbefehle als ungültige Befehle zurückgewiesen, wurde das RSA-Schlüsselpaar für den Router nicht korrekt generiert. Stellen Sie sicher, dass Sie einen Host-Namen und eine Domäne angegeben haben. Führen Sie dann den Befehl **crypto key generate rsa aus, um ein RSA-Schlüsselpaar zu generieren und den SSH-Server zu aktivieren.**

Bei der Konfiguration des RSA-Schlüsselpaars werden möglicherweise folgende Fehlermeldungen angezeigt:

```
No hostname specified
```

Sie müssen mit dem globalen Konfigurationsbefehl **hostname einen Host-Namen für den Router konfigurieren.**

```
No domain specified
```

Sie müssen mit dem globalen Konfigurationsbefehl **ip domain-name eine Host-Domäne für den Router konfigurieren.**

Die zulässige Anzahl von SSH-Verbindungen ist auf die für den Router konfigurierte maximale Zahl von virtuellen Terminals (VTYs) beschränkt. Jede SSH-Verbindung verwendet jeweils eine VTY-Ressource.

SSH verwendet zur Benutzerauthentifizierung entweder das lokale Sicherheitsprotokoll oder das Sicherheitsprotokoll, das per AAA auf dem Router konfiguriert wurde. Wenn Sie AAA konfigurieren, müssen Sie sicherstellen, dass die Konsole nicht unter AAA ausgeführt wird. Dazu müssen Sie AAA im globalen Konfigurationsmodus mithilfe eines Keyword auf der Konsole deaktivieren.

```
Es sind keinerlei SSH-Serververbindungen aktiv.
```

```
carter#show ssh

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

Diese Ausgabe deutet darauf hin, dass der SSH-Server deaktiviert ist oder nicht korrekt aktiviert wurde. Falls Sie SSH bereits konfiguriert haben, empfiehlt sich eine Neukonfiguration des SSH-Servers auf dem Gerät. Gehen Sie wie folgt vor, um den SSH-Server auf dem Gerät neu zu konfigurieren:

Löschen Sie das RSA-Schlüsselpaar. Nachdem das RSA-Schlüsselpaar gelöscht wurde, wird der SSH-Server automatisch deaktiviert.

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

**Hinweis:** Beim Aktivieren von SSH v2 ist es wichtig, ein Schlüsselpaar mit einer Bit-Größe von mindestens 768 zu generieren.

**Achtung:** Dieser Befehl kann nicht rückgängig gemacht werden, nachdem Sie die Konfiguration gespeichert haben und nachdem die RSA-Schlüssel gelöscht wurden, Sie können Zertifikate oder die CA nicht verwenden oder an Zertifikataustausch mit anderen IPSec-Peers (IP Security) teilnehmen, es sei denn, Sie konfigurieren die CA-Interoperabilität neu, indem Sie die RSA-Schlüssel neu generieren, das Zertifikat der CA

abrufen und erneut Ihr eigenes Zertifikat anfordern.Informationen finden Sie unter Verschlüsselungsschlüssel zerozerozeroisieren - Cisco IOS Security Command Reference, Weitere Informationen zu diesem Befehl finden Sie in Version 12.3.

Konfigurieren Sie den Host-Namen und den Domänennamen des Geräts neu.

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

Generieren Sie ein RSA-Schlüsselpaar für den Router. SSH wird dabei automatisch aktiviert.

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

Weitere Informationen zur Verwendung dieses Befehls finden Sie unter crypto key generate rsa - Cisco IOS Security Command Reference, Release 12.3.

**Hinweis:** Sie können `SSH2 0` erhalten: `Unexpected mesg type received angezeigt, weil der Router ein Paket empfangen hat, das er nicht entschlüsseln konnte.` Vergrößern Sie bei der Generierung der RSA-Schlüssel für SSH die Schlüssellänge, um dieses Problem zu beheben.

Konfigurieren Sie den SSH-Server. Wenn Sie SSH auf einem Cisco Router/Switch aktivieren und den Router/Switch als SSH-Server konfigurieren möchten, können Sie SSH-Parameter konfigurieren. Wenn Sie keine SSH-Parameter konfigurieren, werden die Standardwerte verwendet.

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

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

Weitere Informationen zur Verwendung dieses Befehls finden Sie unter ip ssh - Cisco IOS Security Command Reference, Release 12.3.

# Zugehörige Informationen

- How to Configure SSH on Catalyst Switches Running CatOS
- Secure Shell Version 2 Support
- Produkt-Support-Seite zu SSH
- Technischer Support und Dokumentation für Cisco Systeme