

# 라우터 및 스위치에서 SSH 설정

## 목차

---

[소개](#)

[사전 요구 사항](#)

[요구 사항](#)

[사용되는 구성 요소](#)

[표기규칙](#)

[SSH v2 네트워크 다이어그램](#)

[인증 테스트](#)

[SSH를 사용하지 않은 인증 테스트](#)

[SSH를 사용한 인증 테스트](#)

[선택적 설정 세트](#)

[비 SSH 연결 방지](#)

[IOS 라우터 또는 스위치를 SSH 클라이언트로 설정](#)

[RSA 기반 사용자 인증을 수행하는 SSH 서버로 IOS 라우터 설정](#)

[SSH 터미널-라인 액세스 추가](#)

[서브넷으로 SSH 액세스 제한](#)

[SSH 버전 2 설정](#)

[banner 명령 출력에 대한 변형](#)

[Banner 명령 옵션](#)

[Telnet](#)

[SSH v2](#)

[로그인 배너를 표시할 수 없음](#)

[debug 및 show 명령](#)

[디버그 출력 샘플](#)

[라우터 디버그](#)

[서버 디버그](#)

[잘못된 설정](#)

[SSH 클라이언트의 SSH가 DES\(Data Encryption Standard\)로 컴파일되지 않음](#)

[잘못된 암호](#)

[라우터 디버그](#)

[SSH 클라이언트가 지원되지 않는 \(Blowfish\) 암호 전송](#)

[라우터 디버그](#)

["%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for" 오류](#)

[팁](#)

[관련 정보](#)

---

## 소개

이 문서에서는 Cisco IOS ® Software를 실행하는 Cisco 라우터 또는 스위치에서 SSH(Secure

Shell)를 설정 및 디버그하는 방법에 대해 설명합니다.

## 사전 요구 사항

### 요구 사항

SSH를 지원하려면 사용된 Cisco IOS 이미지가 k9(암호화) 이미지여야 합니다. 예를 들어 c3750e-universalk9-tar.122-35.SE5.tar은 k9(crypto) 이미지가 있습니다.

### 사용되는 구성 요소

이 문서의 정보는 Cisco IOS 3600 Software(C3640-IK9S-M), 릴리스 12.2(2)T1을 기준으로 합니다.

SSH는 다음 Cisco IOS 플랫폼 및 이미지에 도입되었습니다.

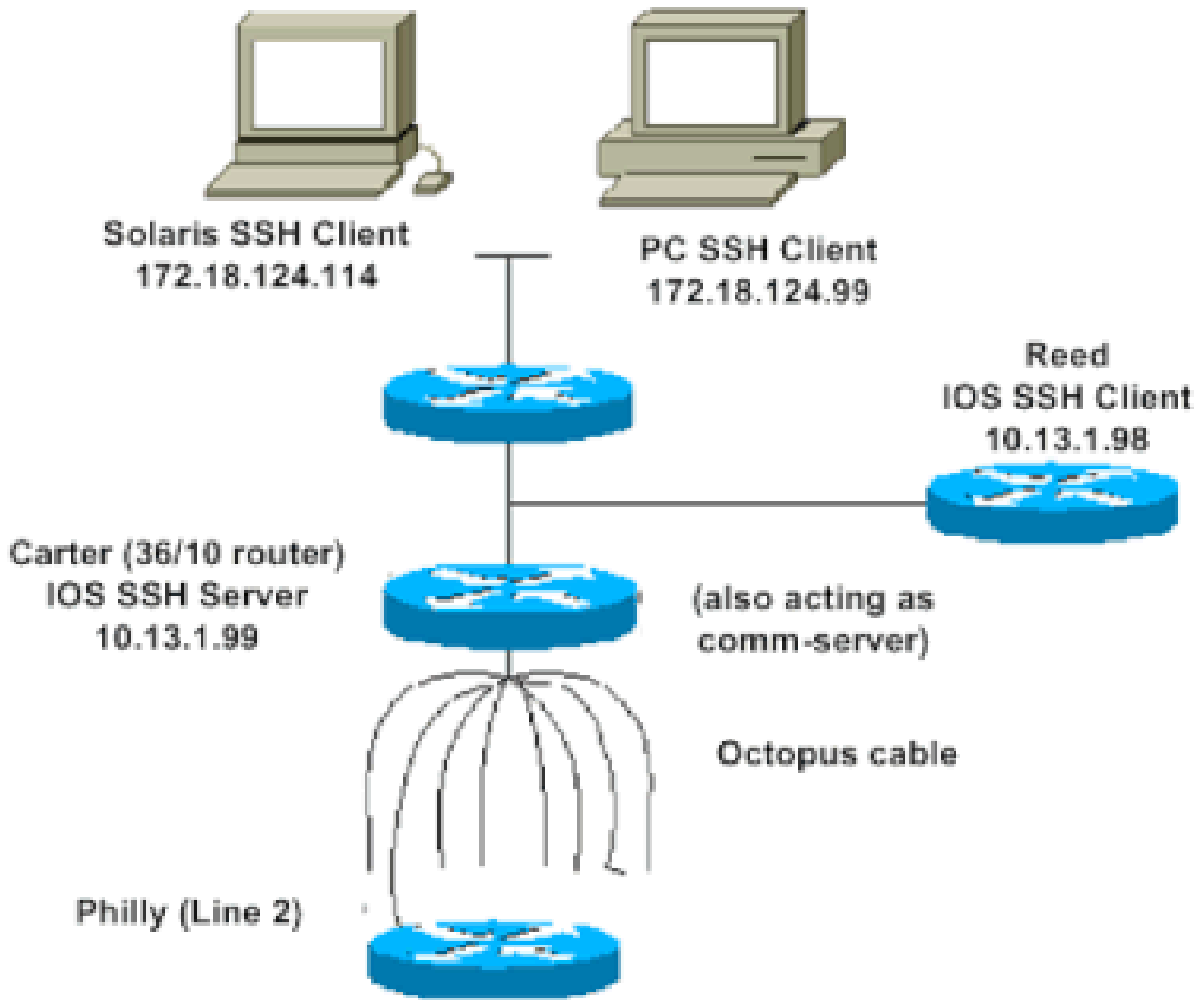
- SSH 터미널-라인 액세스(역방향 Telnet이라고도 함)는 Cisco IOS 소프트웨어 릴리스 12.2.2.T에서 시작하는 Cisco IOS 플랫폼 및 이미지에 도입되었습니다.
- SSH 버전 2.0(SSH v2) 지원은 Cisco IOS 소프트웨어 릴리스 12.1(19)E에서 시작하는 Cisco IOS 플랫폼 및 이미지에서 도입되었습니다.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 현재 네트워크가 작동 중인 경우 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

### 표기 규칙

자세한 내용은 [Cisco 기술 팁 표기 규칙](#)을 참조하십시오.

## SSH v2 네트워크 다이어그램



## 인증 테스트

### SSH를 사용하지 않은 인증 테스트

SSH를 추가하기 전에 라우터 Carter에서 인증이 작동하는지 확인하기 위해 먼저 SSH를 사용하지 않고 인증을 테스트합니다. 인증은 로컬 사용자 이름 및 비밀번호 또는 TACACS+나 RADIUS를 실행하는 AAA(Authentication, Authorization, and Accounting) 서버를 사용하여 수행할 수 있습니다. (SSH를 사용하는 경우 라인 비밀번호를 통한 인증은 사용할 수 없습니다.) 이 예에서는 사용자 이름 cisco와 비밀번호 cisco를 사용하여 Telnet을 통해 라우터에 연결하는 로컬 인증을 보여줍니다.

 참고: 이 문서 전체에서 vty는 가상 터미널 유형을 나타내는 데 사용됩니다.

!--- 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.

## SSH를 사용한 인증 테스트

SSH를 사용하여 인증을 테스트하려면 Carter에서 SSH를 활성화하고 PC 및 UNIX 스테이션에서 SSH를 테스트할 수 있도록 이전 명령문에 추가해야 합니다.

```
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
```

이 시점에서 `show crypto key mypubkey rsa` 명령은 생성된 키를 표시해야 합니다. SSH 컨피그레이션을 추가한 후 PC 및 UNIX 스테이션에서 라우터에 액세스하는 기능을 테스트합니다.

## 선택적 설정 세트

### 비 SSH 연결 방지

비 SSH 연결을 방지하려면 라인 아래에 `transport input ssh` 명령을 추가하여 라우터를 SSH 연결 전용으로 제한합니다. 직접(비 SSH) Telnet은 거부됩니다.

```
line vty 0 4
```

!--- Prevent non-SSH Telnets.

```
transport input ssh
```

비 SSH 사용자가 라우터 Carter에 Telnet을 통해 연결할 수 있는지 테스트합니다.

### IOS 라우터 또는 스위치를 SSH 클라이언트로 설정

Cisco IOS 라우터에서 SSH 지원을 활성화하려면 다음 4단계를 수행해야 합니다.

1. `hostname` 명령을 구성합니다.
2. DNS 도메인을 구성합니다.
3. SSH 키를 생성합니다.

4. vty에 대해 SSH 전송 지원을 활성화합니다.

디바이스 하나가 다른 디바이스의 SSH 클라이언트로 작동하도록 하려는 경우 Reed라는 두 번째 디바이스에 SSH를 추가할 수 있습니다. 그러면 이러한 디바이스가 서버-클라이언트 배열이 되고 Carter는 서버로, Reed는 클라이언트로 작동합니다. Reed의 Cisco IOS SSH 클라이언트 컨피그레이션은 Carter의 SSH 서버 컨피그레이션과 동일합니다.

!--- 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.

이를 테스트하기 위해 Cisco IOS SSH 클라이언트(Reed)에서 Cisco IOS SSH 서버(Carter)로 SSH에 대한 다음 명령을 실행합니다.

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

## RSA 기반 사용자 인증을 수행하는 SSH 서버로 IOS 라우터 설정

RSA 기반 인증을 수행하도록 SSH 서버를 설정하려면 다음 단계를 수행하십시오.

1. 호스트 이름을 지정합니다.

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

2. 기본 도메인 이름을 정의합니다.

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

3. RSA 키 쌍을 생성합니다.

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

4. 사용자 및 서버 인증을 위해 SSH-RSA 키를 구성합니다.

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

5. SSH 사용자 이름을 구성합니다.

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

6. 원격 사용자의 RSA 공개 키를 지정합니다.

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

7. SSH 키 유형 및 버전을 지정합니다. (이 단계는 선택 사항입니다.)

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

8. 현재 모드를 종료하고 권한 EXEC 모드로 돌아갑니다.

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

## SSH 터미널-라인 액세스 추가

아웃바운드 SSH 터미널-라인 인증이 필요한 경우, Philly에 대한 통신 서버 역할을 하는 Carter를 통해 아웃바운드 역방향 Telnet에 대한 SSH를 구성 및 테스트할 수 있습니다.

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

Philly가 Carter 포트 2에 연결된 경우 다음 명령을 사용하여 Reed에서 Carter를 통해 Philly에 대한 SSH를 설정할 수 있습니다.

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

다음 명령을 Solaris에서 사용할 수 있습니다.

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

## 서브넷으로 SSH 액세스 제한

SSH 연결성을 특정 하위 네트워크로 제한해야 합니다. 이 경우, 해당 하위 네트워크를 벗어난 IP에 서의 다른 모든 SSH 시도는 차단됩니다.


다음 단계를 수행하여 동일한 작업을 수행할 수 있습니다.

1. 특정 하위 네트워크의 트래픽을 허용하는 액세스 목록을 정의합니다.

2. `access-class`를 사용하여 VTY 라인 인터페이스로 액세스를 제한합니다.

다음은 컨피그레이션을 보여주는 예입니다. 이 예시에서는 10.10.10.0 255.255.255.0 서브넷에 대한 SSH 액세스만 허용되며, 다른 모든 액세스는 거부됩니다.

```
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
```

 참고: SSH 액세스를 잠그는 동일한 절차가 스위치 플랫폼에도 사용됩니다.


## SSH 버전 2 설정

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

## banner 명령 출력에 대한 변형

banner 명령 출력은 Telnet과 여러 버전의 SSH 연결에 따라 달라집니다. 다음 표에서는 여러 banner 명령 옵션이 다양한 유형의 연결과 작동하는 방식을 보여줍니다.

Banner 명령 옵션	Telnet	SSH v2
배너 로그	디바이스에 로그인하기 전에 표시됩니다.	디바이스에 로그인하기 전에 표시됩니다.
banner motd	디바이스에 로그인하기 전에 표시됩니다.	디바이스에 로그인한 후 표시됩니다.
banner exec	디바이스에 로그인한 후 표시됩니다.	디바이스에 로그인한 후 표시됩니다.

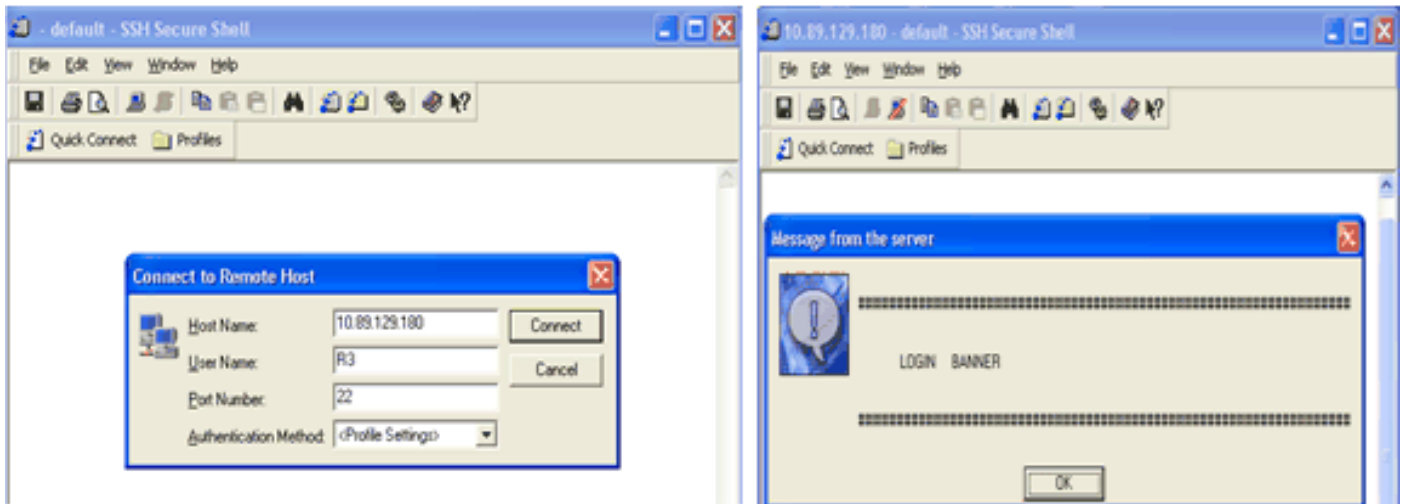
 참고: SSH 버전 1은 더 이상 권장되지 않습니다.

## 로그인 배너를 표시할 수 없음



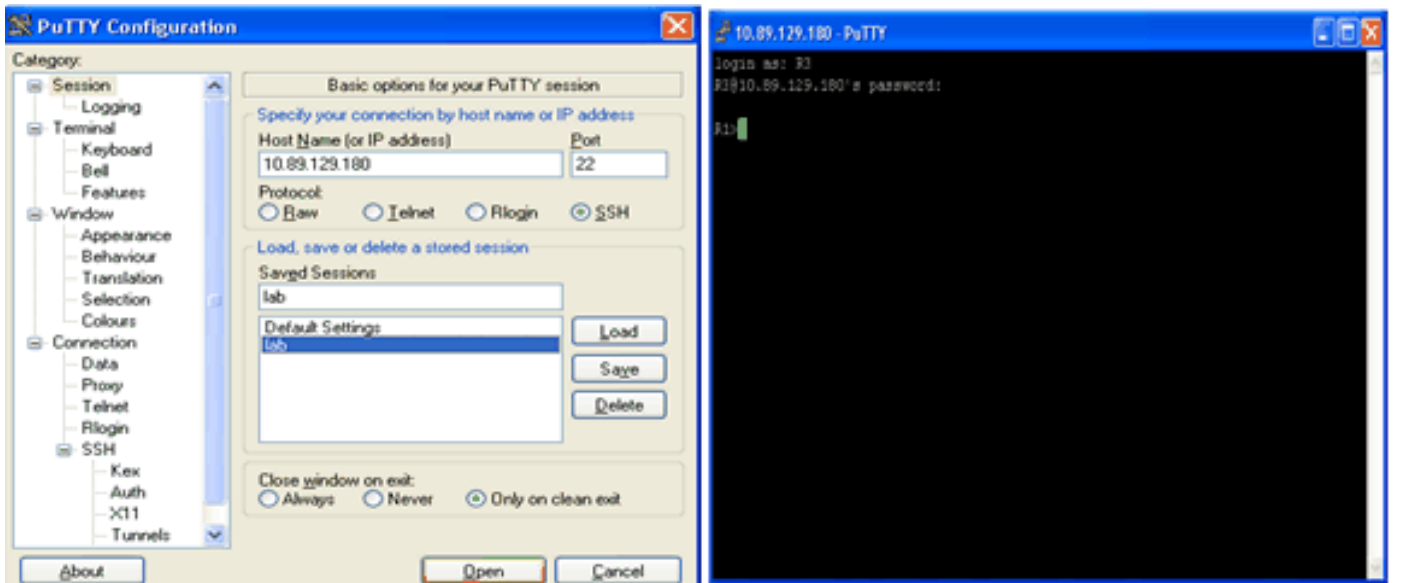
SSH 버전 2는 로그인 배너를 지원합니다. Cisco 라우터를 사용하여 SSH 세션을 시작할 때 SSH 클라이언트가 사용자 이름을 전송하는 경우 로그인 배너가 표시됩니다. 예를 들어, Secure Shell ssh 클라이언트를 사용하는 경우 로그인 배너가 표시됩니다. PuTTY ssh 클라이언트를 사용하는 경우 로그인 배너가 표시되지 않습니다. 이는 SSH가 기본적으로 사용자 이름을 전송하고 PuTTY는 기본적으로 사용자 이름을 전송하지 않기 때문입니다.

SSH 지원 디바이스에 대한 연결을 시작하려면 SSH 클라이언트에는 사용자 이름이 필요합니다. 호스트 이름과 사용자 이름을 입력하지 않으면 Connect(연결) 버튼이 활성화되지 않습니다. 이 화면 이미지는 SSH가 라우터에 연결될 때 로그인 배너가 표시됨을 보여줍니다. 그러면 배너에 비밀번호를 입력하라는 메시지가 표시됩니다.



배너의 비밀번호 프롬프트

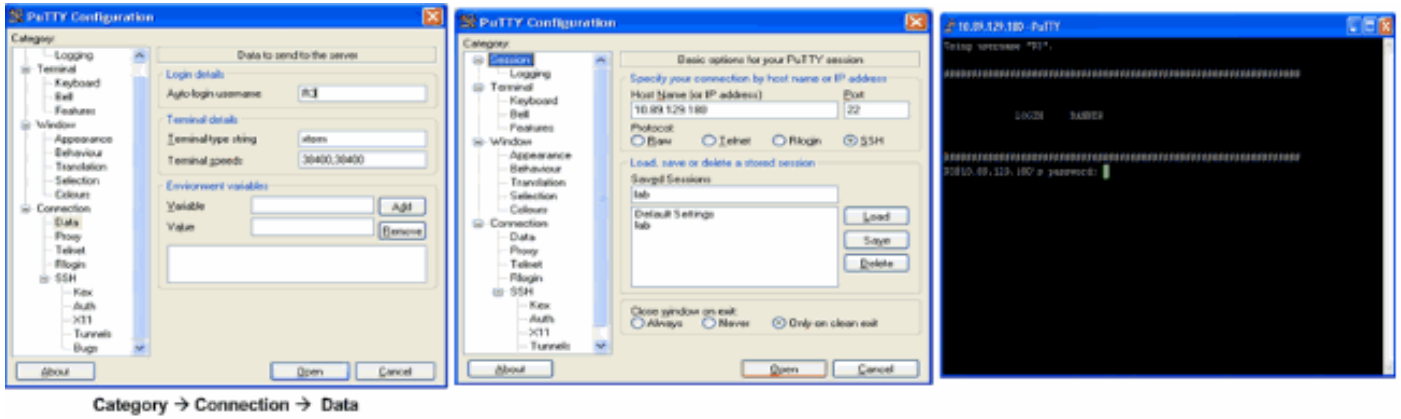
PuTTY 클라이언트는 사용자 이름이 없어도 해당 라우터에 대한 SSH 연결을 시작할 수 있습니다. 이 화면 이미지는 PuTTY 클라이언트가 라우터에 연결되고 사용자 이름과 암호를 입력하라는 메시지가 표시됨을 보여줍니다. 로그인 배너는 표시되지 않습니다.



라우터에 대한 SSH 연결

이 스크린샷은 PuTTY가 라우터로 사용자 이름을 전송하도록 설정된 경우 로그인 배너가 표시됨을

보여줍니다.



라우터로 사용자 이름 전송

## debug 및 show 명령

여기서 설명하는 debug 명령을 실행하기 전에 [Debug 명령에 대한 중요한 정보](#)를 참조하십시오. 일부 show 명령은 [출력 해석기 툴](#)에서 지원되는데(등록된 고객만), 이 툴을 사용하면 show 명령 출력의 분석 결과를 볼 수 있습니다.

- debug ip ssh는 SSH의 디버그 메시지를 표시합니다.
- show ssh는 SSH 서버 연결의 상태를 표시합니다.

```
carter#show ssh
Connection      Version Encryption      State                Username
0                2.0      DES                Session started     cisco
```

- show ip ssh는 SSH에 대한 버전 및 설정 데이터를 표시합니다.

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

## 디버그 출력 샘플

### 라우터 디버그

```
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
```

## 서버 디버그

---

 참고: 다음은 Solaris 시스템 출력입니다.

---

```
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.
```

## 잘못된 설정

다음 섹션에는 여러 가지 잘못된 컨피그레이션의 디버그 출력 샘플이 나와 있습니다.

SSH 클라이언트의 SSH가 DES(Data Encryption Standard)로 컴파일되지 않음

### 잘못된 암호

#### 라우터 디버그

```
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_MSG_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 클라이언트가 지원되지 않는 (Blowfish) 암호 전송

#### 라우터 디버그

```
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
```

"%SSH-3-PRIVATEKEY: Unable to Retrieve RSA Private Key for" 오류

도메인 이름 또는 호스트 이름이 변경되면 이 오류 메시지가 트리거될 수 있습니다. 다음 해결 방법을 사용하십시오.

- RSA 키를 0으로 만들고 다시 생성합니다.

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

- 이전 해결 방법으로 문제가 해결되지 않으면 다음 단계를 시도해 보십시오.
  1. 모든 RSA 키를 0으로 만듭니다.
  2. 디바이스를 다시 로드합니다.
  3. SSH용으로 레이블이 지정된 새 키를 생성합니다.

## 팁

- SSH 컨피그레이션 명령이 잘못된 명령으로 거부된 경우 라우터에 대한 RSA 키 쌍을 생성하지 못합니다. 호스트 이름과 도메인을 지정했는지 확인합니다. 그런 다음 `crypto key generate rsa` 명령을 사용하여 RSA 키 쌍을 생성하고 SSH 서버를 활성화합니다.
- RSA 키 쌍을 설정할 때 이러한 오류 메시지가 표시될 수 있습니다.

1. 호스트 이름이 지정되지 않았습니다.

`hostname` 전역 설정 명령을 사용하여 라우터의 호스트 이름을 설정해야 합니다.

2. 도메인이 지정되지 않았습니다.

`ip domain-name` 전역 설정 명령을 사용하여 라우터의 호스트 도메인을 설정해야 합니다.

- 허용 가능한 SSH 연결 수는 라우터에 대해 구성된 최대 `vty` 수로 제한됩니다. 각 SSH 연결에서는 리소스를 `vty` 사용합니다.
- SSH는 사용자 인증을 위해 라우터에서 AAA를 통해 설정된 보안 프로토콜 또는 로컬 보안을 사용합니다. AAA를 설정할 때는 콘솔이 AAA에서 실행되지 않아야 합니다. 전역 설정 모드에서 키워드를 적용하여 콘솔에서 AAA를 비활성화합니다.
- No SSH server connections running:

```
carter#show ssh
```

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


이 출력은 SSH 서버가 비활성화되었거나 올바르게 활성화되지 않았음을 나타냅니다. 이미 SSH를

구성한 경우에는 디바이스에서 SSH 서버를 재구성하는 것이 좋습니다. 디바이스에서 SSH 서버를 재설정하려면 다음 단계를 수행하십시오.


1. RSA 키 쌍을 삭제합니다. RSA 키 쌍이 삭제되면 SSH 서버가 자동으로 비활성화됩니다.

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

---

 참고: SSH v2를 활성화하는 경우 비트 크기가 768 이상인 키 쌍을 생성해야 합니다.

---

 주의: 설정을 저장한 후에는 이 명령을 취소할 수 없습니다. RSA 키가 삭제된 후에는 RSA 키를 재생성하여 CA 상호 운용성을 재설정하고, CA 인증서를 가져오고, 자체 인증서를 다시 요청하지 않는 한 인증서 또는 CA를 사용하거나 다른 IP 보안(IPSec) 피어와의 인증서 교환에 참여할 수 없습니다.

---

2. 디바이스의 호스트 이름과 도메인 이름을 다시 구성합니다.


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

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


3. 라우터에 대한 RSA 키 쌍을 생성합니다. 이렇게 하면 SSH가 자동으로 활성화됩니다.

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

---

 참고: 이 명령의 사용법에 대한 자세한 내용은 [crypto key generate rsa - Cisco IOS Security 명령 참조, 릴리스 12.3](#)을 참조하십시오.

---

 참고: 라우터가 이해할 수 없는 패킷이 수신되어 SSH2 0: Unexpected mesg type received 오류 메시지가 표시될 수 있습니다. 이 문제를 해결하려면 ssh에 대한 rsa 키를 생성하는 동안 키 길이를 늘리십시오.

---

4. SSH 서버를 설정합니다.

5. SSH 서버에 대해 Cisco 라우터/스위치를 활성화 및 설정하려면 SSH 매개변수를 설정해야 합니다. SSH 매개 변수를 구성하지 않으면 기본값이 사용됩니다.

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

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

## 관련 정보

- [SSH 제품 지원 페이지](#)

이 번역에 관하여

Cisco는 전 세계 사용자에게 다양한 언어로 지원 콘텐츠를 제공하기 위해 기계 번역 기술과 수작업 번역을 병행하여 이 문서를 번역했습니다. 아무리 품질이 높은 기계 번역이라도 전문 번역가의 번역 결과물만큼 정확하지는 않습니다. Cisco Systems, Inc.는 이 같은 번역에 대해 어떠한 책임도 지지 않으며 항상 원본 영문 문서(링크 제공됨)를 참조할 것을 권장합니다.