CatOS를 실행하는 Catalyst 스위치에서 SSH를 구성하는 방법

목차

[소개](#)
[사전 요구 사항](#)
[요구 사항](#)
[사용되는 구성 요소](#)
[표기 규칙](#)
[네트워크 다이어그램](#)
[스위치 구성](#)
[SSH 비활성화](#)
[Catalyst에서 디버그](#)
[정상 연결의 디버그 명령 예](#)
[Solaris에서 Catalyst로, 3DES(Triple Data Encryption Standard), 텔넷 비밀번호](#)
[PC to Catalyst, 3DES, 텔넷 비밀번호](#)
[Solaris에서 Catalyst, 3DES, 인증, 권한 부여 및 계정 관리(AAA) 인증으로](#)
[debug 명령의 오류 발생 예](#)
[클라이언트가 [지원되지 않음] Blowfish 암호를 시도하는 Catalyst 디버그](#)
[텔넷 비밀번호가 잘못된 Catalyst 디버그](#)
[Catalyst 디버그(잘못된 AAA 인증 사용)](#)
[문제 해결](#)
[SSH를 통해 스위치에 연결할 수 없음](#)
[관련 정보](#)

소개

이 문서에서는 Catalyst OS(CatOS)를 실행하는 Catalyst 스위치에서 SSH(Secure Shell) 버전 1을 구성하는 단계별 지침을 제공합니다. 테스트된 버전은 cat6000-**supk9**.6-1-1c.bin입니다.

사전 요구 사항

요구 사항

이 표에서는 스위치에서 SSH 지원 상태를 보여줍니다. 등록된 사용자는 Software Center를 방문하여 이러한 소프트웨어 이미지에 액세스할 [수 있습니다](#).

CatOS SSH	
디바이스	**SSH 지원**
Cat 4000/4500/2948G/2980G(CatOS)	6.1 기준 K9 이

	미지
Cat 5000/5500(CatOS)	6.1 기준 K9 이미지
Cat 6000/6500(CatOS)	6.1 기준 K9 이미지
IOS SSH	
디바이스	**SSH 지원**
Cat 2950*	12.1(12c)EA1 이상
Cat 3550*	12.1(11)EA1 이상
Cat 4000/4500(통합 Cisco IOS 소프트웨어)*	12.1(13)EW 이상 **
Cat 6000/5500(통합 Cisco IOS 소프트웨어)*	12.1(11b)E 이상
Cat 8540/8510	12.1(12c)EY 이상, 12.1(14)E1 이상
SSH 없음	
디바이스	**SSH 지원**
고양이 1900	아니요
고양이 2800	아니요
Cat 2948G-L3	아니요
Cat 2900XL	아니요
Cat 3500XL	아니요
Cat 4840G-L3	아니요
Cat 4908G-L3	아니요

* 컨피그레이션은 Cisco IOS를 실행하는 라우터 및 스위치에서 Secure Shell 구성에 대해 설명합니다.

** Integrated Cisco IOS Software를 실행하는 Catalyst 4000용 12.1E Train에서는 SSH를 지원하지 않습니다.

3DES를 신청하려면 암호화 소프트웨어 내보내기 배포 권한 부여 양식을 참조하십시오.

이 문서에서는 SSH(텔넷 비밀번호, TACACS+ 사용) 또는 RADIUS를 구현하기 전에 인증이 작동한다고 가정합니다. SSH를 구현하기 전에는 Kerberos를 사용하는 SSH가 지원되지 않습니다.

사용되는 구성 요소

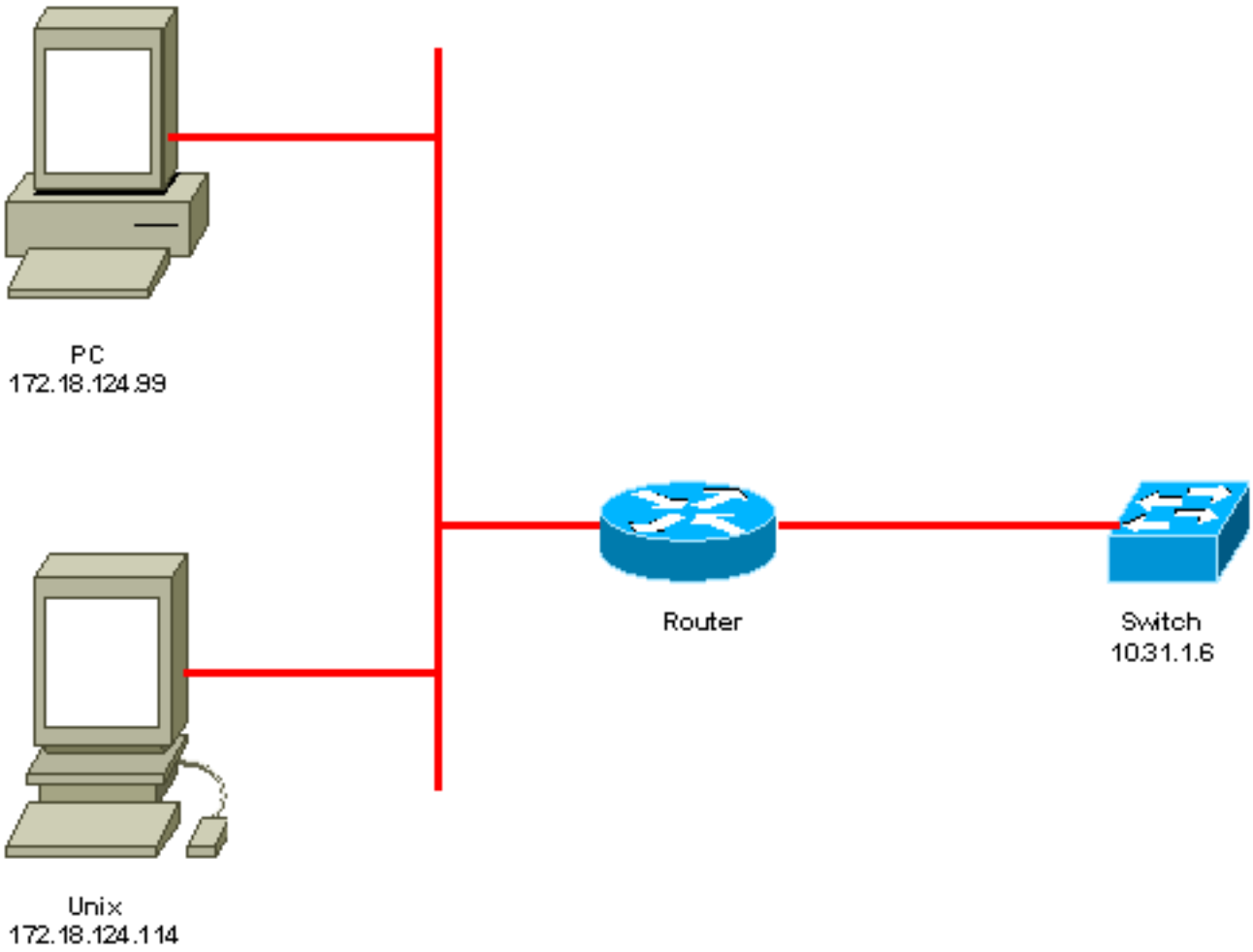
이 문서에서는 CatOS K9 이미지를 실행하는 Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500 Series, Catalyst 5000/5500 Series 및 Catalyst 6000/6500 Series에 대해서만 다룹니다. 자세한 내용은 이 문서의 요구 사항 섹션을 참조하십시오.

이 문서의 정보는 특정 랩 환경의 디바이스를 토대로 작성되었습니다. 이 문서에 사용된 모든 디바이스는 초기화된(기본) 컨피그레이션으로 시작되었습니다. 라이브 네트워크에서 작업 중인 경우, 사용하기 전에 모든 명령의 잠재적인 영향을 미리 숙지하시기 바랍니다.

표기 규칙

문서 규칙에 대한 자세한 내용은 Cisco 기술 팁 표기 규칙을 참조하십시오.

네트워크 다이어그램



스위치 구성

```
!--- 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
199668201930132947097826805906337821547938540549819306165 1
!--- 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
----------------- ------------------ ------
```

SSH 비활성화

경우에 따라 스위치에서 SSH를 비활성화해야 할 수 있습니다. SSH가 스위치에 구성되어 있는지 확인하고 구성된 경우 비활성화해야 합니다.

스위치에 SSH가 구성되었는지 확인하려면 show crypto **key 명령을** 실행합니다. 출력에 RSA 키가 표시되면 스위치에서 SSH가 구성되고 활성화된 것입니다. 여기에 예가 나와 있습니다.

```
sec-cat6000> (enable) show crypto key
RSA keys were generated at: Mon Jul 23 2001, 15:03:30 1024 65537 1514414695360
57733285367170478570985060663476874686971696394035244062067857533870155088525
69969147833053784006695698761020781095949864817996533001801084478586347277306 7
69718525641838624300188100883056124113738169282007867437605827557313344852933 2
19966820193013294709782680590633782154793854054981930616 51
```

암호화 키를 제거하려면 스위치에서 SSH를 **비활성화하려면 clear crypto key rsa** 명령을 실행합니다. 여기에 예가 나와 있습니다.

```
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)
```

Catalyst에서 디버그

디버그를 켜려면 set trace ssh **4 명령을** 실행합니다.

디버그를 끄려면 set trace ssh **0 명령을** 실행합니다.

정상 연결의 디버그 명령 예

Solaris에서 Catalyst로, 3DES(Triple Data Encryption Standard), 텔넷 비밀번호

솔라리스

```
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>
```

촉매

```
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, 텔넷 비밀번호

촉매

```
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.
```

Solaris에서 Catalyst, 3DES, 인증, 권한 부여 및 계정 관리(AAA) 인증으로

솔라리스

```
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.
abcde123@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>
```

촉매

```
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: abcde123
debug: Trying TACACS+ Login
Password authentication for abcde123 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 명령의 오류 발생 예

클라이언트가 [지원되지 않음] Blowfish 암호를 시도하는 Catalyst 디버그

```
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
```

텔넷 비밀번호가 잘못된 Catalyst 디버그

```
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 디버그(잘못된 AAA 인증 사용)

```
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
```

문제 해결

이 섹션에서는 Cisco 스위치의 SSH 컨피그레이션과 관련된 다양한 트러블슈팅 시나리오를 다룹니다.

SSH를 통해 스위치에 연결할 수 없음

문제/장애:

SSH를 사용하여 스위치에 연결할 수 없습니다.

debug **ip ssh 명령은** 다음 출력을 표시합니다.

```
Jun 15 20:29:26.207: SSH2 1: RSA_sign: private key not found
Jun 15 20:29:26.207: SSH2 1: signature creation failed, status -1
```

해결책:

이 문제는 다음 원인 중 하나로 인해 발생합니다.

- 호스트 이름을 변경한 후 새 SSH 연결이 실패합니다.
- 레이블이 지정되지 않은 키(라우터 FQDN 포함)로 구성된 SSH.

이 문제의 해결 방법은 다음과 같습니다.

- 호스트 이름이 변경되었고 SSH가 더 이상 작동하지 않는 경우 새 키를 0으로 만들고 적절한 레이블로 다른 새 키를 만듭니다.
  ```
  crypto key zeroize rsa
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```
- 익명 RSA 키(스위치의 FQDN에서 이름 지정)를 사용하지 마십시오. 대신 레이블이 지정된 키를 사용하십시오.
  ```
  crypto key generate rsa general-keys label (label) mod (modulus) [exportable]
  ```

이 문제를 영구적으로 해결하려면 IOS 소프트웨어를 이 문제가 해결된 버전으로 업그레이드하십시오.

이 문제에 대한 버그가 제출되었습니다. 자세한 내용은 Cisco 버그 ID CSCtc41114(**등록된 고객만 해당)를 참조하십시오**.

관련 정보

- SSH 지원 페이지
- Cisco IOS를 실행 중인 라우터 및 스위치에서 Secure Shell 구성
- 버그 툴킷
- Technical Support - Cisco Systems

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.