Настройка SSH на коммутаторах Catalyst с операционной системой CatOS

Содержание

Введение

Этот документ содержит пошаговые инструкции по настройке Secure Shell (SSH) версии 1 на коммутаторах Catalyst под управлением Catalyst OS (CatOS). **Тестировалась версия cat6000-supk9.6-1-1c.bin.**

Предварительные условия

Требования

Эта таблица показывает статус поддержки SSH в коммутаторах. Зарегистрированные пользователи могут обратиться к этим образам программного обеспечения путем посещения Центра программного обеспечения.

SSH CatOS	
Устройство	**Поддержка SSH**
CAT 4000/4500/2948G/2980G (CatOS)	K9 отображает с 6.1
CAT 5000/5500 (CatOS)	K9 отображает с 6.1
CAT 6000/6500 (CatOS)	K9 отображает с 6.1
SSH IOS	
Устройство	**Поддержка SSH**
CAT 2950*	12.1 (12c) EA1 и позже
Cat 3550*	12.1 (11) EA1 и позже
CAT 4000/4500 (программное обеспечение Интегрированного Cisco IOS) *	12.1 (13) EW и позже **
CAT 6000/5500 (программное обеспечение Интегрированного Cisco IOS) *	12.1 (11b) E и позже
CAT 8540/8510	12.1 (12c) EY и позже, 12.1 (14) E1 и позже
Никакой SSH	
Устройство	**Поддержка SSH**
CAT 1900	нет
CAT 2800	нет
2948G-L3 CAT	нет
CAT 2900XL	нет
CAT 3500XL	нет
4840G-L3 CAT	нет
4908G-L3 CAT	нет

* Конфигурация покрыта Configuring Secure Shell на маршрутизаторах и Коммутаторах Рабочая Cisco IOS.

** Поддержка SSH отсутствует в релизе 12.1E для Catalyst 4000 под управлением программного обеспечения интегрированной Cisco IOS.

См. Разрешение Распределения Экспорта Программного обеспечения для шифрования для просьбы 3DES.

В этом документе предполагается, что аутентификация производится до реализации SSH (через пароль Telnet, TACACS+) или RADIUS. SSH с Kerberos не поддерживается до реализации SSH.

Используемые компоненты

Этот документ обращается только к Catalyst 2948G, Catalyst 2980G, Catalyst 4000/4500 серия, серия Catalyst 5000/5500 и серия Catalyst 6000/6500, выполняющая образ K9 CatOS. Дополнительные сведения см. в разделе Требования данного документа.

Сведения, содержащиеся в данном документе, были получены с устройств в специальной лабораторной среде. Все устройства, описанные в данном документе, были запущены с конфигурацией по умолчанию. При работе с реальной сетью необходимо полностью осознавать возможные результаты использования всех команд.

Условные обозначения

Дополнительные сведения об условных обозначениях см. в документе Технические рекомендации Cisco. Условные обозначения.

Схема сети

Конфигурация коммутатора

```
!--- 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
----------------- ------------------ ------
```

Отключение SSH

В некоторых ситуациях может возникнуть необходимость в отключении SSH на коммутаторе. Необходимо проверить, настроен ли SSH на коммутаторе, и если да, отключить его.

Чтобы проверить, был ли SSH настроен на коммутаторе, введите команду show crypto key. Если выводится ключ RSA, SSH настроен и включен на коммутаторе. Пример выходных данных команды приводится ниже.

```
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
```

Чтобы удалить ключ шифрования, введите команду clear crypto key rsa для отключения SSH на коммутаторе. Пример выходных данных команды приводится ниже.

```
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)
```

отладка в Catalyst

Чтобы включить отладку, введите команду set trace ssh 4.

Чтобы выключить отладку, введите команду set trace ssh 0.

команда debug, примеры хорошего подключения

Solaris для Catalyst, стандарт тройного шифрования данных (3DES), пароль Telnet

Solaris

```
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>
```

Catalyst

```
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>
```

Пароль Telnet, 3DES, ПК к Catalyst

Catalyst

```
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>
```

Solaris до Catalyst, 3DES, аутентификация, авторизация и учет (AAA) аутентфикации

Solaris

```
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>
```

Catalyst

```
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>
```

примеры команды "debug" и возможные проблемы

Отладка Catalyst, когда клиент делает [неподдерживаемую] попытку шифрования по алгоритму Blowfish

```
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>
```

Отладка ускорителя процесса с неверным паролем протокола сети связи

```
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>
```

Отладка Catalyst с недействительной проверкой подлинности AAA

```
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>
```

Устранение неполадок

Этот раздел имеет дело с другими сценариями устранения проблем, отнесенными к конфигурации SSH на коммутаторах Cisco.

Не может соединиться с коммутатором через SSH

Проблема:

Не может соединиться с коммутатором с помощью SSH.

Команда **debug ip ssh** показывает эти выходные данные:

```
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>
```

Решение:

Эта проблема происходит из-за любой из этих причин:

- Новый сбой SSH - подключений после изменения имени хоста.
- SSH, настроенный с немаркированными ключами (имеющий маршрутизатор FQDN).

Обходные пути для этой проблемы:

- Если имя хоста было изменено, и SSH больше не работает, то обнулите новый ключ и создайте другой новый ключ с надлежащей меткой.`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>
```

- Не используйте анонимные ключи RSA (названный в честь FQDN коммутатора). Используйте маркированные ключи вместо этого.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>
```

Для решения этой проблемы навсегда, обновите программное обеспечение IOS к любой из версий, в которых решена эта проблема.

Дефект был подан об этой проблеме. Для получения дополнительной информации обратитесь к идентификатору ошибки Cisco CSCtc41114 (только зарегистрированные клиенты).

Дополнительные сведения

- Страница поддержки SSH
- Настройка протокола Secure Shell на маршрутизаторах и коммутаторах с программным обеспечением Cisco IOS
- Средство обнаружения ошибок
- Техническая поддержка - Cisco Systems