

Configuring Secure Shell

This chapter describes the Secure Shell (SSH) feature. The SSH feature consists of an application and a protocol.

For a complete description of the SSH commands in this chapter, refer to the chapter “Secure Shell Commands” of the *Cisco IOS Security Command Reference*. To locate documentation of other commands that appear in this chapter, use the command reference master index or search online.

To identify the hardware platform or software image information associated with a feature, use the Feature Navigator on Cisco.com to search for information about the feature or refer to the software release notes for a specific release. For more information, see the “Identifying Supported Platforms” section in the chapter “Using Cisco IOS Software.”

In This Chapter

This chapter has the following sections:

- [About Secure Shell](#)
- [SSH Configuration Task List](#)
- [Troubleshooting Tips](#)
- [Monitoring and Maintaining SSH](#)
- [SSH Configuration Examples](#)

About Secure Shell

Secure Shell (SSH) is an application and a protocol that provide a secure replacement to the Berkeley r-tools. The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley **rexec** and **rsh** tools. There are currently two versions of SSH available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.



Note

Hereafter, unless otherwise noted, the term “SSH” will denote “SSH Version 1” only.

This rest of this section covers the following information:

- [How SSH Works](#)
- [Restrictions](#)
- [Related Features and Technologies](#)
- [Prerequisites to Configuring SSH](#)

How SSH Works

This section provides the following information about how SSH works:

- [SSH Server](#)
- [SSH Integrated Client](#)

SSH Server

The SSH Server feature enables a SSH client to make a secure, encrypted connection to a Cisco router. This connection provides functionality that is similar to that of an inbound Telnet connection. Before SSH, security was limited to Telnet security. SSH allows a strong encryption to be used with the Cisco IOS software authentication. The SSH server in Cisco IOS software will work with publicly and commercially available SSH clients.

SSH Integrated Client

The SSH Integrated Client feature is an application running over the SSH protocol to provide device authentication and encryption. The SSH client enables a Cisco router to make a secure, encrypted connection to another Cisco router or to any other device running the SSH server. This connection provides functionality that is similar to that of an outbound Telnet connection except that the connection is encrypted. With authentication and encryption, the SSH client allows for a secure communication over an insecure network.

The SSH client in the Cisco IOS software works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), Triple DES (3DES), and password authentication. User authentication is performed like that in the Telnet session to the router. The user authentication mechanisms supported for SSH are RADIUS, TACACS+ and the use of locally stored user names and passwords.



Note

The SSH client functionality is available only when the SSH server is enabled.

Restrictions

There following are some basic SSH restrictions:

- RSA authentication available in SSH clients is not supported in the SSH server for Cisco IOS software.
- SSH server and SSH client are supported on DES (56-bit) and 3DES (168-bit) data encryption software images only. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- Execution shell is the only application supported.

Related Features and Technologies

For more information about SSH-related features and technologies, review the following:

- Authentication, Authorization, and Accounting (AAA) feature. AAA is a suite of network security services that provide the primary framework through which access control can be set up on your Cisco router or access server. For more information on AAA, refer to the Authentication, Authorization, and Accounting chapters earlier in this book and the *Cisco IOS Security Command Reference*.
- IP Security (IPSec) feature. IPSec is a framework of open standards that provides data confidentiality, data integrity, and data authentication between participating peers. IPSec provides these security services at the IP layer. IPSec uses Internet Key Exchange (IKE) to handle negotiation of protocols and algorithms based on local policy and to generate the encryption and authentication keys to be used by IPSec. IPSec can be used to protect one or more data flows between a pair of hosts, between a pair of security gateways, or between a security gateway and a host. For more information on IPSec, refer to the chapter “Configuring IPSec Network Security” and the *Cisco IOS Security Command Reference*.

Prerequisites to Configuring SSH

Prior to configuring SSH, perform the following tasks:


- Download the required image on your router. (The SSH server requires you to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(1)T downloaded on your router; the SSH client requires you to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T downloaded on your router.) For more information on downloading a software image, refer to the *Cisco IOS Configuration Fundamentals Configuration Guide*.
- Configure a host name and host domain for your router.

To configure a host name and host domain, enter the following commands beginning in global configuration mode:

Command	Purpose
Router(config)# hostname <i>hostname</i>	Configures a host name for your router.
Router(config)# ip domain-name <i>domainname</i>	Configures a host domain for your router.

- Generate an RSA key pair for your router, which automatically enables SSH.

To generate an RSA key pair, enter the following global configuration command:

Command	Purpose
Router(config)# crypto key generate rsa	<p>Enables the SSH server for local and remote authentication on the router.</p> <p>The recommended minimum modulus size is 1024 bits.</p> <hr/> <p> Note To delete the RSA key-pair, use the crypto key zeroize rsa global configuration command. Once you delete the RSA key-pair, you automatically disable the SSH server.</p>

- Configure user authentication for local or remote access. You can configure authentication with or without AAA. For more information, refer to the “Authentication, Authorization, and Accounting (AAA)” chapters earlier in the book.

SSH Configuration Task List

The following sections describe the configuration tasks for SSH. Each task in the list is identified as either optional or required.

- [Configuring SSH Server](#) (Required)
- [Verifying SSH](#) (Optional)

See the section “[SSH Configuration Examples](#)” at the end of this chapter.

Configuring SSH Server



Note

The SSH client feature runs in user EXEC mode and has no specific configuration on the router.



Note

The SSH commands are optional and are disabled when the SSH server is disabled.

To enable and configure a Cisco Router for SSH, you can configure SSH parameters. If you do not configure SSH parameters, the the default values will be used.

To configure SSH server, use the following command in global configuration mode:

Command	Purpose
<pre>Router(config)# ip ssh {[timeout seconds] [authentication-retries integer]}</pre>	<p>(Required) Configures SSH control variables on your router.</p> <ul style="list-style-type: none"> You can specify the timeout in seconds, not to exceed 120 seconds. The default is 120. This setting applies to the SSH negotiation phase. Once the EXEC session starts, the standard timeouts configured for the vty apply. <p>By default, there are 5 vtys defined (0–4), therefore 5 terminal sessions are possible. After the SSH executes a shell, the vty timeout starts. The vty timeout defaults to 10 minutes.</p> <ul style="list-style-type: none"> You can also specify the number of authentication retries, not to exceed 5 authentication retries. The default is 3.

Verifying SSH

To verify that the SSH server is enabled and view the version and configuration data for your SSH connection, use the **show ip ssh** command. The following example shows that SSH is enabled:

```
Router# show ip ssh

SSH Enabled - version 1.5
Authentication timeout: 120 secs; Authentication retries: 3
```

The following example shows that SSH is disabled:

```
Router# show ip ssh

%SSH has not been enabled
```

To verify the status of your SSH server connections, use the **show ssh** command. The following example shows the SSH server connections on the router when SSH is enabled:

```
Router# show ssh
Connection      Version      Encryption    State          Username
0                1.5          3DES          Session Started guest
```

The following example shows that SSH is disabled:

```
Router# show ssh

%No SSH server connections running.
```

Troubleshooting Tips

- If your SSH configuration commands are rejected as illegal commands, you have not successfully generated a RSA key pair for your router. Make sure you have specified a host name and domain. Then use the **crypto key generate rsa** command to generate a RSA key pair and enable the SSH server.
- When configuring the RSA key pair, you might encounter the following error messages:
 - No hostname specified
You must configure a host name for the router using the **hostname** global configuration command. For more information, see [“Prerequisites to Configuring SSH.”](#)
 - No domain specified
You must configure a host domain for the router using the **ip domain-name** global configuration command. For more information, see [“Prerequisites to Configuring SSH.”](#)
- The number of allowable SSH connections is limited to the maximum number of vty configured for the router. Each SSH connection will use a vty resource.
- SSH uses either local security or the security protocol that is configured through AAA on your router for user authentication. When configuring AAA, you must ensure that the console is not running under AAA by applying a keyword in the global configuration mode to disable AAA on the console.

Monitoring and Maintaining SSH

To monitor and maintain your SSH connections, use the following commands in user EXEC mode:

Command	Purpose
Router# show ip ssh	Displays the version and configuration data for SSH.
Router# show ssh	Displays the status of SSH server connections.

SSH Configuration Examples

This section provides the following configuration examples, which are output from the **show running configuration** EXEC command on a Cisco 7200, Cisco 7500, and Cisco 12000.

- [SSH on a Cisco 7200 Series Router Example](#)
- [SSH on a Cisco 7500 Series Router Example](#)
- [SSH on a Cisco 1200 Gigabit Switch Router Example](#)



Note

The **crypto key generate rsa** command is not displayed in the **show running configuration** output.

SSH on a Cisco 7200 Series Router Example

In the following example, SSH is configured on a Cisco 7200 with a timeout that is not to exceed 60 seconds, and no more than 2 authentication retries. Also, before configuring the SSH server feature on the router, TACACS+ is specified as the method of authentication.

```
aaa new-model
aaa authentication login default tacacs+
aaa authentication login aaa7200kw none
enable password enable7200pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter the ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 2

controller E1 2/0

controller E1 2/1

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
no keepalive
no cdp enable

interface Ethernet1/1
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
no cdp enable

no ip classless
ip route 192.168.1.0 255.255.255.0 10.1.10.1
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1

map-list atm
ip 10.1.10.1 atm-vc 7 broadcast
no cdp run
```

```

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7200kw
transport input none
line aux 0
line vty 0 4
password enable7200pw

end

```

SSH on a Cisco 7500 Series Router Example

In the following example, SSH is configured on a Cisco 7500 with a timeout that is not to exceed 60 seconds and no more than 5 authentication retries. Before the SSH Server feature is configured on the router, RADIUS is specified as the method of authentication.

```

aaa new-model
aaa authentication login default radius
aaa authentication login aaa7500kw none
enable password enable7500pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
ip subnet-zero
no ip cef
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 5

controller E1 3/0
channel-group 0 timeslots 1

controller E1 3/1
channel-group 0 timeslots 1
channel-group 1 timeslots 2

interface Ethernet0/0/0
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet0/0/1
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown
interface Ethernet0/0/2
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

```

```
interface Ethernet0/0/3
no ip address
no ip directed-broadcast
no ip route-cache distributed
shutdown

interface Ethernet1/0
ip address 192.168.110.2 255.255.255.0 secondary
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/1
ip address 192.168.109.2 255.255.255.0
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/2
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache

interface Ethernet1/3
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Ethernet1/4
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown
interface Ethernet1/5
no ip address
no ip directed-broadcast
no ip route-cache
no ip mroute-cache
shutdown

interface Serial2/0
ip address 10.1.1.2 255.0.0.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache
no ip mroute-cache

ip classless
ip route 192.168.9.0 255.255.255.0 10.1.1.1
ip route 192.168.10.0 255.255.255.0 10.1.1.1
```

```

tacacs-server host 192.168.109.216 port 9000
tacacs-server key cisco
radius-server host 192.168.109.216 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa7500kw
transport input none
line aux 0
transport input all
line vty 0 4

end

```

SSH on a Cisco 1200 Gigabit Switch Router Example

In the following example, SSH is configured on a Cisco 12000 with a timeout that is not to exceed 60 seconds and no more than 2 authentication retries. Before the SSH Server feature is configured on the router, TACACS+ is specified as the method of authentication.

```

aaa new-model
aaa authentication login default tacacs+ local
aaa authentication login aaa12000kw local
enable password enable12000pw

username mcisco password 0 maryspw
username jcisco password 0 johnspw
redundancy
main-cpu
    auto-sync startup-config
ip subnet-zero
no ip domain-lookup
ip domain-name cisco.com
! Enter ssh commands.
ip ssh time-out 60
ip ssh authentication-retries 2

interface ATM0/0
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown

interface POS1/0
ip address 10.100.100.2 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
no keepalive
crc 16
no cdp enable

interface POS1/1
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

```

```
interface POS1/2
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS1/3
no ip address
no ip directed-broadcast
no ip route-cache cef
shutdown
crc 32

interface POS2/0
ip address 10.1.1.1 255.255.255.0
no ip directed-broadcast
encapsulation ppp
no ip route-cache cef
crc 16

interface Ethernet0
ip address 172.17.110.91 255.255.255.224
no ip directed-broadcast

router ospf 1
network 0.0.0.0 255.255.255.255 area 0.0.0.0

ip classless
ip route 0.0.0.0 0.0.0.0 172.17.110.65

logging trap debugging
tacacs-server host 172.17.116.138
tacacs-server key cisco

radius-server host 172.17.116.138 auth-port 1650 acct-port 1651
radius-server key cisco

line con 0
exec-timeout 0 0
login authentication aaa12000kw
transport input none
line aux 0
line vty 0 4

no scheduler max-task-time
no exception linecard slot 0 sqe-registers
no exception linecard slot 1 sqe-registers
no exception linecard slot 2 sqe-registers
no exception linecard slot 3 sqe-registers
no exception linecard slot 4 sqe-registers
no exception linecard slot 5 sqe-registers
no exception linecard slot 6 sqe-registers
end
```

