Configuring Secure Shell (SSH)

- Finding Feature Information, on page 1
- Prerequisites for Configuring Secure Shell, on page 1
- Restrictions for Configuring Secure Shell, on page 2
- Information about SSH, on page 2
- How to Configure SSH, on page 5
- Monitoring the SSH Configuration and Status, on page 9

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest caveats and feature information, see Bug Search Tool and the release notes for your platform and software release. To find information about the features documented in this module, and to see a list of the releases in which each feature is supported, see the feature information table at the end of this module.

Use Cisco Feature Navigator to find information about platform support and Cisco software image support. To access Cisco Feature Navigator, go to http://www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for Configuring Secure Shell

The following are the prerequisites for configuring the switch for secure shell (SSH):

- For SSH to work, the switch needs an Rivest, Shamir, and Adleman (RSA) public/private key pair. This is the same with Secure Copy Protocol (SCP), which relies on SSH for its secure transport.
- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.
- SCP relies on SSH for security.
- SCP requires that authentication, authorization, and accounting (AAA) authorization be configured so the router can determine whether the user has the correct privilege level.
- A user must have appropriate authorization to use SCP.

- A user who has appropriate authorization can use SCP to copy any file in the Cisco IOS File System (IFS) to and from a switch by using the **copy** command. An authorized administrator can also do this from a workstation.
- The Secure Shell (SSH) server requires an IPsec (Data Encryption Standard [DES] or 3DES) encryption software image; the SSH client requires an IPsec (DES or 3DES) encryption software image.)
- Configure a hostname and host domain for your device by using the **hostname** and **ip domain-name** commands in global configuration mode.

Related Topics

Secure Copy Protocol, on page 4

Restrictions for Configuring Secure Shell

The following are restrictions for configuring the SwitchDevice for secure shell.

- The switch supports Rivest, Shamir, and Adelman (RSA) authentication.
- SSH supports only the execution-shell application.
- The SSH server and the SSH client are supported only on Data Encryption Standard (DES) (56-bit) and 3DES (168-bit) data encryption software. In DES software images, DES is the only encryption algorithm available. In 3DES software images, both DES and 3DES encryption algorithms are available.
- The SwitchDevice supports the Advanced Encryption Standard (AES) encryption algorithm with a 128-bit key, 192-bit key, or 256-bit key. However, symmetric cipher AES to encrypt the keys is not supported.
- This software release does not support IP Security (IPSec).
- When using SCP, you cannot enter the password into the **copy** command. You must enter the password when prompted.
- The login banner is not supported in Secure Shell Version 1. It is supported in Secure Shell Version 2.
- The -l keyword and userid :{number} {ip-address} delimiter and arguments are mandatory when configuring the alternative method of Reverse SSH for console access.

Related Topics

Secure Copy Protocol, on page 4

Information about SSH

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH and Switch Access

Secure Shell (SSH) is a protocol that provides a secure, remote connection to a device. SSH provides more security for remote connections than Telnet does by providing strong encryption when a device is authenticated. This software release supports SSH Version 1 (SSHv1) and SSH Version 2 (SSHv2).

SSH functions the same in IPv6 as in IPv4. For IPv6, SSH supports IPv6 addresses and enables secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

SSH Servers, Integrated Clients, and Supported Versions

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

The SSH server and SSH integrated client are applications that run on the switch. The SSH server works with the SSH client supported in this release and with non-Cisco SSH clients. The SSH client works with publicly and commercially available SSH servers. The SSH client supports the ciphers of Data Encryption Standard (DES), 3DES, and password authentication.

The switch supports an SSHv1 or an SSHv2 server.

The switch supports an SSHv1 client.

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

User authentication is performed like that in the Telnet session to the device. SSH also supports the following user authentication methods:

- TACACS+
- RADIUS
- Local authentication and authorization

Related Topics

Configuring the Switch for Local Authentication and Authorization
TACACS+ and Switch Access
RADIUS and Switch Access

SSH Configuration Guidelines

Follow these guidelines when configuring the switch as an SSH server or SSH client:

- An RSA key pair generated by a SSHv1 server can be used by an SSHv2 server, and the reverse.
- If the SSH server is running on a stack master and the stack master fails, the new stack master uses the RSA key pair generated by the previous stack master.
- If you get CLI error messages after entering the **crypto key generate rsa** global configuration command, an RSA key pair has not been generated. Reconfigure the hostname and domain, and then enter the **crypto key generate rsa** command. For more information, see Related Topics below.
- When generating the RSA key pair, the message No host name specified might appear. If it does, you must configure a hostname by using the **hostname** global configuration command.

- When generating the RSA key pair, the message No domain specified might appear. If it does, you must configure an IP domain name by using the **ip domain-name** global configuration command.
- When configuring the local authentication and authorization authentication method, make sure that AAA is disabled on the console.

Related Topics

Setting Up the SwitchDevice to Run SSH, on page 5
Configuring the Switch for Local Authentication and Authorization

Secure Copy Protocol Overview

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. SCP relies on Secure Shell (SSH), an application and a protocol that provides a secure replacement for the Berkeley r-tools.

For SSH to work, the switch needs an RSA public/private key pair. This is the same with SCP, which relies on SSH for its secure transport.

Because SSH also relies on AAA authentication, and SCP relies further on AAA authorization, correct configuration is necessary.

- Before enabling SCP, you must correctly configure SSH, authentication, and authorization on the switch.
- Because SCP relies on SSH for its secure transport, the router must have an Rivest, Shamir, and Adelman (RSA) key pair.

Note When using SCP, you cannot enter the password into the copy command. You must enter the password when prompted.

Secure Copy Protocol

The Secure Copy Protocol (SCP) feature provides a secure and authenticated method for copying switch configurations or switch image files. The behavior of SCP is similar to that of remote copy (rcp), which comes from the Berkeley r-tools suite, except that SCP relies on SSH for security. SCP also requires that authentication, authorization, and accounting (AAA) authorization be configured so the switch can determine whether the user has the correct privilege level. To configure the Secure Copy feature, you should understand the SCP concepts.

Related Topics

Prerequisites for Configuring Secure Shell, on page 1
Restrictions for Configuring Secure Shell, on page 2

How to Configure SSH

Setting Up the SwitchDevice to Run SSH

Follow these steps to set up your SwitchDevice to run SSH:

Before you begin

Configure user authentication for local or remote access. This step is required. For more information, see Related Topics below.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **hostname** *hostname*
4. **ip domain-name** *domain_name*
5. **crypto key generate rsa**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchDevice> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.
Step 3	**hostname** *hostname* **Example:** `SwitchDevice(config)# hostname your_hostname`	Configures a hostname and IP domain name for your SwitchDevice. **Note** Follow this procedure only if you are configuring the SwitchDevice as an SSH server.
Step 4	**ip domain-name** *domain_name* **Example:**	Configures a host domain for your SwitchDevice.

	Command or Action	Purpose
	`SwitchDevice(config)# ip domain-name your_domain`	
Step 5	**crypto key generate rsa** **Example:** `SwitchDevice(config)# crypto key generate rsa`	Enables the SSH server for local and remote authentication on the SwitchDevice and generates an RSA key pair. Generating an RSA key pair for the SwitchDevice automatically enables SSH. We recommend that a minimum modulus size of 1024 bits. When you generate RSA keys, you are prompted to enter a modulus length. A longer modulus length might be more secure, but it takes longer to generate and to use. **Note** Follow this procedure only if you are configuring the SwitchDevice as an SSH server.
Step 6	**end** **Example:** `SwitchDevice(config)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `SwitchDevice# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Related Topics

SSH Configuration Guidelines, on page 3
Configuring the Switch for Local Authentication and Authorization

Configuring the SSH Server

Follow these steps to configure the SSH server:

Note This procedure is only required if you are configuring the SwitchDevice as an SSH server.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh version** [**1** | **2**]
4. **ip ssh** {**timeout** *seconds* | **authentication-retries** *number*}
5. Use one or both of the following:
   - `line vty`*line_number*[*ending_line_number*]
   - **transport input ssh**
6. **end**
7. **show running-config**
8. **copy running-config startup-config**

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `SwitchDevice> enable`	Enables privileged EXEC mode. Enter your password if prompted.
Step 2	**configure terminal** **Example:** `SwitchDevice# configure terminal`	Enters the global configuration mode.
Step 3	**ip ssh version** [**1**	**2**] **Example:** `SwitchDevice(config)# ip ssh version 1`	(Optional) Configures the SwitchDevice to run SSH Version 1 or SSH Version 2. • **1**—Configure the SwitchDevice to run SSH Version 1. • **2**—Configure the SwitchDevice to run SSH Version 2. If you do not enter this command or do not specify a keyword, the SSH server selects the latest SSH version supported by the SSH client. For example, if the SSH client supports SSHv1 and SSHv2, the SSH server selects SSHv2.
Step 4	**ip ssh** {**timeout** *seconds*	**authentication-retries** *number*} **Example:** `SwitchDevice(config)# ip ssh timeout 90 authentication-retries 2`	Configures the SSH control parameters: • Specify the time-out value in seconds; the default is 120 seconds. The range is 0 to 120 seconds. This parameter applies to the SSH negotiation phase. After the connection is established, the SwitchDevice uses the default time-out values of the CLI-based sessions.

	Command or Action	Purpose
		By default, up to five simultaneous, encrypted SSH connections for multiple CLI-based sessions over the network are available (session 0 to session 4). After the execution shell starts, the CLI-based session time-out value returns to the default of 10 minutes. • Specify the number of times that a client can re-authenticate to the server. The default is 3; the range is 0 to 5. Repeat this step when configuring both parameters.

Step 5	Use one or both of the following:
	• `line vty`*line_number*[*ending_line_number*]
	• **transport input ssh**
	Example:
	`SwitchDevice(config)# line vty 1 10`
	or
	`SwitchDevice(config-line)# transport input ssh`
		(Optional) Configures the virtual terminal line settings.
		• Enters line configuration mode to configure the virtual terminal line settings. For *line_number* and *ending_line_number*, specify a pair of lines. The range is 0 to 15.
		• Specifies that the SwitchDevice prevent non-SSH Telnet connections. This limits the router to only SSH connections.

Step 6	**end** **Example:** `SwitchDevice(config-line)# end`	Returns to privileged EXEC mode.
Step 7	**show running-config** **Example:** `SwitchDevice# show running-config`	Verifies your entries.
Step 8	**copy running-config startup-config** **Example:** `SwitchDevice# copy running-config startup-config`	(Optional) Saves your entries in the configuration file.

Monitoring the SSH Configuration and Status

This table displays the SSH server configuration and status.

Table 1: Commands for Displaying the SSH Server Configuration and Status

Command	Purpose
show ip ssh	Shows the version and configuration information for the SSH server.
show ssh	Shows the status of the SSH server.