SSH Terminal-Line Access

Last Updated: July 04, 2011

The SSH Terminal-Line Access feature provides users secure access to tty (text telephone) lines. tty allows the hearing- and speech-impaired to communicate by using a telephone to type messages.

Finding Feature Information

Your software release may not support all the features documented in this module. For the latest feature information and caveats, see 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 document.

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

Prerequisites for SSH Terminal-Line Access

Download the required image to your router. The secure shell (SSH) server requires the router to have an IPSec (Data Encryption Standard (DES) or 3DES) encryption software image from Cisco IOS Release 12.1(1)T or a later release. The SSH client requires the router to have an IPSec (DES or 3DES) encryption software image from Cisco IOS Release 12.1(3)T or a later release. See the *Cisco IOS Configuration*

Fundamentals Configuration Guide , Release 12.4T for more information on downloading a software image.

The SSH server requires the use of a username and password, which must be defined through the use of a local username and password, TACACS+, or RADIUS.

Note The SSH Terminal-Line Access feature is available on any image that contains SSH.

Restrictions for SSH Terminal-Line Access

Console Server Requirement

To configure secure console server access, you must define each line in its own rotary and configure SSH to use SSH over the network when user want to access each of those devices.

Memory and Performance Impact

Replacing reverse Telnet with SSH may reduce the performance of available tty lines due to the addition of encryption and decryption processing above the vty processing. (Any cryptographic mechanism uses more memory than a regular access.)

Information About SSH Terminal-Line Access

Overview of SSH Terminal-Line Access

Cisco IOS supports reverse Telnet, which allows users to Telnet through the router--via a certain port range--to connect them to tty (asynchronous) lines. Reverse Telnet has allowed users to connect to the console ports of remote devices that do not natively support Telnet. However, this method has provided very little security because all Telnet traffic goes over the network in the clear. The SSH Terminal-Line Access feature replaces reverse Telnet with SSH. This feature may be configured to use encryption to access devices on the tty lines, which provide users with connections that support strong privacy and session integrity.

SSH is an application and a protocol that provides secure replacement for the suite of Berkeley r-tools such as rsh, rlogin, and rcp. (Cisco IOS supports rlogin.) The protocol secures the sessions using standard cryptographic mechanisms, and the application can be used similarly to the Berkeley rexec and rsh tools. Currently two versions of SSH are available: SSH Version 1 and SSH Version 2. Only SSH Version 1 is implemented in the Cisco IOS software.

The SSH Terminal-Line Access feature enables users to configure their router with secure access and perform the following tasks:

- Connect to a router that has multiple terminal lines connected to consoles or serial ports of other routers, switches, or devices.
- Simplify connectivity to a router from anywhere by securely connecting to the terminal server on a specific line.

- Allow modems attached to routers to be used for dial-out securely.
- Require authentication of each of the lines through a locally defined username and password, TACACS+, or RADIUS.

Note The **session slot** command that is used to start a session with a module requires Telnet to be accepted on the virtual tty (vty) lines. When you restrict vty lines only to SSH, you cannot use the command to communicate with the modules. This applies to any Cisco IOS device where the user can telnet to a module on the device.

How to Configure SSH Terminal-Line Access

Configuring SSH Terminal-Line Access

Perform this task to configure a Cisco router to support reverse secure Telnet.

Note SSH must already be configured on the router.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **line** *line-number* [*ending-line-number*]
4. **no exec**
5. **login** {**local** | **authentication** *listname*}
6. **rotary** *group*
7. **transport input** {**all** | **ssh**}
8. **exit**
9. **ip ssh port** *portnum* **rotary** *group*

DETAILED STEPS

	Command or Action	Purpose
Step 1	**enable** **Example:** `Router> enable`	Enables privileged EXEC mode. • Enter your password if prompted.

	Command or Action	Purpose
Step 2	**configure terminal** **Example:** `Router# configure terminal`	Enters global configuration mode.
Step 3	**line** *line-number* [*ending-line-number*] **Example:** `Router(config)# line 1 200`	Identifies a line for configuration and enters line configuration mode. **Note** For router console configurations, each line must be defined in its own rotary, and SSH must be configured to listen in on each rotary. **Note** An authentication method requiring a username and password must be configured for each line. This may be done through the use of a local username and password stored on the router, through the use of TACACS+, or through the use of RADIUS. Neither Line passwords nor the enable password are sufficient to be used with SSH.
Step 4	**no exec** **Example:** `Router(config-line)# no exec`	Disables exec processing on each of the lines.
Step 5	**login** {**local** | **authentication** *listname*} **Example:** `Router(config-line)# login authentication default`	Defines a login authentication mechanism for the lines. **Note** The authentication method must utilize a username and password.
Step 6	**rotary** *group* **Example:** `Router(config-line)# rotary 1`	Defines a group of lines consisting of one or more lines. **Note** All rotaries used must be defined, and each defined rotary must be used when SSH is enabled.
Step 7	**transport input** {**all** | **ssh**} **Example:** `Router(config-line)# transport input ssh`	Defines which protocols to use to connect to a specific line of the router.

	Command or Action	Purpose
Step 8	**exit** **Example:** `Router(config-line)# exit`	Exits line configuration mode.
Step 9	**ip ssh port** *portnum* **rotary** *group* **Example:** `Router(config)# ip ssh port 2000 rotary 1`	Enables secure network access to the tty lines. • Use this command to connect the *portnum* argument with the rotary *group*argument, which is associated with a line or group of lines. **Note** The *group* argument must correspond with the **rotary** *group* number chosen in Step 6.

Verifying SSH Terminal-Line Access

To verify that this functionality is working, you can connect to a router using an SSH client.

Configuration Examples for SSH Terminal-Line Access

Example SSH Terminal-Line Access Configuration

The following example shows how to configure the SSH Terminal-Line Access feature on a modem used for dial-out on lines 1 through 200. To get any of the dial-out modems, use any SSH client and start an SSH session to port 2000 of the router to get to the next available modem from the rotary.

```
line 1 200
 no exec
 login authentication default
 rotary 1
 transport input ssh
 exit
ip ssh port 2000 rotary 1
```

Example SSH Terminal-Line Access for a Console Serial Line Ports Configuration

The following example shows how to configure the SSH Terminal-Line Access feature to access the console or serial line interface of various devices. For this type of access, each line is put into its own rotary, and each rotary is used for a single port. In this example, lines 1 through 3 are used; the port (line) mappings of the configuration are shown in the table below.

Table 1 Port (line) Configuration Mappings

Line Number	SSH Port Number
1	2001
2	2002
3	2003

```
line 1
 no exec
 login authentication default
 rotary 1
 transport input ssh
line 2
 no exec
 login authentication default
 rotary 2
 transport input ssh
line 3
 no exec
 login authentication default
 rotary 3
 transport input ssh
ip ssh port 2001 rotary 1 3
```

Additional References

Related Documents

Related Topic	Document Title
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
SSH	*Cisco IOS Security Configuration Guide: Securing User Services*
SSH commands	*Cisco IOS Security Command Reference*
Dial Technologies	*Cisco IOS Dial Technologies Configuration Guide*
Dial commands	*Cisco IOS Dial Technologies Command Reference*
Downloading a software image	*Cisco IOS Configuration Fundamentals Configuration Guide*

Standards

Standard	Title
	--

MIBs

MIB	MIBs Link
	To locate and download MIBs for selected platforms, Cisco software releases, and feature sets, use Cisco MIB Locator found at the following URL: http://www.cisco.com/go/mibs

RFCs

RFC	Title
None.	--

Technical Assistance

Description	Link
The Cisco Support and Documentation website provides online resources to download documentation, software, and tools. Use these resources to install and configure the software and to troubleshoot and resolve technical issues with Cisco products and technologies. Access to most tools on the Cisco Support and Documentation website requires a Cisco.com user ID and password.	http://www.cisco.com/cisco/web/support/index.html

Feature Information for SSH Terminal-Line Access

The following table provides release information about the feature or features described in this module. This table lists only the software release that introduced support for a given feature in a given software release train. Unless noted otherwise, subsequent releases of that software release train also support that feature.

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

Table 2 Feature Information for SSH Terminal-Line Access

Feature Name	Releases	Feature Information
SSH Terminal-Line Access	12.2(4)JA 12.2(15)T 12.2(6th)S	The SSH Terminal-Line Access feature provides users secure access to tty (text telephone) lines. tty allows the hearing- and speech-impaired to communicate by using a telephone to type messages. This feature was introduced in Cisco IOS Release 12.2(4)JA. This feature was integrated into Cisco IOS Release 12.2(15)T. This feature was integrated into Cisco IOS Release 12.2(6th)S. The following command was introduced or modified: **ip ssh port**.