



SSH Support Over IPv6

Last Updated: November 27, 2012

Secure Shell (SSH) provides support for IPv6 addresses that enable a Cisco device to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

- [Finding Feature Information, page 1](#)
- [Prerequisites for SSH Support over IPv6, page 1](#)
- [Information About SSH Support over IPv6, page 2](#)
- [How to Enable SSH Support over IPv6, page 2](#)
- [Configuration Examples for SSH Support over IPv6, page 3](#)
- [Additional References, page 3](#)
- [Feature Information for SSH Support over IPv6, page 5](#)

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 www.cisco.com/go/cfn. An account on Cisco.com is not required.

Prerequisites for SSH Support over IPv6

- An IPsec (Data Encryption Standard [DES] or 3DES) encryption software image is loaded on your device. IPv6 transport for the SSH server and SSH client requires an IPsec encryption software image.
- A hostname and host domain are configured for your device.
- A Rivest, Shamir, and Adelman (RSA) key pair, which automatically enables SSH, is generated for your device.
- A user authentication mechanism for local or remote access is configured on your device.
- To authenticate SSH clients, configure TACACS+ or RADIUS over an IPv4 transport and then connect to an SSH server over an IPv6 transport.



Americas Headquarters:
Cisco Systems, Inc., 170 West Tasman Drive, San Jose, CA 95134-1706 USA

The basic restrictions for SSH over an IPv4 transport apply to SSH over an IPv6 transport. The use of locally stored usernames and passwords is the only user authentication mechanism supported by SSH over an IPv6 transport. TACACS+ and RADIUS user authentication mechanisms are not supported over an IPv6 transport.

Information About SSH Support over IPv6

- [SSH over an IPv6 Transport, page 2](#)

SSH over an IPv6 Transport

Secure shell (SSH) SSH in IPv6 functions the same and offers the same benefits as SSH in IPv4. The SSH server feature enables an SSH client to make a secure, encrypted connection to a Cisco device, and the SSH client feature enables a Cisco device to make a secure, encrypted connection to another Cisco device or to any other device running an SSH server. IPv6 enhancements to SSH consist of support for IPv6 addresses that enable a Cisco device to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport.

How to Enable SSH Support over IPv6

- [Enabling SSH on an IPv6 Device, page 2](#)

Enabling SSH on an IPv6 Device

This task is optional. If you do not configure SSH parameters, then the default values will be used.

SUMMARY STEPS

1. **enable**
2. **configure terminal**
3. **ip ssh** [*timeout seconds* | *authentication-retries integer*]
4. **exit**
5. **ssh** [*-v* { **1** | **2** } | *c* { **3des** | **aes128-cbc** | **aes192-cbc** | **aes256-cbc** } | *-l userid* | *-l userid:vrfname number ip-address ip-address* | *-l userid:rotary number ip-address* | *-m* { **hmac-md5** | **hmac-md5-96** | **hmac-sha1** | **hmac-sha1-96** } | *-o numberofpasswordprompts n* | *-p port-num*] { *ip-addr* | *hostname* } [*command* | *-vrf*]

DETAILED STEPS

Command or Action	Purpose
Step 1 enable Example: Device> enable	Enables privileged EXEC mode. <ul style="list-style-type: none"> • Enter your password if prompted.

Command or Action	Purpose
Step 2 <code>configure terminal</code> Example: <pre>Device# configure terminal</pre>	Enters global configuration mode.
Step 3 <code>ip ssh [timeout <i>seconds</i> authentication-retries <i>integer</i>]</code> Example: <pre>Device(config)# IP ssh timeout 100 authentication-retries 2</pre>	Configures SSH control variables on your device.
Step 4 <code>exit</code> Example: <pre>Device(config)# exit</pre>	Exits configuration mode, and returns the device to privileged EXEC mode.
Step 5 <code>ssh [-v { 1 2 } c { 3des aes128-cbc aes192-cbc aes256-cbc } -l <i>userid</i> -l <i>userid</i>:<i>vrfname</i> <i>number ip-address ip-address</i> -l <i>userid</i>:<i>rotary number ip-address</i> -m { hmac-md5 hmac-md5-96 hmac-sha1 hmac-sha1-96 } -o <i>numberofpasswordprompts n</i> -p <i>port-num</i>] { <i>ip-addr</i> <i>hostname</i> } [<i>command</i> -vrf]</code> Example: <pre>Device# ssh -l userid1 2001:db8:2222:1044::72</pre>	Starts an encrypted session with a remote networking device.

Configuration Examples for SSH Support over IPv6

- [Example: Enabling SSH on an IPv6 Device, page 3](#)

Example: Enabling SSH on an IPv6 Device

```
Device# configure terminal
Device(config)# ip ssh
Device(config)# exit
Device(config)# ssh -l userid1 2001:db8:2222:1044::72
```

Additional References

Related Documents

Related Topic	Document Title
IPv6 addressing and connectivity	<i>IPv6 Configuration Guide</i>
SSH configuration information	Configuring Secure Shell
Cisco IOS commands	Cisco IOS Master Commands List, All Releases
IPv6 commands	<i>Cisco IOS IPv6 Command Reference</i>
Cisco IOS IPv6 features	Cisco IOS IPv6 Feature Mapping

Standards and RFCs

Standard/RFC	Title
RFC 4292	<i>IP Forwarding Table MIB</i>
RFC 4293	<i>Management Information Base for the Internet Protocol (IP)</i>
RFCs for IPv6	<i>IPv6 RFCs</i>

MIBs

MIB	MIBs Link
<ul style="list-style-type: none"> • CISCO-CONFIG-COPY-MIB • CISCO-CONFIG-MAN-MIB • CISCO-DATA-COLLECTION-MIB • CISCO-FLASH-MIB • CISCO-RTTMON-IPv6-MIB • CISCO-SNMP-TARGET-EXT-MIB • ENTITY-MIB • IP-FORWARD-MIB • IP-MIB • NOTIFICATION-LOG-MIB • SNMP-TARGET-MIB 	<p>To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:</p> <p>http://www.cisco.com/go/mibs</p>

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 Support over IPv6

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 1 Feature Information for SSH Support over IPv6

Feature Name	Releases	Feature Information
SSH Support over IPv6	12.2(8)T 12.2(17a)SX1 12.2(25)SEE 12.2(25)SG 12.2(33)SRA 15.0(2)SG Cisco IOS XE Release 2.1 3.2SG	SSH provides support for IPv6 addresses that enable a Cisco device to accept and establish secure, encrypted connections with remote IPv6 nodes over an IPv6 transport. The following commands were introduced or modified: ip ssh , ssh .

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1110R)

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams,

and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

© 2012 Cisco Systems, Inc. All rights reserved.