



## SSH Support Over IPv6

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.

- [Prerequisites for SSH Support over IPv6, on page 1](#)
- [Information About SSH Support over IPv6, on page 1](#)
- [How to Enable SSH Support over IPv6, on page 2](#)
- [Configuration Examples for SSH Support over IPv6, on page 3](#)
- [Additional References, on page 3](#)
- [Feature Information for SSH Support over IPv6, on page 4](#)

### 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.

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

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

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

#### Procedure

|               | Command or Action   | Purpose  |
|---------------|---|--|
| <b>Step 1</b> | <b>enable</b><br><b>Example:</b><br>Device> enable  | Enables privileged EXEC mode. <ul style="list-style-type: none"> <li>• Enter your password if prompted.</li> </ul> |
| <b>Step 2</b> | <b>configure terminal</b><br><b>Example:</b><br>Device# configure terminal  | Enters global configuration mode.  |
| <b>Step 3</b> | <b>ip ssh [timeout <i>seconds</i>   authentication-retries <i>integer</i>]</b><br><b>Example:</b><br>Device(config)# IP ssh timeout 100<br>authentication-retries 2   | Configures SSH control variables on your device.   |
| <b>Step 4</b> | <b>exit</b><br><b>Example:</b><br>Device(config)# exit  | Exits configuration mode, and returns the device to privileged EXEC mode.  |
| <b>Step 5</b> | <b>ssh [-v { 1   2 }   c { 3des   aes128-cbc   aes192-cbc   aes256-cbc }   -l <i>userid</i>   -l <i>userid:vrfname number ip-address ip-address</i>   -l <i>userid: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]</b><br><b>Example:</b> | Starts an encrypted session with a remote networking device.   |

|  | Command or Action  | Purpose |
|--|--|---------|
|  | Device# <code>ssh -l userid1 2001:db8:2222:1044::72</code> |         |

## Configuration Examples for SSH Support over IPv6

### 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>                              |
| Cisco IOS commands               | <a href="#">Cisco IOS Master Commands List, All Releases</a> |
| IPv6 commands                    | <i>Cisco IOS IPv6 Command Reference</i>                      |
| Cisco IOS IPv6 features          | <i>Cisco IOS IPv6 Feature Mapping</i>                        |

### Standards and RFCs

| Standard/RFC  | Title            |
|---------------|------------------|
| RFCs for IPv6 | <i>IPv6 RFCs</i> |

### MIBs

| MIB   | MIBs Link  |
|---|--|
| No new or modified MIBs are supported by this feature, and support for existing MIBs has not been modified by this feature. | To locate and download MIBs for selected platforms, Cisco IOS releases, and feature sets, use Cisco MIB Locator found at the following URL:<br><br><a href="http://www.cisco.com/go/mibs">http://www.cisco.com/go/mibs</a> |

**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. | <a href="http://www.cisco.com/cisco/web/support/index.html">http://www.cisco.com/cisco/web/support/index.html</a> |

## 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](http://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<br>12.2(17a)SX1<br>12.2(25)SEE<br>12.2(25)SG<br>12.2(33)SRA<br>15.0(2)SG<br>Cisco IOS XE Release 2.1<br>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.<br><br>The following commands were introduced or modified: <b>ip ssh</b> , <b>ssh</b> . |