6

IPv6 Management Security Features

Contents

IPv6 Management Security

This chapter describes management security features that are IPv6 counterparts of IPv4 management security features on the switches covered by this guide.

Feature	Default	CLI
configure authorized IP managers for IPv6	disabled	6-5
configuring secure shell for IPv6	disabled	6-15
enabling secure copy and secure FTP for IPv6	disabled	6-18

This chapter describes the following IPv6-enabled management security features included in software release K.13.01:

- Authorized IP Managers for IPv6
- Secure Shell for IPv6
- Secure Copy and Secure FTP for IPv6

Authorized IP Managers for IPv6

The Authorized IP Managers feature uses IP addresses and masks to determine which stations (PCs or workstations) can access the switch through the network. This feature supports switch access through:

- Telnet and other terminal emulation applications
- Web browser interface
- SNMP (with a correct community name)

As with the configuration of IPv4 management stations, the Authorized IP Managers for IPv6 feature allows you to specify the IPv6-based stations that can access the switch.

Usage Notes

- You can configure up to ten authorized IPv4 and IPv6 manager *addresses* on a switch, where each address applies to either a single management station or a group of stations. Each authorized manager address consists of an IPv4 or IPv6 address and a mask that determines the individual management stations that are allowed access.
    - You configure authorized IPv4 manager addresses using the **ip authorized-managers** command. For more information, refer to the "Using Authorized IP Managers" chapter in the *Access Security Guide*.
    - You configure authorized IPv6 manager addresses using the **ipv6 authorized-managers** command. For more information, see "Configuring Authorized IP Managers for Switch Access" on page 6-5.
- You can block all IPv4-based or all IPv6-based management stations from accessing the switch by entering the following commands:
    - To block access to all IPv4 manager addresses while allowing access to IPv6 manager addresses, enter the **ip authorized-managers 0.0.0.0** command.
    - To block access to all IPv6 manager addresses while allowing access to IPv4 manager addresses, enter the **ipv6 authorized-managers ::** command. (The double colon represents an IPv6 address that consists of all zero's: **0:0:0:0:0:0:0:0**.)

- You configure each authorized manager address with Manager or Operator-level privilege to access the switch in a Telnet, SNMPv1, or SNMPv2c session. (Access privilege for SSH, SNMPv3, and web browser sessions are configured through the access application, not through the Authorized IP Managers feature.)
  - Manager privilege allows full access to all web browser and console interface screens for viewing, configuration, and all other operations available in these interfaces.
  - Operator privilege allows read-only access from the web browser and console interfaces.
- When you configure station access to the switch using the Authorized IP Managers feature, the settings take precedence over the access configured with local passwords, TACACS+ servers, RADIUS-assigned settings, port-based (802.1X) authentication, and port security settings.

  As a result, the IPv6 address of a networked management device must be configured with the Authorized IP Managers feature before the switch can authenticate the device using the configured settings from other access security features. If the Authorized IP Managers feature disallows access to the device, then access is denied. Therefore, with authorized IP managers configured, logging in with the correct passwords is not sufficient to access a switch through the network unless the station requesting access is also authorized in the switch's Authorized IP Managers configuration.

Configuring Authorized IP Managers for Switch Access

To configure one or more IPv6-based management stations to access the switch using the Authorized IP Managers feature, enter the **ipv6 authorized-managers** command

Syntax: ipv6 authorized-managers <*ipv6-addr*> [*ipv6-mask*] [access <operator | manager>]

Configures one or more authorized IPv6 addresses to access the switch, where:

ipv6-mask *specifies the mask that is applied to an IPv6 address to determine authorized stations. For more information, see "Using a Mask to Configure Authorized Management Stations" on page 6-5. Default:* **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**.

access <operator | manager> *specifies the level of access privilege granted to authorized stations and applies only to Telnet, SNMPv1, and SNMPv2c access. Default:* **Manager.**

Note: *The Authorized IP Manager feature does not support the configuration of access privileges on authorized stations that use an SSH, SNMPv3, or the web browser session to access the switch. For these sessions, access privilege is configured with the access application.*

Using a Mask to Configure Authorized Management Stations

The *ipv6-mask* parameter controls how the switch uses an IPv6 address to determine the IPv6 addresses of authorized manager stations on your network. For example, you can specify a mask that authorizes:

- Single station access
- Multiple station access

Note

Mask configuration is a method for determining the valid IPv6 addresses that are authorized for management access to the switch. In the Authorized IP Managers feature, the mask serves a different purpose than an IPv6 subnet mask and is applied in a different manner.

Configuring Single Station Access

To authorize only one IPv6-based station for access to the switch, enter the IPv6 address of the station and set the mask to **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**.

Notes

If you do not enter a value for the *ipv6-mask* parameter when you configure an authorized IPv6 address, the switch automatically uses **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF** as the default mask (see “Configuring Authorized IP Managers for Switch Access” on page 6-5).

If you have ten or fewer management and/or operator stations for which you want to authorize access to the switch, it may be more efficient to configure them by entering each IPv6 address with the default mask in a separate **ipv6 authorized-managers** command.

When used in a mask, “**FFFF**” specifies that each bit in the corresponding 16-bit (hexadecimal) block of an authorized station’s IPv6 address must be identical to the same “on” or “off” setting in the IPv6 address entered in the **ipv6 authorized-managers** command. (The binary equivalent of **FFFF** is 1111 1111 1111 1111, where **1** requires the same “on” or “off” setting in an authorized address.)

For example, as shown in Figure 6-1, if you configure a link-local IPv6 address of FE80::202:B3FF:FE1E:8329 with a mask of **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF**, only a station having an IPv6 address of FE80::202:B3FF:FE1E:8329 has management access to the switch.

	1st Block	2nd Block	3rd Block	4th Block	5th Block	6th Block	7th Block	8th Block	Manager- or Operator-Level Access
IPv6 Mask	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	The “FFFF” in each hexadecimal block of the mask specifies that only the exact value of each bit in the corresponding block of the IPv6 address is allowed. This mask allows management access only to a station having an IPv6 address of FE80::202:B3FF:FE1E:8329.
IPv6 Address	FE80	0000	0000	0000	202	B3FF	FE1E	8329	

Figure 6-1. Mask for Configuring a Single Authorized IPv6 Manager Station

Configuring Multiple Station Access

To authorize multiple stations to access the switch without having to re-enter the **ipv6 authorized-managers** command for each station, carefully select the IPv6 address of an authorized IPv6 manager and an associated mask to authorize a range of IPv6 addresses.

As shown in Figure 6-2, if a bit in any of the 4-bit binary representations of a hexadecimal value in a mask is “on” (set to 1), then the corresponding bit in the IPv6 address of an authorized station must match the ”on” or “off’ setting of the same bit in the IPv6 address you enter with the **ipv6 authorized-managers** command.

Conversely, in a mask, a “0” binary bit means that either the “on” or “off” setting of the corresponding IPv6 bit in an authorized address is valid and does not have to match the setting of the same bit in the specified IPv6 address.

Figure 6-2 shows the binary expressions represented by individual hexadecimal values in an *ipv6-mask* parameter.

Hexadecimal Value in an IPv6 Mask	Binary Equivalent
0	0000
1	0001
2	0010
3	0011
4	0100
5	0101
6	0110
7	0111
8	1000
9	1001
A	1010
B	1011
C	1100
D	1101
E	1110
F	1111

Figure 6-2. Hexadecimal Mask Values and Binary Equivalents

Example. Figure 6-3 shows an example in which a mask that authorizes switch access to four management stations is applied to the IPv6 address: **2001:DB8:0000:0000:244:17FF:FEB6:D37D**. The mask is: **FFFF:FFFF:FFFF:FFF8:FFFF:FFFF:FFFF:FFFC**.

	1st Block	2nd Block	3rd Block	4th Block	5th Block	6th Block	7th Block	8th Block	Manager- or Operator-Level Access
IPv6 Mask	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFC	The "F" value in the first 124 bits of the mask specifies that only the exact value of each corresponding bit in an authorized IPv6 address is allowed. However, the "C" value in the last four bits of the mask allows four possible combinations (D37C, D37D, D37E, and D37F) in the last block of an authorized IPv6 address.
IPv6 Address	2001	DB8	0000	0000	244	17FF	FEB6	D37D	

Figure 6-3. Example: Mask for Configuring Four Authorized IPv6 Manager Stations

Last block in Mask: FFFC
Last block in IPv6 Address: D37D

Bit Numbers	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
Bit Value	F				F				F				C			
FFFC: Last Block in Mask	■	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□
D37D: Last Block in IPv6 Address	■	■	□	■	□	□	■	■	□	■	■	■	■	■	□	■

Bit Setting: ■ = 1 (On) □ = 0 (Off)

Figure 6-4. Example: How a Mask Determines Four Authorized IPv6 Manager Addresses

As shown in Figure 6-4, if you use a mask of **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFC** with an IPv6 address, you can authorize four IPv6-based stations to access the switch. In this mask, all bits except the last two are set to 1 ("on"); the binary equivalent of hexadecimal **C** is 1100.

Therefore, this mask requires the first corresponding 126 bits in an authorized IPv6 address to be the same as in the specified IPv6 address: 2001:DB8:0000:0000:244:17FF:FEB6:D37C. However, the last two bits are set to 0 (“off”) and allow the corresponding bits in an authorized IPv6 address to be either “on” or “off”. As a result, only the four IPv6 addresses shown in Figure 6-5 are allowed access.

	1st Block	2nd Block	3rd Block	4th Block	5th Block	6th Block	7th Block	8th Block
IPv6 Mask	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFF	FFFC
IPv6 Address Entered with the “ipv6 authorized-managers” Command	2001	DB8	0000	0000	244	17FF	FEB6	D37D
Other Authorized IPv6 Addresses	2001	DB8	0000	0000	244	17FF	FEB6	D37C
	2001	DB8	0000	0000	244	17FF	FEB6	D37E
	2001	DB8	0000	0000	244	17FF	FEB6	D37F

Figure 6-5. Example: How Hexadecimal C in a Mask Authorizes Four IPv6 Manager Addresses

Example. Figure 6-6 shows an example in which a mask is applied to the IPv6 address: **2001:DB8:0000:0000:244:17FF:FEB6:D37D/64**. The specified mask **FFFF:FFFF:FFFF:FFF8:FFFF:FFFF:FFFF:FFFF** configures eight management stations as authorized IP manager stations.

Note that, in this example, the IPv6 mask is applied as follows:

- Eight management stations in different subnets are authorized by the value of the fourth block (**FFF8**) in the 64-bit prefix ID (**FFFF:FFFF:FFFF:FFF8**) of the mask. (The fourth block of the prefix ID is often used to define subnets in an IPv6 network.)

  The binary equivalent of **FFF8** that is used to specify valid subnet IDs in the IPv6 addresses of authorized stations is: 1111 1111 1111 1000.

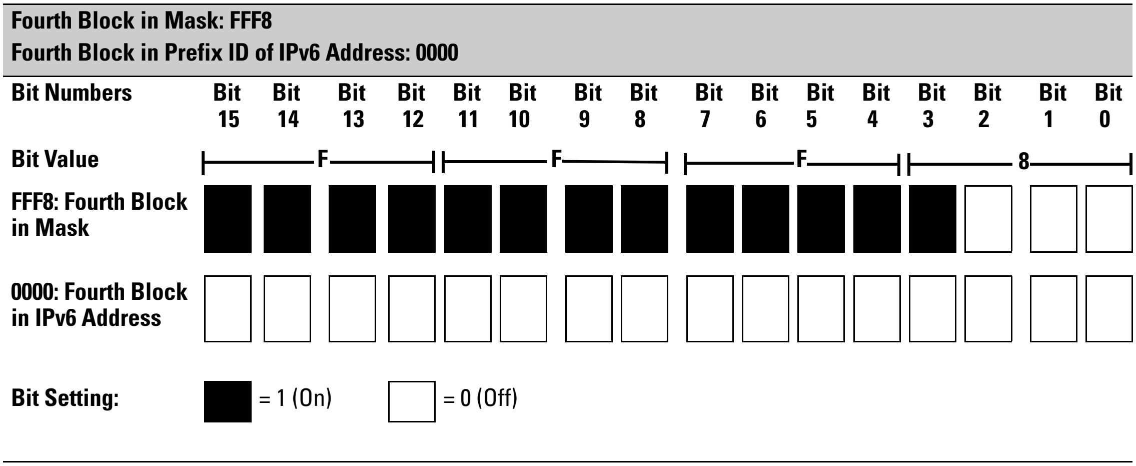
  The three “off” bits (1000) in the last part of the this block (**FFF8**) of the mask allow for eight possible authorized IPv6 stations:
  2001:DB8:0000:0000:244:17FF:FEB6:D37D
  2001:DB8:0000:0001:244:17FF:FEB6:D37D
  2001:DB8:0000:0002:244:17FF:FEB6:D37D
  2001:DB8:0000:0003:244:17FF:FEB6:D37D
  2001:DB8:0000:0004:244:17FF:FEB6:D37D
  2001:DB8:0000:0005:244:17FF:FEB6:D37D
  2001:DB8:0000:0006:244:17FF:FEB6:D37D
  2001:DB8:0000:0007:244:17FF:FEB6:D37D

- Each authorized station has the same 64-bit device ID (**244:17FF:FEB6:D37D**) because the value of the last four blocks in the mask is **FFFF** (binary value 1111 1111).

  FFFF requires all bits in each corresponding block of an authorized IPv6 address to have the same "on" or "off" setting as the device ID in the specified IPv6 address. In this case, each bit in the device ID (last four blocks) in an authorized IPv6 address is fixed and can be only one value: 244:17FF:FEB6:D37D.

	1st Block	2nd Block	3rd Block	4th Block	5th Block	6th Block	7th Block	8th Block	Manager- or Operator-Level Access
IPv6 Mask	FFFF	FFFF	FFFF	FFF8	FFFF	FFFF	FFFF	FFFF	In this example, the IPv6 mask allows up to four stations in different subnets to access the switch. This authorized IP manager configuration is useful if only management stations are specified by the authorized IPv6 addresses. Refer to Figure 6-4 for how the bitmap of the IPv6 mask determines authorized IP manager stations.
Authorized IPv6 Address	2001	DB8	0000	0000	244	17FF	FEB6	D37D	

Figure 6-6. Example: Mask for Configuring Authorized IPv6 Manager Stations in Different Subnets



Fourth Block in Mask: FFF8
Fourth Block in Prefix ID of IPv6 Address: 0000

Bit Numbers	**Bit 15**	**Bit 14**	**Bit 13**	**Bit 12**	**Bit 11**	**Bit 10**	**Bit 9**	**Bit 8**	**Bit 7**	**Bit 6**	**Bit 5**	**Bit 4**	**Bit 3**	**Bit 2**	**Bit 1**	**Bit 0**
Bit Value	F				F				F				8			
FFF8: Fourth Block in Mask	■	■	■	■	■	■	■	■	■	■	■	■	■	□	□	□
0000: Fourth Block in IPv6 Address	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□	□

Bit Setting: ■ = 1 (On) □ = 0 (Off)

Figure 6-7. Example: How a Mask Determines Authorized IPv6 Manager Addresses by Subnet

Figure 6-7 shows the bits in the fourth block of the mask that determine the valid subnets in which authorized stations with an IPv6 device ID of **244:17FF:FEB6:D37D** reside.

FFF8 in the fourth block of the mask means that bits 3 - 15 of the block are fixed and, in an authorized IPv6 address, must correspond to the "on" and "off" settings shown for the binary equivalent 0000 in the fourth block of the IPv6 address. Conversely, bits 0 - 2 are variable and, in an authorized IPv6 address, may be either "on" (1) or "off" (0).

As a result, assuming that the seventh and eighth bytes (fourth hexadecimal block) of an IPv6 address are used as the subnet ID, only the following binary expressions and hexadecimal subnet IDs are supported in this authorized IPv6 manager configuration:

Authorized Subnet ID in Fourth Hexadecimal Block of IPv6 Address	Binary Equivalent
0000	0000 0000
0001	0000 0001
0002	0000 0010
0003	0000 0011
0004	0000 0100
0005	0000 0101
0006	0000 0110
0007	0000 0111

Figure 6-8. Binary Equivalents of Authorized Subnet IDs (in Hexadecimal)

Displaying an Authorized IP Managers Configuration

Use the **show ipv6 authorized-managers** command to list the IPv6 stations authorized to access the switch; for example:

```
ProCurve# show ipv6 authorized-managers

 IPv6 Authorized Managers
---------------------------------------

 Address : 2001:db8:0:7::5
 Mask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
 Access  : Manager

 Address : 2001:db8::a:1c:e3:3
 Mask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:fffe
 Access  : Manager

 Address : 2001:db8::214:c2ff:fe4c:e480
 Mask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
 Access  : Manager

 Address : 2001:db8::10
 Mask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00
 Access  : Operator
```

Figure 6-9. Example of "show ipv6 authorized-managers" Output

By analyzing the masks displayed in Figure 6-9, the following IPv6 stations are granted access:

Mask	Authorized IPv6 Addresses	Number of Authorized Addresses
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFC	2001:db8:0:7::4 through 2001:db8:0:7::7	4
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFE	2001:db8::a:1c:e3:2 and 2001:db8::a:1c:e3:3	2
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF	2001:db8::214:c2ff:fe4c:e480	1
FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FF00	2001:db8::0 through 2001:db8::FF	256

Figure 6-10. How Masks Determine Authorized IPv6 Manager Addresses

Additional Examples of Authorized IPv6 Managers Configuration

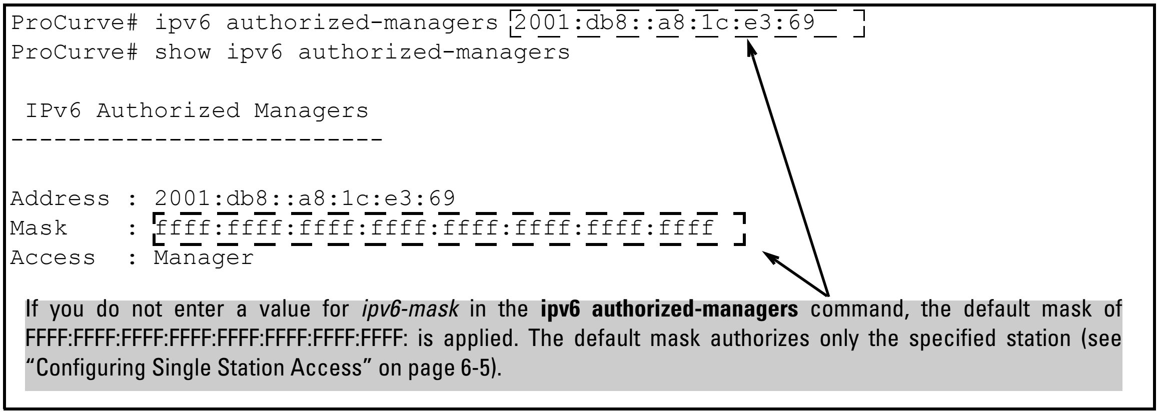
Authorizing Manager Access. The following IPv6 commands authorize manager-level access for one link-local station at a time. Note that when you enter a link-local IPv6 address with the **ipv6 authorized-managers** command, you must also enter a VLAN ID in the format: **%vlan**<*vlan-id*>.

```
ProCurve(config)# ipv6 authorized-managers
fe80::07be:44ff:fec5:c965%vlan2
```

```
ProCurve(config)# ipv6 authorized-managers
fe80::070a:294ff:fea4:733d%vlan2
```

```
ProCurve(config)# ipv6 authorized-managers
fe80::19af:2cff:fe34:b04a%vlan5
```

If you do not enter an *ipv6-mask* value when you configure an authorized IPv6 address, the switch automatically uses **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF** as the default IPv6 mask. Also, if you do not specify an **access** value to grant either Manager- or Operator-level access, by default, the switch assigns Manager access. For example:



```
ProCurve# ipv6 authorized-managers 2001:db8::a8:1c:e3:69
ProCurve# show ipv6 authorized-managers

 IPv6 Authorized Managers
--------------------------

Address : 2001:db8::a8:1c:e3:69
Mask    : ffff:ffff:ffff:ffff:ffff:ffff:ffff:ffff
Access  : Manager
```

If you do not enter a value for *ipv6-mask* in the **ipv6 authorized-managers** command, the default mask of FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF: is applied. The default mask authorizes only the specified station (see “Configuring Single Station Access” on page 6-5).

Figure 6-11. Default IPv6 Mask

The next IPv6 command authorizes operator-level access for sixty-four IPv6 stations: thirty-two stations in the subnets defined by 0x0006 and 0x0007 in the fourth block of an authorized IPv6 address:

```
ProCurve(config)# ipv6 authorized-managers
2001:db8:0000:0007:231:17ff:fec5:c967
ffff:ffff:ffff:fffe:ffff:ffff:ffff:ffe0 access operator
```

The following **ipv6 authorized-managers** command authorizes a single, automatically generated (EUI-64) IPv6 address with manager-level access privilege:

```
ProCurve(config)# ipv6 authorized-managers
::223:04ff:fe03:4501 ::ffff:ffff:ffff:ffff
```

Editing an Existing Authorized IP Manager Entry. To change the mask or access level for an existing authorized IP manager entry, enter the IPv6 address with the new value(s). Any parameters not included in the command are reset to their default values.

The following command replaces the existing mask and access level for IPv6 address 2001:DB8::231:17FF:FEC5:C967 with **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FF00** and **operator**:

```
ProCurve(config)# ipv6 authorized-managers
2001:db8::231:17ff:fec5:c967
ffff:ffff:ffff:ffff:ffff:ffff:ffff:ff00 access operator
```

The following command replaces the existing mask and access level for IPv6 address 2001:DB8::231:17FF:FEC5:3E61 with **FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF:FFFF** and **manager** (the default values). Note that it is not necessary to enter either of these parameters:

```
ProCurve(config)# ipv6 authorized-managers
2001:db8::a05b:17ff:fec5:3f61
```

Deleting an Authorized IP Manager Entry. Enter only the IPv6 address of the configured authorized IP manager station that you want to delete with the **no** form of the command; for example:

```
ProCurve(config)# no ipv6 authorized-managers
2001:db8::231:17ff:fec5:3e61
```

Secure Shell for IPv6

The Secure Shell (SSH) for IPv6 feature provides the same Telnet-like functions through encrypted, authenticated transactions as SSH for IPv4. SSH for IPv6 provides CLI (console) access and secure file transfer functionality. The following types of transactions are supported:

- Client public-key authentication

  Public keys from SSH clients are stored on the switch. Access to the switch is granted only to a client whose private key matches a stored public key.

- Password-only client authentication

  The switch is SSH-enabled but is not configured with the login method that authenticates a client's public-key. Instead, after the switch authenticates itself to a client, users connected to the client authenticate themselves to the switch by providing a valid password that matches the operator- and/or manager-level password configured and stored locally on the switch or on a RADIUS or TACACS+ server.

- Secure Copy (SCP) and Secure FTP (SFTP)

  You can use an SCP or SFTP client application to perform secure file transfers to and from the switch.

Configuring SSH for IPv6

By default, SSH is automatically enabled for IPv4 and IPv6 connections on a switch. As with SSH for IPv4, you can enter the **ip ssh** command to reconfigure the default SSH settings to:

- Restrict access to the SSH server running on the switch to only IPv4 or IPv6 clients.
- Modify the TCP port number and timeout period used in SSH authentication in IPv4 and IPv6 connections.

Syntax:. [no] ip ssh

Enables SSH on the switch and activates the connection with a configured SSH server (RADIUS or TACACS+). To disable SSH on the switch, enter the **no ip ssh** *command.*

[ip-version < 4 | 6 | 4or6 >]

IP version used for SSH connections on the switch:
4 *accepts SSH connections only from IPv4 clients.*
6 *accepts SSH connections only from IPv6 clients.*
4or6 *accepts SSH connections from either IPv4 or IPv6 clients. (Default:* **4or6***).*
To disable SSH connections with IPv4 clients, enter the **ip ssh ip-version 6** *command; to disable SSH connections with IPv6 clients, enter the* **ip ssh ip-version 4** *command.*

[port < 1-65535 | default >]

TCP port number used for SSH sessions in IPv4 and IPv6 connections (Default: 22).
Valid port numbers are from 1 to 65535, except for port numbers 23, 49, 80, 280,443, 1506, 1513 and 9999, which are reserved for other subsystems.

[timeout < 5 - 120 >]

Timeout value allowed to complete an SSH authentication and login on the switch (Default: 120 seconds).

[filetransfer]

Enables SSH on the switch to connect to an SCP or SFTP client application to transfer files to and from the switch over IPv4 or IPv6.
For more information, see "Secure Copy and Secure FTP for IPv6" on page 6-18.

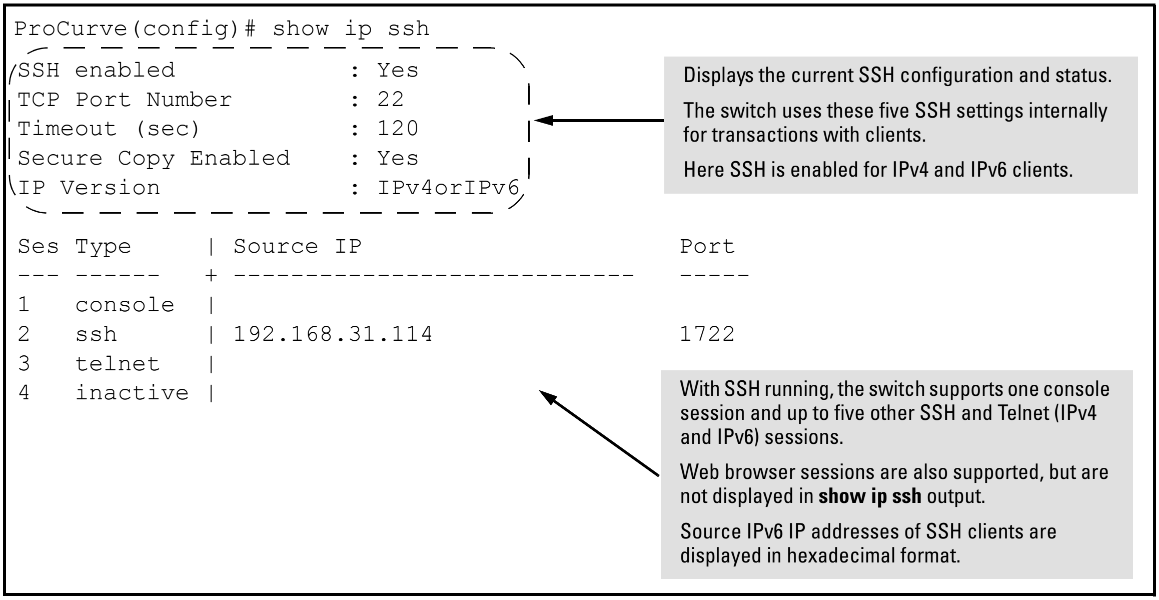
Note

As with IPv4, the switch only supports SSH version 2. You cannot set up an SSH session with a client device running SSH version 1.

For complete information on how to configure SSH for encrypted, authenticated transactions between the switch and SSH-enabled client devices, refer to the "*Configuring Secure Shell (SSH)*" chapter in the *Access Security Guide.*

Displaying an SSH Configuration

To verify an SSH for IPv6 configuration and display all SSH sessions running on the switch, enter the **show ip ssh** command. Information on all current SSH sessions (IPv4 and IPv6) is displayed.



```
ProCurve(config)# show ip ssh

 SSH enabled                 : Yes
 TCP Port Number             : 22
 Timeout (sec)               : 120
 Secure Copy Enabled         : Yes
 IP Version                  : IPv4orIPv6

 Ses Type     | Source IP                      Port
 --- ------   + ----------------------------   -----
 1   console  |
 2   ssh      | 192.168.31.114                 1722
 3   telnet   |
 4   inactive |
```

Displays the current SSH configuration and status.

The switch uses these five SSH settings internally for transactions with clients.

Here SSH is enabled for IPv4 and IPv6 clients.

With SSH running, the switch supports one console session and up to five other SSH and Telnet (IPv4 and IPv6) sessions.

Web browser sessions are also supported, but are not displayed in **show ip ssh** output.

Source IPv6 IP addresses of SSH clients are displayed in hexadecimal format.

Secure Copy and Secure FTP for IPv6

You can take advantage of the Secure Copy (SCP) and Secure FTP (SFTP) client applications to provide a secure alternative to TFTP for transferring sensitive switch information, such as configuration files and login information, between the switch and an administrator workstation.

SCP and SFTP run over an encrypted SSH session allowing you to use a secure SSH tunnel to:

- Transfer files and update ProCurve software images.
- Distribute new software images with automated scripts that make it easier to upgrade multiple switches simultaneously and securely.

By default, SSH is enabled for IPv4 and IPv6 connections on a switch. If you have not disabled SSH connections from IPv6 clients (by entering the **ip ssh ip-version 4** command), you can perform secure file transfers to and from IPv6 client devices by entering the **ip ssh filetransfer** command.

Syntax:. [no] ip ssh filetransfer

Enables SSH on the switch to connect to an SCP or SFTP client application to transfer files to and from the switch.

Use the **no ip ssh filetransfer** *command to disable the switch's ability to perform secure file transfers with an SCP or SFTP client, without disabling SSH on the switch.*

After an IPv6 client running SCP/SFTP successfully authenticates and opens an SSH session on the switch, you can copy files to and from the switch using secure, encrypted file transfers. Refer to the documentation that comes with an SCP or SFTP client application for information on the file transfer commands and software utilities to use.

Notes

The switch supports one SFTP session or one SCP session at a time.

All files on the switch have read-write permission. However, several SFTP commands, such as **create** or **remove**, are not supported and return an error message.

For complete information on how to configure SCP or SFTP in an SSH session to copy files to and from the switch, refer to the *"File Transfers"* appendix in the *Management and Configuration Guide* for your switch.