5

IPv6 Management Features

Contents

Introduction

Feature	Default	CLI
Neighbor Cache	n/a	5-3, 5-5
Telnet6	Enabled	5-6, 5-7, 5-8
SNTP Address	None	5-10
Timep Address	None	5-13
TFTP	n/a	5-15
SNMP Trap Receivers	None	5-21

This chapter focuses on the IPv6 application of management features in software release K.13.01 that support both IPv6 and IPv4 operation. For additional information on these features, refer to the current *Management and Configuration Guide* for your switch.

Viewing and Clearing the IPv6 Neighbors Cache

Neighbor discovery occurs when there is communication between the switch and another, reachable IPv6 device on the same VLAN. A neighbor destination is reachable from a given source address if a confirmation (neighbor solicitation) has been received at the source verifying that traffic has been received at the destination.

The switch maintains an IPv6 neighbor cache that is populated as a result of communication with other devices on the same VLAN. You can view and clear the contents of the neighbor cache using the commands described in this section.

Anycast Addresses. Multiple, duplicate addresses configured as Anycast on different devices are special cases of unicast addresses and are not identified as duplicates by the Neighbor Discovery process. Refer to “Anycast Addresses” on page 3-20.

Viewing the Neighbor Cache

Neighbor discovery occurs when there is communication between IPv6 devices on a VLAN. The Neighbor Cache retains data for a given neighbor until the entry times out. For more on this topic, refer to "Neighbor Discovery (ND)" on page 4-17.

Syntax: show ipv6 neighbors [vlan < *vid* >]

Displays IPv6 neighbor information currently held in the neighbor cache. After a period without communication with a given neighbor, the switch drops that neighbor's data from the cache. The command lists neighbors for all VLAN interfaces on the switch or for only the specified VLAN. The following fields are included for each entry in the cache:

IPv6 Address: *Lists the 128-bit addresses for the local host and any neighbors (on the same VLAN) with whom there has been recent communication.*

MAC Address: *The MAC Address corresponding to each of the listed IPv6 addresses.*

VLAN < ***vid*** **>:** *Optional. Causes the switch to list only the IPv6 neighbors on a specific VLAN configured on the switch.*

Type: *Appears only when VLAN is not specified, and indicates whether the corresponding address is* ***local*** *(configured on the switch) or* **dynamic** *(configured on a neighbor device).*

Age: *Appears only when VLAN is specified, and indicates the length of time the entry has remained unused.*

Port: *Identifies the switch port on which the entry was learned. If this field is empty for a given address, then the address is configured on the switch itself.*

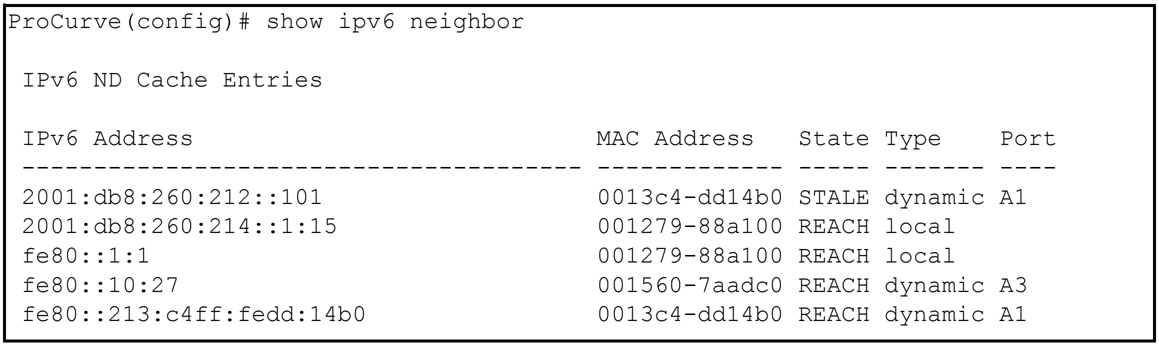
State: *A neighbor destination is reachable from a given source address if confirmation has been received at the source verifying that traffic has been received at the destination. This field shows the reachability status of each listed address:*

- **INCOM** (*Incomplete*): *Neighbor address resolution is in progress, but has not yet been determined.*
- **REACH** (*Reachable*): *The neighbor is known to have been reachable recently.*

— Continued on the next page. —

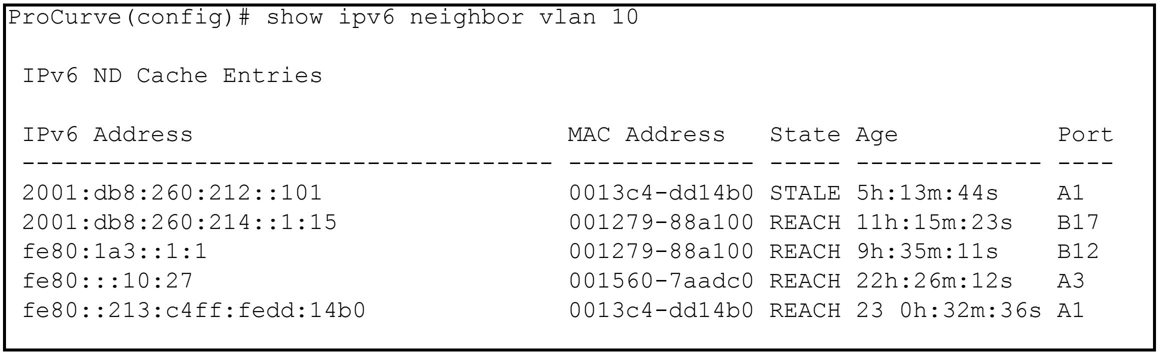
— Continued from previous page. —

- **STALE:** *A timeout has occurred for reachability of the neighbor, and an unsolicited discovery packet has been received from the neighbor address. If the path to the neighbor is then used successfully, this state is restored to* **REACH**.
- **DELAY:** *Indicates waiting for a response to traffic sent recently to the neighbor address. The time period for determining the neighbor's reachability has been extended.*
- **PROBE:** *The neighbor may not be reachable. Periodic, unicast neighbor solicitations are being sent to verify reachability.*



```
ProCurve(config)# show ipv6 neighbor

 IPv6 ND Cache Entries

 IPv6 Address                             MAC Address   State Type    Port
 ---------------------------------------- ------------- ----- ------- ----
 2001:db8:260:212::101                    0013c4-dd14b0 STALE dynamic A1
 2001:db8:260:214::1:15                   001279-88a100 REACH local
 fe80::1:1                                001279-88a100 REACH local
 fe80::10:27                              001560-7aadc0 REACH dynamic A3
 fe80::213:c4ff:fedd:14b0                 0013c4-dd14b0 REACH dynamic A1
```

Figure 5-1. Example of Neighbor Cache Without Specifying a VLAN



```
ProCurve(config)# show ipv6 neighbor vlan 10

 IPv6 ND Cache Entries

 IPv6 Address                           MAC Address   State Age           Port
 -------------------------------------- ------------- ----- ------------- ----
 2001:db8:260:212::101                  0013c4-dd14b0 STALE 5h:13m:44s    A1
 2001:db8:260:214::1:15                 001279-88a100 REACH 11h:15m:23s   B17
 fe80:1a3::1:1                          001279-88a100 REACH 9h:35m:11s    B12
 fe80:::10:27                           001560-7aadc0 REACH 22h:26m:12s   A3
 fe80::213:c4ff:fedd:14b0               0013c4-dd14b0 REACH 23 0h:32m:36s A1
```

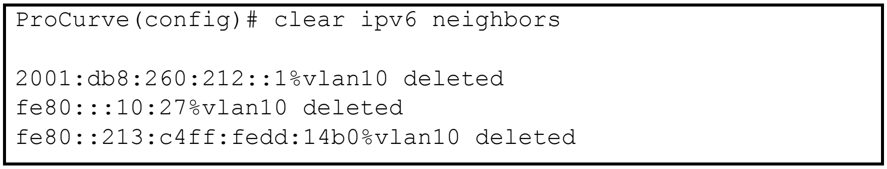
Figure 5-2. Example of Neighbor Cache Content for a Specific VLAN

Clearing the Neighbor Cache

When there is an event such as a topology change or an address change, the neighbor cache may have too many entries to allow efficient use. Also, if an unauthorized client is answering DAD or normal neighbor solicitations with invalid replies, the neighbor cache may contain a large number of invalid entries and communication with some valid hosts may fail and/or the **show ipv6 neighbors** command output may become too cluttered to efficiently read. In such cases, the fastest way to restore optimum traffic movement on a VLAN may be to statically clear the neighbor table instead of waiting for the unwanted entries to time-out.

Syntax: clear ipv6 neighbors

Executed at the global config level, this command removes all nonlocal IPv6 neighbor addresses and corresponding MAC addresses from the neighbor cache. (Local IPv6 addresses, that is, IPv6 addresses configured on the VLAN interface for the switch on which the command is executed, are not removed.) Removed addresses are listed in the command output.



```
ProCurve(config)# clear ipv6 neighbors

2001:db8:260:212::1%vlan10 deleted
fe80:::10:27%vlan10 deleted
fe80::213:c4ff:fedd:14b0%vlan10 deleted
```

Figure 5-3. Example of Clearing the IPv6 Neighbors Cache

Telnet6 Operation

This section describes Telnet operation for IPv6 on the switch. For IPv4 Telnet operation, refer to the *Management and Configuration Guide* for your switch.

Outbound Telnet6 to Another Device

Syntax: telnet < *link-local-addr* >%vlan< *vid* >
telnet < *global-unicast-addr* >

Outbound Telnet6 establishes a Telnet session from the switch CLI to another IPv6 device, and includes these options.

- *Telnet for Link-Local Addresses on the same VLAN requires the link-local address and and interface scope:*

  < *link-local-addr* >: *Specifies the link-local IPv6 address of the destination device.*

  %vlan< *vid* >: *Suffix specifying the interface on which the destination device is located. No spaces are allowed in the suffix.*

- *Telnet for Global Unicast Addresses requires a global unicast address for the destination. Also, the switch must be receiving router advertisements from an IPv6 gateway router.*

  < *global-unicast-addr* >: *Specifies the global IPv6 address of the destination device.*

For example, to Telnet to another IPv6 device having a link-local address of fe80::215:60ff:fe79:8980 and on the same VLAN interface (VLAN 10), you would use the following command:

```
ProCurve(config)# telnet fe80::215:60ff:fe79:980%vlan10
```

If the switch is receiving router advertisements from an IPv6 default gateway router, you can Telnet to a device on the same VLAN or another VLAN or subnet by using its global unicast address. For example, to Telnet to a device having an IPv6 global unicast address of 2001:db8::215:60ff:fe79:980, you would enter the following command:

```
ProCurve(config)# telnet 2001:db8::215:60ff:fe79:980
```

Viewing the Current Telnet Activity on a Switch

Syntax: show telnet

This command shows the active incoming and outgoing telnet sessions on the switch (for both IPv4 and IPv6). Command output includes the following:

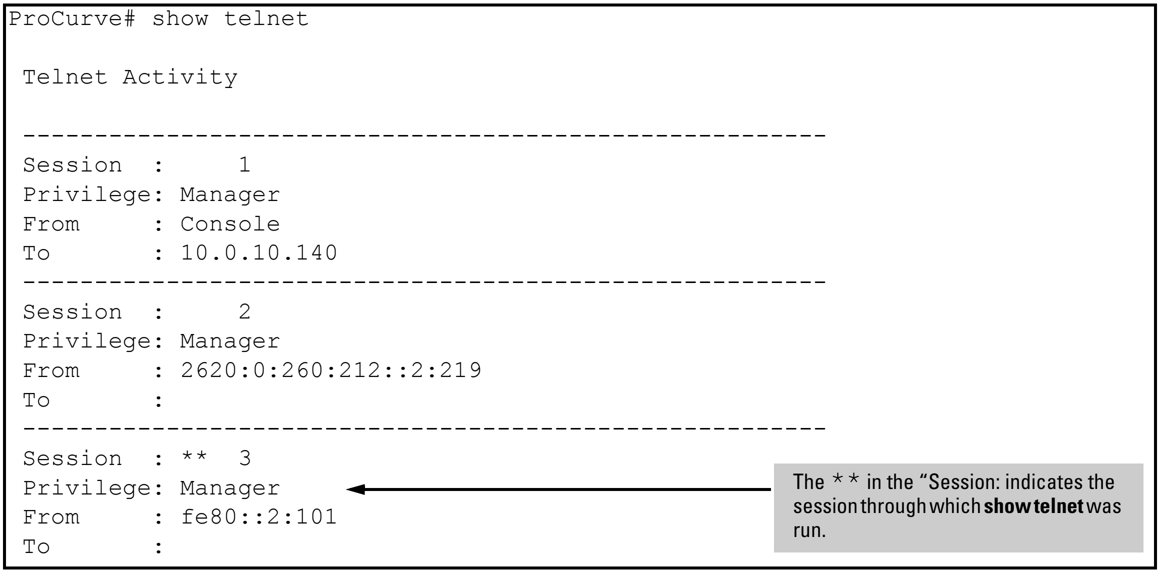
Session: *The session number. The switch allows one outbound session and up to five inbound sessions.*

Privilege: *Manager or Operator.*

From: *Console (for outbound sessions) or the source IP address of the inbound session.*

To: *The destination of the outbound session, if in use.*

For example, the following figure shows that the switch is running one outbound, IPv4 session and is being accessed by two inbound sessions.



```
ProCurve# show telnet

 Telnet Activity

 --------------------------------------------------------
 Session  :     1
 Privilege: Manager
 From     : Console
 To       : 10.0.10.140
 --------------------------------------------------------
 Session  :     2
 Privilege: Manager
 From     : 2620:0:260:212::2:219
 To       :
 --------------------------------------------------------
 Session  : **  3
 Privilege: Manager
 From     : fe80::2:101
 To       :
```

The ** in the "Session: indicates the session through which **show telnet** was run.

Figure 5-4. Example of Show Telnet Output with Three Sessions Active

Enabling or Disabling Inbound Telnet6 Access

Syntax: [no] telnet6-server

This command is used at the global config level to enable (the default) or disable inbound Telnet6 access to the switch.

The **no** *form of the command disables inbound telnet6.*

> ***Note:*** *To disable inbound Telnet access completely, you must disable Telnet access for both IPv6 and IPv4. (The command for disabling Telnet4 access is* **no telnet-server***.)*

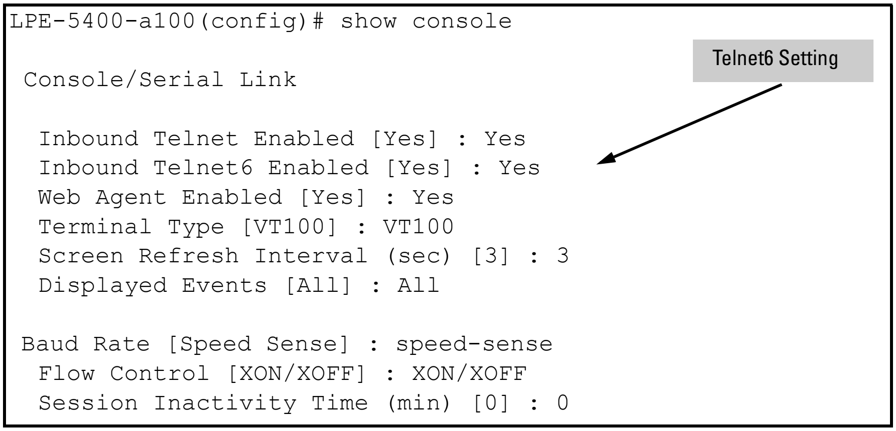
For example, to disable Telnet6 access to the switch, you would use this command:

```
ProCurve(config)# no telnet6-server
```

Viewing the Current Inbound Telnet6 Configuration

Syntax: show console

This command shows the current configuration of IPv4 and IPv6 inbound telnet permissions, as well as other information. For both protocols, the default setting allows inbound sessions.



```
LPE-5400-a100(config)# show console

 Console/Serial Link

  Inbound Telnet Enabled [Yes] : Yes
  Inbound Telnet6 Enabled [Yes] : Yes
  Web Agent Enabled [Yes] : Yes
  Terminal Type [VT100] : VT100
  Screen Refresh Interval (sec) [3] : 3
  Displayed Events [All] : All

 Baud Rate [Speed Sense] : speed-sense
  Flow Control [XON/XOFF] : XON/XOFF
  Session Inactivity Time (min) [0] : 0
```

Telnet6 Setting

Figure 5-5. Show Console Output Showing Default Console Configuration

SNTP and Timep

Configuring (Enabling or Disabling) the SNTP Mode

Software release K.13.01 enables configuration of a global unicast address for IPv6 SNTP time server.

This section lists the SNTP and related commands, including an example of using an IPv6 address. For the details of configuring SNTP on the switch, refer to the chapter titled "Time Protocols" in the *Management and Configuration Guide* for your switch.

The following commands are available at the global config level for SNTP operation.

Commands Affecting SNTP	Function
show sntp	Display the current SNTP configuration.
timesync < sntp | timep >	Enable either SNTP or Timep as the time synchronization method on the switch without affecting the configuration of either.
[no] timesync	Enable time synchronization. (Requires a timesync method to also be enabled.) The no version disable time synchronization without affecting the configuration of the current time synchronization method.)
[no]sntp	Enables SNTP with the current SNTP configuration. The no version disables SNTP without changing the current SNTP configuration.
sntp < unicast | broadcast >	Configures the SNTP mode. (Default: Broadcast)
sntp < 30 - 720 >	Changes the interval between time requests. (Default: 720 seconds)

Configuring an IPv6 Address for an SNTP Server

Note

To use a global unicast IPv6 address to configure an IPv6 SNTP time server on the switch, the switch must be receiving advertisements from an IPv6 router on a VLAN configured on the switch.

To use a link-local IPv6 address to configure an IPv6 SNTP time server on the switch, it is necessary to append **%vlan** followed immediately (without spaces) by the VLAN ID of the VLAN on which the server address is available. (The VLAN must be configured on the switch.) For example:

```
fe80::11:215%vlan10
```

Syntax:. [no] sntp server priority < 1 - 3 > < *link-local-addr* >%vlan< *vid* > [1 - 7]
[no] sntp server priority < 1 - 3 > < *global-unicast-addr* > [1 - 7]

Configures an IPv6 address for an SNTP server.

server priority < 1 - 3 >: *Specifies the priority of the server addressing being configured. When the SNTP mode is set to unicast and more than one server is configured, this value determines the order in which the configured servers will be accessed for a time value. The switch polls multiple servers in order until a response is received or all servers on the list have been tried without success. Up to three server addresses (IPv6 and/or IPv4) can be configured.*

< *link-local-addr* >: *Specifies the link-local IPv6 address of the destination device.*

%vlan< *vid* >: *Suffix specifying the interface on which the destination device is located. No spaces are allowed in the suffix.*

< *global-unicast-addr* >: *Specifies the global IPv6 address of the destination device.*

[1 - 7]: *This optional setting specifies the SNTP server version expected for the specified server. (Default: 3)*

For example, to configure link-local and global unicast SNTP server addresses of:

- fe80::215:60ff:fe7a:adc0 (on VLAN 10, configured on the switch)
- 2001:db8::215:60ff:fe79:8980

as the priority "1" and "2" SNTP servers, respectively, using version 7, you would enter these commands at the global config level, as shown below.

```
ProCurve(config)# sntp server priority 1
fe80::215:60ff:fe7a:adc0%vlan10 7

ProCurve(config)# sntp server priority 2
2001:db8::215:60ff:fe79:8980 7
```

Note

In the preceeding example, using a link-local address requires that you specify the local scope for the address; VLAN 10 in this case. This is always indicated by **%vlan** followed immediately (without spaces) by the VLAN identifier.

Syntax:. show sntp

Displays the current SNTP configuration, including the following:

Time Sync Mode: *Indicates whether timesync is disabled or set to either SNTP or Timep. (Default:* **timep***)*

SNTP Mode: *Indicates whether SNTP uses the broadcast or unicast method of contacting a time server. The broadcast option does not require you to configure a time server address. The unicast option does require configuration of a time server address.*

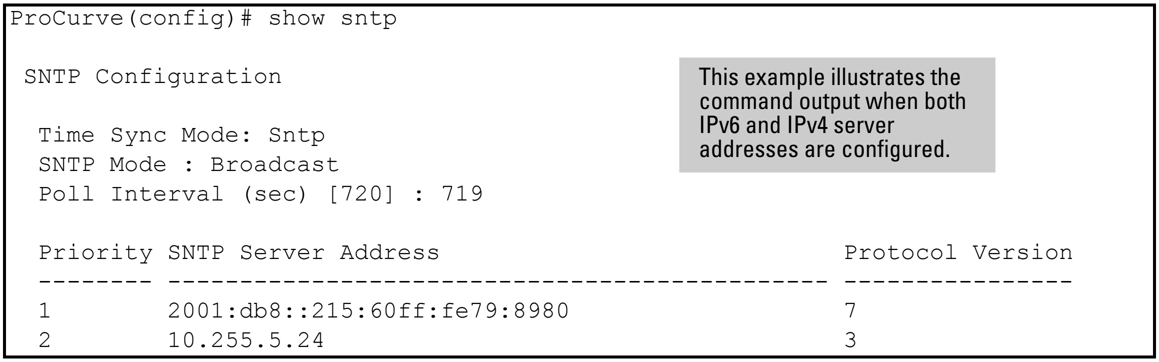
Poll Interval: *Indicates the interval between consecutive time requests to an SNTP server.*

Priority: *Indicates the configured priority for the corresponding SNTP server address.*

SNTP Server Address: *Lists the currently configured SNTP server addresses.*

Protocol Version: *Lists the SNTP server protocol version to expect from the server at the corresponding address.*

For example, the **show sntp** output for the preceeding **sntp server** command example would appear as follows:



```
ProCurve(config)# show sntp

 SNTP Configuration

  Time Sync Mode: Sntp
  SNTP Mode : Broadcast
  Poll Interval (sec) [720] : 719

  Priority SNTP Server Address                             Protocol Version
  -------- ----------------------------------------------- ----------------
  1        2001:db8::215:60ff:fe79:8980                    7
  2        10.255.5.24                                     3
```

This example illustrates the command output when both IPv6 and IPv4 server addresses are configured.

Figure 5-6. Example of Show SNTP Output with Both an IPv6 and an IPv4 Server Address Configured

Note that the **show management** command can also be used to display SNTP server information.

Configuring (Enabling or Disabling) the Timep Mode

Software release K.13.01 enables configuration of a global unicast address for IPv6 Timep time server.

This section lists the Timep and related commands, including an example of using an IPv6 address. For the details of configuring Timep on the switch, refer to the chapter titled "Time Protocols" in the *Management and Configuration Guide* for your switch.

The following commands are available at the global config level for Timep operation.

Commands Affecting Timep	**Function**
show timep	Display the current timep configuration.
timesync < sntp | timep >	Enable either SNTP or Timep as the time synchronization method on the switch without affecting the configuration of either.
ip timep dhcp [interval < 1 - 9999 >]	Enable Timep operation with a Timep server assignment configured from an IPv4 or IPv6 DHCP server. Optionally change the interval between time requests.

ip timep manual < *ipv6-addr* > [interval < 1 - 9999 >]	Enable Timep operation with a statically configured IPv6 address for a Timep server. Optionally change the interval between time requests.
no ip timep	Disables Timep operation. To re-enable Timep, it is necessary to reconfigure either the DHCP or the static option.

Note

To use a global unicast IPv6 address to configure an IPv6 Timep server on the switch, the switch must be receiving advertisements from an IPv6 router on a VLAN configured on the switch.

To use a link-local IPv6 address to configure an IPv6 Timep server on the switch, it is necessary to append **%vlan** followed (without spaces) by the VLAN ID of the VLAN on which the server address is available. The VLAN must be configured on the switch. For example: `fe80::11:215%vlan10`

Syntax:. ip timep dhcp [interval < 1 - 9999 >]
ip timep manual < *ipv6-addr* | *ipv4-addr* > [interval < 1 - 9999 >]

Used at the global config level to configure a Timep server address.

Note: *The switch allows one Timep server configuration.*

timep dhcp: *Configures the switch to obtain the address of a Timep server from an IPv4 or IPv6 DHCP server.*

timep manual: *Specifies static configuration of a Timep server address.*

< ***ipv6-addr*** **>**: *Specifies the IPv6 address of an SNTP server. Refer to preceeding* **Note**.

[Interval < 1 - 9999 >]: *This optional setting specifies the interval in minutes between Timep requests. (Default: 720)*

For example, to configure a link-local Timep server address of:

fe80::215:60ff:fe7a:adc0

where the address is on VLAN 10, configured on the switch, you would enter this command at the global config level, as shown below.

```
ProCurve(config)# ip timep manual
fe80::215:60ff:fe7a:adc0%vlan10
```

Note

In the preceeding example, using a link-local address requires that you specify the local scope for the address; VLAN 10 in this case. This is always indicated by **%vlan** followed immediately (without spaces) by the VLAN identifier. For a global unicast address, you would enter the address *without* the **%vlan** suffix.

Syntax:. show timep

Displays the current Timep configuration, including the following:

Time Sync Mode: *Indicates whether timesync is disabled or set to either SNTP or Timep. (Default: Disabled)*

Timep Mode: *Indicates whether Timep is configured to use a DHCP server to acquire a Timep server address or to use a statically configured Timep server address.*

Server Address: *Lists the currently configured Timep server address.*

Poll Interval (min) [720]: *Indicates the interval between consecutive time requests to the configured Timep server.*

For example, the **show timep** output for the preceeding **ip timep manual** command example would appear as follows:

```
ProCurve(config)# sho timep

 Timep Configuration

  Time Sync Mode: Timep
  TimeP Mode [Disabled] : Manual
  Server Address : fe80::215:60ff:fe7a:adc0%vlan10
  Poll Interval (min) [720] : 720
```

Figure 5-7. Example of Show Timep Output with an IPv6 Server Address Configured

Note that the **show management** command can also be used to display Timep server information.

TFTP File Transfers Over IPv6

TFTP File Transfers over IPv6

You can use TFTP **copy** commands over IPv6 to upload, or download files to and from a physically connected device or a remote TFTP server, including:

- Switch software
- Software images
- Switch configurations
- ACL command files
- Diagnostic data (crash data, crash log, and event log)

For complete information on how to configure TFTP file transfers between the switch and a TFTP server or other host device on the network, refer to the "File Transfers" appendix in the *Management and Configuration Guide* for your switch.

To upload and/or download files to the switch using TFTP in an IPv6 network, you must:

1. Enable TFTP for IPv6 on the switch (see "Enabling TFTP for IPv6" on page 5-16).
2. Enter a TFTP **copy** command with the IPv6 address of a TFTP server in the command syntax (see "Using TFTP to Copy Files over IPv6" on page 5-17).
3. (Optional) To enable auto-TFTP operation, enter the **auto-tftp** command (see "Using Auto-TFTP for IPv6" on page 5-19).

Enabling TFTP for IPv6

TFTP for IPv6 is enabled by default on the switch. However, if it is disabled, you can re-enable it by specifying TFTP client or server functionality with the **tftp6** <**client** | **server**> command. Enter the **tftp6** <**client** | **server**> command at the global configuration level.

Syntax: tftp6 <client | server>

Enables TFTP for IPv6 client or server functionality so that the switch can:

- *Use TFTP client functionality to access IPv6-based TFTP servers in the network to receive downloaded files.*
- *Use TFTP server functionality to be accessed by other IPv6 hosts to upload files to an IPv6 host.*

Usage Notes

To disable all TFTP client or server operation on the switch except for the auto-TFTP feature, enter the **no tftp6** <**client** | **server**> command. To re-enable TFTP client or server operation, re-enter the **tftp6** <**client** | **server**> command.

When TFTP is disabled, instances of TFTP in the CLI **copy** command and the Menu interface “Download OS” screen become unavailable.

The **no tftp6** <**client** | **server**> command does not disable auto-TFTP operation. For more information, see “Using Auto-TFTP for IPv6” on page 5-19.

Using TFTP to Copy Files over IPv6

Use the TFTP **copy** commands described in this section to:

- Download specified files from a TFTP server to a switch on which TFTP client functionality is enabled.
- Upload specified files from a switch, on which TFTP server functionality is enabled, to a TFTP server.

Syntax: copy tftp < *target* > < *ipv6-addr* > < *filename* >

Copies (downloads) a data file from a TFTP server at the specified IPv6 address to a target file on a switch that is enabled with TFTP server functionality.

< ***ipv6-addr*** **>**: *If this is a link-local address, use this IPv6 address format:*

fe80::< *device-id* >%vlan< *vid* >

For example: `fe80::123%vlan10`

If this is a global unicast or anycast address, use this IPv6 format:

< *ipv6-addr* >

For example: `2001:db8::123`

< ***target*** **>** *is one of the following values:*

- **autorun-cert-file**: Copies an autorun trusted certificate to the switch.
- **autorun-key-file**: Copies an autorun key file to the switch.
- **command-file**: Copies a file stored on a remote host and executes the ACL command script on the switch. Depending on the ACL commands stored in the file, one of the following actions is performed in the running-config file on the switch:
  - *A new ACL is created.*
  - *An existing ACL is replaced.*
  - **match**, **permit**, *or* **deny** *statements are added to an existing ACL.*

  For more information on ACLs, refer to "Creating an ACL Offline" in the Access Control Lists (ACLs) chapter in the Access Security Guide.
- **config <** ***filename*** **>**: *Copies the contents of a file on a remote host to a configuration file on the switch.*

- **flash** < **primary** | **secondary** >: *Copies a software file stored on a remote host to primary or secondary flash memory on the switch. To run a newly downloaded software image, enter the* **reload** *or* **boot system flash** *command.*
- **pub-key-file**: *Copies a public-key file to the switch.*
- **startup-config**: *Copies a configuration file on a remote host to the startup configuration file on the switch.*

.

Syntax: copy <*source* > tftp < *ipv6-addr* > < *filename* > < pc | unix >

Copies (uploads) a source data file on a switch that is enabled with TFTP server functionality to a file on the TFTP server at the specified IPv6 address, where <source> is one of the following values:

- **command-output < cli-command >**: *Copies the output of a CLI command to the specified file on a remote host.*
- **config <** ***filename*** **>:** *Copies the specified configuration file to a remote file on a TFTP server.*
- **crash-data < slot-id | master >:** *Copies the contents of the crash data file to the specified file path on a remote host. The crash data is software-specific and used to determine the cause of a system crash. You can copy crash information from an individual slot or from the master crash file on the switch.*
- **crash-log <** ***slot-id*** **| master >:** *Copies the contents of the crash log to the specified file path on a remote host. The crash log contains processor-specific operational data that is used to determine the cause of a system crash. You can copy the contents of the crash log from an individual slot or from the master crash log on the switch.*
- **event-log**: *Copies the contents of the Event Log on the switch to the specified file path on a remote host.*
- **flash < primary | secondary >:** *Copies the software file used as the primary or secondary flash image on the switch to a file on a remote host.*
- **startup-config**: *Copies the startup configuration file in flash memory to a remote file on a TFTP server.*
- **running-config**: *Copies the running configuration file to a remote file on a TFTP server.*

< *ipv6-addr* >: *If this is a link-local address, use this IPv6 address format:*

fe80::< *device-id* >%vlan< *vid* >

For example: `fe80::123%vlan10`

If this is a global unicast or anycast address, use this IPv6 format:

< *ipv6-addr* >

For example: `2001:db8::123`

Using Auto-TFTP for IPv6

The auto-TFTP for IPv6 feature automatically downloads a software image to a switch, on which TFTP client functionality is enabled, from a specified IPv6-based device at switch startup. You must reboot the switch to implement the downloaded software image by entering the **boot system flash primary** or **reload** command

Syntax: auto-tftp <*ipv6-addr*> <*filename*>

Configures the specified software file on the TFTP server at the specified IPv6 address to be automatically downloaded into primary flash memory at switch startup.

Note: *In order for the auto-TFTP feature to copy a software image to primary flash memory, the version number of the downloaded software file (for example, E.10.78) must be different from the version number of the primary flash image.*

The **no** *form of the command disables auto-TFTP operation. This command deletes the* **auto-tftp** *entry from the startup configuration, and prevents auto-tftp operation if the switch reboots.*

The **no auto-tftp** *command does not affect the current TFTP-enabled configuration on the switch.*

SNMP Management for IPv6

As with SNMP for IPv4, you can manage a switch via SNMP from an IPv6-based network management station by using an application such as ProCurve Manager (PCM) or ProCurve Manager Plus (PCM+). (For more on PCM and PCM+, go to the ProCurve Networking web site at **www.procurve.com**.)

SNMP Features Supported

The same SNMP for IPv4 features are supported over IPv6:

- access to a switch using SNMP version 1, version 2c, or version 3
- enhanced security with the configuration of SNMP communities and SNMPv3 user-specific authentication password and privacy (encryption) settings
- SNMP notifications, including:
  - SNMP version 1 or SNMP version 2c traps
  - SNMPv2c informs
  - SNMPv3 notification process, including traps
- Advanced RMON (Remote Monitoring) management
- ProCurve Manager or ProCurve Manager Plus management applications
- Flow sampling using sFlow
- Standard MIBs, such as the Bridge MIB (RFC 1493) and the Ethernet MAU MIB (RFC 1515)

SNMP Configuration Commands Supported

IPv6 addressing is supported in the following SNMP configuration commands: For more information on each SNMP configuration procedure, refer to the “Configuring for Network Management Applications” chapter in the current *Management and Configuration Guide* for your switch.

SNMPv1 and V2c

Syntax:. snmp-server host < *ipv4-addr* | *ipv6-addr* > < *community-name* >
[none | all | non-info | critical | debug] [inform [retries < *count* >]
[timeout < *interval* >]]

Executed at the global config level to configure an SNMP trap receiver to receive SNMPv1 and SNMPv2c traps, SNMPv2c informs, and (optionally) event log messages

SNMPv3

Syntax: snmpv3 targetaddress < *name* > params < *parms_name* >
<*ipv4-addr* | *ipv6-addr*>
[addr-mask < *ip4-addr* >]
[filter < none | debug | all | not-info | critical>]
[max-msg-size < 484-65535 >]
[port-mask < *tcp-udp port* >]
[retries < 0 - 255 >]
[taglist <*tag_name*>]
[timeout < 0 - 2147483647 >]
[udp-port *port-number*]

Executed at the global config level to configure an SNMPv3 management station to which notifications (traps and informs) are sent.

Note

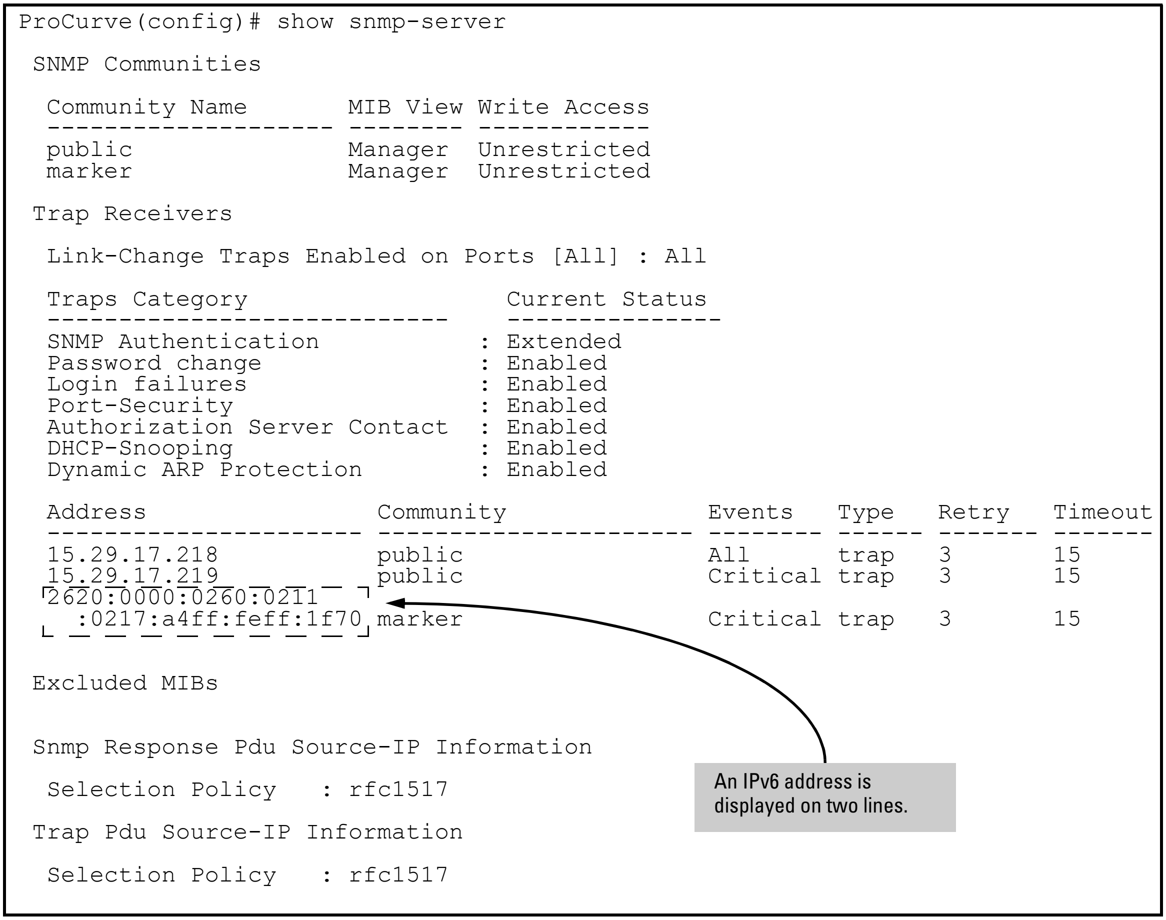
IPv6 is not supported in the configuration of an interface IPv6 address as the default source IP address used in the IP headers of SNMP notifications (traps and informs) or responses sent to SNMP requests. Only IPv4 addresses are supported in the following configuration commands:

snmp-server trap-source < *ipv4-addr* | loopback < 0-7 >>

snmp-server response-source [*dst-ip-of-request* | *ipv4-addr* | loopback < 0-7 >]

IPv6 addresses are supported in SNMP **show** command output as shown in Figure 5-8 and Figure 5-9.

The **show snmp-server** command displays the current SNMP policy configuration, including SNMP communities, network security notifications, link-change traps, trap receivers (including the IPv4 or IPv6 address) that can receive SNMPv1 and SNMPv2c traps, and the source IP (interface) address used in IP headers when sending SNMP notifications (traps and informs) or responses to SNMP requests.

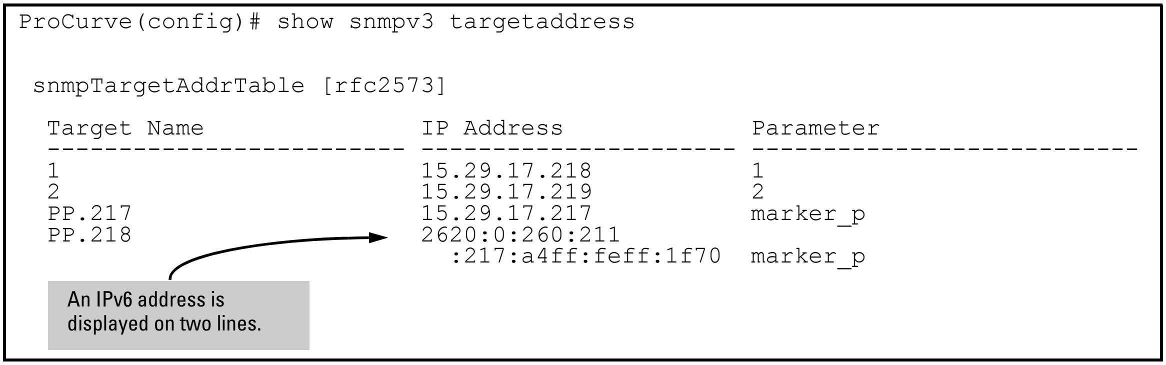


```
ProCurve(config)# show snmp-server

 SNMP Communities

  Community Name       MIB View Write Access
  -------------------- -------- ------------
  public               Manager  Unrestricted
  marker               Manager  Unrestricted

 Trap Receivers

  Link-Change Traps Enabled on Ports [All] : All

  Traps Category                  Current Status
  ----------------------------    ---------------
  SNMP Authentication           : Extended
  Password change               : Enabled
  Login failures                : Enabled
  Port-Security                 : Enabled
  Authorization Server Contact  : Enabled
  DHCP-Snooping                 : Enabled
  Dynamic ARP Protection        : Enabled

  Address                Community              Events   Type   Retry   Timeout
  ---------------------- ---------------------- -------- ------ ------- -------
  15.29.17.218           public                 All      trap   3       15
  15.29.17.219           public                 Critical trap   3       15
  2620:0000:0260:0211
    :0217:a4ff:feff:1f70 marker                 Critical trap   3       15

 Excluded MIBs


 Snmp Response Pdu Source-IP Information

  Selection Policy   : rfc1517

 Trap Pdu Source-IP Information

  Selection Policy   : rfc1517
```

An IPv6 address is displayed on two lines.

Figure 5-8. "show snmp-server" Command Output with IPv6 Address

The **show snmpv3 targetaddress** command displays the configuration (including the IPv4 or IPv6 address) of the SNMPv3 management stations to which notification messages are sent.



```
ProCurve(config)# show snmpv3 targetaddress


 snmpTargetAddrTable [rfc2573]

  Target Name                IP Address              Parameter
  -------------------------- ----------------------- ----------------------------
  1                          15.29.17.218            1
  2                          15.29.17.219            2
  PP.217                     15.29.17.217            marker_p
  PP.218                     2620:0:260:211
                               :217:a4ff:feff:1f70  marker_p
```

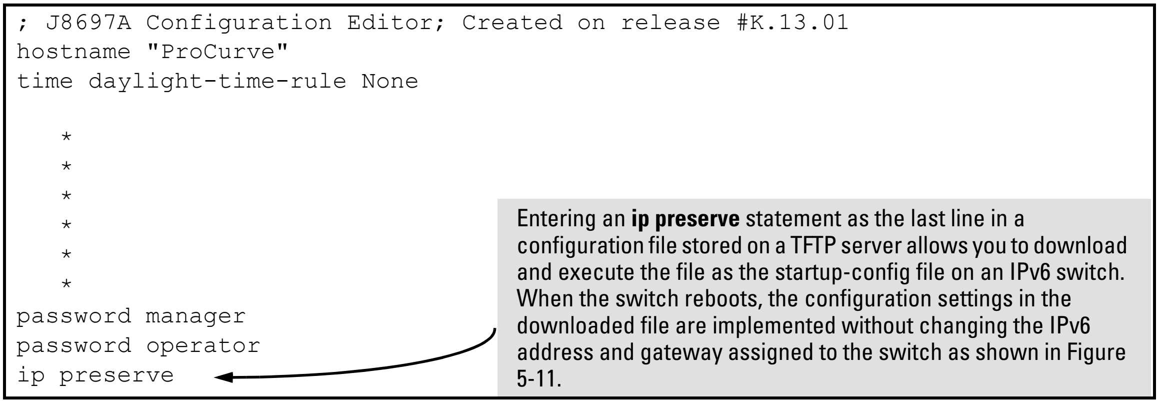
An IPv6 address is displayed on two lines.

Figure 5-9. "show snmpv3 targetaddress" Command Output with IPv6 Address

IP Preserve for IPv6

IPv6 supports the IP Preserve feature, which allows you to copy a configuration file from a TFTP server to multiple switches without overwriting the IPv6 address and subnet mask on VLAN 1 (default VLAN) in each switch, and the Gateway IPv6 address assigned to the switch.

To configure IP Preserve, enter the **ip preserve** statement at the end of the configuration file that will be downloaded from a TFTP server. (Note that you do not invoke IP Preserve by entering a command from the CLI).



```
; J8697A Configuration Editor; Created on release #K.13.01
hostname "ProCurve"
time daylight-time-rule None

   *
   *
   *
   *
   *
   *
password manager
password operator
ip preserve
```

Entering an **ip preserve** statement as the last line in a configuration file stored on a TFTP server allows you to download and execute the file as the startup-config file on an IPv6 switch. When the switch reboots, the configuration settings in the downloaded file are implemented without changing the IPv6 address and gateway assigned to the switch as shown in Figure 5-11.

Figure 5-10. Example of How to Enter IP Preserve in a Configuration File

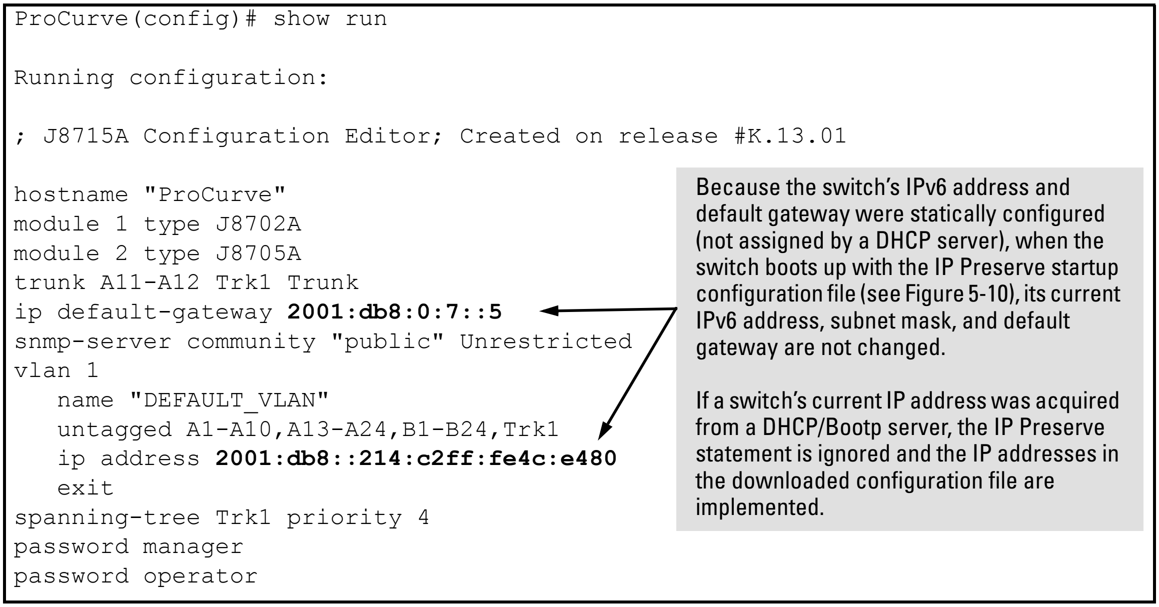
To download an IP Preserve configuration file to an IPv6-based switch, enter the TFTP **copy** command as described in "TFTP File Transfers over IPv6" on page 5-15 to copy the file as the new startup-config file on a switch.

When you download an IP Preserve configuration file, the following rules apply:

- If the switch's current IPv6 address for VLAN 1 was statically configured and not dynamically assigned by a DHCP/Bootp server, the switch reboots and retains its current IPv6 address, subnet mask, and gateway address. All other configuration settings in the downloaded configuration file are applied.
- If the switch's current IPv6 address for VLAN 1 was assigned from a DHCP server and not statically configured, IP Preserve is suspended. The IPv6 addressing specified in the downloaded configuration file is implemented when the switch copies the file and reboots.
  - If the downloaded file specifies DHCP/Bootp as the source for the IPv6 address of VLAN 1, the switch uses the IPv6 address assigned by the DHCP/Bootp server.
  - If the file specifies a dedicated IPv6 address and subnet mask for VLAN 1 and a Gateway IPv6 address, the switch implements these settings in the startup-config file.

To verify how IP Preserve was implemented in a switch, after the switch reboots, enter the **show run** command. Figure 5-11 shows an example in which all configurations settings have been copied into the startup-config file except for the IPv6 address of VLAN 1 (2001:db8::214:c2ff:fe4c:e480) and the default IPv6 gateway (2001:db8:0:7::5), which were retained.

Note that if a switch received its IPv6 address from a DHCP server, the “ip address” field under “vlan 1” would display: **dhcp-bootp**.



```
ProCurve(config)# show run

Running configuration:

; J8715A Configuration Editor; Created on release #K.13.01

hostname "ProCurve"
module 1 type J8702A
module 2 type J8705A
trunk A11-A12 Trk1 Trunk
ip default-gateway 2001:db8:0:7::5
snmp-server community "public" Unrestricted
vlan 1
   name "DEFAULT_VLAN"
   untagged A1-A10,A13-A24,B1-B24,Trk1
   ip address 2001:db8::214:c2ff:fe4c:e480
   exit
spanning-tree Trk1 priority 4
password manager
password operator
```

Because the switch’s IPv6 address and default gateway were statically configured (not assigned by a DHCP server), when the switch boots up with the IP Preserve startup configuration file (see Figure 5-10), its current IPv6 address, subnet mask, and default gateway are not changed.

If a switch’s current IP address was acquired from a DHCP/Bootp server, the IP Preserve statement is ignored and the IP addresses in the downloaded configuration file are implemented.

Figure 5-11. Configuration File with Dedicated IP Addressing After Startup with IP Preserve

For more information on how to use the IP Preserve feature, refer to the “Configuring IP Addressing” chapter in the current *Management and Configuration Guide* for your ProCurve switch.