aaa accounting

Configures RADIUS or TACACS+ accounting for recording information about user activity and system events. When you configure accounting on an HP device, information is sent to an accounting server when specified events occur, such as when a user logs into the device or the system is rebooted.

**EXAMPLE:**
To send an Accounting Start packet to a TACACS+ accounting server when an authenticated user establishes a Telnet or SSH session on the HP device, and an Accounting Stop packet when the user logs out:

```
ProCurveRS(config)# aaa accounting exec default start-stop tacacs+
```

**Syntax:**
```
[no] aaa accounting exec default start-stop radius | tacacs+ | none
```

You can configure accounting for CLI commands by specifying a privilege level whose commands require accounting. For example, to configure the HP device to perform RADIUS accounting for the commands available at the Super User privilege level (that is; all commands on the device), enter the following command:

```
ProCurveRS(config)# aaa accounting commands 0 default start-stop radius
```

**Syntax:**
```
[no] aaa accounting commands <privilege-level> default start-stop radius | tacacs+ | none
```

The `<privilege-level>` parameter can be one of the following:

- **0** – Records commands available at the Super User level (all commands)
- **4** – Records commands available at the Port Configuration level (port-config and read-only commands)
- **5** – Records commands available at the Read Only level (read-only commands)

You can configure accounting to record when system events occur on the HP device. System events include rebooting and when changes to the active configuration are made.

The following command causes an Accounting Start packet to be sent to a TACACS+ accounting server when a system event occurs, and an Accounting Stop packet to be sent when the system event is completed:

```
ProCurveRS(config)# aaa accounting system default start-stop tacacs+
```

**Syntax:**
```
[no] aaa accounting system default start-stop radius | tacacs+ | none
```

**Possible values:** see above

**Default value:** N/A

aaa authentication

Defines an authentication-method list for access to a Routing Switch.
EXAMPLE:
To configure an access method list, enter a command such as the following:

```
ProCurveRS(config)# aaa authentication web-server default local
```

This command configures the device to use the local user accounts to authenticate access to the device through the Web management interface. If the device does not have a user account that matches the user name and password entered by the user, the user is not granted access.

To configure the device to consult a RADIUS server first for Enable access, then consult the local user accounts if the RADIUS server is unavailable, enter the following command:

```
ProCurveRS(config)# aaa authentication enable default radius local
```

**Syntax:**
```
[no] aaa authentication snmp-server | web-server | enable | login | dot1x default <method1> [<method2>] [method3>][method4>][method5>][method6>][method7>]
```

**Syntax:**
```
aaa authentication login privilege-mode
```

The `snmp-server | web-server | enable | login | dot1x` parameter specifies the type of access this authentication-method list controls. You can configure one authentication-method list for each type of access.

The `aaa authentication login privilege-mode` command configures the device so that a user enters Privileged EXEC mode after a Telnet or SSH login.

**NOTE:**
- TACACS/TACACS+ is supported only for enable and login. RADIUS is supported only for enable, login, and dot1x.

The `<method1>` parameter specifies the primary authentication method. The remaining optional `<method>` parameters specify the secondary methods to try if an error occurs with the primary method. A method can be one of the values listed in the Method Value column in the following table.

<table>
<thead>
<tr>
<th>Method Value</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>tacacs</td>
<td>A TACACS/TACACS+ server. You can use either parameter. Each parameter supports both TACACS and TACACS+. You also must identify the server to the device using the <code>tacacs-server</code> command.</td>
</tr>
<tr>
<td>or tacacs+</td>
<td></td>
</tr>
<tr>
<td>radius</td>
<td>A RADIUS server. You also must identify the server to the device using the <code>radius-server</code> command.</td>
</tr>
<tr>
<td>local</td>
<td>A local user name and password you configured on the device. Local user names and passwords are configured using the <code>username...</code> command.</td>
</tr>
<tr>
<td>line</td>
<td>The password you configured for Telnet access. The Telnet password is configured using the <code>enable telnet password...</code> command.</td>
</tr>
<tr>
<td>enable</td>
<td>The super-user &quot;enable&quot; password you configured on the device. The enable password is configured using the <code>enable super-user-password...</code> command.</td>
</tr>
<tr>
<td>none</td>
<td>No authentication is used. The device automatically permits access.</td>
</tr>
</tbody>
</table>

**Possible values:** see above

**Default value:** N/A
aaa authorization

Configures authorization for controlling access to management functions in the CLI. HP devices support RADIUS and TACACS+ authorization.

- When RADIUS authorization is enabled, the HP device consults the list of commands supplied by the RADIUS server during authentication to determine whether a user can execute a command he or she has entered.
- Two kinds of TACACS+ authorization are supported: Exec authorization determines a user's privilege level when they are authenticated; Command authorization consults a TACACS+ server to get authorization for commands entered by the user

**EXAMPLE:**
You enable command authorization by specifying a privilege level whose commands require authorization. For example, to configure the HP device to perform RADIUS authorization for the commands available at the Super User privilege level (that is; all commands on the device), enter the following command:

`ProCurveRS(config)# aaa authorization commands 0 default radius`

**Syntax:** [no] aaa authorization commands <privilege-level> default tacacs+ | radius | none

The <privilege-level> parameter can be one of the following:

- **0** – Authorization is performed for commands available at the Super User level (all commands)
- **4** – Authorization is performed for commands available at the Port Configuration level (port-config and read-only commands)
- **5** – Authorization is performed for commands available at the Read Only level (read-only commands)

**NOTE:** TACACS+ and RADIUS command authorization is performed only for commands entered from Telnet, SSH, or console sessions. No authorization is performed for commands entered using the Web management interface.

**NOTE:** Since RADIUS authorization relies on the command list supplied by the RADIUS server during authentication, you cannot perform RADIUS authorization without RADIUS authentication.

When TACACS+ exec authorization is configured, the HP device consults a TACACS+ server to determine the privilege level for an authenticated user. To configure TACACS+ exec authorization, on the HP device, enter the following command:

`ProCurveRS(config)# aaa authorization exec default tacacs+`

**Syntax:** [no] aaa authorization exec default tacacs+ | none

**Possible values:** see above

**Default value:** N/A

access-list delete

Deletes a specific ACL entry or comment from anywhere in the extended ACL. This command is available on devices running Enterprise software release 07.8.00 and later.

`ProCurveRS(config)# access-list 99 delete 2`

**Syntax:** access-list <acl-number> delete <line-number> [remark ]

The <line-number> parameter specifies the ACL entry to be deleted. The <acl-num> parameter allows you to specify an ACL number if you prefer. If you specify a number, enter a number from 1 – 99 for standard ACLs or 100 – 199 for extended ACLs.

Use the **remark** parameter to delete the comment for the specified ACL entry.

**Possible values:** See above
Default value: N/A

**access-list deny (extended)**

Configures extended ACLs that deny packets based on the following information:

- IP protocol
- Source IP address or host name
- Destination IP address or host name
- Source TCP or UDP port (if the IP protocol is TCP or UDP)
- Destination TCP or UDP port (if the IP protocol is TCP or UDP)

**EXAMPLE:**

```
ProCurveRS(config)# access-list 101 deny tcp host 209.157.22.26 any eq telnet log
ProCurveRS(config)# access-list 101 permit ip any any
ProCurveRS(config)# int eth 1/1
ProCurveRS(config-if-1/1)# ip access-group 101 in
ProCurveRS(config)# write memory
```

**Syntax:**

```
[no] access-list <num> deny <ip-protocol> <source-ip-address>/<subnet-mask> | any | host <source-host-ip-address> | host <source-hostname> <wildcard> 
<operator> <source-udp-port> 
<destination-ip-address>/<subnet-mask> | any | host <destination-host-ip-address> | host <destination-hostname> <wildcard> 
<operator> <destination-udp-port> 
<icmp-type> | <icmp-type-number> | <icmp-code-number> 
[dscp-cos-mapping] 
[dscp-marking <dscp-value> 802.1p-priority-marking <0 – 7> internal priority-marking <0 – 7>] 
[dscp-marking <dscp-value> dscp-cos-mapping] 
[dscp-marking <dscp-value>] 
[established] 
[ip-pkt-len <value>] 
[log] 
[precedence <name> | <num>] 
[tos <num>] 
[priority 0 | 1 | 2 | 3] 
[priority-force 0 | 1 | 2 | 3] 
[priority-mapping <8021p-value>] 
```

The `<num>` parameter indicates the ACL number and can be from 100 – 199 for an extended ACL.
The **deny** parameter drops the traffic that matches the policy.

The **ip-protocol** parameter indicates the type of IP packet you are filtering. In release 07.6.01b and later, you can specify a well-known name for any protocol whose number is less than 255. For other protocols, you must enter the number. Enter "?” instead of a protocol to list the well-known names recognized by the CLI.

The **source-ip-address** parameter specifies the source IP address to be matched. If you want the policy to match on all source addresses, enter **any**. You can also enter **host** and the IP address or name of the source host.

The **wildcard** parameter specifies the portion of the source address to match against. The **wildcard** is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet’s source address must match the **source-ip**. Ones mean any value matches. For example, the **source-ip** and **wildcard** values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in Classless Interdomain Routing (CIDR) format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of "209.157.22.26 0.0.0.255" as "209.157.22.26/24".
NOTE: When you save ACL policies to the startup-config file, the software changes your IP address values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 (if you have enabled display of sub-net lengths) or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in “/<mask-bits>” format. To enable the software to display the CIDR masks, enter the `ip show-subnet-length` command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

NOTE: If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the `show ip access-list` command.

The `<destination-ip-address>` parameter specifies the destination address to be matched. If you want the policy to match on all destination addresses, enter `any`. You can also enter `host` and enter the IP address or name of the destination host.

The `<operator>` parameter specifies a comparison operator for the TCP or UDP port number. This parameter applies only when you specify “tcp” or “udp” as the IP protocol. For example, if you are configuring an entry for HTTP, specify `tcp eq http`. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after `eq`.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after `gt`.
- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after `lt`.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after `neq`.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: `range 23 53`. The first port number in the range must be lower than the last number in the range.
- **established** – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to “1”) in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, “Header Format”, in RFC 793 for information about this field.

NOTE: This operator applies only to destination TCP ports, not source TCP ports.

The `<tcp/udp-port>` parameter specifies the TCP or UDP port number or well-known name. In release 07.6.01b and later, you can specify a well-known name for any application port whose number is less than 1024. For other application ports, you must enter the number. Enter “?” instead of a port to list the well-known names recognized by the CLI.

The `<icmp-type>` parameter specifies the ICMP protocol type if you specified “icmp” for `<ip-protocol>`. The parameter is supported in Enterprise software release 07.2.06 and later. It can have one of the following values, depending on the software version the device is running:

- `any-icmp-type`
- `echo`
- `echo-reply`
- `information-request`
- `log`
- mask-reply
- mask-request
- parameter-problem
- redirect
- source-quench
- time-exceeded
- timestamp-reply
- timestamp-request
- unreachable
- <num>

The <num> parameter can be a value from 0 – 255. If you do not specify a message type, the ACL applies to all types of ICMP messages.

Devices running Enterprise software release 07.8.00 and later can specify the <icmp-type-number> <icmp-code-number> instead of the <icmp-type>. The valid <type-number> and <code-number> combinations are listed in Table 6.2.

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>Type Number</th>
<th>Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>administratively-prohibited</td>
<td>3</td>
<td>13</td>
</tr>
<tr>
<td>any-icmp-type</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>destination-host-prohibited</td>
<td>3</td>
<td>10</td>
</tr>
<tr>
<td>destination-host-unknown</td>
<td>3</td>
<td>7</td>
</tr>
<tr>
<td>destination-net-prohibited</td>
<td>3</td>
<td>9</td>
</tr>
<tr>
<td>destination-network-unknown</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>echo</td>
<td>8</td>
<td>0</td>
</tr>
<tr>
<td>echo-reply</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>general-parameter-problem</td>
<td>12</td>
<td>1</td>
</tr>
</tbody>
</table>

**Note:** This message type indicates that required option is missing.

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>Type Number</th>
<th>Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>host-precedence-violation</td>
<td>3</td>
<td>14</td>
</tr>
<tr>
<td>host-redirect</td>
<td>5</td>
<td>1</td>
</tr>
<tr>
<td>host-tos-redirect</td>
<td>5</td>
<td>3</td>
</tr>
<tr>
<td>host-tos-unreachable</td>
<td>3</td>
<td>12</td>
</tr>
<tr>
<td>host-unreachable</td>
<td>3</td>
<td>1</td>
</tr>
<tr>
<td>information-request</td>
<td>15</td>
<td>0</td>
</tr>
<tr>
<td>log</td>
<td></td>
<td></td>
</tr>
<tr>
<td>mask-reply</td>
<td>18</td>
<td>0</td>
</tr>
</tbody>
</table>
### Table 6.2: ICMP Message Types and Codes

<table>
<thead>
<tr>
<th>ICMP Message Type</th>
<th>Type Number</th>
<th>Code Number</th>
</tr>
</thead>
<tbody>
<tr>
<td>mask-request</td>
<td>17</td>
<td>0</td>
</tr>
<tr>
<td>net-redirect</td>
<td>5</td>
<td>0</td>
</tr>
<tr>
<td>net-tos-redirect</td>
<td>5</td>
<td>2</td>
</tr>
<tr>
<td>net-tos-unreachable</td>
<td>3</td>
<td>11</td>
</tr>
<tr>
<td>net-unreachable</td>
<td>3</td>
<td>0</td>
</tr>
<tr>
<td>packet-too-big</td>
<td>3</td>
<td>4</td>
</tr>
<tr>
<td>parameter-problem</td>
<td>12</td>
<td>0</td>
</tr>
<tr>
<td><strong>Note:</strong> This message includes all parameter problems</td>
<td></td>
<td></td>
</tr>
<tr>
<td>port-unreachable</td>
<td>3</td>
<td>3</td>
</tr>
<tr>
<td>precedence-cutoff</td>
<td>3</td>
<td>15</td>
</tr>
<tr>
<td>protocol-unreachable</td>
<td>3</td>
<td>2</td>
</tr>
<tr>
<td>reassembly-timeout</td>
<td>11</td>
<td>1</td>
</tr>
<tr>
<td>redirect</td>
<td>5</td>
<td>x</td>
</tr>
<tr>
<td><strong>Note:</strong> This includes all redirects.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>router-advertisement</td>
<td>9</td>
<td>0</td>
</tr>
<tr>
<td>router-solicitation</td>
<td>10</td>
<td>0</td>
</tr>
<tr>
<td>source-host-isolated</td>
<td>3</td>
<td>8</td>
</tr>
<tr>
<td>source-quench</td>
<td>4</td>
<td>0</td>
</tr>
<tr>
<td>source-route-failed</td>
<td>3</td>
<td>5</td>
</tr>
<tr>
<td>time-exceeded</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>timestamp-reply</td>
<td>14</td>
<td>0</td>
</tr>
<tr>
<td>timestamp-request</td>
<td>13</td>
<td>0</td>
</tr>
<tr>
<td>ttl-exceeded</td>
<td>11</td>
<td>0</td>
</tr>
<tr>
<td>unreachable</td>
<td>3</td>
<td>x</td>
</tr>
<tr>
<td><strong>Note:</strong> This includes all unreachable messages</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

The **dscp-marking** `<dscp-value>` parameter maps a DSCP value to an internal forwarding priority. The DSCP value can be from 0 – 63.

**NOTE:** The **Internal priority-marking** and **dscp-cos-mapping** parameters override port-based priority settings.

The **dscp-mapping** `<dscp-value>` parameter matches on the packet’s DSCP value.

**NOTE:** This option does not change the packet’s priority through the device or mark the packet.
The **established** parameter applies only to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

The **ip-pkt-len <value>** parameter enables you to filter ICMP packets based on the IP packet length. This parameter matches on the total length field in the IP header of ICMP packets. The IP packet length value can be from 1 -65535.

**NOTE:** This parameter is supported in software release 07.7.00 and later, and applies only if you specified **icmp** as the **<ip-protocol>** value.

The **log** parameter enables SNMP traps and Syslog messages for packets denied by the ACL.

The **precedence <name> | <num>** parameter of the **ip access-list** command specifies the IP precedence. The **precedence** option for an IP packet is set in a three-bit field following the four-bit header-length field of the packet's header. You can specify one of the following:

- **critical** or 5 – The ACL matches packets that have the critical precedence. If you specify the option number instead of the name, specify number 5.
- **flash** or 3 – The ACL matches packets that have the flash precedence. If you specify the option number instead of the name, specify number 3.
- **flash-override** or 4 – The ACL matches packets that have the flash override precedence. If you specify the option number instead of the name, specify number 4.
- **immediate** or 2 – The ACL matches packets that have the immediate precedence. If you specify the option number instead of the name, specify number 2.
- **internet** or 6 – The ACL matches packets that have the internetwork control precedence. If you specify the option number instead of the name, specify number 6.
- **network** or 7 – The ACL matches packets that have the network control precedence. If you specify the option number instead of the name, specify number 7.
- **priority** or 1 – The ACL matches packets that have the priority precedence. If you specify the option number instead of the name, specify number 1.
- **routine** or 0 – The ACL matches packets that have the routine precedence. If you specify the option number instead of the name, specify number 0.

You can specify one of the following:

- **max-reliability** or 2 – The ACL matches packets that have the maximum reliability ToS. The decimal value for this option is 2.
- **max-throughput** or 4 – The ACL matches packets that have the maximum throughput ToS. The decimal value for this option is 4.
- **min-delay** or 8 – The ACL matches packets that have the minimum delay ToS. The decimal value for this option is 8.
- **min-monetary-cost** or 1 – The ACL matches packets that have the minimum monetary cost ToS. The decimal value for this option is 1.

**NOTE:** This value is not supported on and 10 Gigabit Ethernet modules

- **normal** or 0 – The ACL matches packets that have the normal ToS. The decimal value for this option is 0.
- **<num>** – A number from 0 – 15 that is the sum of the numeric values of the options you want. The ToS field is a four-bit field following the Precedence field in the IP header. You can specify one or more of the following. To select more than one option, enter the decimal value that is equivalent to the sum of the numeric values of all the ToS options you want to select. For example, to select the **max-reliability** and **min-delay** options, enter number 10. To select all options, select 15.
The **priority** option enables you to assign traffic that matches the ACL to a specific hardware forwarding queue (qosp0, qosp1, qosp2, or qosp3). The **0 | 1 | 2 | 3** parameter specifies the QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

**NOTE:** This **priority** option provides the same function as the Layer 4 IP access policies supported on 9300 series Chassis devices. If you configure both a Layer 4 IP access policy and an extended ACL to set the hardware forwarding priority for the same traffic, the device uses the ACL instead of the IP access policy.

The **priority-force** parameter allows you assign packets of outgoing traffic that match the ACL to a specific hardware forwarding queue, even though the incoming packet may be assigned to another queue. Specify one of the following QoS queue:

- 0 – qosp0
- 1 – qosp1
- 2 – qosp2
- 3 – qosp3

The **priority-mapping** `<8021p-value>` parameter matches on the packet's 802.1p priority.

**NOTE:** This option does not change the packet's priority through the device or mark the packet. This option is not supported on 10 Gigabit Ethernet modules.

The **tos** `<name> | <num>` parameter of the **ip access-list** command specifies the IP ToS.

**access-list deny (standard)**

Creates standard ACLs that deny packets based on source IP address. You can configure up to 99 standard ACLs. You can configure up to 1024 individual ACL entries. There is no limit to the number of ACL entries an ACL can contain except for the system-wide limitation of 1024 total ACL entries.

Starting in software release 07.6.04, you can use standard ACLs to control the following multicast features:

- Limit the number of multicast groups that are covered by a static rendezvous point (RP). See "rp-address" on page 24-5.
- Control which multicast groups for which candidate RPs sends advertisement messages to bootstrap routers. See "rp-candidate" on page 24-6.
- Identify which multicast group packets will be forwarded or blocked on an interface. See "ip multicast boundary" on page 8-20.

**EXAMPLE:**

To configure a standard ACL and apply it to outgoing traffic on port 1/1, enter the following commands.

```
ProCurveRS(config)# access-list 1 deny host IPHost1 log
ProCurveRS(config)# access-list 1 permit any
ProCurveRS(config)# int eth 1/1
ProCurveRS(config-if-1/1)# ip access-group 1 out
ProCurveRS(config-if-1/1)# write memory
```

The last ACL entry in this ACL permits all packets that are not explicitly denied by the ACL entry.

**Syntax:** [no] access-list <num> deny <source-ip-address> | any | host <ip-address> | host <hostname> | <wildcard> | [log]
The `<num>` parameter is the access list number and can be from 1 – 99.

The `deny` parameter allows packets that match a policy.

The `<source-ip-address>` parameter specifies the source IP address. Alternatively, you can specify the host name.

**NOTE:** To specify the host name instead of the IP address, the host name must be configured using the HP device's DNS resolver. To configure the DNS resolver name, use the `ip dns server-address` command at the global CONFIG level of the CLI.

The `<wildcard>` parameter specifies the mask value to compare against the host address specified by the `<source-ip>` parameter. The `<wildcard>` is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet's source address must match the `<source-ip>`. Ones mean any value matches. For example, the `<source-ip>` and `<wildcard>` values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in CIDR format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of “209.157.22.26 0.0.0.255” as “209.157.22.26/24”.

**NOTE:** When you save ACL policies to the startup-config file, the software changes your `<source-ip>` values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 if you have enabled display of sub-net lengths or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in “/<mask-bits>” format. To enable the software to display the CIDR masks, enter the `ip show-subnet-length` command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

**NOTE:** If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the `show ip access-list` command.

The `host <source-ip> | host <hostname>` parameter lets you specify a host IP address or name. When you use this parameter, you do not need to specify the mask. A mask of all zeros (0.0.0.0) is implied.

The `any` parameter configures the policy to match on all host addresses.

The `log` argument configures the device to generate Syslog entries and SNMP traps for packets that are permitted or denied by the access policy.

Apply the ACL to a port and specify if it is for incoming or outgoing traffic using the “ip access-group” on page 8-7.

**Possible values:** See above

**Default value:** N/A

### access-list insert

Inserts a new ACL entry or a remark into a specific order in an ACL. After the new entry is inserted, the ACL list is renumbered. This command is available on devices running Enterprise software release 07.8.00 and later.

```
ProCurveRS(config)# access-list 99 insert 2 deny 5.6.7.8
```

**Syntax:** `access-list <acl-number> insert <line-number> deny <options> | permit <options> | remark <comment-text>`

The `<acl-num>` parameter identifies the numbered ACL into which the new entry will be inserted. This number can be from 1 - 99 for standard ACLs or from 100 - 199 for extended ACLs.

The `insert` `<line-num>` parameter indicates where the new ACL entry will be inserted. After the new entry is inserted, the ACL list is renumbered.
Use the `deny <options>` parameter if you want to create a filter that blocks traffic. See the “access-list deny (extended)” on page 6-4 and “access-list deny (standard)” on page 6-9 command for <options> you can use to deny the traffic.

Use the `permit <options>` parameter if you want to create a filter that allows traffic. See the “access-list permit (extended)” on page 6-11 and “access-list permit (extended)” on page 6-11 command for <options> you can use to allow the traffic.

Use the `remark <comment-text>` to replace the comment to the ACL entry. The remark can have up to 128 characters in length.

**Possible values:** See above

**Default value:** N/A

### access-list permit (extended)

Configures extended ACLs that permit packets based on the following information:

- IP protocol
- Source IP address or host name
- Destination IP address or host name
- Source TCP or UDP port (if the IP protocol is TCP or UDP)
- Destination TCP or UDP port (if the IP protocol is TCP or UDP)

#### EXAMPLE:

```plaintext
ProCurveRS(config)# access-list 101 permit tcp host 209.157.22.26 any eq telnet log
ProCurveRS(config)# access-list 101 permit ip any any
ProCurveRS(config)# int eth 1/1
ProCurveRS(config-if-1/1)# ip access-group 101 in
ProCurveRS(config)# write memory
```

**Syntax:**

```
[no] access-list <num> permit <ip-protocol> <source-ip-address>[/<subnet-mask>] | any | host <source-host-ip-address> | host <source-hostname> <wildcard>
[<operator> <source-tcp/udp-port>]
<destination-ip-address>[/<subnet-mask>] | any | host <destination-host-ip-address> | host <destination-hostname> <wildcard>
[<operator> <destination-tcp/udp-port>]
[<icmp-type> | <icmp-type-number> | <icmp-code-number>]
[dscp-cos-mapping]
[dscp-marking <dscp-value> 802.1p-priority-marking <0 – 7> internal priority-marking <0 – 7>]
[dscp-marking <dscp-value> dscp-cos-mapping]
[dscp-mapping <dscp-value>]
[established]
[ip-pkt-len <value>]
[log]
[precedence <name> | <num>]
[tos <num>]
[priority 0 | 1 | 2 | 3]
[priority-force 0 | 1 | 2 | 3]
[priority-mapping <8021p-value>]
```

The <num> parameter indicates the ACL number and can be from 100 – 199 for an extended ACL.

The `permit` parameter allows the traffic that matches the policy.

The `<ip-protocol>` parameter indicates the type of IP packet you are filtering. In release 07.6.01b and later, you can specify a well-known name for any protocol whose number is less than 255. For other protocols, you must enter the number. Enter “?” instead of a protocol to list the well-known names recognized by the CLI.
The `<source-ip-address>` parameter specifies the source IP address to be matched. If you want the policy to match on all source addresses, enter `any`. You can also enter `host` and the IP address or name of the source host.

The `<wildcard>` parameter specifies the portion of the source address to match against. The `<wildcard>` is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet’s source address must match the `<source-ip>`. Ones mean any value matches. For example, the `<source-ip>` and `<wildcard>` values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.

If you prefer to specify the wildcard (mask value) in Classless Interdomain Routing (CIDR) format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of "209.157.22.26 0.0.0.255" as "209.157.22.26/24".

**NOTE:** When you save ACL policies to the startup-config file, the software changes your IP address values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 (if you have enabled display of sub-net lengths) or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in "/<mask-bits>" format. To enable the software to display the CIDR masks, enter the `ip show-subnet-length` command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

**NOTE:** If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the `show ip access-list` command.

The `<destination-ip-address>` parameter specifies the destination address to be matched. If you want the policy to match on all destination addresses, enter `any`. You can also enter `host` and enter the IP address or name of the destination host.

The `<operator>` parameter specifies a comparison operator for the TCP or UDP port number. This parameter applies only when you specify "tcp" or "udp" as the IP protocol. For example, if you are configuring an entry for HTTP, specify `tcp eq http`. You can enter one of the following operators:

- **eq** – The policy applies to the TCP or UDP port name or number you enter after `eq`.
- **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after `gt`.
- **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after `lt`.
- **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after `neq`.
- **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: `range 23 53`. The first port number in the range must be lower than the last number in the range.
- **established** – This operator applies only to TCP packets. If you use this operator, the policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

**NOTE:** This operator applies only to destination TCP ports, not source TCP ports.

The `<tcp/udp-port>` parameter specifies the TCP or UDP port number or well-known name. In release 07.6.01b and later, you can specify a well-known name for any application port whose number is less than 1024. For other application ports, you must enter the number. Enter "?" instead of a port to list the well-known names recognized by the CLI.
The `<icmp-type>` parameter specifies the ICMP protocol type if you specified "icmp" for `<ip-protocol>`. The parameter is supported in Enterprise software release 07.2.06 and later. It can have one of the following values, depending on the software version the device is running:

- any-icmp-type
- echo
- echo-reply
- information-request
- log
- mask-reply
- mask-request
- parameter-problem
- redirect
- source-quench
- time-exceeded
- timestamp-reply
- timestamp-request
- unreachable
- `<num>`

The `<num>` parameter can be a value from 0 – 255. If you do not specify a message type, the ACL applies to all types of ICMP messages.

Devices running Enterprise software release 07.8.00 and later can specify the `<icmp-type-number> <icmp-code-number>` instead of the `<icmp-type>`. The valid `<type-number>` and `<code-number>` combinations are listed in Table 6.6.

The `dscp-marking` `<dscp-value>` parameter maps a DSCP value to an internal forwarding priority. The DSCP value can be from 0 – 63.

**NOTE:** The **Internal priority-marking** and **dscp-cos-mapping** parameters override port-based priority settings.

The `dscp-mapping` `<dscp-value>` parameter matches on the packet's DSCP value.

**NOTE:** This option does not change the packet's priority through the device or mark the packet.

The `established` parameter applies only to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

The `ip-pkt-len` `<value>` parameter enables you to filter ICMP packets based on the IP packet length. This parameter matches on the total length field in the IP header of ICMP packets. The IP packet length value can be from 1 -65535.

**NOTE:** This parameter is supported in software release 07.7.00 and later, and applies only if you specified `icmp` as the `<ip-protocol>` value.

The `log` parameter enables SNMP traps and Syslog messages for packets denied by the ACL.

The `precedence` `<name> | <num>` parameter of the `ip access-list` command specifies the IP precedence. The `precedence` option for an IP packet is set in a three-bit field following the four-bit header-length field of the packet’s header. You can specify one of the following:
• **critical** or 5 – The ACL matches packets that have the critical precedence. If you specify the option number instead of the name, specify number 5.

• **flash** or 3 – The ACL matches packets that have the flash precedence. If you specify the option number instead of the name, specify number 3.

• **flash-override** or 4 – The ACL matches packets that have the flash override precedence. If you specify the option number instead of the name, specify number 4.

• **immediate** or 2 – The ACL matches packets that have the immediate precedence. If you specify the option number instead of the name, specify number 2.

• **internet** or 6 – The ACL matches packets that have the internetwork control precedence. If you specify the option number instead of the name, specify number 6.

• **network** or 7 – The ACL matches packets that have the network control precedence. If you specify the option number instead of the name, specify number 7.

• **priority** or 1 – The ACL matches packets that have the priority precedence. If you specify the option number instead of the name, specify number 1.

• **routine** or 0 – The ACL matches packets that have the routine precedence. If you specify the option number instead of the name, specify number 0.

You can specify one of the following:

• **max-reliability** or 2 – The ACL matches packets that have the maximum reliability ToS. The decimal value for this option is 2.

• **max-throughput** or 4 – The ACL matches packets that have the maximum throughput ToS. The decimal value for this option is 4.

• **min-delay** or 8 – The ACL matches packets that have the minimum delay ToS. The decimal value for this option is 8.

• **min-monetary-cost** or 1 – The ACL matches packets that have the minimum monetary cost ToS. The decimal value for this option is 1.

**NOTE:** This value is not supported on and 10 Gigabit Ethernet modules

• **normal** or 0 – The ACL matches packets that have the normal ToS. The decimal value for this option is 0.

• **<num>** – A number from 0 – 15 that is the sum of the numeric values of the options you want. The ToS field is a four-bit field following the Precedence field in the IP header. You can specify one or more of the following. To select more than one option, enter the decimal value that is equivalent to the sum of the numeric values of all the ToS options you want to select. For example, to select the **max-reliability** and **min-delay** options, enter number 10. To select all options, select 15.

The **priority** option enables you to assign traffic that matches the ACL to a specific hardware forwarding queue (qosp0, qosp1, qosp2, or qosp3). The **0 | 1 | 2 | 3** parameter specifies the QoS queue:

• 0 – qosp0
• 1 – qosp1
• 2 – qosp2
• 3 – qosp3

**NOTE:** This **priority** option provides the same function as the Layer 4 IP access policies supported on 9300 series Chassis devices. If you configure both a Layer 4 IP access policy and an extended ACL to set the hardware forwarding priority for the same traffic, the device uses the ACL instead of the IP access policy.

The **priority-force** parameter allows you assign packets of outgoing traffic that match the ACL to a specific hardware forwarding queue, even though the incoming packet may be assigned to another queue. Specify one of the following QoS queue:
Global CONFIG Commands

• 0 – qosp0
• 1 – qosp1
• 2 – qosp2
• 3 – qosp3

The priority-mapping <8021p-value> parameter matches on the packet's 802.1p priority.

NOTE: This option does not change the packet's priority through the device or mark the packet. This option is not supported on 10 Gigabit Ethernet modules.

The tos <name> | <num> parameter of the ip access-list command specifies the IP ToS.

Apply the ACL to a port and specify if it is for incoming or outgoing traffic using the “ip access-group” on page 8-7.

access-list permit (standard)

Creates standard ACLs that permit packets based on source IP address. You can configure up to 99 standard ACLs. You can configure up to 1024 individual ACL entries. There is no limit to the number of ACL entries an ACL can contain except for the system-wide limitation of 1024 total ACL entries.

Starting in software release 07.6.04, you can use standard ACLs to control the following multicast features:

• Limit the number of multicast groups that are covered by a static rendezvous point (RP). See “rp-address” on page 24-5.

• Control which multicast groups for which candidate RPs sends advertisement messages to bootstrap routers. See "rp-candidate" on page 24-6.

• Identify which multicast group packets will be forwarded or blocked on an interface. See “ip multicast boundary” on page 8-20.

EXAMPLE:

To configure a standard ACL and apply it to outgoing traffic on port 1/1, enter the following commands.

ProCurveRS(config)# access-list 1 permit host IPHost1 log
ProCurveRS(config)# access-list 1 deny 10.10.10.1 ... int eth 1/1
ProCurveRS(config-if-1/1)# ip access-group 1 out
ProCurveRS(config-if-1/1)# write memory

The last ACL entry in this ACL permits all packets that are not explicitly denied by the the ACL entries.

Syntax: [no] access-list <num> deny <source-ip-address> | any | host <ip-address> | host <hostname> | <wildcard> [log]

The <num> parameter is the access list number and can be from 1 – 99.

The permit parameter allows packets that match a policy.

The <source-ip-address> parameter specifies the source IP address. Alternatively, you can specify the host name.

NOTE: To specify the host name instead of the IP address, the host name must be configured using the HP device's DNS resolver. To configure the DNS resolver name, use the ip dns server-address... command at the global CONFIG level of the CLI.

The <wildcard> parameter specifies the mask value to compare against the host address specified by the <source-ip> parameter. The <wildcard> is a four-part value in dotted-decimal notation (IP address format) consisting of ones and zeros. Zeros in the mask mean the packet's source address must match the <source-ip>. Ones mean any value matches. For example, the <source-ip> and <wildcard> values 209.157.22.26 0.0.0.255 mean that all hosts in the Class C sub-net 209.157.22.x match the policy.
If you prefer to specify the wildcard (mask value) in CIDR format, you can enter a forward slash after the IP address, then enter the number of significant bits in the mask. For example, you can enter the CIDR equivalent of “209.157.22.26 0.0.0.255” as “209.157.22.26/24”.

**NOTE:** When you save ACL policies to the startup-config file, the software changes your <source-ip> values if appropriate to contain zeros where the packet value must match. For example, if you specify 209.157.22.26/24 or 209.157.22.26 255.255.255.0, then save the startup-config file, the values appear as 209.157.22.0/24 (if you have enabled display of sub-net lengths) or 209.157.22.0 255.255.255.0 in the startup-config file.

If you enable the software to display IP sub-net masks in CIDR format, the mask is saved in the file in “/<mask-bits>” format. To enable the software to display the CIDR masks, enter the `ip show-subnet-length` command at the global CONFIG level of the CLI. You can use the CIDR format to configure the ACL entry regardless of whether the software is configured to display the masks in CIDR format.

**NOTE:** If you use the CIDR format, the ACL entries appear in this format in the running-config and startup-config files, but are shown with sub-net mask in the display produced by the `show ip access-list` command.

The host <source-ip> | host <hostname> parameter lets you specify a host IP address or name. When you use this parameter, you do not need to specify the mask. A mask of all zeros (0.0.0.0) is implied.

The any parameter configures the policy to match on all host addresses.

The log argument configures the device to generate Syslog entries and SNMP traps for packets that are permitted or denied by the access policy.

Apply the ACL to a port and specify if it is for incoming or outgoing traffic using the “ip access-group” on page 8-7.

Possible values: see above

Default value: N/A

**access-list rate-limit**

Configures a rate-limiting ACL.

**NOTE:** After you configure the rate limiting policy, you need to apply the policy to an interface for the policy to take effect. See “rate-limit input | output” on page 7-70.

**EXAMPLE:**

The following command configures a rate limit ACL to characterize the traffic. In this case, the rate policy is for a specific host, so the rate limit ACL specifies a host MAC address.

```
ProCurveRS(config)# access-list rate-limit 100 aaaa.bbbb.cccc
```

**Syntax:** [no] access-list rate-limit <num> <mac-addr> | <precedence> | mask <precedence-mask>

The <num> parameter specifies the ACL number.

The <mac-addr> | <precedence> | mask <precedence-mask> parameter specifies a MAC address, an IP precedence, or a mask value representing a set of IP precedence values.

To specify a MAC address, enter the address in the following format: xxxx.xxxx.xxxx.

To specify an IP precedence, specify one of the following:

- 0 – The ACL matches packets that have the routine precedence.
- 1 – The ACL matches packets that have the priority precedence.
- 2 – The ACL matches packets that have the immediate precedence.
- 3 – The ACL matches packets that have the flash precedence.
- 4 – The ACL matches packets that have the flash override precedence.
- 5 – The ACL matches packets that have the critical precedence.
• 6 – The ACL matches packets that have the internetwork control precedence.
• 7 – The ACL matches packets that have the network control precedence.

To specify a mask value for a set of IP precedence values, enter \texttt{mask} followed by a two-digit hexadecimal number for the precedence values.

The precedence values are in an 8-bit field in the IP packet header. To calculate the hexadecimal number for a combination of precedence values, write down the values for the entire field to create the binary number for the mask value, then convert the number to hexadecimal. For example, to specify a mask for precedences 2, 4, and 5, write down the following values for the precedence field:

<table>
<thead>
<tr>
<th>Bit Positions</th>
<th>8</th>
<th>7</th>
<th>6</th>
<th>5</th>
<th>4</th>
<th>3</th>
<th>2</th>
<th>1</th>
</tr>
</thead>
<tbody>
<tr>
<td>Precedence</td>
<td>7</td>
<td>6</td>
<td>5</td>
<td>4</td>
<td>3</td>
<td>2</td>
<td>1</td>
<td>0</td>
</tr>
<tr>
<td>Bit Pattern</td>
<td>0</td>
<td>0</td>
<td>1</td>
<td>1</td>
<td>0</td>
<td>1</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>

Then, reading the digits from right to left, convert the number to hexadecimal. In this case, 00110100 binary becomes 0x34. Enter the mask as \texttt{mask 34}.

For simplicity, you can convert the digits in groups of four bits each.

For example, you can convert \texttt{bits 1 – 4} (binary 0100) to get hexadecimal "4" for the right digit. Then convert \texttt{bits 5 – 8} (binary 0011) to get hexadecimal "3" for the left digit. The result is “34”.

Alternatively, you can enter the entire eight-bit binary number in a calculator, then convert the number to hexadecimal. For example, you can enter the binary number "00110100" and convert it to hexadecimal to get “34”. (Without the leading zeros, enter “110100.”)

The least significant digit is the rightmost digit (bit position 1) and the most significant digit is the leftmost digit (bit position 8).

\textbf{Possible values:} See above
\textbf{Default value:} N/A

\textbf{access-list remark}

Creates a remark for the next ACL entry that you will be creating.

\textbf{EXAMPLE:}

\texttt{ProCurveRS(config)# access-list 101 remark Stop igmp traffic}

\textbf{Syntax:} \texttt{[no] access-list <num> remark <comment-text>}

Enter a number for the \texttt{<acl-num>} parameter. Enter a number from 1 – 99 for standard ACLs or 100 – 199 for extended ACLs.

Enter up to 128 characters for \texttt{<comment-text>}. When you use this command, the comment must be entered separately from the actual ACL entry; that is, you cannot enter the ACL entry and the ACL comment with the same \texttt{access-list} command. Also, in order for the remark to be displayed correctly in the output of \texttt{show} commands, the comment must be entered immediately before the ACL entry it describes.

\textbf{Possible values:} See above
\textbf{Default value:} N/A

\textbf{access-list replace}

Replaces the definition or remark of an existing ACL entry. This command is available on devices running Enterprise software release 07.8.00 and later.

To insert a new ACL entry in line 2 of ACL 99.

\texttt{ProCurveRS(config)# access-list 99 replace 2 deny 5.6.7.8}
**Syntax:** access-list <acl-number> replace <line-number> deny <options> | permit <options> | remark <comment-text>

**Possible Values:**
Enter a number for the <acl-num> parameter. Enter a number from 1 – 99 for standard ACLs or 100 – 199 for extended ACLs.

The `replace <line-number>` parameter specifies the ACL entry to be replaced.

Use the `deny <options>` parameter if you want to create a filter that blocks traffic. See the "access-list deny (extended)" on page 6-4 and "access-list deny (standard)" on page 6-9 command for <options> you can use to deny the traffic.

Use the `permit <options>` parameter if you want to create a filter that allows traffic. See the "access-list permit (extended)" on page 6-11 and "access-list permit (standard)" on page 6-15 command for <options> you can use to allow the traffic.

Use the `remark <comment-text>` to replace the comment to the ACL entry. The remark can have up to 128 characters in length.

**Possible values:** See above

**Default value:** N/A

**acl-denied-icmp-msg**
Enables a Routing Switch to send an ICMP unreachable message to a device when an ACL denies a packet from the device.

By default, an HP device does not send a message to another device when an ACL on the HP device denies a packet from the other device.

**NOTE:** This command applies only to Routing Switches.

**NOTE:** This command does not take effect in the following cases:

—Hardware-based ACLs are enabled.

—The `hw-drop-acl-denied-packet` command is in effect.

In either case, all packets denied by the ACL are dropped by hardware without sending an ICMP message.

**EXAMPLE:**
ProCurveRS(config)# acl-denied-icmp-msg

**Syntax:** [no] acl-denied-icmp-msg

The command applies globally to all ACLs configured on the device.

**Possible values:** N/A

**Default value:** Disabled

**aggregated-vlan**
Enables a larger Ethernet frame size for VLAN aggregation. This feature changes the maximum Ethernet size to 1530 bytes.

**NOTE:** Use this command when you are configuring Super Aggregated VLANs. See the "Configuring VLANs" chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches.*
Global CONFIG Commands

NOTE: This command is not applicable on the ProCurve 9408sl. The ProCurve 9408sl automatically enables the Super Aggregate VLAN mode when you tag the device.

EXAMPLE:
ProCurveRS(config)# aggregated-vlan

Syntax: aggregated-vlan

Possible values: N/A

Default value: Disabled

aggregated-vlan-copy-cos

Configures an untagged interface to copy the QoS bits from the tag value set by the edge device to the tag value set by the core device. The HP device copies the QoS bits when it adds the additional tag type as the packets enter the core network. This way, the HP device can prioritize SAV traffic transmitted through the network core.

NOTE: Use this command when you are configuring Super Aggregated VLANs. See the “Configuring VLANs” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches.

EXAMPLE:
To enable the HP device to copy the QoS marking from packets entering interface e 4/1 to the tag value set by the core device when it applies the additional 802.1Q tag type, enter the following command on the untagged port of the core device. After entering this command, the HP device will prioritize high-priority customer traffic as it traverses through the core of the network.

ProCurveRS(config)# int e 4/1
ProCurveRS(config-if-e1000-4/1)# aggregated-vlan-copy-cos

Syntax: [no] aggregated-vlan-copy-cos

Possible values: N/A

Default value: Disabled

all-client

Restricts management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device through Telnet (CLI), the Web (Web management interface), or SNMP.

If you want to restrict access for some of the management platforms but not all of them, use one or two of the following commands:

• snmp-client – restricts all SNMP access. See “snmp-client” on page 6-139.
• telnet-client – restricts Telnet access. See “telnet-client” on page 6-160.
• web-client – restricts web access. See “web-client” on page 6-169.

EXAMPLE:
To restrict all management access to the HP device to the host with IP address 209.157.22.26, enter the following command:

ProCurveRS(config)# all-client 209.157.22.26

Syntax: [no] all-client <ip-addr>

Possible values: a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

Default value: N/A
appletalk arp-age
Defines how long an AppleTalk ARP entry will remain active before being aged out.

EXAMPLE:
ProCurveRS(config)# appletalk arp-age 115
Syntax: appletalk arp-age <1 – 240>
Possible values: 1 – 240 minutes
Default value: 10 minutes

appletalk arp retransmit-count
Allows you to modify the maximum number of times that a packet will be sent out for ARP cache informational updates. The packet will be sent out to the maximum amount defined, until the information is received.
If no response is received before the count number expires, no additional packets will be sent.

EXAMPLE:
To modify the number of times packet requests will be sent out for ARP updates from the default value of 2 to 8, enter the following:
ProCurveRS(config)# appletalk arp retransmit-count 8
Syntax: appletalk arp retransmit-count <value>
Possible values: 1 – 10
Default value: 2

appletalk arp retransmit-interval
Allows you to modify the interval between the transmission of ARP packets.

EXAMPLE:
To modify the retransmission interval from the default value of 1 to 15 seconds, enter the following:
ProCurveRS(config)# appletalk arp retransmit-interval 15
Syntax: appletalk arp retransmit-interval <value>
Possible values: 1 – 120 seconds
Default value: 1

appletalk glean-packets
When the glean-packets parameter is enabled on an AppleTalk router, it will try to learn the MAC address from the packet instead of sending out an AARP request.

EXAMPLE:
To enable glean packets on an AppleTalk router, enter the following:
ProCurveRS(config)# appletalk glean-packets
Syntax: appletalk glean-packets
Possible values: enabled or disabled
Default value: disabled

appletalk qos socket
You can use the Quality of Service (QoS) socket parameter to assign a higher priority to specific AppleTalk sockets. Enter a value from 0 – 7.
For information about HP QoS, see the "Quality of Service" chapter in the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.
EXAMPLE:
To assign socket 123 to the premium queue, enter the following command:

ProCurveRS(config)# appletalk qos socket 123 priority 7

Syntax: [no] appletalk qos socket <num> priority <num>
The first <num> parameter specifies the socket number.
The second <num> parameter can be from 0 – 7 and specifies the IEEE 802.1 equivalent to one of the four QoS queues.

Possible values: See above.
Default value: By default, all AppleTalk sockets are in the best effort queue.

appletalk rtmp-update-interval
Allows you to modify how often RTMP updates are sent out on AppleTalk interfaces.

EXAMPLE:
To change the value to 50 seconds from a default value of 10 seconds, enter the following:

ProCurveRS(config)# appletalk rtmp-update-interval 50

Syntax: appletalk rtmp-update-interval <seconds>
Possible values: 1 – 3600 seconds
Default value: 10 seconds

appletalk zip-query-interval
Allows you to modify how often ZIP query messages are retransmitted.

EXAMPLE:
To change the ZIP query interval to 30 seconds from a default value of 10 seconds, enter the following:

ProCurveRS(config)# appletalk zip-query-interval 30

Syntax: appletalk zip-query-interval <seconds>
Possible values: 1 – 1000 seconds
Default value: 10 seconds

arp
Enters a static IP ARP entry for static routes on a ProCurve Routing Switch.

EXAMPLE:
ProCurveRS(config)# arp 1 192.53.4.2 1245.7654.2348 e 4/11

Syntax: [no] arp <num> <ip-addr> <mac-addr> ethernet <portnum>
The <num> parameter specifies the entry number. You can specify a number from 1 up to the maximum number of static entries allowed on the device.
The <ip-addr> command specifies the IP address of the device that has the MAC address of the entry.
The <mac-addr> parameter specifies the MAC address of the entry.
The ethernet <portnum> command specifies the port number attached to the device that has the MAC address of the entry.

NOTE: The clear arp command clears learned ARP entries but does not remove any static ARP entries.

Possible values: The maximum number of ARP entries you can add depends on the device. To display the maximum number you can configure on your device, enter the show default values command and look at the row of information for the ip-arp parameter. See “show default” on page 40-23.
Default value: N/A

**auto-acl-rebind**

Enables automatic unbinding and rebinding of ACLs. Use this command if you going to copy a configuration file containing ACLs into the device's running-config.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# auto-acl-rebind
ProCurveRS(config)# end
ProCurveRS# copy tftp running newacls.cfg
```

**Syntax:** auto-acl-rebind

**Possible values:** Enabled or disabled

**Default value:** Disabled

**banner exec**

Configures the HP device to display a message when a user enters the Privileged EXEC CLI level.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# banner exec $ (Press Return)
Enter TEXT message, End with the character '$'.
You are entering Privileged EXEC level
Don’t foul anything up! $
```

**Syntax:** [no] banner exec <delimiting-character>

A delimiting character is established on the first line of the **banner exec** command. You begin and end the message with this delimiting character. The delimiting character can be any character except " (double-quatation mark) and cannot appear in the banner text. In this example, the delimiting character is $ (dollar sign). The text in between the dollar signs is the contents of the banner. The banner text can be up to 2048 characters long and can consist of multiple lines. To remove the banner, enter the **no banner exec** command.

**Possible values:** N/A

**Default value:** N/A

**banner incoming**

Configures the HP device to display a message on the Console when a user establishes a Telnet session. This message indicates where the user is connecting from and displays a configurable text message.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# banner incoming $ (Press Return)
Enter TEXT message, End with the character '$'.
Incoming Telnet Session!! $
```

When a user connects to the CLI using Telnet, the following message appears on the Console:

```plaintext
Telnet from 209.157.22.63
Incoming Telnet Session!!
```

**Syntax:** [no] banner incoming <delimiting-character>

A delimiting character is established on the first line of the **banner incoming** command. You begin and end the message with this delimiting character. The delimiting character can be any character except " (double-quatation mark) and cannot appear in the banner text. In this example, the delimiting character is $ (dollar sign). The text in between the dollar signs is the contents of the banner. The banner text can be up to 2048 characters long and can consist of multiple lines. To remove the banner, enter the **no banner incoming** command.

**Possible values:** N/A

**Default value:** N/A
**banner motd**

Configures the HP device to display a message on a user's terminal when he or she establishes a Telnet CLI session.

**EXAMPLE:**

To display the message “Welcome to 9315M!” when a Telnet CLI session is established:

```
ProCurveRS(config)# banner motd $ (Press Return)
Enter TEXT message, End with the character '$'.
Welcome to 9315M! $
```

**Syntax:** [no] banner <delimiting-character> | [motd <delimiting-character>]

A delimiting character is established on the first line of the `banner motd` command. You begin and end the message with this delimiting character. The delimiting character can be any character except " (double-quotation mark) and cannot appear in the banner text. In this example, the delimiting character is $ (dollar sign). The text in between the dollar signs is the contents of the banner. The banner text can be up to 2048 characters long and can consist of multiple lines. To remove the banner, enter the `no banner motd` command.

When you access the Web management interface, the banner is displayed on the login panel.

**NOTE:** The `banner <delimiting-character>` command is equivalent to the `banner motd <delimiting-character>` command.

**Possible values:** N/A

**Default value:** N/A

**boot system bootp**

Configures the device to use BootP as the primary boot source.

**NOTE:** If you enter another `boot system` command at the global CONFIG level after entering this command, the software adds the new boot source as the primary source and changes the previously entered source to be the secondary source.

**EXAMPLE:**

```
ProCurveRS(config)# boot system bootp
```

**Syntax:** boot system bootp

**Possible values:** N/A

**Default value:** primary flash

**boot system flash primary**

Configures the device to use the primary flash location as the primary boot source. This is the default primary boot source.

**NOTE:** If you enter another `boot system` command at the global CONFIG level after entering this command, the software adds the new boot source as the primary source and changes the previously entered source to be the secondary source.

**EXAMPLE:**

```
ProCurveRS(config)# boot system flash primary
```

**Syntax:** boot system flash primary

**Possible values:** N/A

**Default value:** primary flash
**boot system flash secondary**

Configures the device to use the secondary flash location as the primary boot source.

**NOTE:** If you enter another `boot system` command at the global CONFIG level after entering this command, the software adds the new boot source as the primary source and changes the previously entered source to be the secondary source.

**EXAMPLE:**

```bash
ProCurveRS(config)# boot system flash secondary
```

**Syntax:** `boot system flash secondary`

**Possible values:** N/A

**Default value:** primary flash

**boot system tftp**

Configures the device to use a TFTP server as the primary boot source.

**NOTE:** If you enter another `boot system` command at the global CONFIG level after entering this command, the software adds the new boot source as the primary source and changes the previously entered source to be the secondary source.

**EXAMPLE:**

```bash
ProCurveRS(config)# boot system tftp 192.22.33.44 current.img
```

**NOTE:** Before entering the TFTP boot command, you must first assign an IP address, IP mask and default gateway (if applicable) at the boot prompt as shown.

**EXAMPLE:**

```bash
boot> ip address 192.22.33.44 255.255.255.0
boot> ip default-gateway 192.22.33.1
```

You now can proceed with the `boot system tftp`... command.

**Syntax:** `boot system tftp <ip-addr> <filename>`

**Possible values:** N/A

**Default value:** primary flash

**bootp-relay-max-hops**

Defines the maximum number of hops that a BootP request will be allowed to traverse before being dropped.

**EXAMPLE:**

```bash
ProCurveRS(config)# bootp-relay-max-hops 5
```

**Syntax:** `bootp-relay-max-hops <value>`

**Possible values:** 1 – 15

**Default value:** 4

**broadcast filter**

Configures a Layer 2 broadcast packet filter. You can filter on all broadcast traffic or on IP UDP broadcast traffic.

**EXAMPLE:**

To configure a Layer 2 broadcast filter to filter all types of broadcasts, then apply the filter to ports 1/1, 1/2, and 1/3, enter the following commands:

```bash
ProCurveRS(config)# broadcast filter 1 any
```
Global CONFIG Commands

EXAMPLE:
To configure two filters, one to filter IP UDP traffic on ports 1/1 – 1/4, and the other to filter all broadcast traffic on port 4/6, enter the following commands:

ProCurveRS(config)# broadcast filter 1 ip udp
ProCurveRS(config-bcast-filter-id-1)# exclude-ports ethernet 1/1 to 1/4
ProCurveRS(config-bcast-filter-id-1)# exit
ProCurveRS(config)# broadcast filter 2 any
ProCurveRS(config-bcast-filter-id-2)# exclude-ports ethernet 4/6
ProCurveRS(config-bcast-filter-id-2)# write memory

EXAMPLE:
To configure an IP UDP broadcast filter and apply that applies only to port-based VLAN 10, then apply the filter to two ports within the VLAN, enter the following commands:

ProCurveRS(config)# broadcast filter 4 ip udp vlan 10
ProCurveRS(config-bcast-filter-id-4)# exclude-ports eth 1/1 eth 1/3
ProCurveRS(config-bcast-filter-id-4)# write memory

Syntax:

The `<filter-id>` specifies the filter number and can a number from 1 – 8. The software applies the filters in ascending numerical order. As soon as a match is found, the software takes the action specified by the filter (block the broadcast) does not compare the packet against additional broadcast filters.

You can specify any or ip udp as the type of broadcast traffic to filter. The any parameter prevents all broadcast traffic from being sent on the specified ports. The ip udp parameter prevents all IP UDP broadcasts from being sent on the specified ports but allows other types of broadcast traffic.

If you specify a port-based VLAN ID, the filter applies only to the broadcast domain of the specified VLAN, not to all broadcast domains (VLANs) on the device.

As soon as you press Enter after entering the command, the CLI changes to the configuration level for the filter you are configuring. You specify the ports to which the filter applies at the filter’s configuration level.

Syntax: `[no] exclude-ports ethernet <portnum> to <portnum>`

Or

Syntax: `[no] exclude-ports ethernet <portnum> ethernet <portnum>`

These commands specify the ports to which the filter applies.

NOTE: This is the same command syntax as that used for configuring port-based VLANs. Use the first command for adding a range of ports. Use the second command for adding separate ports (not in a range). You also can combine the syntax. For example, you can enter `exclude-ports ethernet 1/4 ethernet 2/6 to 2/9`.

Possible values: see above

Default value: N/A

broadcast limit

Specifies the maximum number of broadcast packets the device can forward each second. By default the device sends broadcasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited broadcast traffic, this command allows you to relieve those devices by throttling the broadcasts at the HP device.

June 2005
NOTE: The broadcast limit does not affect multicast or unicast traffic. However, you can use the multicast limit and unknown-unicast limit commands to control these types of traffic. See “multicast limit” on page 6-116 and “unknown-unicast limit” on page 6-164.

EXAMPLE:
ProCurveRS(config)# broadcast limit 30000

Syntax: broadcast limit <num>

Possible values: 0 – 4294967295; if you specify 0, limiting is disabled.

Default value: N/A

cam-partition

Specifies CAM partition percentages on the device. See the Diagnostic Guide for ProCurve 9300/9400 Series Routing Switches for information on how to configure this feature.

EXAMPLE:

NOTE: See the example following this one for the command syntax on the ProCurve 9408sl.

ProCurveRS(config)# cam-partition l2 0 l3 100 l4 0
Slot 1 (DMA 0) CAM Partition:
  Standard Module, Total Size 1Mbits
    L2 232.530029Mbits 88789.002929%, L3 0.75Mbits 75%, L4 232.655029Mbits 88801.502929%
    L3 = 12288 (level2 = 2048, level3 = 2048), Pool0 = 2048, Pool1 = 2048, Pool2 = 54488408, Pool3 = 0
Slot 1 (DMA 2) CAM Partition:
  Standard Module, Total Size 1Mbits
    L2 232.530029Mbits 88789.002929%, L3 0.75Mbits 75%, L4 232.655029Mbits 88801.502929%
    L3 = 12288 (level2 = 2048, level3 = 2048), Pool0 = 2048, Pool1 = 2048, Pool2 = 54488408, Pool3 = 0
Cold start required. Please write memory and then reload or power cycle.

Syntax: cam-partition l2 <percent> l3 <percent> l4 <percent> (router image)

Syntax: cam-partition l2 <percent> l4 <percent> (switch image)

NOTE: You must reload the software after enabling this protocol to place the change into effect.

Possible values: 1 – 100

On devices running a router image, you cannot set CAM to zero percent (0%). Also, the minimum value for Layer 4 CAM is one-fourth or 25% of the total CAM

Default value: See the Diagnostic Guide for ProCurve 9300/9400 Series Routing Switches for the default CAM partitions.

EXAMPLE:

To specify CAM partitions on the ProCurve 9408sl, enter commands such as the following:

ProCurveRS(config)# cam-partition session 25% mac 12.5% ip 62.5%
ProCurveRS(config)# write memory
ProCurveRS(config)# exit
ProCurveRS# reload

These commands increase the Layer 4 partition to 25%, maintain the default setting of the Layer 2 partition at 12.5%, and decrease the Layer 3 partition to 62.5%.
NOTE:  After resizing the CAM partitions, you must save the configuration and reload the software.

**Syntax:** cam-partition ip <number>%  mac <number>%  session <number>%

**Possible values:**
You can specify the ip, mac, and session keywords in any order. If the HP device is running routing switch software, you must specify the mac keyword with a minimum of 1% of CAM assigned to it. If the HP device is running 9408sl Routing Switch software, you must specify the mac and ip keywords with a minimum of 1% of CAM assigned to each.

The <number> parameter specifies the percentage of the CAM assigned to a partition. With the ip and mac keywords, you can specify a number in increments of 0.5, for example, 86.5 or 88. With the session keyword, you can specify a number in increments of 12.5, for example, 25 and 37.5.

**Default values:**  See the *Diagnostic Guide for ProCurve 9300/9400 Series Routing Switches* for the default CAM partitions.

cdp run
Enables an HP device to intercept and display Cisco Discovery Protocol (CDP) packets.

**NOTE:**  When you enable interception of CDP packets, the HP device drops the packets. As a result, Cisco devices will no longer receive the packets.

**EXAMPLE:**
ProCurveRS(config)# cdp run

**Syntax:** [no] cdp run
The feature is disabled by default.

**Possible values:** N/A

**Default value:** Disabled

chassis name
Assigns an administrative ID to the device.

**NOTE:**  This command does not change the CLI prompt. To change the CLI prompt, use the hostname command. See “hostname” on page 6-45.

**EXAMPLE:**
ProCurveRS(config)# chassis name routernyc

**Syntax:** chassis name <text>

**Possible values:** Up to 32 alphanumeric characters

**Default value:** Null string

chassis poll-time
Changes the number of seconds between polls of the power supply, fan, and temperature status.
Use the show chassis command to display the hardware status.

**EXAMPLE:**
To change the hardware poll time from 60 seconds (the default) to 30 seconds:
ProCurveRS(config)# chassis poll-time 30

**Syntax:** chassis poll-time <num>

**Possible values:** 0 – 65535
chassis trap-log
Disables or re-enables status polling for individual power supplies and fans. When you disable status polling, a fault in the power supply does not generate a trap in the system log.

**EXAMPLE:**
To disable polling of power supply 2, enter the following command:

```
ProCurveRS(config)# no chassis trap-log ps2
```

**Syntax:** [no] chassis trap-log ps1 | ps2 | ps3 | ps4 | fan1 | fan2 | fan3 | fan4

**Possible values:** see above

To disable a fan failure trap or power supply trap, use one of the following values:

- ps1
- ps2
- ps3
- ps4
- fan1
- fan2
- fan3
- fan4

**Default value:** all traps enabled

clock summer-time
Causes daylight savings time to be automatically activated and deactivated for the relevant time zones.

**EXAMPLE:**
```
ProCurveRS# clock summer-time
```

**Syntax:** clock summer-time

**Possible values:** N/A

**Default value:** N/A

clock timezone
Allows you to define the time zone of the clock. This parameter is used in conjunction with the `clock set` command or for timestamps obtained from an SNTP server. The `clock set`... command is configured at the privileged EXEC level of the CLI.

**NOTE:** Use this `clock` command before all others to ensure accuracy of the clock settings.

**NOTE:** For those time zones that recognize daylight savings time, the `clock summer-time` command will also need to be defined.

**NOTE:** Clock settings are not saved over power cycles; however, you can configure the system to reference an SNTP server at power up. This server will then automatically download the correct time reference for the network. The local device will then adjust the time according to its time zone setting. For more details on setting up an SNTP reference clock, refer to the `snmp` command at the privileged EXEC level and the `snmp poll-interval` and `snmp server` commands at the global CONFIG level.
EXAMPLE:
ProCurveRS# clock timezone us eastern

Syntax: clock timezone gmt gmt | us <timezone>

Possible values: The following time zones can be entered for US or GMT:
- US time zones: alaska, aleutian, arizona, central, east-indiana, eastern, hawaii, michigan, mountain, pacific, samoa
- GMT time zones: gmt+12, gmt+11, gmt+10...fmt+01, gmt+00, gmt-01...gmt-10, gmt-11, gmt-12

Default value: pacific

confirm-port-up
Reduces the number of up-status confirmations the software requires before bringing a port up for use. This command is useful for network interface cards (NICs) that are designed to come up very quickly in certain applications and are sensitive to the slight delay caused by the HP ports as they wait for the multiple status indications before coming up. You can configure a ProCurve Routing Switch to reduce the number of status indications the software requires before bringing up a 10/100Base-Tx port.

NOTE: Do not use this command unless advised to do so by HP technical support.

By default, the Routing Switches wait for multiple indications that a port is good before bringing the port up. Specific types of networking devices are sensitive to the very slight delay caused by the multiple status indications. In this case, you can use one of the following methods to reduce the number of status indications the software requires before bringing up a 10/100Base-Tx port.

You can set this parameter on individual ports.

EXAMPLE:
By default, Chassis devices bring a 10/100 Base-Tx port up after receiving three consecutive up-status indications for the port. You can reduce this number to just one indication. To reduce the up-status indications required to bring up 10/100 ports 1/1 – 1/8 to just one, enter the following commands:

ProCurveRS(config)# int ethernet 1/1 to 1/8
ProCurveRS(config-mif-1/1-1/8)# confirm-port-up 1
ProCurveRS(config-mif-1/1-1/8)# write memory

Syntax: [no] confirm-port-up <num>
The <num> parameter specifies the number of indications required by the software and can be from 1 – 10. The default is 3.

Possible values: 1 – 10
Default value: 3

console
Times out idle serial management sessions.

By default, an HP device does not time out serial CLI sessions. A serial session remains open indefinitely until you close it. You can configure the device to time out serial CLI sessions if they remain idle for a specified number of minutes. You can configure an idle timeout value from 0 – 240 minutes. The default is 0.

NOTE: If a session times out, the device does not close the connection. Instead, the CLI changes to the User EXEC mode (for example: ProCurveRS>).

EXAMPLE:
To configure the idle timeout for serial CLI sessions, enter a command such as the following:

ProCurveRS(config)# console timeout 20
This command configures the idle timeout value to 20 minutes.

**Syntax:** `[no] console timeout <num>`

The `<num>` parameter specifies the number of minutes the serial CLI session can remain idle before it times out. You can specify from 0 – 240 minutes. The default is 0 (sessions never time out).

**Possible values:** 0 – 240 minutes

**Default value:** 0 (sessions never time out)

**cpupro-action hardware max-entries**

Configures the number of CAM entries allocated for each type of traffic when the HP device performs hardware flooding. To accommodate the hardware flooding/dropping actions, the device allocates Layer 2 CAM entries to match broadcast traffic, multicast traffic, and unknown unicast traffic. These Layer 2 CAM entries exist in three sections of Layer 2 CAM space, one section for each type of traffic. By default, each of these sections consists of 256 CAM entries. This command allows you change this number of CAM entries.

**EXAMPLE:**

To allocate 128 CAM entries for unknown-unicast flooding, enter the following command:

```
ProCurveRS(config)# cpupro-action hardware unknown-unicast-flooding max-entries 128
```

**Syntax:** `[no] cpupro-action hardware broadcast-flooding | multicast-flooding | unknown-unicast-flooding max-entries <entries>`

**Possible values:** 1 – 256 CAM entries

**Default value:** 256 CAM entries

**cpupro-action hardware mode**

Specifies whether to flood to drop when traffic unknown-unicast, broadcast, or multicast traffic actions are enabled.

**EXAMPLE:**

To cause unknown-unicast traffic to be dropped when the device enters exhausted mode, enter the following command:

```
ProCurveRS(config)# cpupro-action hardware unknown-unicast-flooding mode drop
```

**Syntax:** `[no] cpupro-action hardware broadcast-flooding | multicast-flooding | unknown-unicast-flooding mode flood | drop`

**Possible values:** The `flood` parameter causes the device to forward the traffic in hardware, flooding it to all ports in the VLAN. The `drop` parameter configures the device to drop the traffic.

**Default value:** `flood`

**cpupro-action hardware ve-not-to-cpu**

Globally allows hardware flooding on virtual routing interfaces and disables the device from copying packets to the CPU. By default, hardware flooding on virtual routing interfaces causes the device to copy packets to the CPU. This command configures the device to allow hardware flooding without copying packets to the CPU.

**EXAMPLE:**

```
ProCurveRS(config)# cpupro-action hardware ve-not-to-cpu
```

**Syntax:** `[no] cpupro-action hardware ve-not-to-cpu`

**Possible values:** N/A

**Default value:** See above.

**cpupro-action hardware-flooding**

Activates the CPU protection feature, causing the device to perform hardware flooding when thresholds related to high CAM usage are exceeded. Hardware flooding actions are supported on devices only.
Global CONFIG Commands

EXAMPLE:
ProCurveRS(config)# cpupro-action hardware-flooding enable

**Syntax:** [no] cpupro-action hardware-flooding enable

**Possible values:** N/A

**Default value:** The CPU protection feature is disabled by default.

**cpupro-action quick-aging**
Activates the CPU protection feature, causing the device to perform dynamic aging adjustment control when thresholds related to high CPU usage are exceeded.

When the device performs dynamic aging adjustment control, the age limit value for CAM entries is dynamically changed to a smaller value, decreasing from 70 seconds to 35 seconds. When the system re-enters normal mode, the age limit value for CAM entries goes back to 70 seconds. Dynamic aging adjustment control is supported on both Standard and devices.

EXAMPLE:
ProCurveRS(config)# cpupro-action quick-aging enable

**Syntax:** [no] cpupro-action quick-aging enable

**Possible values:** N/A

**Default value:** The CPU protection feature is disabled by default.

**cpupro-condition sys cam**
Modifies the default percentages for the CAM usage condition.

EXAMPLE:
ProCurveRS(config)# cpupro-condition sys cam declaring 95 clearing 60

**Syntax:** [no] cpupro-condition sys cam declaring <percent> clearing <percent>

**Possible values:** The **declaring** <percent> parameter specifies the threshold for CAM utilization percentage that will send the device from normal to exhausted mode. The **clearing** <percent> parameter specifies the threshold for CAM utilization percentage that will send the device from exhausted mode back to normal mode. The percentage specified in the declaring parameter must be greater that the percentage specified in the clearing parameter.

**Default value:** The declaring watermark is Layer 2 CAM usage at 90%, and the clearing watermark is Layer 2 CAM usage at 60%.

**cpupro-condition sys cpu**
Modifies the default percentages for the CPU utilization condition.

EXAMPLE:
ProCurveRS(config)# cpupro-condition sys cpu declaring 95 clearing 60

**Syntax:** [no] cpupro-condition sys cpu declaring <percent> clearing <percent>

**Possible values:** The **declaring** <percent> parameter specifies the threshold for CPU utilization percentage that will send the device from normal to exhausted mode. The **clearing** <percent> parameter specifies the threshold for CPU utilization percentage that will send the device from exhausted mode back to normal mode. The percentage specified in the declaring parameter must be greater that the percentage specified in the clearing parameter.

**Default value:** The declaring watermark is CPU usage at 90%, and the clearing watermark is CPU usage at 60%.
**cpu-usage**

Enables and disables an ProCurve 9408sl system to perform usage averaging calculations on tasks handled by the management module's CPU. If you enable the calculation performance, you can display usage averages for all tasks performed by the management module's CPU for an interval of up to 1 hour through the `show cpu` command.

**EXAMPLE:**

To enable usage averaging calculations:

```
ProCurveRS(config)# cpu-usage on
```

**Syntax:** `cpu-usage on | off`

- **on** enables performance of usage averaging calculations.
- **off** disables performance of usage averaging calculations.

**Possible values:** See above.

**Default value:** Performance of the calculations is disabled. When disabled, you can use the `show cpu` command without optional parameters to display usage averages for all tasks performed by the management module's CPU in the last 1 second.

**crypto key**

Configures a host RSA public and private key pair for SSH. The host RSA key pair is stored in the HP device's system-config file. Only the public key is readable. The host RSA key pair is used to negotiate a session key and encryption method with the SSH clients trying to connect to it.

**EXAMPLE 1:**

To generate a public and private host RSA key pair:

```
ProCurveRS(config)# crypto key generate rsa
ProCurveRS(config)# wri mem
```

A host RSA key pair is stored in the system-config file, and SSH is enabled on the device.

**EXAMPLE 2:**

To delete the host RSA key pair from the system-config file:

```
ProCurveRS(config)# crypto key zeroize rsa
ProCurveRS(config)# wri mem
```

The host RSA key pair is deleted from the system-config file, and SSH is disabled on the device.

**NOTE:** The SSH key generation process causes UDLD-enabled interfaces to go down instantaneously. This in turn requires the reconvergence of the route tables on the routers across the network. Non-UDLD-enabled interfaces do not experience this issue.

**Syntax:** `crypto key generate | zeroize rsa`

**Possible values:** N/A

**Default value:** N/A

**crypto random-number-seed**

Creates a new seed for generating a random number that is used for generating the dynamically created server RSA key pair for SSH.

**EXAMPLE:**

```
ProCurveRS(config)# crypto random-number-seed generate
```

**Syntax:** `crypto random-number-seed generate`

**Possible values:** N/A
crypto-ssl certificate generate
Generates an SSL certificate.

**EXAMPLE:**
After you have imported the digital certificate, generate the SSL certificate by entering the following command:

```
ProCurveRS(config)# crypto-ssl certificate generate
```

**Syntax:** [no] crypto-ssl certificate generate

If you did not already import a digital certificate from a client, the device can create a default certificate. To do this, enter the following command:

```
ProCurveRS(config)# crypto-ssl certificate generate default
```

**Syntax:** [no] crypto-ssl certificate generate default

**Possible values:** N/A

**Default value:** N/A

crypto-ssl certificate zeroize
Deletes the SSL certificate on the device.

**EXAMPLE:**

```
ProCurveRS(config)# crypto-ssl certificate zeroize
```

**Syntax:** [no] crypto-ssl certificate zeroize

**Possible values:** N/A

**Default value:** N/A

default-max-frame-size
Globally increases the MTU size on the ProCurve 9408sl.

**NOTE:** To increase the MTU size on devices other than the ProCurve 9408sl, use the `default-mtu` command.

For the ProCurve 9408sl, you can configure an MTU up to 14336 bytes, on a global or individual interface basis.

**EXAMPLE:**
To globally enable jumbo support on all ports, enter commands such as the following:

```
ProCurveRS(config)# default-max-frame-size 7168
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** [no] default-max-frame-size <num>

The `<num>` parameter specifies the maximum number of bytes an Ethernet frame can have in order to be forwarded on a port. You can specify from 64 – 14436 bytes. The default is 1518.

**NOTE:** You must save the configuration change and then reload the software to place the jumbo support into effect.

**Possible values:** 64 – 14436

**Default value:** 1518
**default-mtu**
Globally increases the MTU size.

**NOTE:** This command applies only to Enhanced Performance modules.

**NOTE:** See `default-max-frame-size` for MTU configuration on the ProCurve 9408sl.

Chassis device
You can configure an MTU up to 14336 bytes, on a global or individual interface basis.

**EXAMPLE:**
To globally enable jumbo support on all ports, enter commands such as the following:

```
ProCurveRS(config)# default-mtu 7168
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] default-mtu <num>`

The `<num>` parameter specifies the maximum number of bytes an Ethernet frame can have in order to be forwarded on a port. You can specify from 64 – 14436 bytes. The default is 1518.

If the 802.1X authentication is used and 802.1X supplicant will be sending packet that is greater than 1500 MTU, then set `default-mtu` to 1700 bytes.

**NOTE:** You must save the configuration change and then reload the software to place the jumbo support into effect.

**Possible values:**
64 – 14436 bytes on Chassis device

**Default value:** 1518

**default-vlan-id**
When you enable port-based VLAN operation, all ports are assigned to VLAN 1 by default. As you create additional VLANs and assign ports to them, the ports are removed from the default VLAN. All ports that you do not assign to other VLANs remain members of default VLAN 1. This behavior ensures that all ports are always members of at least one VLAN.

You can change the VLAN ID for the default VLAN by entering the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# default-vlan-id 4095
```

You must specify a valid VLAN ID that is not already in use. For example, if you have already defined VLAN 10, do not try to use "10" as the new VLAN ID for the default VLAN. Valid VLAN IDs are numbers from 1 – 4095.

**NOTE:** Changing the default VLAN name does not change the properties of the default VLAN. Changing the name allows you to use the VLAN ID "1" as a configurable VLAN.

**dot1x-enable**
Enables 802.1X port security on an HP device and launches you into the dot1x configuration level.

**EXAMPLE:**
```
ProCurveRS(config)# dot1x-enable
ProCurveRS(config-dot1x)#
```

**Syntax:** `[no] dot1x-enable`

**Possible values:** N/A
enable
Three levels of passwords can be assigned to provide a range of access point for various users within the network.
The three levels are:
• Super user: This user has unlimited access to all levels of the CLI. This level is generally reserved for system administration. The super user is also the only user that can assign a password access level to another user.
• Configure Port: This user has the ability to configure interface parameters only. The user can also use the show commands.
• Read only: A user with this password level is able to use only the show commands. No configuration is allowed with this access type.

EXAMPLE:
ProCurveRS(config)# enable super-user-password Larry
ProCurveRS(config)# enable read-only-password Moe
ProCurveRS(config)# enable port-config-password Curly

Syntax: enable super-user-password | read-only-password | port-config-password <text>
Possible values: Up to 32 alphanumeric characters can be assigned in the <text> field. The password cannot begin with a number.

Default value: No system default

enable aaa console
Configures the device to perform command authorization and command accounting for commands entered at the console.

EXAMPLE:
ProCurveRS(config)# enable aaa console

Syntax: enable aaa console

NOTE: If you have previously configured the device to perform command authorization using a RADIUS server, entering the enable aaa console command may prevent the execution of any subsequent commands entered on the console.
This happens because RADIUS command authorization requires a list of allowable commands from the RADIUS server. This list is obtained during RADIUS authentication. For console sessions, RADIUS authentication is performed only if you have configured Enable authentication and specified RADIUS as the authentication method (for example, with the aaa authentication enable default radius command). If RADIUS authentication is never performed, the list of allowable commands is never obtained from the RADIUS server. Consequently, there would be no allowable commands on the console.

NOTE: In releases prior to 07.8.00, the enable aaa console command only enabled command authorization and command accounting for CLI commands entered at the console. Starting with release 07.8.00, AAA support for commands entered at the console can include the following:
• Login prompt that uses AAA authentication, using authentication-method Lists
• Exec Authorization
• Exec Accounting
• System Accounting

Possible values: N/A
enable password-display

Enables clear-text display of passwords and authentication strings in the output of some show commands:

- Enables display of SNMP community strings in the output of the \textit{show snmp server} command
- Enables display of MD5 authentication strings for BGP4 neighbors and peer groups in the output of the \textit{show ip bgp neighbors} command
- Enables display of passwords and MD5 authentication strings for OSPF virtual links in the output of the \textit{show ip ospf virtual-links} command

\textbf{NOTE:} This command does not override encryption of passwords and authentication strings in the running-config and startup-config file.

\textbf{EXAMPLE:}

```
ProCurveRS(config)# enable password-display
```

\textbf{Syntax:} enable password-display

\textbf{Possible values:} N/A

\textbf{Default value:} Disabled

enable password-min-length

Configures the device to require that Line (Telnet), Enable, and Local passwords be at least a specified length.

\textbf{EXAMPLE:}

```
ProCurveRS(config)# enable password-min-length 8
```

\textbf{Syntax:} enable password-min-length \textless number-of-characters\textgreater

\textbf{Possible values:} 1 – 48

\textbf{Default value:} By default, the HP device imposes no minimum length on the Line, Enable, or Local passwords.

enable skip-page-display

Removes the stop page display characteristic for the \textit{write terminal} command. For example, by default, when you enter the command \textit{write terminal}, the full configuration file displayed will generally involve more than a single page display. You are prompted to press the Return key to view the next page of information. When this command is enabled, this page-by-page prompting will be removed and the entire display will roll on the screen until the end is reached.

To re-enable the stop page display characteristic, enter the \textbf{no enable skip-page-display} command.

\textbf{EXAMPLE:}

```
To remove the page-by-page display of configuration information, enter the following:
```

```
ProCurveRS(config)# enable skip-page-display
```

\textbf{Syntax:} enable skip-page-display

\textbf{Possible values:} N/A

\textbf{Default value:} Disabled

enable snmp config-radius

Enables users of SNMP management applications to configure RADIUS authentication parameters on the HP device.

\textbf{EXAMPLE:}

```
To enable SNMP users to configure RADIUS authentication parameters on the HP device, enter the following:
```

```
ProCurveRS(config)# enable snmp config-radius
```
Global CONFIG Commands

**Syntax:** enable snmp config-radius

**Possible values:** N/A

**Default value:** Disabled

**enable snmp config-tacacs**

Enables users of SNMP management applications to configure TACACS/TACACS+ authentication parameters on the HP device.

**EXAMPLE:**

To enable SNMP users to configure TACACS/TACACS+ authentication parameters on the HP device, enter the following:

```
ProCurveRS(config)# enable snmp config-tacacs
```

**Syntax:** enable snmp config-tacacs

**Possible values:** N/A

**Default value:** Disabled

**enable telnet authentication**

Allows you to use local access control, a RADIUS server, or a TACACS/TACACS+ server to authenticate telnet access to the device.

**EXAMPLE:**

```
ProCurveRS(config)# enable telnet authentication
```

**Syntax:** [no] enable telnet authentication

**Possible values:** N/A

**Default value:** Disabled

**enable telnet password**

Allows you to assign a password for Telnet session access. To close a Telnet session, enter `logout`.

**EXAMPLE:**

```
ProCurveRS(config)# enable telnet password secretsalso
```

**Syntax:** enable telnet password <text>

**Possible values:** Up to 32 alphanumeric characters can be assigned as the password.

**Default value:** No system default.

**enable-acl-counter**

Enables ACL accounting. Once accounting is enabled, you can disable it with the `no enable-acl-counter` command. Disabling and then re-enabling ACL accounting resets the counters to zero.

**EXAMPLE:**

```
ProCurveRS(config)# enable-acl-counter
```

**Syntax:** [no] enable-acl-counter

**Possible values:** N/A

**Default value:** By default, ACL accounting is disabled.

**end**

Moves activity to the privileged EXEC level from any level of the CLI, with the exception of the user level.

**EXAMPLE:**

To move to the privileged level, enter the following from any level of the CLI:
ProCurveRS(config)# end
ProCurveRS#

Syntax: end
Possible values: N/A
Default value: N/A

exit
Moves activity up one level from the current level. In this case, activity will be moved to the privileged level.

EXAMPLE:
To move from the global level, back to the privileged level, enter the following:
ProCurveRS(config)# exit
ProCurveRS#

Syntax: exit
Possible values: N/A
Default value: N/A

fan init
Manually initializes the fan control modules on the ProCurve 9408sl chassis.

EXAMPLE:
To manually initialize both fan control modules, enter the following:
ProCurveRS(config)# fan 2 init

Syntax: fan <fan> init
For the fan parameter, you can specify the following:
0 – The system initializes fan 0.
1 – The system initializes fan 1.
2 – The system initializes both fan 0 and fan 1.

fan-read-speed
Displays the status and speed of one or both of the two four-speed fans in the ProCurve 9408sl chassis.

EXAMPLE:
To display the status and speed of both four-speed fans, enter the following command:
ProCurveRS# fan 2 read-speed
Fan0: Status = OK, Speed = LOW, ISP
Fan1: Status = OK, Speed = LOW, ISP

Syntax: fan <fan> read-speed
For the fan parameter, you can specify the following:
0 – The system initializes fan 0.
1 – The system initializes fan 1.
2 – The system initializes both fan 0 and fan 1.

NOTE: “Fan 0” refers to the fan marked “Fan A” on the ProCurve 9408sl chassis rear, and “Fan 1” refers to the fan marked “Fan B.”
The displays show the following information:

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Status</td>
<td>The status can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• OK – The fan is functioning properly and is keeping the temperature of each module within an acceptable temperature range.</td>
</tr>
<tr>
<td></td>
<td>• Failed – The fan is not functioning properly or the fan control module cannot control the fan.</td>
</tr>
<tr>
<td>Speed</td>
<td>The speed can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• LOW – The fan is functioning at 50 percent of capacity.</td>
</tr>
<tr>
<td></td>
<td>• MEDIUM – The fan is functioning at 75 percent of capacity.</td>
</tr>
<tr>
<td></td>
<td>• MEDIUM-HIGH – The fan is functioning at 90 percent of capacity.</td>
</tr>
<tr>
<td></td>
<td>• HIGH – The fan is functioning at 100 percent of capacity.</td>
</tr>
<tr>
<td>ISP</td>
<td>The fan is a version suited for use in an ISP setting.</td>
</tr>
</tbody>
</table>

**fan read-temp**

Displays the temperature of one or both fan modules on the ProCurve 9408sl chassis.

**EXAMPLE:**

To display the temperature of both fan control modules, enter the following command:

```
ProCurveRS# fan 2 read-temp
Fan0: Temperature = 31.40C
Fan1: Temperature = 33.6C
```

**Syntax:** `fan <fan> read-temp`

For the `<fan>` parameter, you can specify the following:

0 – The system reads the temperature of fan 0.
1 – The system reads the temperature of fan 1.
2 – The system reads the temperature of both fan 0 and fan 1.

**fan set-speed**

Manually sets the speed of one or both fans on the ProCurve 9408sl chassis.

**EXAMPLE:**

To manually set the fan speed of fan 0 to medium-high, enter the following:

```
ProCurveRS(config)# fan 0 set-speed 2
```

**Syntax:** `fan <fan> set-speed <fan-speed>`

For the `fan` parameter, you can specify the following:

0 – The system sets the speed of fan 0.
1 – The system sets the speed of fan 1.
2 – The system sets the speed of both fan 0 and fan 1.

For the `fan-speed` parameter, you can specify the following:

0 – The system sets the fan speed to low.
1 – The system sets the fan speed to medium.
2 – The system sets the fan speed to medium-high.
3 – The system sets the fan speed to high.
fan-threshold

Allows you to set fan speed based on high and low temperature thresholds. Temperature thresholds can be set individually for interface modules, management module, and switch fabric.

- If the temperature of all modules falls between the low and high thresholds for a fan speed, the fan continues to operate at that fan speed.

- If the temperature of a management module or the switch fabric module or two interface modules exceeds the high threshold specified for a fan speed, the fan increases its speed to the next higher speed. If the temperature of any of these module(s) exceeds the high threshold for the high speed for 3 minutes (the actual number of polls is determined by the setting of the temp-poll-period command), the system shuts down the module(s) to prevent damage.

- If the temperature of a management module, the switch fabric module, and all interface modules falls below the low threshold for a fan speed, the fan decreases its speed to the next lower speed. If the temperature of all modules falls below the high threshold for the low speed, the fan operates at the low speed.

**EXAMPLE:**

To change the low and high thresholds of the medium fan speed for the management modules to 56°C and 72°C, respectively, enter the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# fan-threshold mp med 56 72
```

**Syntax:** fan-threshold <module> [low <high-threshold>] [med <low-threshold> <high-threshold>] [med-hi <low-threshold> <high-threshold>] [hi <low-threshold> <high-threshold>]

**Possible values:** N/A

**Default value:** Table 6.4 outlines the default low and high temperature thresholds for each module and fan speed.
Table 6.4: Default Low and High Temperature Thresholds For Modules and Fan Speeds

<table>
<thead>
<tr>
<th>Fan Speed</th>
<th>Low Temperature Threshold</th>
<th>High Temperature Threshold</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Management modules</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>77°C</td>
<td>85°C</td>
</tr>
<tr>
<td>Medium-high</td>
<td>67°C</td>
<td>80°C</td>
</tr>
<tr>
<td>Medium</td>
<td>57°C</td>
<td>70°C</td>
</tr>
<tr>
<td>Low</td>
<td>–</td>
<td>60°C</td>
</tr>
<tr>
<td><strong>Interface modules</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>72°C</td>
<td>85°C</td>
</tr>
<tr>
<td>Medium-high</td>
<td>67°C</td>
<td>80°C</td>
</tr>
<tr>
<td>Medium</td>
<td>62°C</td>
<td>75°C</td>
</tr>
<tr>
<td>Low</td>
<td>–</td>
<td>70°C</td>
</tr>
<tr>
<td><strong>Switch fabric module</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>72°C</td>
<td>85°C</td>
</tr>
<tr>
<td>Medium-high</td>
<td>67°C</td>
<td>80°C</td>
</tr>
<tr>
<td>Medium</td>
<td>62°C</td>
<td>75°C</td>
</tr>
<tr>
<td>Low</td>
<td>–</td>
<td>70°C</td>
</tr>
</tbody>
</table>

**fast port-span**
Configures the Fast Port Span feature, which allows faster STP convergence on ports that are attached to end stations.

**EXAMPLE:**
To enable Fast Port Span:

```
ProCurveRS(config)# fast port-span
```

**EXAMPLE:**
To exclude a port from Fast Port Span, while leaving Fast Port Span enabled globally:

```
ProCurveRS(config)# fast port-span exclude ethernet 1/1
```

**Syntax:** [no] fast port-span [exclude ethernet <portnum> [ethernet <portnum>… | to <portnum>]]

**Possible values:** Valid port numbers

**Default value:** Enabled

**fast uplink-span**
Configures the Fast Uplink Span feature, which reduces the convergence time for uplink ports to another device to just four seconds (two seconds for listening and two seconds for learning).

**EXAMPLE:**
To configure a group of ports for Fast Uplink Span, enter the following commands:

```
ProCurveRS(config)# fast uplink-span ethernet 4/1 to 4/4
```
**Syntax:** [no] fast uplink-span [ethernet <portnum> [ethernet <portnum>… | to <portnum>]

**Possible values:** Ports that have redundant uplinks on a wiring closet switch.

**Default value:** Disabled

**fdp holdtime**

Changes the FDP hold time. By default, an HP device that receives an FDP update holds the information until one of the following events occurs:

- The device receives a new update.
- 180 seconds have passed since receipt of the last update. This is the hold time.

Once either of these events occurs, the device discards the update.

**EXAMPLE:**

ProCurveRS(config)# fdp holdtime 360

**Syntax:** [no] fdp holdtime <secs>

The `<secs>` parameter specifies the number of seconds an HP device that receives an FDP update can hold the update before discarding it.

**Possible values:** 10 – 255 seconds

**Default value:** 180 seconds

**fdp run**

Enables an HP device to send FDP packets. The FDP enables HP devices to advertise themselves to other Routing Switches on the network.

**EXAMPLE:**

ProCurveRS(config)# fdp run

**Syntax:** [no] fdp run

**Possible values:** N/A

**Default value:** Disabled

**fdp timer**

Changes the FDP update timer.

ProCurveRS(config)# fdp timer 120

**Syntax:** [no] fdp timer <secs>

The `<secs>` parameter specifies the number of seconds between updates.

**Possible values:** 5 – 900 seconds

**Default value:** 60 seconds

**flash <num>**

Changes the block size for TFTP file transfers.

When you use TFTP to copy a file to or from a device, the device transfers the data in blocks of 8192 bytes by default. You can change the block size to one of the following if needed:

- 4096
- 2048
- 1024
- 512
- 256
GLOBAL CONFIG COMMANDS

- 128
- 64
- 32
- 16

EXAMPLE:
To change the block size for TFTP file transfers, enter a command such as the following at the global CONFIG level of the CLI:

ProCurveRS(config)# flash 2047
set flash copy block size to 2048

Syntax: [no] flash <num>

The software rounds up the <num> value you enter to the next valid power of two, and displays the resulting value. In this example, the software rounds the value up to 2048.

NOTE: If the value you enter is one of the valid powers of two for this parameter, the software still rounds the value up to the next valid power of two. Thus, if you enter 2048, the software rounds the value up to 4096.

Possible values: See above
Default value: 8192

FLOW-CONTROL

Allows you to turn flow control (802.3x) for full-duplex ports on or off (no). By default, flow control is on. To turn the feature off, enter the command no flow-control.

EXAMPLE:
ProCurveRS(config)# no flow-control
To turn the feature back on later, enter the following command:
ProCurveRS(config)# flow-control

Syntax: [no] flow-control

Possible values: N/A
Default value: on

GIG-DEFAULT

Changes the default negotiation mode for Gigabit ports. You can configure the default Gigabit negotiation mode to be one of the following:

- Negotiate-full-auto – The port first tries to perform a handshake with the other port to exchange capability information. If the other port does not respond to the handshake attempt, the port uses the manually configured configuration information (or the defaults if an administrator has not set the information). This is the default.
- Auto-Gigabit – The port tries to perform a handshake with the other port to exchange capability information.
- Negotiation-off – The port does not try to perform a handshake. Instead, the port uses configuration information manually configured by an administrator.

See the "Configuring Basic Features" chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches for more information.

EXAMPLE:
To change the mode globally to negotiation-off, enter the following command:

ProCurveRS(config)# gig-default neg-off
To override the global default on an individual Gigabit port, see "gig-default" on page 8-6.
Syntax: gig-default neg-full-auto | auto-gig | neg-off
Possible values: see above
Default value: neg-full-auto

gig-default auto-gig rfn

NOTE: This command is supported in software releases 07.8.00 and later, and on fiber ports only.

Globally enables the transmit ports to notify the remote ports whenever a fiber cable is either physically disconnected or has failed. When this feature is enabled, the device disables the link and turns OFF both LEDs associated with the ports.

For more information about this command, see the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches.

EXAMPLE:
To enable Remote Fault Notification (RFN) globally, on the entire device, enter the following command:
ProCurveRS(config)# gig-default auto-gig rfn
To disable RFN after enabling it, use the no parameter with the command.

Syntax: gig-default auto-gig rfn

global-protocol-vlan

The software places this command into the configuration the first time you configure a protocol VLAN. When you save the configuration to the startup-config file, the software places the command in the file.

NOTE: The protocol VLAN flag is not directly configurable. This command is used only by the software.

gvrp-base-vlan-id

Changes the GVRP base VLAN ID.

By default, GVRP uses VLAN 4093 as a base VLAN for the protocol. All ports that are enabled for GVRP become tagged members of this VLAN. If you need to use VLAN ID 4093 for a statically configured VLAN, you can change the GVRP base VLAN ID.

NOTE: If you want to change the GVRP base VLAN ID, you must do so before enabling GVRP.

EXAMPLE:
ProCurveRS(config)# gvrp-base-vlan-id 1001
This command changes the GVRP VLAN ID from 4093 to 1001.

Syntax: [no] gvrp-base-vlan-id <vlan-id>
The <vlan-id> parameter specifies the new VLAN ID. You can specify a VLAN ID from 2 – 4092 or 4095.

Possible values: 2 – 4092 or 4095
Default value: 4093

gvrp-enable

Enables GVRP and changes the CLI to the GVRP configuration level.

EXAMPLE:
ProCurveRS(config)# gvrp-enable
ProCurveRS(config-gvrp)#

Syntax: [no] gvrp-enable
Global CONFIG Commands

For information about the commands at the GVRP configuration level, see “GVRP Commands” on page 34-1.

**Possible values:** N/A

**Default value:** Disabled

gvrp-max-leaveall-timer

Increases the maximum value you can specify for the GVRP Leaveall timer.

By default, the highest value you can specify for the Leaveall timer is 300000 ms. You can increase the maximum configurable value of the Leaveall timer to 1000000 ms.

**NOTE:** You must enter this command before enabling GVRP. Once GVRP is enabled, you cannot change the maximum Leaveall timer value.

**NOTE:** This command does not change the default value of the Leaveall timer itself. The command only changes the maximum value to which you can set the Leaveall timer.

**EXAMPLE:**

ProCurveRS(config)# gvrp-max-leaveall-timer 1000000

**Syntax:** `[no] gvrp-max-leaveall-timer <ms>

The `<ms>` parameter specifies the maximum number of ms to which you can set the Leaveall timer. You can specify from 300000 – 1000000 (one million) ms. The value must be a multiple of 100 ms. The default is 300000 ms.

**Possible values:** 300000 – 1000000 (one million) ms

**Default value:** 300000 ms

hostname

Changes the hostname field to more easily identify HP devices within the network.

**EXAMPLE:**

To change the hostname to “Router1” from the default, “ProCurveRS”, enter the following:

ProCurveRS(config)# hostname Router1

Router1(config)#

**Syntax:** hostname <text>

**Possible values:** Up to 32 alphanumeric characters can be assigned to hostname text string.

**Default value:** The product name

hw-drop-acl-denied-packet

Enables hardware filtering of packets denied by ACLs.

By default, packets denied by ACLs are filtered by the CPU. You can enable the device to create Content Addressable Memory (CAM) entries for packets denied by ACLs. This causes the filtering to occur in hardware instead of in the CPU.

When you enable hardware filtering of denied packets, the first time the device filters a packet denied by an ACL, the device sends the packet to the CPU for processing. The CPU also creates a CAM entry for the denied packet. Subsequent packets with the same address information are filtered using the CAM entry. The CAM entry ages out after two minutes if not used.

**EXAMPLE:**

ProCurveRS(config)# hw-drop-acl-denied-packet

**Syntax:** `[no] hw-drop-acl-denied-packet

June 2005 6 - 45
Possible values: N/A
Default value: Disabled

hw-module
Specifies a hardware module to which to change the CAM partition. See the Diagnostics Guide for ProCurve 9300/9400 Series Routing Switches for more information on CAM partitioning.

EXAMPLE:
ProCurveRS(config)# hw-module 3
ProCurveRS(config-module-3/8)#

Syntax: hw-module <module>
Possible values: Module number
Default value: N/A

interface
Accesses the interface CONFIG level of the CLI. You can define a physical interface, loopback interface, or virtual interface (ve) at the Interface level.

By default, you can add up to 24 IP addresses to a physical, virtual, or loopback interface.

You can configure up to 255 virtual interfaces on a Routing Switch.

You can configure up to eight loopback interfaces on a Routing Switch.

NOTE: You also can increase the total number of IP sub-net interfaces that you can configure on a Routing Switch. See “system-max” on page 6-155.

EXAMPLE:
To add a virtual interface to a Routing Switch, enter the following. Use commands at the Virtual Interface level (vif) to configure the interface.

ProCurveRS(config)# inter ve 1
ProCurveRS(config-vif-1)#

Syntax: interface ve <num>
The <num> parameter specifies the virtual interface number. You can specify from 1 to the maximum number of virtual interfaces supported on the device. To display the maximum number of virtual interfaces supported on the device, enter the show default values command. The maximum is listed in the System Parameters section, in the Current column of the virtual-interface row.

Possible values: See above
Default value: N/A

EXAMPLE:
To add a loopback interface to a Routing Switch, enter the following:

ProCurveRS(config)# int loopback 1
ProCurveRS(config-lbif-1)# ip address 10.0.0.1/24

Syntax: interface loopback <num>
Possible values: 1 – 15
Default value: N/A

NOTE: For information about the commands you can enter at the interface configuration level, see “Interface Commands” on page 8-1.
interface group-ve

Begins configuration of a virtual interface group. A virtual interface group allows you to configure virtual interface attributes one time, then apply the attributes to multiple virtual interfaces.

NOTE: This feature applies only to VLAN groups. See the "Configuring Virtual LANs (VLANs)" chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches.

EXAMPLE:
To configure a virtual interface group, enter commands such as the following:

ProCurveRS(config)# vlan-group 1
ProCurveRS(config-vlan-group-1)# group-router-interface
ProCurveRS(config-vlan-group-1)# exit
ProCurveRS(config)# interface group-ve 1
ProCurveRS(config-vif-group-1)# ip address 10.10.10.1/24

These commands enable VLAN group 1 to have a group virtual interface, then configure virtual interface group 1. The software always associates a virtual interface group only with the VLAN group that has the same ID. In this example, the VLAN group ID is 1, so the corresponding virtual interface group also must have ID 1.

Syntax: group-router-interface

Syntax: interface group-ve <num>

Syntax: [no] ip address <ip-addr> <ip-mask> [secondary]

or

Syntax: [no] ip address <ip-addr>/<mask-bits> [secondary]

The router-interface-group command enables a VLAN group to use a virtual interface group. Enter this command at the configuration level for the VLAN group. This command configures the VLAN group to use the virtual interface group that has the same ID as the VLAN group. You can enter this command when you configure the VLAN group for the first time or later, after you have added tagged ports to the VLAN and so on.

The <num> parameter in the interface group-ve <num> command specifies the ID of the VLAN group with which you want to associate this virtual interface group. The VLAN group must already be configured and enabled to use a virtual interface group. The software automatically associates the virtual interface group with the VLAN group that has the same ID. You can associate a virtual interface group only with the VLAN group that has the same ID.

The syntax and usage for the ip address command is the same as when you use the command at the interface level to add an IP interface.

Possible values: See above

Default value: N/A

interface link-hold-down

Delays initialization of the device's ports following a software reload.

By default, the software brings up the ports on an HP device as soon as the software has fully finished booting. Some devices attached to the HP device might require more time to properly initialize and establish a link with the HP device.

In this case, you can configure the software to delay bringing up the device's ports for an additional number of milliseconds, up to 100 (one second).

NOTE: The actual amount of time it takes to bring a port up is slightly longer than the hold-down time. After fully booting the software, the device initializes the ports, which takes an additional few seconds.
EXAMPLE:
To delay port initialization on an HP device, enter a command such as the following at the global CONFIG level for
the port:

```
ProCurveRS(config)# interface link-hold-down 50
```

This command delays initialization of the device’s ports for 50 milliseconds (one half second) following completion
of a software reload.

**Syntax:** [no] interface link-hold-down <msecs>

The `<msecs>` parameter specifies the number of milliseconds to wait before initializing the ports. You can specify
from 0 – 100. The default is 0.

**Possible values:** See above

**Default value:** Disabled

**ip access-list**
Confines a named IP ACL.

You can use this command to configure a standard or extended IP ACL.

The `ip access-list` command can be used to configure numbered and named ACLs. You can also configure
numbered ACLs using the `access-list` command.

When you use the `ip access-list` command, you can configure named ACLs as well as numbered ACL. Also,
when you enter the `ip access-list` command, you specify the ID (name or number) and the ACL type (standard or
extended). The command then places you at the named ACL configuration level. Once you enter the configuration
level for the named ACL, the command syntax is the same as the syntax for numbered ACLs.

**EXAMPLE:**
To configure a named standard ACL entry, enter commands such as the following.

```
ProCurveRS(config)# ip access-list standard Net1
ProCurveRS(config-standard-nacl)# deny host 209.157.22.26 ... exit
ProCurveRS(config)# int eth 1/1
ProCurveRS(config-if-1/1)# ip access-group Net1 out
```

The commands in this example configure a standard ACL named “Net1”. The entries in this ACL deny packets
from three source IP addresses from being forwarded on port 1/1. Since the implicit action for an ACL is “deny”,
the last ACL entry in this ACL permits all packets that are not explicitly denied by the first three ACL entries. For
an example of how to configure the same entries in a numbered ACL, see the “Configuring Standard ACLs”
section of the “Using Access Control Lists (ACLs)” chapter of the *Advanced Configuration and Management Guide
for ProCurve 9300/9400 Series Routing Switches*.

Notice that the command prompt changes after you enter the ACL type and name. The “std” in the command
prompt indicates that you are configuring entries for a standard ACL. For an extended ACL, this part of the
command prompt is “ext”. The “nacl” indicates that are configuring a named ACL.

**Syntax:** [no] ip access-list extended | standard <string> | <num>
[delete <line-number> | insert <line-number> | replace <line-number> [remark [<comment-text>]]
<options>

The **extended | standard** parameter indicates the ACL type.

The `<string>` parameter is the ACL name. You can specify a string of up to 256 alphanumeric characters. You can
use blanks in the ACL name if you enclose the name in quotation marks (for example, “ACL for Net1”). The
`<num>` parameter allows you to specify an ACL number if you prefer. If you specify a number, you can specify
from 1 – 99 for standard ACLs or 100 – 199 for extended ACLs.

**Possible values:** See above
Global CONFIG Commands

Default value: N/A

**ip access-list disable-log-to-cpu**

Globally disables ACL logging.

This command is useful for EP devices. Hardware-based ACLs do not support the `log` option. Even when hardware-based ACLs are enabled, if an ACL entry has the `log` option, traffic that matches that ACL is sent to the CPU for processing.

If your configuration already contains ACLs that you want to use with hardware-based ACLs, but some of the ACLs contain the `log` option, you can globally disable ACL logging without the need to remove the `log` option from each ACL entry. When you globally disable ACL logging, the ACL entries remain unchanged but the `log` option is ignored and the ACL can use the hardware-based ACL mode.

**EXAMPLE:**

ProCurveRS(config)# ip access-list disable-log-to-cpu

**Syntax:** `[no] ip access-list disable-log-to-cpu`

To re-enable ACL logging, enter the following command:

ProCurveRS(config)# no ip access-list disable-log-to-cpu

**Possible values:** N/A

Default value: ACL logging is enabled

**ip access-list frag-rate-on-interface**

Sets the fragment threshold for EP rule-based ACLs, for individual interfaces. If an individual interface receives more than the specified maximum number of fragments, the device takes the exceed action you specify.

The device can send to the CPU only the number of fragments you specify per second, regardless of which interfaces the fragments come in on. If the threshold is exceeded, the device takes the exceed action you specify.

By default, when you enable CPU filtering of packet fragments, all fragments are sent to the CPU.

**NOTE:** This command applies only to EP devices.

**EXAMPLE:**

ProCurveRS(config)# ip access-list frag-rate-on-interface 5000 exceed-action forward reset-interval 5

This command sets the fragment threshold at 5,000 for individual interfaces. If any interface on the device receives more than 5,000 fragments in a one-second interval, the device takes the specified action. In this case, the action is to forward the fragments in hardware without filtering them. The device continues forwarding fragments in hardware for five minutes before beginning to send fragments to the CPU again.

**Syntax:** `[no] ip access-list frag-rate-on-interface <num> exceed-action drop | forward reset-interval <mins>`

The `<num>` parameter specifies the maximum number of fragments the device or an individual interface can receive and send to the CPU in a one-second interval.

The `<num>` parameter specifies the maximum number of fragments per second. You can specify from 300 – 8000.

The `drop | forward` parameter specifies the action to take if the threshold (`<num>` parameter) is exceeded:

- **drop** – fragments are dropped without filtering by the ACLs
- **forward** – fragments are forwarded in hardware without filtering by the ACLs

The `<mins>` parameter specifies the number of minutes the device will enforce the drop or forward action after a threshold has been exceeded. You can specify from 1 – 30 minutes.

**Possible values:** see above
Default value: see above

**ip access-list frag-rate-on-system**

Sets the fragment threshold for EP rule-based ACLs, for the entire device. The device can send to the CPU only the number of fragments you specify per second, regardless of which interfaces the fragments come in on. If the threshold is exceeded, the device takes the exceed action you specify.

By default, when you enable CPU filtering of packet fragments, all fragments are sent to the CPU.

**NOTE:** This command applies only to EP devices.

**EXAMPLE:**

ProCurveRS(config)# ip access-list frag-rate-on-system 15000 exceed-action drop reset-interval 10

This command sets the fragment threshold at 15,000 per second, for the entire device. If the device receives more than 15,000 packet fragments in a one-second interval, the device takes the specified action. The action specified with this command is to drop the excess fragments and continue dropping fragments for a holddown time of ten minutes. After the ten minutes have passed, the device starts sending fragments to the CPU again for processing.

**Syntax:** [no] ip access-list frag-rate-on-system <num> exceed-action drop | forward reset-interval <mins>

The `<num>` parameter specifies the maximum number of fragments the device or an individual interface can receive and send to the CPU in a one-second interval.

The `<num>` parameter specifies the maximum number of fragments per second. You can specify from 600 – 12800.

The `drop | forward` parameter specifies the action to take if the threshold `<num>` parameter is exceeded:

- **drop** – fragments are dropped without filtering by the ACLs
- **forward** – fragments are forwarded in hardware without filtering by the ACLs

The `<mins>` parameter specifies the number of minutes the device will enforce the drop or forward action after a threshold has been exceeded. You can specify from 1 – 30 minutes.

**Possible values:** see above

**Default value:** see above

**ip access-list logging-age**

Configures the Layer 4 session log timer, which is used for keeping track of packets explicitly denied by an ACL. In releases prior to 07.6.04, the timer interval was set to 5 minutes and was not configurable.

The timer keeps track of all packets explicitly denied by the ACL entries. When the timer expires, the software generates a single Syslog entry for each ACL entry that has denied a packet. The message indicates the number of packets denied by the ACL entry from the time that the timer was started. If no ACL entries explicitly permit or deny packets during an entire timer interval, the timer stops. The timer restarts when an ACL entry explicitly permits or denies a packet.

To store information about denied packets during the timer interval, the device makes entries in its Layer 4 session table. If a large number of packets are denied by the ACL during the timer interval, it can consume a large portion of the device's Layer 4 resources. To prevent this from happening, starting in release 07.6.04, you can configure the timer interval to be a shorter length of time.

**EXAMPLE:**

For example, to set the timer interval to 2 minutes, enter the following command:

ProCurveRS(config)# ip access-list logging-age 2

**Syntax:** ip access-list logging-age <minutes>

**Possible values:** You can set the timer to between 1 and 10 minutes.
**Global CONFIG Commands**

**Default:** The default is 5 minutes.

**ip access-policy**
Configures permit and deny policies and Layer 4 QoS policies on Routing Switches. See the "Policies and Filters" appendix of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches for more information.

**NOTE:** Access policies on Routing Switches can permit or deny packets (filter) or allocate packets to specific QoS levels.

**NOTE:** After you configure an IP access policy, you need to apply it to specific ports using the ip access-policy-group command at the Interface level of the CLI. See “ip access-policy-group” on page 8-10.

**Permit and Deny Policies**
IP access policies are rules that determine whether the device forwards or drops IP packets. You create an IP access policy by defining an IP filter, then applying it to an interface. The filter consists of source and destination IP information and the action to take when a packet matches the values in the filter. You can configure an IP filter to permit (forward) or deny (drop) the packet.

You can apply an IP filter to inbound or outbound packets. When you apply the filter to an interface, you specify whether the filter applies to inbound packets or outbound packets. Thus, you can use the same filter on multiple interfaces and specify the filter direction independently on each interface.

**EXAMPLE:**
To configure an IP access policy to explicitly permit HTTP traffic (TCP port 80) from IP address 10.0.0.1 on port 1/2, enter the following commands:

```
ProCurveRS(config)# ip access-policy 2 permit 10.0.0.1 255.0.0.0 tcp eq 80
ProCurveRS(config)# int e 1/2
ProCurveRS(config-if-1/2)# ip access-policy-group in 2
```

**Syntax:**
```
ip access-policy <num> deny | permit <ip-addr> <mask> | any <ip-addr> <ip-mask> | any icmp | igmp | igrp | ospf | tcp | udp | <num> [<operator> [<tcp/udp-port-num>]] [log]
```

**Syntax:**
ip access-policy-group in | out <policy-list>

The <num> parameter is the policy number.

**Syntax:**
ip access-policy <num> priority <0-7> <ip-addr> <ip-mask> | any <ip-addr> <ip-mask> | any tcp | udp [<operator> [<tcp/udp-port-num>]]

**Syntax:**
ip access-policy-group in | out <policy-list>

The <num> parameter is the policy number.

The priority <0-7> and high | normal parameters specify the QoS priority level. The defaults are 0 (normal priority). The highest priority is 7.

The <ip-addr> <ip-mask> | any <ip-addr> <ip-mask> | any parameters specify the source and destination IP addresses. If you specify a particular IP address, you also need to specify the mask for that address. If you specify any to apply the policy to all source or destination addresses, you do not need to specify any again for the mask. Make sure you specify a separate address and mask or any for the source and destination address.

The icmp | igmp | igrp | ospf | tcp | udp | <num> parameter specifies the Layer 4 port to which you are applying the policy. If you specify tcp or udp, you also can use the optional <operator> and <tcp/udp-port-num> parameters to fine-tune the policy to apply to specific TCP or UDP ports.

The <operator> parameter applies only if you use the tcp or udp parameter above. Use the <operator> parameter to specify the comparison condition for the specific TCP or UDP ports. For example, if you are configuring QoS for HTTP, specify tcp eq http. You can enter one of the following operators:
• **eq** – The policy applies to the TCP or UDP port name or number you enter after `eq`.

• **gt** – The policy applies to TCP or UDP port numbers greater than the port number or the numeric equivalent of the port name you enter after `gt`.

• **lt** – The policy applies to TCP or UDP port numbers that are less than the port number or the numeric equivalent of the port name you enter after `lt`.

• **neq** – The policy applies to all TCP or UDP port numbers except the port number or port name you enter after `neq`.

• **range** – The policy applies to all TCP or UDP port numbers that are between the first TCP or UDP port name or number and the second one you enter following the range parameter. The range includes the port names or numbers you enter. For example, to apply the policy to all ports between and including 23 (Telnet) and 53 (DNS), enter the following: `range 23 53`. The first port number in the range must be lower than the last number in the range.

• **established** – This operator applies only to TCP packets. If you use this operator, the QoS policy applies to TCP packets that have the ACK (Acknowledgment) or RST (Reset) bits set on (set to "1") in the Control Bits field of the TCP packet header. Thus, the policy applies only to established TCP sessions, not to new sessions. See Section 3.1, "Header Format", in RFC 793 for information about this field.

### ip arp-age

Defines how long an ARP entry will be resident in the ARP cache before it is aged out.

**EXAMPLE:**

```
ProCurveRS(config)# ip arp-age 20
```

**Syntax:** `ip arp-age <num>`

The `<num>` parameter specifies the number of minutes and can be from 0 – 240. The default is 10. If you specify 0, aging is disabled.

**Possible values:** 0 – 240 minutes

**Default value:** 10 minutes

### ip as-path

Configures an AS-path ACL. You can use AS-path ACLs to permit or deny routes based on their AS path information.

**EXAMPLE:**

To configure an AS-path list that uses ACL 1, enter a command such as the following:

```
ProCurveRS(config)# ip as-path access-list 1 permit 100
ProCurveRS(config)# router bgp
ProCurveRS(config-bgp-router)# neighbor 10.10.10.1 filter-list 1 in
```

The `ip as-path` command configures an AS-path ACL that permits routes containing AS number 100 in their AS paths. The `neighbor` command then applies the AS-path ACL to advertisements and updates received from neighbor 10.10.10.1. In this example, the only routes the Routing Switch permits from neighbor 10.10.10.1 are those whose AS-paths contain AS-number 100.

**Syntax:** `ip as-path access-list <string> [seq <seq-value>] deny | permit <regular-expression>`

The `<string>` parameter specifies the ACL name. (If you enter a number, the CLI interprets the number as a text string.)

The `seq` `<seq-value>` parameter is optional and specifies the AS-path list's sequence number. You can configure up to 199 entries in an AS-path list. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with number 5. The software interprets the entries in an AS-path list in numerical order, beginning with the lowest sequence number.
The deny | permit parameter specifies the action the software takes if a route’s AS-path list matches a match statement in this ACL. To configure the AS-path match statements in a route map, use the match as-path command. See “match” on page 27-1.

The <regular-expression> parameter specifies the AS path information you want to permit or deny to routes that match any of the match statements within the ACL. You can enter a specific AS number or use a regular expression. For the regular expression syntax, see the “Configuring BGP4” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The neighbor command uses the filter-list parameter to apply the AS-path ACL to the neighbor. See “neighbor” on page 17-11.

Possible values: see above

Default value: N/A

**ip broadcast-zero**

Enables or disables support for zero-based IP sub-net broadcasts. By default, the Routing Switch treats IP packets with all ones in the host portion of the address as IP broadcast packets, but does not treat packets with all zeros in the host portion as IP sub-net broadcasts.

**NOTE:** When you enable the Routing Switch for zero-based sub-net broadcasts, it still treats IP packets with all ones the host portion as IP sub-net broadcasts too. Thus, the Routing Switch can be configured to support all ones only (the default) or all ones and all zeroes.

**EXAMPLE:**

To enable the Routing Switch for zero-based IP sub-net broadcasts in addition to ones-based IP sub-net broadcasts, enter the following command.

```
ProCurveRS(config)# ip broadcast-zero
```

**Syntax:** [no] ip broadcast-zero

Possible values: enabled or disabled

Default value: disabled

**ip cache-age**

Removes the IP cache if it has been idle for a specified number of minutes.

**EXAMPLE:**

To clear the IP cache if it has been idle for 4 minutes, enter the following command:

```
ProCurveRS(config)# ip cache-age 4
```

**Syntax:** ip cache-age <1–7>

**Possible values:** 1– 7 is the number of minutes

**Default value:** 5 minutes

**ip community-list**

Configures a community ACL. You can use community ACLs to permit or deny routes based on their communities.

**EXAMPLE:**

To configure community ACL 1, enter a command such as the following:

```
ProCurveRS(config)# ip community-list 1 permit 123:2
```

This command configures a community ACL that permits routes that contain community 123:2.
NOTE: See "match" on page 27-1 for information about how to use a community list as a match condition in a route map.

Syntax: ip community-list standard <string> [seq <seq-value>] deny | permit <community-num>

Syntax: ip community-list extended <string> [seq <seq-value>] deny | permit <community-num> | <regular-expression>

The <string> parameter specifies the ACL name. (If you enter a number, the CLI interprets the number as a text string.)

The standard or extended parameter specifies whether you are configuring a standard community ACL or an extended one. A standard community ACL does not support regular expressions whereas an extended one does. This is the only difference between standard and extended IP community lists.

The seq <seq-value> parameter is optional and specifies the community list's sequence number. You can configure up to 199 entries in a community list. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with number 5. The software interprets the entries in a community list in numerical order, beginning with the lowest sequence number.

The deny | permit parameter specifies the action the software takes if a route's community list matches a match statement in this ACL. To configure the community-list match statements in a route map, use the match community command.

The <community-num> parameter specifies the community type or community number. This parameter can have the following values:

- <num>:<num> – A specific community number
- internet – The Internet community
- no-export – The community of sub-ASs within a confederation. Routes with this community can be exported to other sub-ASs within the same confederation but cannot be exported outside the confederation to other ASs or otherwise sent to EBGP neighbors.
- local-as – The local sub-AS within the confederation. Routes with this community can be advertised only within the local subAS.
- no-advertise – Routes with this community cannot be advertised to any other BGP4 routers at all.

The <regular-expression> parameter is a regular expression. For syntax information for the regular expressions, see the "Using Regular Expressions" section of the "Configuring BGP4" chapter in the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches. You can specify a regular expression only in an extended community ACL.

Possible values: see above

Default value: N/A

ip default-network

Configures a default network route, use one of the following methods. You can configure up to four default network routes.

EXAMPLE:

To configure a default network route, enter commands such as the following:

ProCurveRS(config)# ip default-network 209.157.22.0
ProCurveRS(config)# write memory

Syntax: ip default-network <ip-addr>

The <ip-addr> parameter specifies the network address.

To verify that the route is in the route table, enter the following command at any level of the CLI:
ProCurveRS(config)# show ip route

<table>
<thead>
<tr>
<th>Destination</th>
<th>NetMask</th>
<th>Gateway</th>
<th>Port</th>
<th>Cost</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>209.157.20.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>lb1</td>
<td>1</td>
<td>D</td>
</tr>
<tr>
<td>209.157.22.0</td>
<td>255.255.255.0</td>
<td>0.0.0.0</td>
<td>4/11</td>
<td>1</td>
<td>*D</td>
</tr>
</tbody>
</table>

This example shows two routes. Both of the routes are directly attached, as indicated in the Type column. However, one of the routes is shown as type “*D”, with an asterisk (*). The asterisk indicates that this route is a candidate default network route.

**Possible values:** valid IP network address

**Default value:** N/A

**ip dhcp-valid-check**

Disables the forwarding of Microsoft RIS DHCP packets. In releases prior to 07.2.08, HP devices did not forward Microsoft RIS DHCP packets. Starting with release 07.2.08, Microsoft RIS DHCP packets are forwarded by default, but you can disable forwarding of these packets with this command.

**EXAMPLE:**

ProCurveRS(config)# ip dhcp-valid-check

**Syntax:** [no] ip dhcp-valid-check

**Possible values:** N/A

**Default value:** disabled (Microsoft RIS DHCP packets are forwarded)

**ip directed-broadcast**

Enables or disables forwarding of directed IP broadcasts on a Routing Switch.

**EXAMPLE:**

ProCurveRS(config)# ip directed-broadcast

**Syntax:** [no] ip directed-broadcast

**Possible values:** N/A

**Default value:** disabled

**ip dns domain-name**

Defines a domain name for a range of addresses on the ProCurve Routing Switch. This eliminates the need to type in the domain name. It will automatically be appended to the hostname.

**EXAMPLE:**

ProCurveRS(config)# ip dns domain-name newyork.com

**Syntax:** ip dns domain-name

**Possible values:** N/A

**Default value:** N/A

**ip dns server-address**

Up to four DNS servers can be defined for each DNS entry. The first entry serves as the primary default address (207.95.6.199). If a query to the primary address fails to be resolved after three attempts, the next gateway address will be queried for three times as well. This process will continue for each defined gateway address until a query is resolved. The order in which the default gateway addresses are polled is tied to the order in which they are entered when initially defined as shown in the example.
EXAMPLE:
ProCurveRS(config)# ip dns server-address 207.95.6.199 205.96.7.1 5 208.95.7.25 201.98.7.15

**Syntax:** ip dns server-address <ip-addr> [<ip-addr>] [<ip-addr>] [<ip-addr>]

**Possible values:** Up to four IP addresses

**Default value:** N/A

---

**ip dont-use-acl**

Disables all packet-forwarding IP ACLs (those associated with specific ports) and also prevents you from associating an IP ACL with a port. However, the command does not remove existing IP ACLs from the startup-config file. In addition, the command does not affect IP ACLs used for controlling management access to the device.

**NOTE:** A Routing Switch cannot actively use both IP access policies and IP ACLs for filtering IP traffic. When you boot a Routing Switch with software release 06.6.05 or higher, the software checks the device's startup-config file for **ip access-policy-group** commands, which associate IP access policies with ports. If the software finds an **ip access-policy-group** command in the file, the software disables all packet-forwarding IP ACLs (those associated with specific ports) and also prevents you from applying an IP ACL to a port.

The next time you save the startup-config file, the software adds the **ip dont-use-acl** command near the top of the file, underneath the ver (software version) statement.

---

**EXAMPLE:**

**Disabling ACL Mode**

If the ACL mode is enabled, a message is displayed when you try to apply an IP access policy to a port, as shown in the following CLI example:

ProCurveRS(config-if-e1000-1/1)# ip access-policy-group 1 in

Must disable ACL mode first by using ip dont-use-acl command, write memory and reload

To disable the ACL mode, enter the following commands:

ProCurveRS(config-if-e1000-1/1)# exit
ProCurveRS(config)# ip dont-use-acl
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload

**EXAMPLE:**

**Enabling ACL Mode**

If you try to apply an IP ACL to a port when the ACL mode is disabled (when the **ip dont-use-acl** command is in effect), a message is displayed, as shown in the following CLI example:

ProCurveRS(config-if-e1000-1/1)# ip access-group 1 out

Must enable ACL mode first by using no ip dont-use-acl command and removing all ip access-policy-group commands from interfaces, write memory and reload

As the message states, if you want to use IP ACLs, you must first enable the ACL mode. To do so, use either of the following methods.

To enable the ACL mode, enter the following commands:

ProCurveRS(config-if-e1000-1/1)# exit
ProCurveRS(config)# no ip dont-use-acl
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
The write memory command removes the **ip dont-use-acl** command from the startup-config file. The reload command reloads the software. When the software finishes loading, you can apply IP ACLs to ports.

The commands that configure the IP access policies and apply them to ports remain in the startup-config file in case you want to use them again, but they are disabled. If you later decide you want to use the IP access policies again instead of IP ACLs, you must disable the IP ACL mode again. See Example 1 above.

**Syntax:** [no] ip dont-use-acl

**Possible values:** N/A

**Default value:** see above

### ip dr-aggregate

Optimizes the CAM for devices that have few explicit routes (about 30 or fewer) and use the default route for most of the traffic.

Without CAM default route aggregation, the device programs a CAM entry for each destination that uses an explicit route in the route table and also programs a separate CAM entry for each destination that uses the default route. For example, suppose the IP route table contains two explicit routes, 20.0.0.x and 30.0.0.x and uses the default route for all other destinations. When the device needs to forward traffic to 20.0.0.x, the device uses the existing CAM entry for the destination. If this is the first time the device is forwarding traffic to the destination and the CAM entry therefore hasn't been programmed yet, the device programs the entry for 20.0.0.x.

The same process occurs for traffic destined to a network that doesn't have an explicit route in the IP route table. When the device needs to forward traffic to a destination that requires the default route, the device creates a CAM entry for the destination network. For example, if the device needs to forward traffic to 40.40.40.x and 40.41.41.x, the device creates two CAM entries, one for 40.40.40.x and another for 40.41.41.x.

When the device needs to forward traffic on the default route, the device attempts to build an aggregate route that does not conflict with an explicit route in the IP route table. (A conflict occurs if an explicit host route in the table overlaps with the aggregate.) For example, with CAM default route aggregation enabled, the device creates a single CAM entry, 40.0.0.0/8, for 40.40.40.x and 40.41.41.x. In fact, traffic for any network that overlaps with 40.0.0.0/8 uses the same CAM entry.

The device begins with a /8 aggregate.

- If there are no conflicts with explicit routes, the device programs the /8 aggregate into the CAM.
- If there is a conflict, the device tries a /12 aggregate, and so on in increments of 4 (/16, /20, /24, and so on) until a non-conflicting entry can be programmed into the CAM.

**NOTE:** CAM default route aggregation requires a default route in the IP route table.

Compare with “ip net-aggregate” on page 6-74.

**EXAMPLE:**

```
ProCurveRS(config)# ip dr-aggregate
```

**Syntax:** [no] ip dr-aggregate

**Possible values:** N/A

**Default value:** Disabled

### ip flow-aggregation cache

Configures an aggregate cache for NetFlow.

**EXAMPLE:**

```
ProCurveRS(config)# ip flow-aggregation cache as
ProCurveRS(config-flow-cache_as)#
```
This command begins configuration for the AS aggregate cache. Notice that the CLI prompt changes to the configuration level for the aggregate cache. At the aggregate cache's configuration level, you can change cache parameters. Here is an example:

ProCurveRS(config)# ip flow-aggregation cache as
ProCurveRS(config-flow-cache_as)# cache entries 2046
ProCurveRS(config-flow-cache_as)# cache timeout inactive 200
ProCurveRS(config-flow-cache_as)# cache timeout active 45
ProCurveRS(config-flow-cache_as)# export destination 10.42.42.1 9992
ProCurveRS(config-flow-cache_as)# enabled

The cache commands change cache parameters. The enable command enables the cache. A cache does not go into effect until you enable it.

**Syntax:** [no] ip flow-aggregation cache as | destination-prefix | prefix | protocol-port | source-prefix

The as | destination-prefix | prefix | protocol-port | source-prefix parameter specifies the cache type.

- **as** – Configures an AS cache. Flows are aggregated based on AS number.
- **destination-prefix** – Configures a destination prefix cache. Flows are aggregated based on destination network prefix.
- **prefix** – Configures a prefix cache. Flows are aggregated based on both source and destination network prefixes.
- **protocol-port** – Configures a protocol port cache. Flows are aggregated based on source and destination IP protocol port.
- **source-prefix** – Configures a source prefix cache. Flows are aggregated based on source network prefix.

The following command specifies the collector. You can specify one collector for an aggregate cache.

**Syntax:** [no] export destination <ip-addr> <udp-portnum>

The following command specifies the maximum number of flows the cache can contain.

**Syntax:** [no] cache entries <num>

The <num> parameter specifies the maximum number of flows and can be from 1024 – 524288. The default is 4096.

The following commands specify the active and inactive timeouts.

**Syntax:** [no] cache timeout inactive <secs>

**Syntax:** [no] cache timeout active <mins>

The inactive <secs> parameter specifies the maximum number of seconds an inactive flow can remain in the cache.

The active <mins> parameter specifies the maximum number of minutes an active flow can remain in the cache.

The following command enables the cache.

**Syntax:** [no] enabled

**NOTE:** The enabled command is required to enable the cache. The cache commands are optional.

**Possible values:** See above

**Default value:** None configured

**ip flow-cache timeout**

Changes an age timer for NetFlow.

NetFlow uses the following age timers to age flows out of the cache for export.

- **Inactive** – The inactive timer ages out a flow after it has been unused for the specified number of seconds.
• Active – The active timer ages out a flow that is in use if the flow has remained in use continuously for the specified number of minutes.

**NOTE:** In addition to using these timers, NetFlow also ages out normally terminated TCP flows, and ages out flows when the cache becomes full.

**NOTE:** The main flow cache and the aggregate caches (if you configure them) use separate timeouts. Changing the main flow cache’s timeouts does not affect the timeouts for the aggregate caches.

**EXAMPLE:**
ProCurveRS(config)# ip flow-cache timeout active 45
This command changes the maximum age for active flows to 45 minutes.

**Syntax:** `[no] ip flow-cache timeout active <mins> | inactive <secs>`
The `active <mins>` parameter specifies the maximum number of minutes an active flow can remain in the cache. You can specify from 1 – 60 minutes. The default is 30 minutes.

The `inactive <secs>` parameter specifies the maximum number of seconds an inactive flow can remain in the cache. You can specify from 10 – 600 seconds. The default is 60 seconds.

**Possible values:** See above
**Default value:** See above

**ip flow-export destination**
Specifies a data export collector for NetFlow.

**EXAMPLE:**
ProCurveRS(config)# ip flow-export destination 10.10.10.1 8080 1
This command specifies a UDP port on the collector that listens for the exported flow packets.

**Syntax:** `[no] ip flow-export destination <ip-addr> <udp-portnum> [ <collector-id> ]`
The `<ip-addr>` parameter specifies the IP address of the collector.
The `<udp-portnum>` specifies the UDP port on the collector.
The `<collector-id>` is a number from 1 – 10. This number applies only to the HP device and is not related to configuration information on the collector itself.

• If you are specifying more than one collector, make sure you also specify the collector ID and use a different ID for each collector.
• If you are specifying only one collector, you do not need to specify the ID. In this case, the software automatically assigns ID 1 to the collector.

**NOTE:** If you do not specify the collector ID, the software always uses ID 1. If you already have added a collector whose ID is 1, and you add another collector with ID 1, the software replaces the older collector with the new collector.

**Possible values:** See above
**Default value:** See above

**ip flow-export enable**
Enables NetFlow.

**EXAMPLE:**
ProCurveRS(config)# ip flow-export enable

**Syntax:** `[no] ip flow-export enable`
NOTE: This command enables the feature globally. However, to begin flow collection and export, you must enable collection for individual interfaces. NetFlow collects and exports flows only for the interfaces on which you enable the feature.

NOTE: If you plan to use aggregate caches instead, you do not need to globally enable NetFlow or specify collector information. Instead, you perform this configuration as part of the aggregate cache configuration.

Possible values: N/A
Default value: Disabled

ip flow-export origin-as

Enables collection and export of the AS information for NetFlow.

EXAMPLE:
ProCurveRS(config)# ip flow-export peer-as

Syntax: [no] ip flow-export origin-as | peer-as

The origin-as | peer-as parameter specifies the type of AS information you want to enable. You can enable one or the other but not both. By default, neither type of AS information is enabled.

Possible values: N/A
Default value: No AS information is collected

ip flow-export protocol-disable

Reduces flow exports to NetFlow collectors.

By default, NetFlow exports flows for all IP protocols (TCP, UDP, IGRP, OSPF, and so on).

EXAMPLE:
ProCurveRS(config)# ip flow-export protocol-disable udp

Syntax: [no] ip flow-export protocol-disable tcp | udp | other

The tcp | udp | other parameter specifies the protocol for which you are disabling export. You can specify one of the following:

• tcp – TCP
• udp – udp
• other – All IP protocols except TCP and UDP

Possible values: See above
Default value: All protocols are exported

ip flow-export source

Specifies a source interface for NetFlow.

By default, the HP device uses the port that is connected to a collector as the source interface for flows exported to that collector. You can specify an Ethernet port, a loopback interface, or the null interface as the source for NetFlow export packets.

• Ethernet port – NetFlow sends the export packets out the specified interface.
• Loopback interface – NetFlow sends the export packets from the specified loopback address, using a physical port connected to the collector to transmit the packet.
• Null interface – NetFlow continues to collect flows but does not export them to the collector. Use this type of interface when you want to administratively stop flow export without stopping flow collection and without removing configuration information.
**EXAMPLE:**
ProCurveRS(config)# ip flow-export source ethernet 1/1

This command configures port 1/1 to be the source interface for NetFlow packets. Since the command does not specify the collector ID, NetFlow exports the flows to collector 1.

To specify the collector ID, enter a command such as the following:
ProCurveRS(config)# ip flow-export source ethernet 1/1 2

This command uses port 1/1 as the source for flows exported to collector 2.

**Syntax:**
```
[n] ip flow-export source ethernet | loopback <portnum> [collector-id]
```

The `ethernet` | `loopback` `<portnum>` specifies a physical port or loopback interface.

The `null` parameter discards the export packets instead of sending them to a collector. However, **NetFlow** continues to collect flows.

The `<collector-id>` specifies the collector. If you do not specify the collector ID, the device assumes you mean collector 1.

**Possible values:** See above

**Default value:** The interface connected to the collector.

**ip flow-export version**

Changes the format version for data export packets sent by NetFlow.

By default, NetFlow uses format version 5 for exporting flows from the main cache to the external collector.

ProCurveRS(config)# ip flow-export version 1

**Syntax:**
```
[n] ip flow-export version 1 | 5
```

**NOTE:** The format for the main cache is not related to the format for aggregate caches. The software automatically uses format 8 for export packets from the aggregate caches.

**Possible values:** See above

**Default value:** 5

**ip forward-protocol**

This command is used in conjunction with the UDP helper feature to define the type of application traffic (port number socket) that is being forwarded to the server.

**EXAMPLE:**
ProCurveRS(config)# ip forward-protocol udp snmp-trap

**Syntax:**
ip forward-protocol udp <udp-port-name> | <udp-port-num>
Possible values:

<table>
<thead>
<tr>
<th>number</th>
<th>echo</th>
<th>snmp-trap</th>
</tr>
</thead>
<tbody>
<tr>
<td>bootpc</td>
<td>mobile-ip</td>
<td>tacacs</td>
</tr>
<tr>
<td>bootps</td>
<td>netbios-dgm</td>
<td>talk</td>
</tr>
<tr>
<td>discard</td>
<td>netbios-ns</td>
<td></td>
</tr>
<tr>
<td>dnsix</td>
<td>ntp</td>
<td></td>
</tr>
<tr>
<td>tftp</td>
<td>snmp</td>
<td></td>
</tr>
</tbody>
</table>

In addition, you can specify any UDP application by using the application's UDP port number.

**Default value:** By default, when an IP helper address is configured on an interface, UDP broadcast forwarding is enabled for the following UDP packet types: bootps, domain, tftp, time, netbios-dgm, netbios-ns and tacacs.

**ip helper-use-responder-ip**

Configures the HP device so that a BOOTP/DHCP reply to a client contains the server's IP address as the source address instead of the router's IP address.

**EXAMPLE:**

```bash
ProCurveRS(config)# ip helper-use-responder-ip
```

**Syntax:** `[no] ip helper-use-responder-ip`

**Possible values:** N/A

**Default value:** N/A

**ip high-perf**

Disables the unicast high-performance mode.

**NOTE:** To place a change to the high-performance mode into effect, you must reload the software after saving the change to the startup-config file.

**EXAMPLE:**

To disable the high-performance mode, enter the following commands:

```bash
ProCurveRS(config)# no ip high-perf
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

To enable the high-performance mode, enter the following commands:

```bash
ProCurveRS(config)# ip high-perf
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] ip high-perf`

**Possible values:** N/A

**Default value:** Enabled

**NOTE:** The feature is disabled by default in software releases earlier than 07.5.04.
**Global CONFIG Commands**

**ip hw-drop-on-def-route**
Confuges the HP device to drop default route traffic sent to the null0 interface in hardware.

**EXAMPLE:**
ProCurveRS(config)# ip route 0.0.0.0 0.0.0.0 null0
ProCurveRS(config)# ip hw-drop-on-def-route

**Syntax:** [no] ip hw-drop-on-def-route

**Possible values:** N/A

**Default value:** In releases prior to 07.7.00, traffic sent to the null0 interface was dropped in software. In release 07.7.00 and later, non-default route traffic sent to the null0 interface is dropped in hardware. Default route traffic is dropped in software unless this command is configured.

**ip icmp**
Causes the HP device to drop ICMP packets when excessive numbers are encountered, as is the case when the device is the victim of a Smurf attack. This command allows you to set threshold values for ICMP packets targeted at the router and drop them when the thresholds are exceeded.

**EXAMPLE:**
In the following example, if the number of ICMP packets received per second exceeds 5,000, the excess packets are dropped. If the number of ICMP packets received per second exceeds 10,000, the device drops all ICMP packets for the next 300 seconds (five minutes).

ProCurveRS(config)# ip icmp burst-normal 5000 burst-max 10000 lockup 300

You can set threshold values for ICMP packets received on an interface and drop them when the thresholds are exceeded. For example:

ProCurveRS(config)# int e 3/11
ProCurveRS(config-if-e100-3/11)# ip icmp burst-normal 5000 burst-max 10000 lockup 300

**Syntax:** ip icmp burst-normal <value> burst-max <value> lockup <seconds>

The burst-normal value can be from 1 – 100000.
The burst-max value can be from 1 – 100000.
The lockup value can be from 1 – 10000.

The number of incoming ICMP packets per second are measured and compared to the threshold values as follows:

- If the number of ICMP packets exceeds the burst-normal value, the excess ICMP packets are dropped.
- If the number of ICMP packets exceeds the burst-max value, all ICMP packets are dropped for the number of seconds specified by the lockup value. When the lockup period expires, the packet counter is reset and measurement is restarted.

**Possible values:** The burst-normal and burst-max values can be between 1 – 100000 packets. The burst-normal value must be smaller than the burst-max value. The lockup value can be between 1 – 10000 seconds.

**Default value:** N/A

**ip icmp echo broadcast-request**
Disables ICMP echo (ping) replies. By default, HP devices are enabled to respond to broadcast ICMP echo packets, which are ping requests. You can disable response to ping requests on a global basis.

**EXAMPLE:**
To disable response to broadcast ICMP echo packets (ping requests), enter the following command:

ProCurveRS(config)# no ip icmp echo broadcast-request

**Syntax:** [no] ip icmp echo broadcast-request
If you need to re-enable response to ping requests, enter the following command:

```
ProCurveRS(config)# ip icmp echo broadcast-request
```

**Possible values:** enabled or disabled  
**Default value:** enabled  

### ip icmp redirects

Disables ICMP redirect messages on a global basis.

**NOTE:** The device forwards misdirected traffic to the appropriate router, even if you disable the redirect messages.

**EXAMPLE:**  
To disable ICMP redirect messages globally, enter the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# no ip icmp redirects
```

**Syntax:** `[no] ip icmp redirects`  
**Possible values:** N/A  
**Default value:** Redirect messages are enabled

### ip icmp unreachable

Disables ICMP Destination Unreachable messages. By default, when an HP device receives an IP packet that the device cannot deliver, the device sends an ICMP Unreachable message back to the host that sent the packet. You can selectively disable an HP device’s response to the following types of ICMP Unreachable messages:

- **Administration** – The packet was dropped by the HP device due to a filter or ACL configured on the device.
- **Fragmentation-needed** – The packet has the Don’t Fragment bit set in the IP Flag field, but the HP device cannot forward the packet without fragmenting it.
- **Host** – The destination network or sub-net of the packet is directly connected to the HP device, but the host specified in the destination IP address of the packet is not on the network.
- **Network** – The HP device cannot reach the network specified in the destination IP address of the packet.
- **Port** – The destination host does not have the destination TCP or UDP port specified in the packet. In this case, the host sends the ICMP Port Unreachable message to the HP device, which in turn sends the message to the host that sent the packet.
- **Protocol** – The TCP or UDP protocol on the destination host is not running. This message is different from the Port Unreachable message, which indicates that the protocol is running on the host but the requested protocol port is unavailable.
- **Source-route-failure** – The device received a source-routed packet but cannot locate the next-hop IP address indicated in the packet’s Source-Route option.

**EXAMPLE:**  
To disable all ICMP Unreachable messages, enter the following command:

```
ProCurveRS(config)# no ip icmp unreachable
```

**Syntax:** `[no] ip icmp unreachable [network | host | protocol | administration | fragmentation-needed | port | source-route-fail]`  

If you enter the command without specifying a message type (as in the example above), all types of ICMP Unreachable messages listed above are disabled. If you want to disable only specific types of ICMP Unreachable messages, you can specify the message type. To disable more than one type of ICMP message, enter the `no ip icmp unreachable` command for each messages type.

The **network** parameter disables ICMP Network Unreachable messages.
The **host** parameter disables ICMP Host Unreachable messages.

The **protocol** parameter disables ICMP Protocol Unreachable messages.

The **administration** parameter disables ICMP Unreachable (caused by Administration action) messages.

The **fragmentation-needed** parameter disables ICMP Fragmentation-Needed But Don’t-Fragment Bit Set messages.

The **port** parameter disables ICMP Port Unreachable messages.

The **source-route-fail** parameter disables ICMP Unreachable (caused by Source-Route-Failure) messages.

To disable ICMP Host Unreachable messages and ICMP Network Unreachable messages but leave the other types of ICMP Unreachable messages enabled, enter the following commands instead of the command shown above:

```
ProCurveRS(config)# no ip icmp unreachable host
ProCurveRS(config)# no ip icmp unreachable network
```

If you have disabled all ICMP Unreachable message types but you want to re-enable certain types, you can do so entering commands such as the following:

```
ProCurveRS(config)# ip icmp unreachable host
ProCurveRS(config)# ip icmp unreachable network
```

The commands shown above re-enable ICMP Unreachable Host messages and ICMP Network Unreachable messages.

**Possible values:** see above

**Default value:** all types of ICMP Destination Unreachable messages are enabled

### ip igmp group-membership-time

Defines how long a group will remain on an interface in the absence of a group report, if DVMRP is enabled on the router.

**NOTE:** You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

**EXAMPLE:**

```
ProCurveRS(config)# ip igmp group-membership-time 240
```

**Syntax:** `ip igmp group-membership-time <value>`

For `<value>`, enter the following:

- For IGMP V1 and V2: 1 – 7200 seconds
- For IGMP V3: 20 – 7200 seconds and the default value is 140 seconds.

**Possible values:** See above

**Default value:** 140 seconds

### ip igmp max-response-time

Defines how many seconds the Routing Switch will wait for an IGMP response from an interface before concluding that the group member on that interface is down and removing the interface from the group.

**NOTE:** You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

**EXAMPLE:**

```
ProCurveRS(config)# ip igmp max-response-time 8
```

**Syntax:** `ip igmp max-response-time <value>`
**Possible values:**  1 – 10 seconds  
**Default value:**  5 seconds

**ip igmp query-interval**  
Defines how often the router will query an interface for group membership.

**NOTE:**  You must enter the **ip multicast-routing** command before entering this command. Otherwise, the command does not take effect and the software uses the default value.

**EXAMPLE:**  
ProCurveRS(config)# ip igmp query 120

**Syntax:**  ip igmp query-interval <value>

For <value>, enter the following:

- For IGMP V1 and V2:  1 – 3600 seconds
- For IGMP V3:  10 – 3,600 seconds, but the value you enter must be a little more than twice the group membership time.

**Possible values:**  See above  
**Default value:**  60 seconds

**ip igmp version**  
Globally specifies the IGMP version on an HP device.

**EXAMPLE:**  
ProCurveRS(config)# ip igmp version 3

**Syntax:**  ip igmp version <version-number>

Enter 1, 2, or 3 for <version-number>. Version 2 is the default version.

**Possible values:**  See above  
**Default value:**  N/A

**ip irdp**  
Enables a router to advertise its network IP addresses to the network. The router will also answer queries. IRDP stands for ICMP Router Discovery Protocol (IRDP). The ICMP Router Discovery Protocol (IRDP) is used by ProCurve Routing Switches to advertise the IP addresses of its router interfaces to directly attached hosts. IRDP is disabled by default.

When IRDP is enabled, the Routing Switch periodically sends Router Advertisement messages out all its IP interfaces. The messages advertise the Routing Switch's IP addresses to directly attached hosts who listen for the messages. In addition, hosts can be configured to query the Routing Switch for the information by sending Router Solicitation messages.

Some types of hosts use Router Solicitation messages to discover their default gateway. When IRDP is enabled on the ProCurve Routing Switch, it responds to the Router Solicitation messages. Some clients interpret this response to mean that the Routing Switch is the default gateway. If another router is actually the default gateway for these clients, leave IRDP disabled on the ProCurve Routing Switch.

When IRDP is enabled, the Routing Switch sends the Router Advertisement messages every 450 – 600 seconds. The interval the device selects is random for each message and is not affected by traffic loads or other network factors. The interval is not configurable.

**EXAMPLE:**  
ProCurveRS(config)# ip irdp

**Syntax:**  [no] ip irdp
Global CONFIG Commands

### Possible values:
- n/a

### Default value:
- disabled

#### ip load-sharing
Allows traffic being sent from one router to another to be sent across multiple paths of equal cost for faster transmission when using OSPF or BGP4 routing. OSPF or BGP4 routing must be enabled on the router for this command to operate. IP load sharing is enabled by default.

See the "Configuring IP" chapter of the *Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches* for more information about this feature.

**EXAMPLE:**

```
ProCurveRS(config)# ip load-sharing 6
```

**Syntax:**
- `ip load-sharing [<num>]`

The `<num>` parameter specifies the number of equal paths across which the Routing Switch will load share traffic to a given destination. You can specify from 2 – 8. The destinations among which the device load shares can be network addresses or individual host addresses, depending on the load sharing method that is enabled. See "ip load-sharing by-host".

**Possible values:**
- 2 – 8

**Default value:**
- 4

#### ip load-sharing by-host
Disables network-based load sharing (load sharing using destination address aggregation) and configures the Routing Switch to instead perform load sharing based on individual host destination addresses.

See the "Configuring IP" chapter of the *Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches* for more information about this feature.

**EXAMPLE:**

To enable host-based IP load sharing, enter the following command:

```
ProCurveRS(config)# ip load-sharing by-host
```

This command enables host-based IP load sharing on the device. The command also disables network-based IP load-sharing (the default) at the same time.

**Syntax:**
- `[no] ip load-sharing by-host`

**NOTE:** The T-Flow uses hash-based load balancing regardless of the type of IP load sharing enabled (by-host or by-network). On the T-Flow, a hash value is calculated based on the source and destination IP addresses. Each of the paths to a given destination is associated with one of the possible hash values, and the traffic flow is assigned to a path based on its calculated hash value.

**Possible values:**
- see above

**Default value:**
- disabled

#### ip load-sharing route-by-host
Overrides network-based IP load sharing for a specific destination network. Use this feature when you want to use network-based load sharing by default but also want to use host-based load sharing for specific destinations (hosts or sub-nets).

**NOTE:** Use this feature only when network-based load sharing is enabled.

When you configure host-based load sharing for a specific destination network, the Routing Switch distributes traffic to hosts on the network evenly across the available paths. For other networks, the Routing Switch uses a single path for all traffic to hosts on a given network.
NOTE: The host-based load sharing for the destination takes effect only if the IP route table contain an entry that exactly matches the destination network you specify. For example, if you configure host-based load sharing for destination network 207.95.7.0/24, the IP route table must contain a route entry for that network. In fact, for load sharing to occur, the IP route table needs to contain multiple equal-cost paths to the network.

EXAMPLE:
To enable host-based load sharing for a specific destination network, enter a command such as the following at the global CONFIG level of the CLI:

ProCurveRS(config)# ip load-sharing route-by-host 207.95.7.0/24

This command configures the Routing Switch to use host-based load sharing for traffic to destinations on the 207.95.7.0/24 network. The Routing Switch uses network-based load sharing for traffic to other destination networks.

Syntax: [no] ip load-sharing route-by-host <ip-addr> <ip-mask>

or

Syntax: [no] ip load-sharing route-by-host <ip-addr>/<mask-bits>

You can disable host-based load sharing for specific destination networks or for all networks. When you disable host-based load sharing for a destination network (or for all destination networks), the software removes the host-based forwarding cache entries for the destination network(s) and uses network-based forwarding entries instead.

NOTE: This method applies only to networks for which you have explicitly enabled host-based load sharing. If you have enabled host-based load sharing globally but want to change to network-based load sharing, enter the no ip load-sharing by-host command at the global CONFIG level of the CLI.

To disable host-based load sharing for all the destination networks for which you have explicitly enabled the host-based load sharing, enter the following command at the global CONFIG level of the CLI:

ProCurveRS(config)# no ip load-sharing route-by-host

To disable host-based load sharing for a specific destination network, enter a command such as the following:

ProCurveRS(config)# no ip load-sharing route-by-host 207.95.7.0/24

This command removes the host-based load sharing for the 207.95.7.0/24 network, but leaves the other host-based load sharing configurations intact.

Possible values: a network address

Default value: disabled

ip mroute
Configures a static multicast route. If you configure more than one static multicast route, the Routing Switch always uses the most specific route that matches a multicast source address. Thus, if you want to configure a multicast static route for a specific multicast source and also configure another multicast static route for all other sources, you can configure two static routes.

NOTE: Static multicast routes are not supported for DVMRP.

EXAMPLE:

ProCurveRS(config)# ip mroute 1 207.95.10.0/24 interface ethernet 1/2 distance 1

Syntax: mroute <routenum> <ip-addr> interface ethernet <portnum> [ve <num> [distance <num>]]

or

Syntax: mroute <routenum> <ip-addr> rpf_address <rpf-num>

Possible values: The <ip-addr> parameter specifies the PIM source for the route.
NOTE: In IP multicasting, a route is handled in terms of its source, rather than its destination.

You can use the `ethernet <portnum>` parameter to specify a physical port or the `ve <num>` parameter to specify a virtual interface.

**NOTE:** The `ethernet <portnum>` parameter does not apply to PIM SM.

The `distance <num>` parameter sets the administrative distance for the route. When comparing multiple paths for a route, the Routing Switch prefers the path with the lower administrative distance.

**NOTE:** Regardless of the administrative distances, the Routing Switch always prefers directly connected routes over other routes.

The `rpf_address <rpf-num>` parameter specifies an RPF number.

Default value: N/A

---

**ip multicast**

Globally enables or disables the IP Multicast Traffic Reduction feature.

Beginning with software release 07.7.00, this command is available on Routing Switches.

By default, HP devices forward all IP multicast traffic out all ports except the port on which the traffic was received. To reduce multicast traffic through the device, you can enable IP Multicast Traffic Reduction. This feature configures the device to forward multicast traffic only on the ports attached to multicast group members. The device determines the ports that are attached to multicast group members based on entries in the IGMP table. Each entry in the table consists of a MAC address and the device ports from which the device has received Group Membership reports for that group.

After you enable IP Multicast Traffic Reduction, when the device receives traffic for an IP multicast group, the device looks in the IGMP table for an entry corresponding to that group. If the device finds an entry, the device forwards the group traffic out the ports listed in the group entry. If the table does not contain an entry corresponding to that group, the device broadcasts the traffic.

When you enable IP Multicast Traffic Reduction on the device, IGMP also is enabled. The device uses IGMP to maintain a table of the Group Membership reports received by the device. You can use active or passive IGMP mode. The default mode is passive.

- **Active** – When active IGMP mode is enabled, a device actively sends out IGMP queries to identify IP multicast groups on the network and makes entries in the IGMP table based on the Group Membership reports received from the network.

  **NOTE:** Routers in the network generally handle this operation. Use the active IGMP mode only when the device is in a stand-alone switched network with no external IP multicast router attachments. In this case, enable the active IGMP mode on only one of the devices and leave the other devices configured for passive IGMP mode.

- **Passive** – When passive IGMP mode is enabled, the device listens for IGMP Group Membership reports but does not send IGMP queries. The passive mode is sometimes called “IGMP snooping”. Use this mode when another device in the network is actively sending queries.

  **NOTE:** Routing Switches: If the "route-only" feature is enabled on Routing Switches, then IP Multicast Traffic Reduction will not work. Also, IP Multicast Traffic Reduction is not supported on the default VLAN of Routing Switches.

---

**ip multicast age-interval**

Changes the IGMP age interval on devices configured for IP Multicast Traffic Reduction.

Beginning with software release 07.7.00, this command is also available on Routing Switches.
When the device receives a Group Membership report, it makes an entry in the IGMP group table for the group in the report. The age interval specifies how long the entry can remain in the table without the device receiving another Group Membership report.

**EXAMPLE:**
To modify the age interval, enter a command such as the following:

```bash
ProCurveRS(config)# ip multicast age-interval 280
```

**Syntax:** `[no] ip multicast age-interval <interval>

The `<interval>` parameter specifies the interval between queries. You can specify a value from 10 – 1220 seconds. The default is 140 seconds.

**Possible values:** 10 – 1220 seconds

**Default value:** 140 seconds

**ip multicast filter**
Enables IP multicast filtering on devices that are enabled for IP Multicast Traffic Reduction.

Beginning with software release 07.7.00, this command is also available on Routing Switches.

When device starts up, it forwards all multicast groups even though multicast traffic filters are configured. This process continues until the device receives a group membership report. Once the group membership report is received, the device drops all multicast packets for groups other than the ones for which the device has received the group membership report. The device then forwards traffic for only for the groups in the membership report.

**ip multicast-perf**
Enables the device to forward all the fragments of fragmented IP multicast packet through hardware. By default, a ProCurve Routing Switch forwards the first fragment of a fragmented IP multicast packet through hardware, but forwards the remaining fragments through the software.

**EXAMPLE:**

```bash
ProCurveRS(config)# ip multicast-perf
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] ip multicast-perf

**NOTE:** You must save the configuration and reload the software to place the change into effect.

**Possible values:** N/A

**Default value:** Disabled

**ip multicast query-interval**
Changes the IGMP query interval for IP Multicast Traffic Reduction. This command specifies how often a device enabled for active IP Multicast Traffic Reduction sends Group Membership queries.

Beginning with software release 07.7.00, this command is also available on Routing Switches.

**NOTE:** The query interval applies only to the active mode of IP Multicast Traffic reduction.

**EXAMPLE:**
To modify the query interval, enter a command such as the following:

```bash
ProCurveRS(config)# ip multicast query-interval 120
```

**Syntax:** `[no] ip multicast query-interval <interval>`
The `<interval>` parameter specifies the interval between queries. You can specify a value from 10 – 600 seconds. The default is 60 seconds.

**Possible values:** 10 – 600 seconds

**Default value:** 60 seconds

**ip multicast-routing**

Allows you to change the following global IP Multicast parameters:

- IGMP query interval
- IGMP group membership time
- IGMP maximum response time

**NOTE:** You must enter the `ip multicast-routing` command before changing these parameters. Otherwise, the changes do not take effect and the software uses the default values.

**EXAMPLE:**

ProCurveRS(config)# ip multicast-routing

**Syntax:** `[no] ip multicast-routing`  
**Possible values:** N/A  
**Default value:** Disabled

**ip nat inside destination list**

Configures a source IP address list for dynamic inside destination NAT. You also need to configure an IP ACL and an address pool. See "ip nat pool" on page 6-73.

**EXAMPLE:**

To configure dynamic inside-destination NAT, enter commands such as the following at the global CONFIG level of the CLI:

ProCurveRS(config)# access-list 1 permit 209.157.1.2/24  
ProCurveRS(config)# ip nat pool InAdds 10.10.10.0 10.10.10.254 prefix-length 24  
ProCurveRS(config)# ip nat inside destination list 1 pool InAdds

These commands configure a standard ACL for the public network 10.10.10.x/24, then enable inside-destination NAT for the network. Make sure you specify `permit` in the ACL, rather than `deny`. If you specify `deny`, the HP device will not provide NAT for the addresses.

**Syntax:** `[no] ip nat inside destination list <acl-name-or-num> pool <pool-name>`

The **inside destination** parameter specifies that the translation applies to public addresses sending traffic to private addresses.

The **list** `<acl-id>` parameter specifies an IP ACL (standard or extended). You can specify a numbered or named ACL.

**NOTE:** Named ACLs are not supported with NAT. You must use a numbered ACL.

The **pool** `<pool-name>` parameter specifies the pool. You must create the pool before you can use it with this command.

**Possible values:** See above  
**Default value:** Not configured

**ip nat inside destination static**

Configures static inside destination NAT for an IP address.
EXAMPLE:
To configure static inside-destination NAT for an IP address, enter a command such as the following:

```
ProCurveRS(config)# ip nat inside destination static 209.157.1.69 10.10.10.69
```

The command in this example statically maps the Internet address 209.157.1.69 to the private address 10.10.10.69.

To include TCP or UDP application port numbers in the translation, enter a command such as the following:

```
ProCurveRS(config)# ip nat inside destination static tcp 209.157.1.69 80 10.10.10.69 8080
```

This command provides the same IP address translation as the previous command example. However, this command also translates TCP port 80 to TCP port 8080. The translation applies to the destination port, for inbound traffic.

**Syntax:** `[no] ip nat inside destination static <private-ip> <global-ip>`

**Syntax:** `[no] ip nat inside destination static tcp | udp <private-ip> <private-tcp/udp> <global-ip> <global-tcp/udp>`

The `inside destination` parameter specifies that the mapping applies to the Internet address sending traffic to the private network.

The `<private-ip>` parameter specifies the private IP address.

The `<global-ip>` parameter specifies the Internet address.

**NOTE:** Neither of the IP address parameters needs a network mask.

The `tcp | udp` parameter indicates that you are creating a static mapping for a specify application (TCP or UDP port).

The `<global-tcp/udp>` parameter specifies the application port on the public host.

The `<private-tcp/udp>` parameter specifies the application port on the private host.

**Possible values:** See above

**Default value:** Not configured

**ip nat inside source list**
Configures a source IP address list for dynamic inside source NAT. You also need to configure an IP ACL and an address pool. See "ip nat pool" on page 6-73.

**EXAMPLE:**

```
ProCurveRS(config)# access-list 1 permit 10.10.10.0/24
ProCurveRS(config)# ip nat pool OutAdds 209.157.1.2 209.157.2.254 prefix-length 24
ProCurveRS(config)# ip nat inside source list 1 pool OutAdds
```

These commands configure a standard ACL for the private sub-net 10.10.10.x/24, then enable inside NAT for the sub-net. Make sure you specify permit in the ACL, rather than deny. If you specify deny, the HP device will not provide NAT for the addresses.

**Syntax:** `[no] ip nat inside source list <acl-name-or-num> pool <pool-name> [overload]

This command associates a private address range with a pool of Internet addresses and optionally enables the Port Address Translation feature.

The `inside source` parameter specifies that the translation applies to private addresses sending traffic to global addresses (Internet addresses).

The `list <acl-id>` parameter specifies a standard or extended ACL. You can specify a numbered or named ACL.

**NOTE:** Named ACLs are not supported with NAT. You must use a numbered ACL.
The **pool** `<pool-name>` parameter specifies the pool. You must create the pool before you can use it with this command.

The overload parameter enables the Port Address Translation feature. Use this parameter if the IP address pool does not contain enough addresses to ensure NAT for each private address. The Port Address Translation feature conserves Internet addresses by mapping the same Internet address to more than one private address and using a TCP or UDP port number to distinguish among the private hosts. The device supports up to 50 global IP addresses with this feature enabled.

**Possible values:** See above

**Default value:** Not configured

### ip nat inside source static

Configures static inside source NAT for an IP address.

**EXAMPLE:**

```
ProCurveRS(config)# ip nat inside source static 10.10.10.69 209.157.1.69
```

The commands in this example statically map the private address 10.10.10.69 to the Internet address 209.157.1.69.

**Syntax:**

```
[no] ip nat inside source static <private-ip> <global-ip>
```

This command associates a specific private address with a specific Internet address. Use this command when you want to ensure that the specified addresses are always mapped together.

The **inside source** parameter specifies that the mapping applies to the private address sending traffic to the Internet.

The `<private-ip>` parameter specifies the private IP address.

The `<global-ip>` parameter specifies the Internet address. The device supports up to 256 global IP addresses.

Neither of the IP address parameters needs a network mask.

**Possible values:** See above

**Default value:** Not configured

### ip nat pool

Configures a pool for use in a source IP address list for dynamic NAT.

**EXAMPLE:**

```
ProCurveRS(config)# access-list 1 permit 10.10.10.0/24
ProCurveRS(config)# ip nat pool Out Adds 209.157.1.2 209.157.2.254 prefix-length 24
ProCurveRS(config)# ip nat inside source list 1 pool Out Adds
```

These commands configure a standard ACL for the private sub-net 10.10.10.x/24, then enable inside NAT for the sub-net. Make sure you specify permit in the ACL, rather than deny. If you specify deny, the HP device will not provide NAT for the addresses.

**Syntax:**

```
[no] ip nat pool <pool-name> <start-ip> <end-ip> netmask <ip-mask> | prefix-length <length>
[type match-host | rotary]
```

This command configures the address pool.

The `<pool-name>` parameter specifies the pool name. The name can be up to 255 characters long and can contain special characters and internal blanks. If you use internal blanks, you must use quotation marks around the entire name.

The `<start-ip>` parameter specifies the IP address at the beginning of the pool range. Specify the lowest-numbered IP address in the range.

The `<end-ip>` parameter specifies the IP address at the end of the pool range. Specify the highest-numbered IP address in the range.
The address range cannot contain any gaps. Make sure you own all the IP addresses in the range. If the range contains gaps, you must create separate pools containing only the addresses you own.

The `netmask <ip-mask> | prefix-length <length>` parameter specifies a classical sub-net mask (example: `netmask 255.255.255.0`) or the length of a Classless Interdomain Routing prefix (example: `prefix-length 24`).

The maximum number of global IP addresses you can configure depends on how much memory the Routing Switch has and whether you enable the Port Address Translation feature. Regardless of the amount of memory, you cannot configure more than 256 global IP addresses.

The `type match-host | rotary` parameter specifies the method the software uses to assign the host portion of the translated address.

- **match-host** – The software uses the same host address as the untranslated address. For example, if the untranslated address is 192.2.4.69 and the host portion of the address is 69, the translated address also uses the host address 69. This method results in the translated addresses always having the same host addresses as their untranslated counterparts.

- **rotary** – The software assigns a host address from 1 – 254, beginning with 1 for the first translated address. This is the default.

**Possible values:** N/A

**Default value:** Disabled

**ip nat translation**

Changes the age timeout for NAT translations.

**EXAMPLE:**

To change the age timeout for all entries that do not use Port Address Translation to 1800 seconds (one half hour), enter a command such as the following at the global CONFIG level of the CLI:

```bash
ProCurveRS(config)# ip nat timeout 1800
```

**Syntax:** `[no] ip nat translation timeout | udp-timeout | tcp-timeout | finrst-timeout | dns-timeout <secs>`

Use one of the following parameters to specify the dynamic entry type:

- **timeout** – All entries that do not use Port Address Translation. The default is 120 seconds.

- **udp-timeout** – Dynamic entries that use Port Address Translation based on UDP port numbers. The default is 120 seconds.

- **tcp-timeout** – Dynamic entries that use Port Address Translation based on TCP port numbers. The default is 120 seconds.

- **finrst-timeout** – TCP FIN (finish) and RST (reset) packets, which normally terminate TCP connections. The default is 120 seconds.

- **dns-timeout** – Connections to a Domain Name Server (DNS). The default is 120 seconds.

The `<secs>` parameter specifies the number of seconds. For each entry type, you can enter a value from 1 – 3600.

**Possible values:** See above

**Default value:** See above

**ip net-aggregate**

Optimizes the CAM for devices that have very large IP route tables (100,000 or more), where most of those routes use the same next hops as the default route.

When you enable standard optimization of CAM network aggregation, the feature divides the IP address space into 4096 aggregates. Each aggregate has a 12-bit prefix (/12).
With standard optimization of CAM network aggregation enabled, the device forwards IP traffic as follows:

The device checks the CAM for an entry with the traffic's destination.

- If the CAM contains an entry, the device uses the entry.
- If the CAM does not contain an entry, the device checks to see whether all explicit routes in the IP route table that are in the same /12 aggregate as the needed route (all routes that overlap with the /12 aggregate), have the same set of next hops as the default route.
  - If all explicit routes in the IP route table that are within the same /12 aggregate use the same next hops as the default route, the device programs a single CAM entry that aggregates the route information for all routes within the aggregate. The device uses this single CAM entry to forward traffic to any destination within the aggregate.
  - If one or more explicit routes within the same /12 aggregate uses a next hop that is not also used by the default route, the device does not program an aggregate entry into the CAM but instead programs a separate route entry for the individual destination network.

After programming a CAM entry for the traffic's destination, the device uses the entry to forward further traffic to the same destination. If the device was able to program an aggregate entry, the device uses the entry for traffic to any destination within the aggregate.

**NOTE:** CAM network aggregation requires a default route in the IP route table.

Compare with "ip dr-aggregate" on page 6-57, "ip net-aggregate premium" on page 6-75, and "ip net-aggregate supreme" on page 6-76.

**EXAMPLE:**
ProCurveRS(config)# ip net-aggregate

**Syntax:** [no] ip net-aggregate [<secs>]

The <secs> parameter specifies the update interval and can be from 1 – 60 seconds. The default is 1 second. Specifying a longer interval can help conserve CPU resources.

**Possible values:** See above

**Default value:** Disabled

**ip net-aggregate premium**

**NOTE:** This command is supported in software releases 07.8.00 and later.

Optimizes the CAM for devices that have very large IP route tables (100,000 or more), where most of those routes use the same next hops as the default route.

When you enable premium optimization of CAM network aggregation, the software divides the IP address space into 8192 ($2^{13}$) aggregate entries and applies a 13-bit prefix to each aggregate entry.

With premium optimization of CAM network aggregation enabled, the device forwards IP traffic as follows:

The device checks the CAM for an entry with the traffic's destination.

- If the CAM contains an entry, the device uses the entry.
- If the CAM does not contain an entry, the device checks to see whether all explicit routes in the IP route table that are in the same /13 aggregate as the needed route (all routes that overlap with the /13 aggregate), have the same set of next hops as the default route.
  - If all explicit routes in the IP route table that are within the same /13 aggregate use the same next hops as the default route, the device programs a single CAM entry that aggregates the route information for all routes within the aggregate. The device uses this single CAM entry to forward traffic to any destination within the aggregate.
  - If one or more explicit routes within the same /13 aggregate uses a next hop that is not also used by the
default route, the device does not program an aggregate entry into the CAM but instead programs a separate route entry for the individual destination network.

After programming a CAM entry for the traffic's destination, the device uses the entry to forward further traffic to the same destination. If the device was able to program an aggregate entry, the device uses the entry for traffic to any destination within the aggregate.

**NOTE:** CAM network aggregation requires a default route in the IP route table.

Compare with “ip dr-aggregate” on page 6-57, “ip net-aggregate” on page 6-74, and “ip net-aggregate supreme” on page 6-76.

**EXAMPLE:**

ProCurveRS(config)# ip net-aggregate premium

**Syntax:** [no] ip net-aggregate premium

**Possible values:** N/A

**Default value:** Disabled

**ip net-aggregate supreme**

**NOTE:** This command is supported in software releases 07.8.00 and later.

Optimizes the CAM for devices that have very large IP route tables (100,000 or more), where most of those routes use the same next hops as the default route.

When you enable supreme optimization of CAM network aggregation, the software divides the IP address space into 16,384 (214) aggregate entries and applies a 14-bit prefix to each aggregate entry.

With supreme optimization of CAM network aggregation enabled, the device forwards IP traffic as follows:

The device checks the CAM for an entry with the traffic's destination.

- If the CAM contains an entry, the device uses the entry.
- If the CAM does not contain an entry, the device checks to see whether all explicit routes in the IP route table that are in the same /14 aggregate as the needed route (all routes that overlap with the /14 aggregate), have the same set of next hops as the default route.
  - If all explicit routes in the IP route table that are within the same /14 aggregate use the same next hops as the default route, the device programs a single CAM entry that aggregates the route information for all routes within the aggregate. The device uses this single CAM entry to forward traffic to any destination within the aggregate.
  - If one or more explicit routes within the same /14 aggregate uses a next hop that is not also used by the default route, the device does not program an aggregate entry into the CAM but instead programs a separate route entry for the individual destination network.

After programming a CAM entry for the traffic's destination, the device uses the entry to forward further traffic to the same destination. If the device was able to program an aggregate entry, the device uses the entry for traffic to any destination within the aggregate.

**NOTE:** CAM network aggregation requires a default route in the IP route table.

Compare with “ip dr-aggregate” on page 6-57, “ip net-aggregate” on page 6-74, and “ip net-aggregate supreme” on page 6-75.

**EXAMPLE:**

ProCurveRS(config)# ip net-aggregate supreme

**Syntax:** [no] ip net-aggregate supreme

**Possible values:** N/A
Global CONFIG Commands

Default value: Disabled

**ip next hop-movement log-disable**
Disables logging of movement for the next hop router from one port to another.

**EXAMPLE:**
ProCurveRS(config)# ip next-hop-movement log-disable

**Syntax:** [no] ip next-hop-movement log-disable

**Possible values:** N/A

**Default value:** N/A

**ip policy prefer-direct-route**
Configures a Policy-Based Routing (PBR) policies to always use the most direct route available.

**NOTE:** This command applies only to EP devices running software release 07.6.04 or later.

**EXAMPLE:**
ProCurveRS(config)# ip policy prefer-direct-route

**Syntax:** [no] ip policy prefer-direct-route

**ip policy route-map**
Enables Policy-Based Routing (PBR) on the Routing Switch.

**EXAMPLE:**
To enable PBR globally, enter a command such as the following:

ProCurveRS(config)# ip policy route-map test-route

This command applies a route map named “test-route” to all interfaces on the device for PBR.

**Syntax:** [no] ip policy route-map <map-name>

**Possible values:** the name of a configured route map

**Default value:** N/A

**ip prefix-list**
Configures an IP prefix list. You can configure a range of IP prefixes for routes you want to send to or receive from individual neighbors.

**EXAMPLE:**
To configure an IP prefix list and apply it to a neighbor, enter commands such as the following:

ProCurveRS(config)# ip prefix-list Routesfor20 permit 20.20.0.0/24
ProCurveRS(config)# router bgp
ProCurveRS(config-bgp-router)# neighbor 10.10.10.1 prefix-list Routesfrom20 out

These commands configure an IP prefix list named Routesfor20, which permits routes to network 20.20.0.0/24. The neighbor command configures the Routing Switch to use IP prefix list Routesfor20 to determine which routes to send to neighbor 10.10.10.1. The Routing Switch sends routes that go to 20.20.x.x to neighbor 10.10.10.1 because the IP prefix list explicitly permits these routes to be sent to the neighbor.

**Syntax:** ip prefix-list <name> [seq <seq-value>] [description <string>] deny | permit <network-addr>/<mask-bits> [ge <ge-value>] [le <le-value>]

The **<name>** parameter specifies the prefix list name. You use this name when applying the prefix list to a neighbor.

The **description** **<string>** parameter is a text string describing the prefix list.
The `seq <seq-value>` parameter is optional and specifies the IP prefix list's sequence number. You can configure up to 100 prefix list entries. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with prefix list entry 5. The software interprets the prefix list entries in numerical order, beginning with the lowest sequence number.

The `deny` | `permit` parameter specifies the action the software takes if a neighbor's route is in this prefix list.

The `prefix-list` matches only on this network unless you use the `ge <ge-value>` or `le <le-value>` parameters. (See below.)

The `<network-addr>/<mask-bits>` parameter specifies the network number and the number of bits in the network mask.

You can specify a range of prefix length for prefixes that are more specific than `<network-addr>/<mask-bits>`.

- If you specify only `ge <ge-value>`, then the mask-length range is from `<ge-value>` to 32.
- If you specify only `le <le-value>`, then the mask-length range is from length to `<le-value>`.

The `<ge-value>` or `<le-value>` you specify must meet the following condition:

\[ \text{length} < \text{ge-value} \leq \text{le-value} \leq 32 \]

If you do not specify `ge <ge-value>` or `le <le-value>`, the prefix list matches only on the exact network prefix you specify with the `<network-addr>/<mask-bits>` parameter.

For the syntax of the `neighbor` command shown in the example above, see “neighbor” on page 17-11.

**Possible values:** see above

**Default value:** N/A

**ip proxy-arp**

Allows a router to act as a proxy for devices on its interfaces when responding to ARP requests.

**EXAMPLE:**

```
ProCurveRS(config)# ip proxy
```

**Syntax:** `[no] ip proxy-arp`

**Possible values:** On or off

**Default value:** Off

**ip radius source-interface**

Configures the device to use the lowest-numbered IP address configured on an interface as the source for all RADIUS packets from the device. The software uses the lowest-numbered IP address configured on the interface as the source IP address for the packets.

**EXAMPLE:**

To specify the lowest-numbered IP address configured on a virtual interface as the device's source for all RADIUS packets, enter commands such as the following:

```
ProCurveRS(config)# int ve 1
ProCurveRS(config-vif-1)# ip address 10.0.0.3/24
ProCurveRS(config-vif-1)# exit
ProCurveRS(config)# ip radius source-interface ve 1
```

The commands in this example configure virtual interface 1, assign IP address 10.0.0.3/24 to the interface, then designate the interface as the source for all RADIUS packets from the Routing Switch.

**Syntax:** `ip radius source-interface ethernet <portnum> | loopback <num> | ve <num>`

**Possible values:** see above

**Default value:** The lowest-numbered IP address configured on the interface through which the packet is sent. The address therefore changes, by default, depending on the interface.
ip rarp
Enables Reverse Addressing Resolution Protocol (RARP) and allows the router to assign IP addresses for hosts based on their MAC addresses. A router will check the RARP table for an IP match to a MAC address sent from a host. If the table contains an entry for the MAC address, the router will answer back with the IP address.

EXAMPLE:
ProCurveRS(config)# ip rarp

Syntax: ip rarp

Possible values: N/A

Default value: N/A

ip rebind-acl
Reapplies ACLs to their interfaces.

NOTE: This command applies on EP devices running software release 07.6.01b or later.

For flow-based and hardware-based ACLs, if you make an ACL configuration change, you must reapply the ACLs to their interfaces to place the change into effect. An ACL configuration change includes any of the following:

• Adding, changing, or removing an ACL or an entry in an ACL
• Changing a PBR policy
• Changing the port membership of a VLAN that has an ACL on its virtual routing interface
• Enabling or disabling the TCP strict mode or UDP strict mode (flow-based ACLs only)
• Changing EP ToS-based QoS mappings (since EP QoS uses the Layer 4 CAM)

EXAMPLE:
ProCurveRS(config)# ip rebind-acl all
This command reapplies all ACLs to their interfaces.
To reapply a specific ACL, enter a command such as the following:
ProCurveRS(config)# ip rebind-acl 101
This command reapplies ACL 101 only.

Syntax: [no] ip rebind-acl <num> | <name> | all

Possible values: See above.

Default value: N/A

ip route
Allows you to configure static IP routes on a Routing Switch.

EXAMPLE:
ProCurveRS(config)# ip route 192.128.2.0 255.255.255.0 209.157.22.1

Syntax: ip route <dest-ip-addr> <dest-mask>
<nexthop-ip-addr> |
ethernet <portnum> | ve <num>
[<metric>] [distance <num>]

or

Syntax: ip route <dest-ip-addr>/<mask-bits>
<nexthop-ip-addr> |
ethernet <portnum> | ve <num>
[<metric>] [distance <num>] [lsp <name> | static-lsp <name>]
The <dest-ip-addr> is the route’s destination. The <dest-mask> is the network mask for the route’s destination IP address. Alternatively, you can specify the network mask information by entering a forward slash followed by the number of bits in the network mask. For example, you can enter 192.0.0.0 255.255.255.0 as 192.0.0.0/24. You can enter multiple static routes for the same destination for load balancing or redundancy. See the “Defining Static IP Routes” section in the “Configuring IP” chapter in the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The <next-hop-ip-addr> is the IP address of the next-hop router (gateway) for the route.

If you do not want to specify a next-hop IP address, you can instead specify a port or interface number on the Routing Switch. The <num> parameter is a virtual interface number. If you instead specify an Ethernet port, the <portnum> is the port’s number (including the slot number). In this case, the Routing Switch forwards packets destined for the static route’s destination network to the specified interface. Conceptually, this feature makes the destination network like a directly connected network, associated with a specific Routing Switch interface.

NOTE: The port or virtual interface you use for the static route must have at least one IP address configured on it. The address does not need to be in the same sub-net as the destination network.

NOTE: You cannot specify null0 or another interface as the next hop in the Base Layer 3 image.

The <metric> parameter can be a number from 1 – 16. The default is 1.

NOTE: If you specify 16, RIP considers the metric to be infinite and thus also considers the route to be unreachable.

The distance <num> parameter specifies the administrative distance of the route. When comparing otherwise equal routes to a destination, the Routing Switch prefers lower administrative distances over higher ones, so make sure you use a low value for your default route. The default is 1.

NOTE: You can also assign the default router as the destination by entering 0.0.0.0 0.0.0.0.

Default value: metric 1, distance 1

NOTE: The Routing Switch will replace the static route if the router receives a route with a lower administrative distance. See the “Configuring BGP4” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches for a list of the default administrative distances for all types of routes.

The syntax above is for all types of static routes except “null” routes. To configure a null static route, use the following syntax.

Syntax: ip route <ip-addr> <ip-mask> null0 [<metric>] [distance <num>]
or

Syntax: ip route <ip-addr>/<mask-bits> null0 [<metric>] [distance <num>]

The null0 parameter indicates that this is a null route. You must specify this parameter to make this a null route. For more information, see the “Configuring IP” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

ip router-id

Assigns a router ID to a ProCurve Routing Switch. OSPF and BGP4 use router IDs to identify routers. A Routing Switch can have one router ID, which is used by both OSPF and BGP4 if both are enabled.

Router IDs are in IP address format (for example, 1.1.1.1). The default router ID is the IP address configured on the lowest numbered loopback interface configured on the Routing Switch. If the device does not have any loopback interfaces, the default router ID is the lowest numbered IP interface configured on the device. This ensures that the router ID on each router is unique even if you use the default value.
EXAMPLE:
ProCurveRS(config)# ip router-id 1.1.1.1

Syntax: ip router-id <ip-addr>

Possible values: N/A

Default value: the numerically lowest IP address configured on the Routing Switch

ip session tcp-msl

NOTE: This command is supported in software release 07.7.00 and later.

Sets the amount of time a session table entry stays in the delete queue following a TCP FIN from a client.

By default, upon receiving a TCP FIN (finish) from a client, the HP device puts the session in a delete queue and ages out the session table entry in 8 seconds. In software release 07.7.00, you can optionally configure the device to age out session table entries in 0 to 40 seconds.

EXAMPLE:
ProCurveRS(config)# ip session tcp-msl 16

This command causes the device to age out the session table entry in 16 seconds.

Syntax: [no] ip session tcp-msl <seconds>

Possible values:

<seconds> can be from 0 – 40 seconds

To set the TCP fast aging interval to the default (8 seconds) after you have configured an interval other than the default interval, use the no parameter or enter ip session tcp-msl 0.

Default value: 8 seconds

ip show-acl-service-number

NOTE: This command is available in software releases 07.6.05 and later.

Changes the display of TCP/UDP application information from the TCP/UDP well-known port name to the TCP/UDP port number. For example, entering the following command causes the HP device to display 80 (the port number) instead of http (the well-known port name) in the output of show commands and other commands that contain application port information.

EXAMPLE:
9300 series(config)# ip show-acl-service-number

Syntax: [no] ip show-acl-service-number

Possible values: N/A

Default value: By default, HP devices display TCP/UDP application information in named notation.

ip show-portname

Displays the name of the interface instead of its number. By default an interface's slot number (if applicable) and port number are displayed when you display Syslog messages. In software release 07.6.04 and later, if you want to display the name of the interface instead of its number, enter a command such as the following:

EXAMPLE:
ProCurveRS(config)# ip show-portname

This command is applied globally to all interfaces.

Syntax: [no] ip show-portname
When you display the messages in the Syslog, you see the interface name under the Dynamic Log Buffer section. The actual interface number is appended to the interface name. For example, if the interface name is "lab" and its port number is "2", you see "lab2". For an example screen display, see the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches*.

**Possible values:** N/A  
**Default value:** N/A

### ip show-service-number-in-log
Changes the display of TCP/UDP application information from the TCP/UDP well-known port name to the TCP/UDP port number. For example, entering the following command causes the HP device to display `http` (the well-known port name) instead of `80` (the port number) in the output of `show` commands, and other commands that contain application port information. By default, HP devices display TCP/UDP application information in named notation.

**EXAMPLE:**

```
9300 series(config)# ip show-service-number-in-log
```

**Syntax:** `[no] ip show-service-number-in-log`

**Possible values:** N/A  
**Default value:** N/A

### ip show-subnet-length
Changes display of network mask information from class-based notation (`xxx.xxx.xxx.xxx`) to Classless Interdomain Routing (CIDR) notation. By default, HP devices display network mask information in class-based notation.

**EXAMPLE:**

```
ProCurveRS(config)# ip show-subnet-length
```

**Syntax:** `[no] ip show-subnet-length`

**Possible values:** N/A  
**Default value:** Disabled

### ip source-route
Disables or re-enables forwarding of IP source-routed packets.

**EXAMPLE:**

To disable forwarding of IP source-routed packets, enter the following command:

```
ProCurveRS(config)# no ip source-route
```

**Syntax:** `[no] ip source-route`

To re-enable forwarding of source-routed packets, enter the following command:

```
ProCurveRS(config)# ip source-route
```

**Possible values:** N/A  
**Default value:** Disabled

### ip ssh authentication-retries
Sets the number of SSH authentication retries.

**EXAMPLE:**

The following command changes the number of authentication retries to 5:

```
ProCurveRS(config)# ip ssh authentication-retries 5
```

**Syntax:** `ip ssh authentication-retries <number>`
Global CONFIG Commands

Possible values: 1 – 5
Default value: 3

**ip ssh client**
Restricts SSH management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device’s CLI through SSH.

**EXAMPLE:**
To restrict SSH access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
ProCurveRS(config)# ip ssh client 209.157.22.26
```

**Syntax:** [no] ip ssh client <ip-addr>

Starting in release 07.8.00, you can restrict SSH access to the HP device based on the MAC address of a connecting client. For example, the following command allows SSH access to the HP device only to the host with IP address 209.157.22.39 and MAC address 0007.e90f.e9a0:

```
ProCurveRS(config)# ip ssh client 209.157.22.39 0007.e90f.e9a0
```

**Syntax:** [no] ip ssh client <ip-addr> <mac-addr>

The following command allows SSH access to the HP device to a host with any IP address and MAC address 0007.e90f.e9a0:

```
ProCurveRS(config)# ip ssh client any 0007.e90f.e9a0
```

**Syntax:** [no] ip ssh client <mac-addr>

**Possible values:** A valid address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

**Default value:** N/A

**ip ssh idle-time**
Sets the amount of time an SSH session can be inactive before the HP device closes it.

**EXAMPLE:**

```
ProCurveRS(config)# ip ssh idle-time 30
```

**Syntax:** ip ssh idle-time <minutes>

**Possible values:** 0 – 240 minutes

**Default value:** 0 minutes

**ip ssh key-size**
Sets the SSH key size.

**EXAMPLE:**
The following command changes the server RSA key size to 896 bits:

```
ProCurveRS(config)# ip ssh key-size 896
```

**Syntax:** ip ssh key-size <number>

**NOTE:** The size of the host RSA key that resides in the system-config file is always 1024 bits and cannot be changed.

**Possible values:** 512 – 896 bits

**Default value:** 768 bits

**ip ssh password-authentication**
Disables SSH password authentication.
After the SSH server on the HP device negotiates a session key and encryption method with the connecting client, user authentication takes place. Of the methods of user authentication available in SSH, HP’s implementation of SSH supports password authentication only.

With password authentication, users are prompted for a password when they attempt to log into the device (unless empty password logins are not allowed; see “ip ssh permit-empty-passwd”). If there is no user account that matches the user name and password supplied by the user, the user is not granted access.

You can deactivate password authentication for SSH. However, since password authentication is the only user authentication method supported for SSH, this means that no user authentication is performed at all. Deactivating password authentication essentially disables the SSH server entirely.

**EXAMPLE:**
To deactivate password authentication:

```
ProCurveRS(config)# ip ssh password-authentication no
```

*Syntax:* `ip ssh password-authentication no | yes`

*Possible values:* N/A

*Default value:* Enabled

**ip ssh permit-empty-passwd**

Enables empty password SSH logins. By default, empty password logins are not allowed. This means that users with an SSH client are always prompted for a password when they log into the device. To gain access to the device, each user must have a user name and password. Without a user name and password, a user is not granted access. See the *Security Guide for ProCurve 9300/9400 Series Routing Switches* for information on setting up user names and passwords on HP devices.

If you enable empty password logins, users are not prompted for a password when they log in. Any user with an SSH client can log in without being prompted for a password.

**EXAMPLE:**
To enable empty password logins:

```
ProCurveRS(config)# ip ssh permit-empty-passwd yes
```

*Syntax:* `ip ssh permit-empty-passwd no | yes`

*Possible values:* N/A

*Default value:* Disabled

**ip ssh port**

Changes the TCP port used for SSH. By default, SSH traffic occurs on TCP port 22. You can change this port number.

**EXAMPLE:**
The following command changes the SSH port number to 2200:

```
ProCurveRS(config)# ip ssh port 2200
```

Note that if you change the default SSH port number, you must configure SSH clients to connect to the new port. Also, you should be careful not to assign SSH to a port that is used by another service. If you change the SSH port number, HP recommends that you change it to a port number greater than 1024.

*Syntax:* `ip ssh port <number>`

*Possible values:* a valid TCP port number

*Default value:* 22

**ip ssh pub-key-file**

Causes a public key file to be loaded onto the HP device.
EXAMPLE:
To cause a public key file called pkeys.txt to be loaded from a TFTP server each time the HP device is booted, enter a command such as the following:

ProCurveRS(config)# ip ssh pub-key-file tftp 192.168.1.234 pkeys.txt

NOTE: This command is not supported on the ProCurve 9408sl.

Syntax: [no] ip ssh pub-key-file tftp <tftp-server-ip-addr> <filename>
To reload the public keys from the file on the TFTP server, enter the following command:

ProCurveRS(config)# ip ssh pub-key-file reload

Syntax: [no] ip ssh pub-key-file reload
To make the public keys in the active configuration part of the startup-config file, enter the following commands:

ProCurveRS(config)# ip ssh pub-key-file flash-memory
ProCurveRS(config)# write memory

NOTE: This command is not supported on the ProCurve 9408sl.

Syntax: [no] ip ssh pub-key-file flash-memory
Possible values: N/A
Default value: N/A

ip ssh rsa-authentication
Disables or re-enables RSA challenge-response authentication.

EXAMPLE:
To disable RSA challenge-response authentication:

ProCurveRS(config)# ip ssh rsa-authentication no

Syntax: [no] ip ssh rsa-authentication yes | no
Possible values: yes or no
Default value: RSA challenge-response authentication is enabled by default.

ip ssh scp
Disables or re-enables Secure Copy (SCP).

EXAMPLE:
To disable SCP:

ProCurveRS(config)# ip ssh scp disable

Syntax: [no] ip ssh scp disable | enable
Possible values: disable or enable
Default value: SCP is enabled by default.

NOTE: If you disable SSH, SCP is also disabled.

ip ssh source-interface
Configures the device to use the lowest-numbered IP address configured on an interface as the source for all SSH packets from the device. The software uses the lowest-numbered IP address configured on the interface as the source IP address for the packets.
EXAMPLE:
To specify the lowest-numbered IP address configured on a virtual interface as the device's source for all SSH packets, enter commands such as the following:

```
ProCurveRS(config)# int ve 1
ProCurveRS(config-vif-1)# ip address 10.0.0.3/24
ProCurveRS(config-vif-1)# exit
ProCurveRS(config)# ip ssh source-interface ve 1
```

The commands in this example configure virtual interface 1, assign IP address 10.0.0.3/24 to the interface, then designate the interface as the source for all SSH packets from the Routing Switch.

**Syntax:** `ip ssh source-interface ethernet <portnum> | loopback <num> | ve <num>`

**Possible values:** see above

**Default value:** The lowest-numbered IP address configured on the interface through which the packet is sent. The address therefore changes, by default, depending on the interface.

---

**ip ssh timeout**

Changes the SSH timeout value. When the SSH server attempts to negotiate a session key and encryption method with a connecting client, it waits a maximum of 120 seconds for a response from the client. If there is no response from the client after 120 seconds, the SSH server disconnects.

**EXAMPLE:**

```
ProCurveRS(config)# ip ssh timeout 60
```

**Syntax:** `ip ssh timeout <seconds>`

**Possible values:** 1 – 120 second

**Default value:** 120 seconds

---

**ip ssl certificate-data-file**

Imports a digital certificate file using TFTP.

To allow a client to communicate with the HP device using an SSL connection, you configure a set of digital certificates and RSA public-private key pairs on the device. A digital certificate is used for identifying the connecting client to the server. It contains information about the issuing Certificate Authority, as well as a public key. You can either import digital certificates and private keys from a server, or you can allow the HP device to create them. This command allows you to import a digital certificate using TFTP.

**EXAMPLE:**

```
ProCurveRS(config)# ip ssl certificate-data-file tftp 192.168.9.210 certfile
```

**Syntax:** `[no] ip ssl certificate-data-file tftp <ip-addr> <certificate-filename>`

**Possible values:** The `<ip-addr>` is the IP address of a TFTP server that contains the digital certificate. The `<certificate-filename>` is the name of the digital certificate. The digital certificate file can be no larger than 2048 bytes.

**Default value:** N/A

---

**ip ssl port**

Specifies a port for SSL communication.

**EXAMPLE:**

```
ProCurveRS(config)# ip ssl port 334
```

**Syntax:** `[no] ip ssl port <port-number>`

**Possible values:** Port number

**Default value:** 443
**ip ssl private-key-file**
Imports a private key file using TFTP.

To allow a client to communicate with the HP device using an SSL connection, you configure a set of digital certificates and RSA public-private key pairs on the device. A digital certificate is used for identifying the connecting client to the server. It contains information about the issuing Certificate Authority, as well as a public key. You can either import digital certificates and private keys from a server, or you can allow the HP device to create them. This command allows you to import a private key file using TFTP.

**EXAMPLE:**
```
ProCurveRS(config)# ip ssl private-key-file tftp 192.168.9.210 keyfile
```

**Syntax:** `[no] ip ssl private-key-file tftp <ip-addr> <key-filename>

The `<ip-addr>` is the IP address of a TFTP server that contains the digital certificate or private key.

**Possible values:** The `<ip-addr>` is the IP address of a TFTP server that contains the private key file. The `<key-filename>` is the name of the private key file.

**Default value:** N/A

**ip strict-acl-out**
Enables the software to process outbound ACLs as in releases prior to 07.6.01. You can enable this feature in software releases 07.6.05 and later.

In releases prior to 07.6.01, an outbound ACL implicitly subjects examination of all inbound traffic to all inbound ACLs, in order to determine whether to forward the traffic. For TCP traffic, only TCP control traffic is subject to examination by the inbound ACLs. Non-control TCP traffic is not subject to examination.

In releases 07.6.01 and later, an outbound ACL subjects examination of the inbound traffic to the outbound ACL only. This method is more efficient, as the software examines only the traffic that is subject to the ACL.

**EXAMPLE:**
```
ProCurveRS(config)# ip strict-acl-out
ProCurveRS(config)# ip rebind-acl all
```

**Syntax:** `[no] ip strict-acl-out

**Possible value:** N/A

**Default value:** Disabled

**ip strict-acl-tcp**
Enables the strict ACL TCP mode.

By default, when you use ACLs to filter TCP traffic, the HP device does not compare all TCP packets against the ACLs. Instead, the device compares TCP control packets against the ACLs, but not data packets. Control packets include packet types such as SYN (Synchronization) packets, FIN (Finish) packets, and RST (Reset) packets.

In normal TCP operation, TCP data packets are present only if a TCP control session for the packets also is established. For example, data packets for a session never occur if the TCP SYN for that session is dropped. Therefore, by filtering the control packets, the HP device also implicitly filters the data packets associated with the control packets. This mode of filtering optimizes forwarding performance for TCP traffic by forwarding data packets without examining them. Since the data packets are present in normal TCP traffic only if a corresponding TCP control session is established, comparing the packets for the control session to the ACLs is sufficient for filtering the entire session including the data.

However, it is possible to generate TCP data packets without corresponding control packets, in test or research situations for example. In this case, the default ACL mode does not filter the data packets, since there is no corresponding control session to filter. To filter this type of TCP traffic, use the strict ACL TCP mode. This mode compares all TCP packets to the configured ACLs, regardless of whether the packets are control packets or data packets. If the ACLs permit the packet, the device creates a session entry for forwarding other TCP packets with the same Layer 3 and Layer 4 addresses.
NOTE: Regardless of whether the strict mode is enabled or disabled, the device always compares TCP control packets against the configured ACLs before creating a session entry for forwarding the traffic.

NOTE: If the device’s configuration currently has ACLs associated with interfaces, remove the ACLs from the interfaces before changing the ACL mode.

EXAMPLE:
To enable the strict ACL TCP mode, enter the following command at the global CONFIG level of the CLI:

ProCurveRS(config)# ip strict-acl-tcp

Syntax: [no] ip strict-acl-tcp

This command configures the device to compare all TCP packets against the configured ACLs before forwarding them.

To disable the strict ACL mode and return to the default ACL behavior, enter the following command:

ProCurveRS(config)# no ip strict-acl-tcp

Possible values: N/A

Default value: Disabled

ip strict-acl-udp

Configures the device to send all UDP packets to the CPU for ACL processing.

By default, when you use ACLs to filter UDP traffic, the HP device does not compare all UDP packets against the ACLs. Instead, the device compares the source and destination information against entries in the session table. The session table contains forwarding entries based on Layer 3 and Layer 4 information.

- If the session table contains a matching entry, the device forwards the packet, assuming that the first packet the device received that contains the same address information was permitted by the ACLs.

- If the session table does not contain a matching entry, the device sends the packet to the CPU, where the software compares the packet against the ACLs. If the ACLs permit the packet (explicitly by a permit ACL entry or implicitly by the absence of a deny ACL entry), the CPU creates a session table entry for the packet’s forwarding information and forwards the packet.

For tighter control, the software provides the strict ACL UDP mode. When you enable strict UDP processing, the device sends every UDP packet to the CPU and compares the packet against the configured ACLs.

NOTE: If the device’s configuration currently has ACLs associated with interfaces, remove the ACLs from the interfaces before changing the ACL mode.

EXAMPLE:
To enable the strict ACL UDP mode, enter the following command at the global CONFIG level of the CLI:

ProCurveRS(config)# ip strict-acl-udp

Syntax: [no] ip strict-acl-udp

This command configures the device to compare all UDP packets against the configured ACLs before forwarding them.

To disable the strict ACL mode and return to the default ACL behavior, enter the following command:

ProCurveRS(config)# no ip strict-acl-udp

Possible values: N/A

Default value: Disabled
ip supernet connected
Configures the device to program directly connected routes as supernet routes in CAM. This command applies to HP devices running Enterprise software release 07.8.00 or higher.

By default, for supernet routes of directly connected routes, the HP device creates 32-bit host CAM entries for traffic using these routes. If a network has traffic destined to a large number of different hosts, creating the 32-bit supernet routes can consume a large portion of CAM space.

See "CAM Support for Directly Connected Routes" in the *Diagnostic Guide for ProCurve 9300/9400 Series Routing Switches* for more information.

**EXAMPLE:**
To configure the device to program directly connected routes as supernet routes in CAM, enter the following command:

```
IPv6 Configuration Guide for the 9408sl Routing Switch (config)# ip supernet connected
```

**Syntax:**
```
[no] ip supernet connected
```

This feature takes effect immediately after you enter the `ip supernet connected` command. CAM entries that have already been programmed are not affected, however; consequently, you may want to save the configuration and restart the HP device after enabling the feature.

**Possible values:** N/A

**Default value:** Disabled

ip tacacs source-interface
Configures the device to use the first IP address configured on an interface as the source for all TACACS/TACACS+ packets from the device. The software uses the lowest-numbered IP address configured on the interface as the source IP address for the packets.

**EXAMPLE:**
To specify the lowest-numbered IP address configured on a virtual interface as the device's source for all TACACS/TACACS+ packets, enter commands such as the following:

```
ProCurveRS(config)# int ve 1
ProCurveRS(config-vif-1)# ip address 10.0.0.3/24
ProCurveRS(config-vif-1)# exit
ProCurveRS(config)# ip tacacs source-interface ve 1
```

The commands in this example configure virtual interface 1, assign IP address 10.0.0.3/24 to the interface, then designate the interface as the source for all TACACS/TACACS+ packets from the Routing Switch.

**Syntax:** `ip tacacs source-interface ethernet <portnum> | loopback <num> | ve <num>`

**Possible values:** see above

**Default value:** The lowest-numbered IP address configured on the interface through which the packet is sent. The address therefore changes, by default, depending on the interface.

ip tcp burst-normal
Causes the HP device to drop TCP SYN packets when excessive numbers are encountered, as is the case when the device is the victim of a TCP SYN attack. This command allows you to set threshold values for TCP SYN packets targeted at the router and drop them when the thresholds are exceeded.

**EXAMPLE:**
In the following example, if the number of TCP SYN packets received per second exceeds 10, the excess packets are dropped. If the number of TCP SYN packets received per second exceeds 100, the device drops all TCP SYN packets for the next 300 seconds (five minutes).

```
ProCurveRS(config)# ip tcp burst-normal 10 burst-max 100 lockup 300
```

You can set threshold values for TCP SYN packets received on an interface and drop them when the thresholds are exceeded. For example:
ProCurveRS(config)# int e 3/11
ProCurveRS(config-if-e100-3/11)# ip tcp burst-normal 10 burst-max 100 lockup 300

**Syntax:** ip tcp burst-normal <value> burst-max <value> lockup <seconds>

The burst-normal value can be from 1 – 100000.
The burst-max value can be from 1 – 100000.
The lockup value can be from 1 – 10000.
The number of incoming TCP SYN packets per second are measured and compared to the threshold values as follows:

- If the number of TCP SYN packets exceeds the burst-normal value, the excess TCP SYN packets are dropped.
- If the number of TCP SYN packets exceeds the burst-max value, all TCP SYN packets are dropped for the number of seconds specified by the lockup value. When the lockup period expires, the packet counter is reset and measurement is restarted.

**Possible values:** The burst-normal and burst-max values can be between 1 – 100000 packets. The burst-normal value must be smaller than the burst-max value. The lockup value can be between 1 – 10000 seconds.

**Default value:** N/A

**ip tcp keepalive**

Changes TCP keepalive parameters.

The HP device sends keepalive messages to another device if there is no activity on a given TCP session with the device for a certain period. For example, if a Telnet client or BGP4 neighbor’s TCP session with the HP device is inactive for two minutes (the default keepalive timeout), the HP device sends a TCP keepalive message to the device. If the device responds to the keepalive message, the HP device continues using the session. If the device does not respond, the HP device assumes that the other end is dead and terminates the session.

By default, the HP device sends a keepalive message when a session has been inactive for 120 seconds. The HP device sends up to three keepalive messages, at 60-second intervals. If the other device does not respond within 60 seconds after the last message is sent, the HP device terminates the session.

**EXAMPLE:**

ProCurveRS(config)# ip tcp keepalive 300 60 5

**Syntax:** [no] ip tcp keepalive <timeout> <interval> <nummsgs>

The <timeout> parameter specifies the number of seconds the HP device allows a TCP session to be inactive before sending a keepalive packet. You can specify any number of seconds for the timeout. If you specify 0, TCP keepalive messages are disabled, in which case the HP device assumes that all open TCP sessions are active. The default timeout is 120 seconds.

The <interval> parameter specifies the number of seconds between TCP keepalive messages. You can specify any number of seconds. The default is 60 seconds.

The <nummsgs> parameter specifies the number of TCP keepalive messages the HP device will send. The HP device sends one message at each keepalive interval. If the other device does not respond within the keepalive interval after the last message is sent, the HP device terminates the session. You can specify any number of messages. The default is 3 messages.

**Possible values:** See above

**Default value:** timeout is 120 seconds; interval is 60 seconds; number of messages is 3

**ip tcp tcp-security**

**NOTE:** This command is supported starting in software release 07.6.06.
Enables a TCP security feature that improves upon the handling of TCP inbound segments. This enhancement eliminates or minimizes the possibility of a TCP reset attack, in which a perpetrator attempts to prematurely terminate an active TCP session, and a data injection attack, wherein an attacker injects or manipulates data in a TCP connection.

The TCP security enhancement prevents and protects against the following three types of attacks:

- Blind TCP reset attack using the reset (RST) bit.
- Blind TCP reset attack using the synchronization (SYN) bit
- Blind TCP packet injection attack

The TCP security enhancement is automatically enabled in software releases 07.6.06 and later. If necessary, you can disable this feature. When you disable this feature, the HP device reverts to the original behavior (i.e., processes TCP segments as in releases prior to 07.6.06).

For more information about TCP security and the enhancements in 07.6.06, see the Security Guide for ProCurve 9300/9400 Series Routing Switches.

**EXAMPLE:**
To disable the TCP security enhancement, enter the following command at the Global CONFIG level of the CLI:

```
ProCurveRS(config)# no ip tcp tcp-security
```

To re-enable the TCP security enhancement once it has been enabled, enter the following command:

```
ProCurveRS(config)# ip tcp tcp-security
```

**Syntax:** [no] ip tcp tcp-security

**Possible values:** N/A

**Default value:** Enabled

**ip telnet source-interface**

Configures the device to use the lowest-numbered IP address configured on an interface as the source for all Telnet packets from the device. The software uses the lowest-numbered IP address configured on the interface as the source IP address for the packets.

**NOTE:** When you specify a single Telnet source, you can use only that source address to establish Telnet management sessions with the HP device.

**EXAMPLE:**
To specify the lowest-numbered IP address configured on a loopback interface as the device’s source for all Telnet packets, enter commands such as the following:

```
ProCurveRS(config)# int loopback 2
ProCurveRS(config-lbif-2)# ip address 10.0.0.2/24
ProCurveRS(config-lbif-2)# exit
ProCurveRS(config)# ip telnet source-interface loopback 2
```

The commands in this example configure loopback interface 2, assign IP address 10.0.0.2/24 to the interface, then designate the interface as the source for all Telnet packets from the Routing Switch.

**Syntax:** ip telnet source-interface ethernet <portnum> | loopback <num> | ve <num>

The following commands configure an IP interface on an Ethernet port and designate the address port as the source for all Telnet packets from the Routing Switch.

```
ProCurveRS(config)# interface ethernet 1/4
ProCurveRS(config-if-1/4)# ip address 209.157.22.110/24
ProCurveRS(config-if-1/4)# exit
ProCurveRS(config)# ip telnet source-interface ethernet 1/4
```

**Possible values:** see above
Default value: The lowest-numbered IP address configured on the interface through which the packet is sent. The address therefore changes, by default, depending on the interface.

ip tftp source-interface

Configures the device to use the lowest-numbered IP address configured on an interface as the source for all TFTP packets from the device. The software uses the lowest-numbered IP address configured on the interface as the source IP address for the packets.

EXAMPLE:
To specify the lowest-numbered IP address configured on a virtual interface as the device's source for all TFTP packets, enter commands such as the following:

```
ProCurveRS(config)# int ve 1
ProCurveRS(config-vif-1)# ip address 10.0.0.3/24
ProCurveRS(config-vif-1)# exit
ProCurveRS(config)# ip tftp source-interface ve 1
```

The commands in this example configure virtual interface 1, assign IP address 10.0.0.3/24 to the interface, then designate the interface's address as the source address for all TFTP packets.

Syntax: `ip tftp source-interface ethernet <portnum> | loopback <num> | ve <num>

Possible values: see above

Default value: The default is the lowest-numbered IP address configured on the port through which the packet is sent. The address therefore changes, by default, depending on the port.

ip ttl

Sets the maximum time that a packet will live on the network.

EXAMPLE:

```
ProCurveRS(config)# ip ttl 25
ProCurveRS(config)# exit
ProCurveRS# write memory
```

Syntax: `ip ttl <hops>

Possible values: 1 – 255 hops

Default value: 64 hops

ipv6 access-class

Controls incoming and outgoing connections to and from a router. To control the connections, you must create an ACL and then apply the ACL to incoming or outgoing connections to the router.

EXAMPLE:
To permit incoming connections from remote hosts (2000:2383:e0bb::2/128 and 2000:2383:e0bb::3/128) to a router (30ff:3782::ff89/128), enter commands such as the following:

```
ProCurveRS(config)# ipv6 access-list remote-hosts permit 2000:2383:e0bb::2/128 30ff:3782::ff89/128 priority 10
ProCurveRS(config)# ipv6 access-list remote-hosts permit 2000:2383:e0bb::3/128 30ff:3782::ff89/128 priority 20
ProCurveRS(config)# ipv6 access-class remote-hosts in
```

Because of the implicit deny command at the end of each IPv6 ACL, the router denies incoming connections from all other IPv6 hosts.

Syntax: `ipv6 access-class <ipv6-acl-name> in | out

For the `<ipv6-acl-name>` parameter, specify the name of an IPv6 ACL created using the `ipv6 access-list` command.
The in keyword applies the specified IPv6 ACL to incoming connections from remote hosts to the router. The out keyword applies the specified IPv6 ACL to outgoing connections from the router to remote hosts.

**Possible values:** See above

### ipv6 access-list

Creates IPv6 ACLs. You can configure up to 100 ACLs; however, the total number of all conditional statements on a device cannot exceed 1024, which can be either in a single ACL or in multiple ACLs. Each statement is applied to packets in the order in which they are specified.

**NOTE:** Unlike IPv4, there is no distinction between standard and extended ACLs in IPv6.

After you enter the `ipv6 access-list` command, the HP device enters the IPv6 Access List configuration level, where you can access several commands for configuring IPv6 ACL entries. For information about these commands, see “IPv6 Access List Commands” on page 12-1.

**EXAMPLE:**

```
ProCurveRS(config)# ipv6 access-list netw
ProCurveRS(config-ipv6-access-list-netw)#
```

**Syntax:**

```[no] ipv6 access-list <acl name>```

The `<name>` parameter specifies a name for the IPv6 ACL. An IPv6 ACL name cannot start with a numeral, for example, 1access. Also, an IPv4 ACL and an IPv6 ACL cannot share the same name.

### ipv6 dns domain-name

Defines an IPv6 DNS domain name.

**EXAMPLE:**

To define an IPv6 domain name as "HPnet.com" use the following command:

```
ProCurveRS(config)# ipv6 dns domain-name HPnet.com
```

**Syntax:**

```[no] ipv6 dns domain-name <domain name>```

### ipv6 dns server-address

Defines an IPv6 DNS server address.

**EXAMPLE:**

To define an IPv6 server address as "200::1" use the following command:

```
ProCurveRS(config)# ipv6 dns server-address 200::1
```

**Syntax:**

```[no] ipv6 dns server-address <ipv6-addr> [<ipv6-addr>] [<ipv6-addr>] [<ipv6-addr>]```

### ipv6 hop-limit

Limits the number of hops an IPv6 packet can traverse.

**EXAMPLE:**

To change the maximum number of hops to 70, you can enter commands such as the following:

```
ProCurveRS(config)# ipv6 hop-limit 70
```

**Syntax:**

```[no] ipv6 hop-limit <number>```

**Possible values:** 1 – 255

**Default value:** 64
**ipv6 icmp error-interval**

Adjust the following elements related to the token bucket algorithm:

- The interval at which tokens are added to the bucket.
- The maximum number of tokens in the bucket. The default is 10 tokens.

To illustrate how this algorithm works, imagine a virtual bucket that contains a number of tokens. Each token represents the ability to send one ICMP error message. Tokens are placed in the bucket at a specified interval until the maximum number of tokens allowed in the bucket is reached. For each error message that ICMP sends, a token is removed from the bucket. If ICMP generates a series of error messages, messages can be sent until the bucket is empty. If the bucket is empty of tokens, error messages cannot be sent until a new token is placed in the bucket.

**EXAMPLE:**

To adjust the interval to 1000 milliseconds and the number of tokens to 100 tokens, enter the following command:

```
ProCurveRS(config)# ipv6 icmp error-interval 1000 100
```

**Syntax:**

```
ipv6 icmp error-interval <interval> [number-of-tokens>
```

The `<interval>` parameter specifies the interval in milliseconds at which tokens are placed in the bucket. You can specify a range from 0 – 2147483647. To disable ICMP rate limiting, set the interval to zero.

The `<number-of-tokens>` parameter specifies the number of tokens the bucket can store. You can specify a range from 1 – 200.

**NOTE:** If you retain the default interval value or explicitly set the value to 100 milliseconds, output from the `show run` command does not include the setting of the `ipv6 icmp error-interval` command because the setting is the default.

Also, if you configure the interval value to a number that does not evenly divide into 100000 (100 milliseconds), the system rounds up the value to a next higher value that does divide evenly into 100000. For example, if you specify an interval value of 150, the system rounds up the value to 200.

**Possible values:** See above

**Default value:** ICMP rate limiting is enabled by default. The default interval at which tokens are added to the bucket is 100 milliseconds. The default number of tokens in the bucket is 10.

**ipv6 load-sharing**

Enables and disables ECMP load sharing and specifies the number of sharing paths.

**EXAMPLE:**

ECMP load sharing for IPv6 is enabled by default. To disable this feature, enter the following command:

```
ProCurveRS(config)# no ipv6 load-sharing
```

If you want to re-enable the feature after disabling it, enter the following command:

```
ProCurveRS(config)# ipv6 load-sharing
```

By default, IPv6 ECMP load sharing allows traffic to be balanced across up to four equal paths. You can change the maximum number of paths the device supports to a value from 2 – 8. To change the number of ECMP load sharing paths for IPv6 to 8, enter the following command:

```
ProCurveRS(config)# ipv6 load-sharing 8
```

**Syntax:**

```
[no] ipv6 load-sharing <num>
```

`<num>` specifies the number of paths and can be from 2 – 8.

**Possible values:** as shown above

**Default value:** ECMP load sharing is enabled by default. The default number of paths is 4
ipv6 load-sharing by-host
Enables host-based ECMP load sharing on a device. This command also disables network-based ECMP load-sharing at the same time.

**EXAMPLE:**
To enable host-based ECMP load sharing, enter the following command:

```
ProCurveRS(config)# ipv6 load-sharing by-host
```

**Syntax:** [no] ipv6 load-sharing by-host

**Possible values:** N/A

**Default value:** Network-based ECMP load sharing.

ipv6 mld max-response-time
Defines the maximum amount of time a multicast listener has to respond to queries.

**EXAMPLE:**
```
ProCurveRS(config)#ipv6 mld max-response-time 5
```

**Syntax:** ipv6 mld max-response-time <seconds>

**Possible values:** 1 – 10 seconds

**Default value:** 5 seconds

ipv6 mld query-interval
Defines the frequency at which MLD query messages are sent.

**EXAMPLE:**
```
ProCurveRS(config)#ipv6 mld query-interval 50
```

**Syntax:** ipv6 mld query-interval <seconds>

**Possible values:** 1 – 3600 seconds

**Default value:** 60 seconds.

ipv6 neighbor
Adds a static entry to the IPv6 neighbor discovery cache, which causes a neighbor to be reachable at all times without using neighbor discovery. A static entry in the IPv6 neighbor discovery cache functions like a static ARP entry in IPv4.

**EXAMPLE:**
To add a static entry for a neighbor with the IPv6 address 3001:ffe0:2678:47b and link-layer address 0004.6a2b.8641 that is reachable through Ethernet interface 1, enter the following command:

```
ProCurveRS(config)# ipv6 neighbor 3001:ffe0:2678:47b ethernet 1 0004.6a2b.8641
```

**Syntax:** [no] ipv6 neighbor <ipv6-address> ethernet <port> | ve <ve-number> [ethernet <port>] <link-layer-address>

The <ipv6-address> parameter specifies the address of the neighbor.

The ethernet | ve parameter specifies the interface through which to reach a neighbor. If you specify an Ethernet interface, specify the port number of the Ethernet interface. If you specify a VE, specify the VE number and then the Ethernet port numbers associated with the VE. The link-layer address is a 48-bit hardware address of the neighbor.

**Possible values:** See above

**Default value:** N/A
ipv6 prefix-list

Configures up to 100 IPv6 prefix lists, which you can use for basic traffic filtering. An IPv6 prefix list is composed of one or more conditional statements that pose an action (permit or deny) if a packet matches a specified prefix. In prefix lists with multiple statements, you can specify a sequence number for each statement. The specified sequence number determines the order in which the statement appears in the prefix list.

You can configure an IPv6 prefix list on a global basis, then use it as input to other commands or processes, such as route aggregation, route redistribution, route distribution, route maps, and so on. When an interface sends or receives an IPv6 packet, it applies the statement(s) within the IPv6 prefix list in their order of appearance to the packet. As soon as a match occurs, the HP device that supports IPv6 takes the specified action (permit or deny the packet) and stops further comparison for that packet.

You can use permit statements in the prefix list to specify the traffic that you want to send to the other feature. If you use deny statements, the traffic specified by the deny statements is not supplied to the other feature.

**EXAMPLE:**

To configure an IPv6 prefix list that permits the inclusion of routes with the IPv6 prefix 2001::/16 in IPv6 RIP routing updates sent from Ethernet interface 1, enter commands such as the following:

```
ProCurveRS(config)# ipv6 prefix-list routesfor2001 permit 2001::/16
ProCurveRS(config)# ipv6 router rip
ProCurveRS(config-ripng-router)# distribute-list prefix-list routesfor2001 out ethernet 1
```

**Syntax:**

```
[no] ipv6 prefix-list <name> [seq <sequence-number>] deny <ipv6-prefix>/<prefix-length> | permit <ipv6-prefix>/<prefix-length> | description <string> [ge <ge-value>] [le <le-value>]
```

The `<name>` parameter specifies the prefix list name. You use this name when using the prefix list as input to command or route map.

The `seq <seq-number>` parameter is optional and specifies the IPv6 prefix list's sequence number. If you do not specify a sequence number, the software numbers them in increments of 5, beginning with prefix list entry 5. The router interprets the prefix list entries in numerical order, beginning with the lowest sequence number.

The `description <string>` parameter is a text string describing the prefix list.

The `deny <ipv6-prefix>/<prefix-length>` | `permit <ipv6-prefix>/<prefix-length>` parameters specify the action the router takes if a packet contains a route specified in this prefix list.

You must specify the `<ipv6-prefix>` parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373.

You must specify the `<prefix-length>` parameter as a decimal value. A slash mark (/) must follow the `<ipv6-prefix>` parameter and precede the `<prefix-length>` parameter.

The prefix list matches only on the specified prefix/prefix length unless you use the `ge <prefix-length>` or `le <prefix-length>` parameters. (See below.)

You can specify a range of prefix lengths for prefixes that are more specific than `<ipv6-prefix>/<prefix-length>`.

- If you specify only `ge <ge-value>`, then the range is from `<ge-value>` to 128.
- If you specify only `le <le-value>`, then the range is from `<le-value>` to the `<prefix-length>` parameter.

The `ge <ge-value>` or `le <le-value>` you specify must meet the following condition:

```
prefix-length < ge-value <= le-value <= 128
```

If you do not specify `ge <ge-value>` or `le <le-value>`, the prefix list matches only on the exact prefix you specify with the `<ipv6-prefix>/<prefix-length>` parameter.

To delete the prefix list entry, use the `no` form of this command.

**Possible values:** See above

**Default value:** N/A
**ipv6 route**

Configures a static IPv6 route, which is a manually configured route that creates a path between two IPv6 routers. You can configure a static IPv6 route to be redistributed into a routing protocol, but you cannot redistribute routes learned by a routing protocol into the static IPv6 routing table.

Before configuring a static IPv6 route, you must enable the forwarding of IPv6 traffic on the router using the `ipv6 unicast-routing` command and enable IPv6 on at least one interface by configuring an IPv6 address or explicitly enabling IPv6 on that interface. For more information, see the "ipv6 unicast-routing" on page 6-99, "ipv6 address" on page 8-38, and "ipv6 enable" on page 8-39, respectively.

**EXAMPLE:**

To configure a static IPv6 route for a destination network with the prefix 8eff::0/32, a next-hop gateway with the global address 4fee:2343:0:ee44::1, and an administrative distance of 110, enter a command such as the following:

```
ProCurveRS(config)# ipv6 route 8eff::0/32 4fee:2343:0:ee44::1 distance 110
```

**Syntax:** `ipv6 route <dest-ipv6-prefix>/<prefix-length> <next-hop-ipv6-address> [metric] [distance <number>]`

To configure a static IPv6 route for a destination network with the prefix 8eff::0/32 and a next-hop gateway with the link-local address fe80::1 that the router can access through Ethernet interface 1, enter a command such as the following:

```
ProCurveRS(config)# ipv6 route 8eff::0/32 ethernet 1 fe80::1
```

**Syntax:** `ipv6 route <dest-ipv6-prefix>/<prefix-length> <interface> <port> <next-hop-ipv6-address> [metric] [distance <number>]`

To configure a static IPv6 route for a destination network with the prefix 8eff::0/32 and a next-hop gateway that the router can access through tunnel 1, enter the following command:

```
ProCurveRS(config)# ipv6 route 8eff::0/32 tunnel 1
```

**Syntax:** `ipv6 route <dest-ipv6-prefix>/<prefix-length> <interface> <port> [metric] [distance <number>]`

Table 6.5 describes the parameters associated with this command and indicates the status of each parameter.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Details</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>The IPv6 prefix and prefix length of the route’s destination network.</td>
<td>You must specify the <code>&lt;dest-ipv6-prefix&gt;</code> parameter in hexadecimal using 16-bit values between colons as documented in RFC 2373. You must specify the <code>&lt;prefix-length&gt;</code> parameter as a decimal value. A slash mark (/) must follow the <code>&lt;ipv6-prefix&gt;</code> parameter and precede the <code>&lt;prefix-length&gt;</code> parameter.</td>
<td>Mandatory for all static IPv6 routes.</td>
</tr>
</tbody>
</table>
Table 6.5: Static IPv6 route parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Configuration Details</th>
<th>Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>The route’s next-hop gateway, which can be one of the following:</td>
<td>You can specify the next-hop gateway as one of the following types of IPv6 addresses:</td>
<td>Mandatory for all static IPv6 routes.</td>
</tr>
<tr>
<td>• The IPv6 address of a next-hop gateway.</td>
<td>• A global address.</td>
<td></td>
</tr>
<tr>
<td>• A tunnel interface.</td>
<td>• A link-local address.</td>
<td></td>
</tr>
<tr>
<td>If you specify a global address, you do not need to specify any additional parameters for the next-hop gateway.</td>
<td>If you specify a link-local address, you must also specify the interface through which to access the address. You can specify one of the following interfaces:</td>
<td></td>
</tr>
<tr>
<td>If you specify an Ethernet interface, also specify the port number associated with the interface. If you specify a VE or tunnel interface, also specify the VE or tunnel number.</td>
<td>• An Ethernet interface.</td>
<td></td>
</tr>
<tr>
<td>You can also specify the next-hop gateway as a tunnel interface. If you specify a tunnel interface, also specify the tunnel number.</td>
<td>• A tunnel interface.</td>
<td></td>
</tr>
<tr>
<td>• A virtual interface (VE).</td>
<td>• A link-local address.</td>
<td></td>
</tr>
<tr>
<td>The route’s metric.</td>
<td>You can specify a value from 1 – 16.</td>
<td>Optional for all static IPv6 routes. (The default metric is 1.)</td>
</tr>
<tr>
<td>The route’s administrative distance.</td>
<td>You must specify the distance keyword and any numerical value.</td>
<td>Optional for all static IPv6 routes. (The default administrative distance is 1.)</td>
</tr>
</tbody>
</table>

Possible values: See above

Default value: N/A

**ipv6 router ospf**

Enables OSPF version 3 globally on an HP device that supports IPv6.

After you enter ipv6 router ospf command, the HP device enters the IPv6 OSPF configuration level, where you can access several commands that allow you to configure OSPF version 3. For information about these commands, see “OSPF Version 3 Commands” on page 16-1.

**EXAMPLE:**

```
ProCurveRS(config)#ipv6 router ospf
ProCurveRS(config-ospf6-router)#
```

**Syntax:** [no] ipv6 router ospf

To disable OSPF version 3, enter the no form of this command.

Possible values: See above.
**Global CONFIG Commands**

**Default value:** OSPF version 3 is disabled.

**ipv6 router pim**

Enters the IPv6 PIM configuration level.

**EXAMPLE:**

```
ProCurveRS(config)# ipv6 router pim
```

**Possible values:** N/A

**Default value:** N/A

**ipv6 router rip**

Enables IPv6 RIP globally on an HP device that supports IPv6. To enable IPv6 RIP, you must enable it globally on the HP device and also on individual interfaces. For information about enabling IPv6 RIP on individual interfaces, see “ipv6 router rip” on page 8-49.

After you enter the **ipv6 router rip** command, the HP device enters the IPv6 RIP configuration level, where you can access several commands that allow you to configure IPv6 RIP. For information about these commands, see “IPv6 RIP Commands” on page 14-1.

**NOTE:** Enabling IPv6 RIP globally on the HP device does not enable it on individual router interfaces.

**EXAMPLE:**

```
ProCurveRS(config)# ipv6 router rip
ProCurveRS(config-ripng-router)#
```

**Syntax:**

```
[no] ipv6 router rip
```

To disable IPv6 RIP globally, use the **no** form of this command.

**Possible values:** See above.

**Default value:** IPv6 RIP is disabled.

**ipv6 unicast-routing**

Enables the forwarding of IPv6 traffic globally on an HP devices that support IPv6. To disable the forwarding of IPv6 traffic globally on the HP device, enter the **no** form of this command.

**EXAMPLE:**

```
ProCurveRS(config)# ipv6 unicast-routing
```

**Syntax:**

```
[no] ipv6 unicast-routing
```

**Possible values:** N/A

**Default value:** IPv6 routing is disabled.

**ipx forward-filter**

Defines forward filters for IPX routes.

IPX must be enabled on the ProCurve Routing Switch and a network number and frame type defined for each IPX interface, for this command to be operational.

**EXAMPLE:**

```
ProCurveRS(config)# ipx forward-filter 2 permit 1110005 451 11101050 120 any
```

**Syntax:**

```
ipx forward-filter <index> permit | deny <source-network-number> | any <source-node-number> | any <destination-network-number> | any <destination-node-number> | any <destination-socket-number> | any
```

**Possible values:** up to 32 forward filters

**Default value:** N/A
**ipx gns-round-robin**

Configures the Routing Switch to use round-robin to rotate among servers of a given service type when responding to GNS requests, instead of the default behavior of responding with the most recently learned server supporting the requested service.

**EXAMPLE:**
To enable the Routing Switch to use round-robin to select servers for replies to GNS requests:

```
ProCurveRS(config)# ipx gns-round-robin
```

**Syntax:** [no] ipx gns-round-robin

**Possible values:** N/A

**Default value:** N/A

**ipx netbios-allow**

Enables NetBIOS broadcasts (type 20) to be routed over IPX. IPX must be enabled on the router and a network number and frame type defined for each IPX interface.

**EXAMPLE:**

```
ProCurveRS(config)# ipx netbios-allow
```

**Syntax:** ipx netbios-allow

**Possible values:** N/A

**Default value:** disabled

**ipx rip-filter**

Defines IPX/RIP filters for the router. IPX must be enabled on the router for this command to be operational.

**EXAMPLE:**

```
ProCurveRS(config)# ipx rip-filter 2 permit 11005000 fffff00
-OR-
ProCurveRS(config)# ipx rip-filter 2 permit any any
```

**Syntax:** ipx rip-filter <index> permit | deny <network-number> | any <network-mask> | any

**Possible values:** up to 32 RIP filters can be defined for a router

**Default value:** N/A

**ipx rip-filter-group**

Allows a group of filters to be applied globally to all IPX interfaces at the Global Level, or individually to an IPX interface at the Interface Level. The filter can be applied to either incoming or outgoing traffic.

**EXAMPLE:**

To apply previously defined filters 1, 2, 3, and 10 to all incoming IPX RIP routes across all interfaces, enter the following command:

```
ProCurveRS(config)# ipx rip-filter-group in 1 2 3 10
```

To apply filters on an individual interface (e.g. interface 4/11) basis versus globally, enter the following:

```
ProCurveRS(config)# int e 4/11
ProCurveRS(config-if-4/11)# ipx rip-filter-group in 1 2 3 10
```

**Syntax:** ipx rip-filter-group in | out <index>

**Possible values:** in | out, filter I ds

**Default value:** disabled
Global CONFIG Commands

ipx sap-access-list
Configures access lists for filtering Service Advertisement Protocol (SAP) replies sent on a Routing Switch's IPX interfaces. You configure IPX SAP access lists on a global basis, then apply them to the IPX inbound or outbound filter group on specific interfaces. You can configure up to 32 access lists. The same access list can be applied to multiple interfaces.

EXAMPLE:
ProCurveRS(config-ipx-router)# ipx sap-access-list 10 deny efef.1234.1234.1234

Syntax: [no] ipx sap-access-list <num> deny | permit <network>[.<node>] [ <network-mask>.<node-mask> ] [ <service-type>[<server-name>]]

Possible values: The <num> parameter specifies the access list number and can be from 1 – 32.
The deny | permit parameter specifies whether the Routing Switch allows the SAP update or denies it.
The <network>[.<node>] parameter specifies the IPX network. Optionally, you also can specify a specific node (host) on the network. The <network> parameter can be an eight-digit hexadecimal number from 1 – FFFFFFFE. To specify all networks ("any"), enter –1 as the network number. If the network number has leading zeros, you do not need to specify them. For example, you can specify network 0000abab as "abab".
The node is a 48-bit value represented by three four-digit numbers joined by periods; for example, 1234.1234.1234.
The [<network-mask>.<node-mask>] parameter lets you specify a comparison mask for the network and node. The mask consists of zeros (0) and ones (f). Ones indicate significant bits. For example, to configure a mask that matches on network abcdefxx, where xx can be any value and the node address can be any value, specify the following mask: ffffff00.0000.0000.0000

The in | out parameter of the ipx sap-filter-group command specifies whether the ACLs apply to incoming traffic or outgoing traffic.
Default value: N/A

ipx sap-filter
Defines IPX/SAP filters for all IPX interfaces on the router. The IPX network number and frame type must be defined for the interfaces for this command to be operational.

EXAMPLE:
ProCurveRS(config)# ipx sap-filter 5 permit any server1
-OR-
ProCurveRS(config)# ipx sap-filter 5 permit 0004 any

Syntax: ipx sap-filter <index> permit | deny <server-type> | any <server-name> | any

Possible values: Filter IDs
Default value: Disabled

ipx sap-filter-group
Allows a group of defined IPX/SAP filters to be applied either globally (at the Global Level) or individually (at the Interface Level) to IPX interfaces on the router.
The filter can be applied to either incoming or outgoing traffic.

EXAMPLE:
To apply previously defined filters 2, 3, and 10 to all incoming IPX SAP server traffic across all interfaces, enter the following command:

ProCurveRS(config)# ipx sap-filter-group in 2 3 5

To apply filters on an individual interface basis instead of a global basis (for example, apply a filter to interface 4/11), enter the following:
ProCurveRS(config)# int 4/11
ProCurveRS(config-if)# ipx sap-filter-group in 2 3 5

**Syntax:**`ipx sap-filter-group in | out <index>`

**Possible values:** in or out, defined filter indexes

**Default value:** N/A

**NOTE:** If the 8012.1X authentication is used and the 802.1X supplicant will be sending packet that is greater than 1500 MTU, then **jumbo 1920** must be configured.

---

**jumbo1920**

**NOTE:** This command applies to Standard devices running software release 07.6.04 or later. If the 802.1X authentication is used and the 802.1X supplicant will be sending packet that is greater than 1500 MTU, then **jumbo 1920** must be configured.

Configures some Ethernet interfaces on a Standard device to have an MTU of 1518 bytes and others to have an MTU of 1920 bytes. Software releases prior to 07.6.04 supported an MTU of 1920 bytes, but it had to be applied globally to all interfaces on the device.

For VE traffic, the fragmentation boundary is based on the MTU of the physical outbound interface. No fragmentation is performed on Layer 2 frames. Layer 2 frames that exceed the MTU of the outbound interface are dropped.

**EXAMPLE:**

To change the default MTU for Ethernet interfaces to 1920 bytes, enter the following command:

```
ProCurveRS(config)# jumbo1920
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:**`[no] jumbo1920`

**Possible values:** N/A

**Default value:** Disabled

---

**link-keepalive ethernet <portnum>**

Enables Uni-Directional Link Detection (UDLD) on a trunk group.

**EXAMPLE:**

To enable UDLD on a port, enter a command such as the following at the global CONFIG level of the CLI:

```
ProCurveRS(config)# link-keepalive ethernet 1/1
```

To enable the feature on a trunk group, enter commands such as the following:

```
ProCurveRS(config)# link-keepalive ethernet 1/1 ethernet 1/2
ProCurveRS(config)# link-keepalive ethernet 1/3 ethernet 1/4
```

These commands enable UDLD on ports 1/1 – 1/4. You can specify up to two ports on the same command line.

To allows ports to receive and send UDLD control packets tagged with a specific VLAN ID, enter commands such as the following:

```
ProCurveRS(config)# link-keepalive ethernet 1/18 vlan 22
```

This commands enables UDLD on port 1/18 and allows UDLD control packet tagged with VLAN 22 to be received and sent on port 1/18.

**Syntax:**`[no] link-keepalive ethernet <portnum> [ethernet <portnum>] [vlan <vlan-id>]`
**link-keepalive interval**
Changes the Uni-Directional Link Detection (UDLD) interval.

**EXAMPLE:**
ProCurveRS(config)# link-keepalive interval 3

**Syntax:** [no] link-keepalive interval <num>
The <num> parameter specifies how often the ports send a UDLD packet.

**Possible values:** 1 – 60, in 100 ms increments
Default value: 5 (500 ms)

**link-keepalive retries**
Changes the maximum number of keepalive attempts the Uni-Directional Link Detection (UDLD) feature makes before taking down a port.

**EXAMPLE:**
ProCurveRS(config)# link-keepalive retries 4

**Syntax:** [no] link-keepalive retries <num>
The <num> parameter specifies the maximum number of times the port will try the health check.

**Possible values:** 3 – 10
Default value: 5

**lock-address ethernet**
Allows you to limit the number of devices that have access to a specific port. Access violations are reported by SNMP traps.

**EXAMPLE:**
ProCurveRS(config)# lock-address eth 4/11 addr 15

**Syntax:** lock-address ethernet <portnum> [addr-count <number>]

**Possible values:** Address count: 1 – 2,048
Default value: Address count: 8

**logging**
You can save SNMP traps locally to an event log on the Routing Switch by turning this feature on. You also can configure the device to use up to six third-party Syslog servers and modify the message level and facility using this command. In addition, you can change the number of log messages the local Syslog buffer will retain.

**EXAMPLE:**
To disable logging of SNMP traps to a locally saved event log, enter the following command:
ProCurveRS(config)# no logging on

To re-enable logging, enter the following command:
ProCurveRS(config)# logging on

**Syntax:** [no] logging on [udp-port]

**Possible values:** See above
Default value: on (enabled); UDP port 514

**EXAMPLE:**

**NOTE:** The syntax in this example applies to releases prior to 07.7.00. See the next example for the command syntax in releases 07.7.00 and later.
To specify two third-party Syslog servers to receive Syslog messages in addition to the device's local Syslog buffer, enter commands such as the following. You can specify up to six servers.

```bash
ProCurveRS(config)# logging 10.0.0.99
ProCurveRS(config)# logging 209.157.23.69
```

**Syntax:** `logging <ip-addr> | <server-name>`

**Note:** If you specify more than one Syslog server, the HP device uses the same facility and message level for messages to all the servers.

**Possible values:** N/A

**Default value:** N/A

**Example:**

To change the logging facility from the default facility user to local7, enter the following command:

```bash
ProCurveRS(config)# logging local7
```

**Syntax:** `logging facility <facility-name>`

**Possible values:**
- **kern** – kernel messages
- **user** – random user-level messages
- **mail** – mail system
- **daemon** – system daemons
- **auth** – security/authorization messages
- **syslog** – messages generated internally by Syslog
- **lpr** – line printer subsystem
- **news** – netnews subsystem
- **uucp** – uucp subsystem
- **sys9** – cron/at subsystem
- **sys10** – reserved for system use
- **sys11** – reserved for system use

**Note:** The syntax in this example applies to releases 07.7.00 and later, and ProCurve 9408sl software releases 01.0.01 and later. See the prior example for the command syntax in releases prior to 07.7.00 and 01.0.01.
Global CONFIG Commands

- **sys12** – reserved for system use
- **sys13** – reserved for system use
- **sys14** – reserved for system use
- **cron** – cron/at subsystem
- **local0** – reserved for local use
- **local1** – reserved for local use
- **local2** – reserved for local use
- **local3** – reserved for local use
- **local4** – reserved for local use
- **local5** – reserved for local use
- **local6** – reserved for local use
- **local7** – reserved for local use

Default value: user

**EXAMPLE:**
To disable logging of debugging and informational messages, enter the following commands:

```bash
ProCurveRS(config)# no logging buffered debugging
ProCurveRS(config)# no logging buffered informational
```

**Syntax:** `[no] logging buffered <level>`

**Possible values:** The `<level>` can be **emergencies**, **alerts**, **critical**, **errors**, **warnings**, **notifications**, **informational**, or **debugging**.

**Default value:** All message levels are enabled by default. You can disable message levels individually.

**EXAMPLE:**
To change the local buffer capacity from the default 50 to 100, enter the following command:

```bash
ProCurveRS(config)# logging buffered 100
```

**Syntax:** `logging buffered <num-entries>`

**Possible values:** For releases 07.6.04 and later, `<num entries>` can be from 1 - 1000 on on all devices. For releases prior to 07.6.04, `<num-entries>` can be from 1 – 1000. The change takes effect immediately and does not require you to reload the software.

**Default value:** default local buffer capacity on all devices is 50 entries.

**EXAMPLE:**
By default, a message is logged whenever a user logs into or out of the CLI’s User EXEC or Privileged EXEC mode. If you want to disable logging of users’ CLI access, enter the following command:

```bash
ProCurveRS(config)# no logging enable user-login
```

**Syntax:** `[no] logging enable user-login`

**Possible values:** N/A

**Default value:** User logins are logged by default.

**EXAMPLE:**
To enable real-time display of Syslog messages in the CLI, enter the following command at the global CONFIG level of the CLI:

```bash
ProCurveRS(config)# logging console
```

**Syntax:** `[no] logging console`
This command enables the real-time display of Syslog messages on the serial console. You can enter this command from the serial console or a Telnet or SSH session.

To also enable the real-time display for a Telnet or SSH session, enter the `terminal monitor` command from the Privileged EXEC level of the session. See “terminal monitor” on page 5-44.

Possible values: N/A

Default value: Logging to the console is disabled by default.

**lp boot system flash**

Specifies an automatic boot for all interfaces modules or a specified interface module from either the primary or secondary 9408sl software image in the interface module’s flash memory. Provided that you save this configuration by entering the `write memory` command, the system will implement the automatic boot starting with the next software reload or system reset and each reload or reset after that.

**EXAMPLE:**
The following example specifies an automatic boot from the primary 9408sl software image in the interface module’s flash memory for all interface modules.

```
ProCurveRS(config)# lp boot system flash primary all
```

**Syntax:** `lp boot system flash primary | secondary all | <slot-number>`

- **primary and secondary** specify the primary or secondary 9408sl software image in the interface module’s flash memory.
- **all | <slot-number>** parameter specifies that the automatic boot applies to all interface modules in the ProCurve 9408sl or to an interface module in the specified chassis slot number only. You can specify 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.

Possible values: see above

Default value: N/A

**lp boot system interactive**

Specifies an automatic interactive boot for all interface modules or a specified interface module. Provided that you save this configuration by entering the `write memory` command, the system will implement the automatic boot starting with the next software reload or system reset and each reload or reset after that.

**EXAMPLE:**
The following example specifies an automatic interactive boot for all interface modules.

```
ProCurveRS(config)# lp boot system interactive all
```

**Syntax:** `lp boot system interactive all | <slot-number>`

- **all | <slot-number>** parameter specifies that the automatic boot applies to all interface modules in the ProCurve 9408sl or to an interface module in the specified chassis slot number only. You can specify 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.

At the next reload or system reset, the system enters the interface module’s monitor mode. For example, to boot from the primary 9408sl software image in the interface module’s flash memory, enter the following command at the monitor prompt:

```
LP MONITOR> boot system flash primary
```

Possible values: see above

Default value: N/A

**lp boot system mp**

Specifies an automatic boot for all interface modules or a specified interface module from either the primary or secondary 9408sl software image in the management module’s flash memory. Provided that you save this configuration by entering the `write memory` command, the system will implement the automatic boot starting with the next software reload or system reset and each reload or reset after that.
EXAMPLE:
The following example specifies an automatic boot from the primary 9408sl software image in the management module's flash memory for all interface modules.

ProCurveRS(config)# lp boot system mp primary all

**Syntax:** lp boot system mp primary | secondary all | <slot-number>

*primary* and *secondary* specify the primary or secondary 9408sl software image in the management module's flash memory.

<slot-number> specifies that the automatic boot applies to all interface modules in the ProCurve 9408sl chassis or to an interface module in the specified chassis slot number only. You can specify 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.

**Possible values:** see above

**Default value:** N/A

**lp boot system slot 1 | slot 2**

Specifies an automatic boot for all interface modules or a specified interface module from a specified management module's PCMCIA Slot. Provided that you save this configuration by entering the *write memory* command, the system will implement the automatic boot starting with the next software reload or system reset and each reload or reset after that.

**EXAMPLE:**
The following example specifies an automatic boot for all interface modules from the management module's PCMCIA slot 1:

ProCurveRS(config)# lp boot system slot1 primary all

**Syntax:** lp boot system slot1 | slot2 <filename> all | <slot-number>

*slot1* and *slot2* indicate the management module's PCMCIA slot from which to boot the interface module.

<filename> specifies the name of the image from which to boot the interface module.

<slot-number> specifies that the automatic boot applies to all interface modules in the ProCurve 9408sl or to an interface module in the specified chassis slot number only. You can specify 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.

**Possible values:** see above

**Default value:** N/A

**lp boot system tftp**

Specifies an automatic boot for all interface modules or a specified interface module from a specified TFTP server. Provided that you save this configuration by entering the *write memory* command, the system will implement the automatic boot starting with the next software reload or system reset and each reload or reset after that.

**EXAMPLE:**
The following example specifies an automatic boot for all interface modules from a TFTP server.

ProCurveRS(config)# lp boot system tftp 123.123.123.123 primary all

**Syntax:** lp boot system tftp <ip-address> primary | secondary all | <filename>

<ip-address> specifies the IP address of the TFTP server from which the interface module will be booted. <filename> specifies the name of the image from which to boot the interface module.

<slot-number> specifies that the automatic boot applies to all interface modules in the ProCurve 9408sl or to an interface module in the specified chassis slot number only. You can specify 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.

**Possible values:** see above

**Default value:** N/A
lp-slot-priority
Prioritizes ProCurve 9408sl slots in which the interface modules are installed. If you assign the same priority to all slots, the leftmost slot has the highest priority, while the rightmost slot has the lowest priority.

**EXAMPLE:**
To set the priority of chassis slot 1 to the highest priority (8), enter the following command:

```
ProCurveRS(config)# lp-slot-priority 1 8
```

**Syntax:** lp-slot-priority <slot-number> <priority>

- `<slot-number>` indicates that the chassis slot number for which you are changing the priority. You can specify slots 1 – 8: 1 indicates the leftmost chassis slot, while 8 indicates the rightmost chassis slot.
- `<priority>` indicates that the priority of the chassis slot if the chassis loses power. You can specify a value of 1 – 8, where 1 is the lowest priority and 8 is the highest priority. You can set one, some, or all chassis slots to the same priority or each chassis slot to a different priority.

**Possible values:** see above

**Default value:** N/A

mac-age-time
This parameter sets the aging period for ports on the device, defining how long a port address remains active in the address table.

**EXAMPLE:**
```
ProCurveRS(config)# mac-age 600
```

**Syntax:** mac-age-time <age-time>

**Possible values:** The `<age-time>` can be 0 or a number from 67 – 65535. If you specify 0, the entries do not age.

**Default value:** 300 seconds

mac-authentication auth-fail-vlan-id
When RADIUS authentication for a MAC address fails, and the device is configured to move the port on which the traffic was received to a restricted VLAN, this command specifies the ID of this restricted VLAN.

**EXAMPLE:**
```
ProCurveRS(config)# mac-authentication auth-fail-vlan-id 200
```

**Syntax:** [no] mac-authentication auth-fail-vlan-id <vlan-id>

**Possible values:** The restricted VLAN must already exist on the device. You cannot configure the restricted VLAN to be a non-existent VLAN. If the port is a tagged or dual-mode port, you cannot use a restricted VLAN as the authentication-failure action. If the ID for the restricted VLAN is not specified at the interface level, the global restricted VLAN ID applies for the interface.

**Default value:** Disabled

mac-authentication auth-passwd-format
Specifies the format of the MAC addresses sent to the RADIUS server for the Multi-Device Port Authentication feature. When Multi-Device Port Authentication is configured, the HP device authenticates MAC addresses by sending username and password information to a RADIUS server. The username and password is the MAC address itself; that is, the device uses the MAC address for both the username and the password in the request sent to the RADIUS server.

**EXAMPLE:**
```
ProCurveRS(config)# mac-authentication auth-passwd-format xxxx.xxxx.xxxx
```

**Syntax:** mac-authentication auth-passwd-format xxxx.xxxx.xxxx | xx-xx-xx-xx-xx-xx | xxxxxxxxxxxx

**Possible values:** Each option configures the device to send the MAC address in a different format. For example, abcd.4321.34e0, ab-cd-43-21-34-e0, or abcd432134e0.
Default value: By default, the MAC address is sent to the RADIUS server in the format xxxxxxxxxxxx.

**mac-authentication disable-aging**

Disables aging for authenticated MAC addresses. MAC addresses that have been authenticated or denied by a RADIUS server are aged out if no traffic is received from the MAC address for a certain period of time.

- Authenticated MAC addresses or non-authenticated MAC addresses that have been placed in the restricted VLAN are aged out if no traffic is received from the MAC address over the device’s normal MAC aging interval.

- Non-authenticated MAC addresses that are blocked by the device are aged out if no traffic is received from the address over a fixed hardware aging period (70 seconds), plus a configurable software aging period. (See the next section for more information on configuring the software aging period).

You can optionally disable aging for MAC addresses subject to authentication.

**EXAMPLE:**

```
ProCurveRS(config)# mac-authentication disable-aging
```

**Syntax:** [no] mac-authentication disable-aging

**Possible values:** N/A

**Default value:** N/A

**mac-authentication enable**

Enables the Multi-Device Port Authentication feature. To enable Multi-Device Port Authentication, you first enable the feature globally on the device, then enable it on individual interfaces.

**EXAMPLE:**

To globally enable Multi-Device Port Authentication on the device, enter the following command:

```
ProCurveRS(config)# mac-authentication enable
```

**Syntax:** [no] mac-authentication enable

To enable MAC authentication on an individual interface, enter a command such as the following:

```
ProCurveRS(config)# mac-authentication enable ethernet 3/1
```

**Syntax:** [no] mac-authentication enable <portnum> | all

**Possible values:** The **all** option enables the feature on all interfaces at once.

**Default value:** Disabled

**mac-authentication mac-filter**

Specifies a MAC address filter for use with the Multi-Device Port Authentication feature. MAC address filters used in this way specify MAC addresses that do not have to go through Multi-Device Port Authentication. These MAC addresses are considered pre-authenticated, and are not subject to RADIUS authentication.

You should use a MAC address filter when the RADIUS server itself is connected to an interface where MAC authentication is enabled. If a MAC address filter is not defined for the MAC address of the RADIUS server and applied on the interface, the RADIUS authentication process would fail since the device would drop all packets from the RADIUS server itself.

**EXAMPLE:**

The following command defines a MAC address filter for address 0010.dc58.aca4:

```
ProCurveRS(config)# mac-authentication mac-filter 1 0010.dc58.aca4
```

**Syntax:** [no] mac-authentication mac-filter <filter-num> permit | deny <src-mac> <mask> | any <dest-mac> <mask> | any etype | IIc | snap eq | gt | lt | neq <frame-type>

**Possible values:** See “mac filter”, below.

**Default value:** N/A
**mac-authentication max-age**

Specifies the aging time for blocked MAC addresses. When the HP device is configured to drop traffic from non-authenticated MAC addresses, traffic from the blocked MAC addresses is dropped in hardware, without being sent to the CPU. A Layer 2 CAM entry is created that drops traffic from the blocked MAC address in hardware. If no traffic is received from the blocked MAC address for a certain amount of time, this Layer 2 CAM entry is aged out. If traffic is subsequently received from the MAC address, then an attempt can be made to authenticate the MAC address again.

Aging of the Layer 2 CAM entry for a blocked MAC address occurs in two phases, known as **hardware aging** and **software aging**. The hardware aging period is fixed at 70 seconds and is non-configurable. The software aging time is configurable through the CLI.

Once the HP device stops receiving traffic from a blocked MAC address, the hardware aging begins and lasts for a fixed period of time. After the hardware aging period ends, the software aging period begins. The software aging period lasts for a configurable amount of time (by default 120 seconds). After the software aging period ends, the blocked MAC address ages out, and can be authenticated again if the HP device receives traffic from the MAC address.

**EXAMPLE:**

To change the length of the software aging period for blocked MAC addresses, enter a command such as the following:

```
ProCurveRS(config)# mac-authentication max-age 180
```

**Syntax:** `[no] mac-authentication max-age <seconds>`

**Possible values:** You can specify from 1 – 65535 seconds.

**Default value:** The default is 120 seconds.

**mac-authentication no-override-restrict-vlan**

Keeps a port that has been assigned to the restricted VLAN in the restricted VLAN, even if a subsequent RADIUS Access-Accept message specifies a different VLAN for the port.

If a previous authentication attempt for a MAC address failed, and as a result the port was placed in the restricted VLAN, but a subsequent authentication attempt was successful, the RADIUS Access-Accept message may specify a VLAN for the port. By default, the HP device moves the port out of the restricted VLAN and into the RADIUS-specified VLAN. You can optionally configure the device to ignore the RADIUS-specified VLAN in the RADIUS Access-Accept message, and leave the port in the restricted VLAN.

**EXAMPLE:**

```
ProCurveRS(config)# mac-authentication no-override-restrict-vlan
```

**Syntax:** `[no] mac-authentication no-override-restrict-vlan`

**Possible values:** N/A

**Default value:** Disabled

**mac-authentication save-dynamicvlan-to-config**

Configures the HP device to save the RADIUS-specified VLAN assignments to the device's startup-config file.

**EXAMPLE:**

```
ProCurveRS(config)# mac-authentication save-dynamicvlan-to-config
```

**Syntax:** `mac-authentication save-dynamicvlan-to-config`

**Possible values:** N/A

**Default value:** By default, the dynamic VLAN assignments are not saved to the startup-config file. Entering the `show running-config` command does not display dynamic VLAN assignments, although they can be displayed with the `show vlan` and `show authenticated-mac-address detail` commands.
mac filter

Allows you to filter on MAC addresses.

**NOTE:** MAC filters do not block management access to the HP device. For example, if you apply a filter to block a specific host, the filter blocks switch traffic from the host but does not prevent the host from establishing a management connection to the device through Telnet. To block management access, use an Access Control List (ACL). See the "IP Access Control Lists (ACLs) chapter in the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

**NOTE:** You cannot use Layer 2 filters to filter Layer 4 information. To filter Layer 4 information, use IP access policies.

**EXAMPLE:**
To configure and apply a MAC filter, enter commands such as the following:

```
ProCurveRS(config)# mac filter 1 deny 3565.3475.3676 ffff.0000.0000 any etype eq 806
ProCurveRS(config)# mac filter 1 permit any any
ProCurveRS(config)# int e 1/1
ProCurveRS(config-if-1/1)# mac filter-group 1
```

These commands configure a filter to deny ARP traffic with a source MAC address that begins with "3565" to any destination. The second filter permits all traffic that is not denied by another filter.

**NOTE:** Once you define a MAC filter, the device drops Layer 2 traffic that does not match a MAC permit filter.

**Syntax:**
```
mac filter <filter-num> permit | deny <src-mac> <mask> | any <dest-mac> <mask> | any etype | llc | snap eq | gt | lt | neq <frame-type>
```

**Possible values:**
The `<filter-num>` can be a number from 1 – 128.

The `permit` | `deny` argument determines the action the software takes when a match occurs.

The `<src-mac> <mask>` | `any` parameter specifies the source MAC address. You can enter a specific address value and a comparison mask or the keyword any to filter on all MAC addresses. Specify the mask using 1’s (ones) and zeros. For example, to match on the first two bytes of the address aabb.cccddee, use the mask ffff.0000.0000. In this case, the filter matches on all MAC addresses that contain "aabb" as the first two bytes. The filter accepts any value for the remaining bytes of the MAC address. If you specify any, do not specify a mask. In this case, the filter matches on all MAC addresses.

The `<dest-mac> <mask>` | `any` parameter specifies the destination MAC address. The syntax rules are the same as those for the `<src-mac> <mask>` | `any` parameter.

Use the `etype` | `llc` | `snap` argument if you want to filter on information beyond the source and destination address. The MAC filter allows you for to filter on the following encapsulation types:

- `etype` (EtherType) – a two byte field indicating the protocol type of the frame. This can range from 0x0600 to 0xFFFF.
- `llc` (IEEE 802.3 LLC1 SSAP and DSAP) – a two byte sequence providing similar function as the EtherType but for an IEEE 802.3 frame.
- `snap` (IEEE 802.3 LLC1 SNAP) – a specific LLC1 type packet.

To determine which type of frame is used on your network, use a protocol analyzer. If byte 12 of an Ethernet packet is equal to or greater than 0600 (hex), it is an Ethernet framed packet. Any number below this indicates an IEEE 802.3 frame (byte 12 will now indicate the length of the data field). Some well-known Ethernet types are 0800 (TCP/IP), 0600 (XNS), and 8137 (Novell Netware). Refer to RFC 1042 for a complete listing of EtherTypes.
For IEEE 802.3 frame, you can further distinguish the SSAP and DSAP of LLC header. Some well-known SAPs include: FE (OSI), F0 (NetBIOS), 42 (Spanning Tree BPDU), and AA (SNAP). Usually the DSAP and SSAP are the same.

**NOTE:** You must type in both bytes, otherwise the software will fill the field, left justified with a 00. Refer to RFC 1042 for a complete listing of SAP numbers.

SNAP is defined as an IEEE 802.3 frame with the SSAP, DSAP, and control field set to AA, AA, and 03. Immediately following these is a five-byte SNAP header. The first three bytes in this header are not used by the MAC filters. However, the next two bytes usually are set to the EtherType, so you can define the EtherType inside the SNAP header that you want to filter on.

The `eq`, `gt`, `lt`, `neq` argument specifies the possible operator: `eq` (equal), `gt` (greater than), `lt` (less than) and `neq` (not equal).

The `<frame-type>` argument is a hexadecimal number for the frame type. For example, the hex number for ARP is 806.

**Default value:** N/A

**Additional Examples of Layer 2 MAC Filter Definitions**

ProCurveRS(config)# mac filter 1 permit any any etype eq 0800
This filter configures the device to permit (forward) any inbound packet with the Ethertype field set to 0800 (IP).

ProCurveRS(config)# mac filter 2 deny 0080.0020.0000 ffff.ffff.0000 any etype eq 0800
This filter configures the device to deny an inbound packet with the first four bytes set to 0800.0020.xxxx and an EtherType field set to 0800 (IP). The destination field does not matter.

ProCurveRS(config)# mac filter 3 deny any 00e0.5200.1234 ffff.ffff.ffff snap eq 0800
This filter configures the device to deny any inbound IEEE 802.3 packet with a destination set to 00e0.5200.1234 and a SNAP EtherType set to 0800. The source address does not matter.

ProCurveRS(config)# mac filter 32 permit any any
This filter permits all packets. This filter is used as the last filter assigned in a filter-group that has previous deny filters in the group.

**Abbreviating the Address or Mask**

Address and Mask abbreviations are allowed. However, be careful when configuring them. The default fill character is a 0 and it will fill a byte range as left-justified. This applies only to the MAC address and mask. A range of frame types cannot be filtered. Each frame type must be entered. Here are some examples.

ProCurveRS(config)# mac filter 1 deny 0800.0700 ffff.ff00 any
This command expands to the following: **mac filter 1 deny 0800.0700.0000 ffff.ff00.0000**

The filter shown above denied forwarding of an inbound frame that has the source address set to 080007 as the first three bytes. All other information is not significant.

Here is another example of the fill feature.

ProCurveRS(config)# mac filter 2 deny 0260.8C00.0102 0.0.ffff any
This command expands to the following: **mac filter 1 deny 0260.8C00.0102 0000.0000.ffff any**

Since the fill character is 0’s and the fill is left justified, certain filters will not allow for abbreviations. For example, suppose you want to deny an inbound packet that contained a broadcast destination address. Enter the following command:

ProCurveRS(config)# mac filter 5 deny any ff ff
This command contains a destination of address all F’s and mask of F’s. The command expands to the following:

ProCurveRS(config)# mac filter 1 deny any 00ff.0000.0000 00ff.0000.0000
Here is another example for DSAP and SSAP:

ProCurveRS(config)# mac filter 10 deny any any llc eq F0

This command expands to the following: `mac filter 2 deny any any llc eq 00f0`

If you want to filter on both the SSAP and DSAP, then the following example shows this:

ProCurveRS(config)# mac filter 4 deny any 0020.0010.1000 ffff.ffff.0000 llc eq e0e0

**mac filter log-enable**

Enables logging of packets that are denied by Layer 2 MAC filters. When you enable this feature, the device generates Syslog entries and SNMP traps for denied packets.

See “show logging” on page 40-135 for information about log entries generated by this feature.

**EXAMPLE:**

ProCurveRS(config)# mac filter log-enable

**Syntax:** mac filter log-enable

**Possible values:** N/A

**Default value:** Disabled

**mcast-hw-replic-disable**

Disables hardware multicast forwarding for tagged ports.

**NOTE:** This command applies to Layer 3 multicast traffic on EP Routing Switches only. All Layer 2 multicast traffic on EP or Standard devices is forwarded by the CPU.

**EXAMPLE:**

ProCurveRS(config)# mcast-hw-replic-disable
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload

**Syntax:** [no] mcast-hw-replic-disable

**NOTE:** You must save the configuration change and reload the software to place the change into effect.

**Possible values:** N/A

**Default value:** Enabled on EP Layer 3 devices. Disabled on all other devices.

**mcast-hw-replic-oar**

Enables hardware forwarding of multicast traffic in one-armed-router configurations.

**NOTE:** This command applies to Layer 3 multicast traffic on EP Routing Switches only. All Layer 2 multicast traffic on EP or Standard devices is forwarded by the CPU. This command is supported in software release 07.6.01b and later.

By default, EP devices running software releases later than 07.6.01b forward multicast traffic destined to multiple VLANs on tagged ports, without the need to send the traffic to the CPU for forwarding. However, this default behavior does not apply to one-armed-router configurations, in which traffic received on a port is destined to another VLAN on the same port.

For example, assume that ports 1/1 and 1/2 are members of two port-based VLANs (10 and 20), and each VLAN has a virtual routing interface. If port 1/1 receives multicast traffic from VLAN 10 and needs to forward the traffic to the virtual routing interface on VLAN 20, the device forwards the traffic to port 1/2 in hardware but uses the CPU to process the same traffic for forwarding back onto port 1/1.
You can enable the device to forward multicast traffic in hardware even in one-armed-router configurations. When you enable this support, the devices still forward multicast traffic between ports in hardware.

**NOTE:** You cannot use sFlow or port monitoring and hardware forwarding of multicast traffic in one-armed-router configurations on the same device. If you plan to enable hardware forwarding of multicast traffic in one-armed-router configurations, you must first make sure that sFlow and port monitoring are disabled on all ports. If either of these features is enabled when you enable multicast traffic in one-armed-router configurations, you may get unexpected results.

**EXAMPLE:**

```
ProCurveRS(config)# mcast-hw-repl-oar
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] mcast-hw-repl-oar`

**NOTE:** You must save the configuration change and reload the software to place the change into effect.

**NOTE:** For hardware forwarding of multicast traffic in one-armed-router configurations to take effect, hardware forwarding of multicast traffic on tagged ports must be enabled. If you disable hardware forwarding of multicast traffic on tagged ports (by entering the `mcast-hw-repl-disable` command), the `mcast-hw-repl-oar` command does not take effect.

**Possible values:** N/A

**Default value:** Disabled

**mirror-port**

Enables and assigns a specific port to operate as a mirror port for other ports. After you enable the feature, you can connect an external traffic analyzer to the port for traffic analysis.

Use the following considerations when configuring mirroring for inbound traffic on a Chassis device. The guidelines are applicable whether you configure multiple mirror ports or just one mirror port.

- **Chassis device**
  - Configure only one mirror port to monitor input traffic on a given module. If you configure multiple mirror ports on the same module, the inbound traffic for all the monitored ports on the module is sent to all the mirror ports on the same module. For example, if you configure ports 1/1 and 1/13 as mirror ports, then enable monitoring of inbound traffic on ports 1/2 and 1/14, the traffic from both ports is mirrored to both the mirror ports, 1/1 and 1/13. This occurs regardless of the mirror ports you assign to the monitor ports.
  - When inbound traffic on a monitored port on one module is switched normally to another module, the switched traffic will be mirrored to the mirror ports on the other module. For example, if inbound traffic on a monitored port on the module in slot 1 is switched to the module in slot 2, mirror ports on the module in slot 2 will receive copies of the traffic. These guidelines do not apply to outbound traffic.

These guidelines do not apply to outbound traffic.

**EXAMPLE:**

To assign port 1 on module 1 as the mirror port and port 5 on the same module as the port to be monitored, enter the following:

```
ProCurveRS(config)# mirror-port ethernet 1/1
ProCurveRS(config)# interface ethernet 1/5
ProCurveRS(config-if-1/5)# monitor both
```

**Syntax:** `[no] mirror-port ethernet <portnum> [input | output]`

The `<portnum>` parameter specifies the port. You can configure up to 64 mirror ports.

**Possible values:** See above
Default value: Not configured

**module**

Adds a hardware module.

**EXAMPLE:**

To add an 8-port Gigabit Ethernet management module to slot 3 in an 9308M, enter the following command:

```
ProCurveRS(config)# module 3 bi-8-port-gig-management-module
```

**Syntax:** module <slot-num> <module-type>

The <slot-num> parameter indicates the chassis slot number.
- Slots on a 4-slot chassis are numbered 1 – 4, from top to bottom.
- Slots on an 8-slot chassis are numbered 1 – 8, from left to right.
- Slots on a 15-slot chassis are numbered 1 – 15, from left to right.

The <module-type> parameter specifies the module. For a list of the valid module types, enter `module <slot-num> ?` at the CLI prompt.

**Possible values:** see above

**Default value:** N/A

**multicast filter**

Configures a Layer 2 filter for multicast packets. You can filter on all multicast packets or on specific multicast groups.

**EXAMPLE:**

To configure a Layer 2 multicast filter to filter all multicast groups, then apply the filter to ports 2/4, 2/5, and 2/8, enter the following commands:

```
ProCurveRS(config)# multicast filter 1 any
ProCurveRS(config-mcast-filter-id-1)# exclude-ports ethernet 2/4 to 2/5 ethernet 2/8
ProCurveRS(config-mcast-filter-id-1)# write memory
```

**EXAMPLE:**

To configure a multicast filter to block all multicast traffic destined for multicast addresses 0100.5e00.5200 – 0100.5e00.52ff on port 4/8, enter the following commands:

```
ProCurveRS(config)# multicast filter 2 any 0100.5e00.5200 ffff.ffff.ff00
ProCurveRS(config-mcast-filter-id-2)# exclude-ports ethernet 4/8
ProCurveRS(config-mcast-filter-id-2)# write memory
```

The software calculates the range by combining the mask with the multicast address. In this example, all but the last two bits in the mask are “significant bits” (ones). The last two bits are zeros and thus match on any value.

**Syntax:** [no] multicast filter <filter-ID> any | ip udp mac <multicast-address> | any [mask <mask>] [vlan <vlan-id>]

The parameter values are the same as for the **broadcast filter** command (see “broadcast filter” on page 6-24). In addition, the **multicast filter** command requires the `mac <multicast-address>` | any parameter, which specifies the multicast address. Enter `mac any` to filter on all multicast addresses. Enter `mac` followed by a specific multicast address to filter only on that multicast address.

To filter on a range of multicast addresses, use the `mask <mask>` parameter. For example, to filter on multicast groups 0100.5e00.5200 – 0100.5e00.52ff, use mask `fff.ffff.ff00`. The default mask matches all bits (is all Fs). You can leave the mask off if you want the filter to match on all bits in the multicast address.

**Possible values:** see above

**Default value:** N/A
multicast limit

Specifies the maximum number of multicast packets the device can forward each second. By default the device sends multicasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited multicast traffic, this command allows you to relieve those devices by throttling the multicasts at the HP device.

NOTE: The multicast limit does not affect broadcast or unicast traffic. However, you can use the broadcast limit and unknown-unicast limit commands to control these types of traffic. See “broadcast limit” on page 6-25 and “unknown-unicast limit” on page 6-164.

EXAMPLE:
ProCurveRS(config)# multicast limit 30000

Syntax: multicast limit <num>

Possible values: 0 – 4294967295; if you specify 0, limiting is disabled.

Default value: N/A

no

Disables other commands. To disable a command, place the word no before the command.

packet-logging

Enables or disables logging of packets transmitted, received, or both transmitted and received by a management or interface module in the ProCurve 9408sl chassis.

EXAMPLE:
To enable packet logging of packets transmitted and received by the interface module:
ProCurveRS(config)# packet-logging 1 start 0

Syntax: packet-logging <slot-number> start <packet-direction> | stop

<slot-number> you can specify 1 – 10. 1 – 8 indicate interface modules: 1 indicates the interface module installed in the leftmost chassis slot, while 8 indicates the module installed in the rightmost chassis slot. 9 – 10 indicate management modules: 9 indicates the module installed in the top slot, while 10 indicates the module installed in the bottom slot.

start - enables packet logging and writes the log to the system’s memory. If you enable packet logging, you can display the packet log using the show packet-logging command.

You must also specify the direction of packets that you want logged by entering one of the following for the <packet-direction> parameter:

• 0 – Logs packets transmitted and received by the specified module.
• 1 – Logs packets received by the specified module.
• 2 – Logs packets transmitted by the specified module.

stop - Stops packet logging.

Possible values: As described above.

Default value: Default state is packet-logging disabled.

packet-logging flash

Copies the the packet log in the system's memory to the management module's flash memory.

EXAMPLE:
To copy a log of packets transmitted and received by the interface module installed in chassis slot 1 to the management module’s flash memory:
ProCurveRS(config)# packet-logging 1 flash 0
**Syntax:** packet-logging <slot-number> flash <packet-direction>

<slot-number> you can specify 1 – 10. 1 – 8 indicate interface modules: 1 indicates the interface module installed in the leftmost chassis slot, while 8 indicates the module installed in the rightmost chassis slot. 9 – 10 indicate management modules: 9 indicates the module installed in the top slot, while 10 indicates the module installed in the bottom slot.

You must also specify the direction of packets that you want logged by entering one of the following for the <packet-direction> parameter:

- 0 – Logs packets transmitted and received by the specified module.
- 1 – Logs packets received by the specified module.
- 2 – Logs packets transmitted by the specified module.

**Possible values:** As described above.

**Default value:** Default state is for packets not to be copied to flash.

### password-change

Allows you to define those access points from which the system password can be defined. Options are cli, console-cli, telnet-cli, or any. The any option allows the password to be modified from a serial port or Telnet session at any level of the user interface.

**EXAMPLE:**

To allow password changes from a serial port console connection only, enter the following command:

```
ProCurveRS(config)# password-change console-cli
```

**Syntax:** password-change cli | console-cli | telnet-cli | any

**Possible values:** cli, console-cli, telnet-cli, or any

**Default value:** None

### perf-mode

Allows you to define the performance mode as 'high' to allow flow control to activate at an earlier stage, when heavy congestion exists on the network. This feature must be saved to memory and the system reset before it becomes active.

**EXAMPLE:**

```
ProCurveRS(config)# perf-mode hi
```

**Syntax:** perf-mode normal | hi

**Possible values:** normal | hi

**Default value:** normal

### ping

Verifies connectivity to other device. The command performs an ICMP echo test to confirm connectivity to the specified device.

**NOTE:** If you address the ping to the IP broadcast address, the device lists the first four responses to the ping.

**EXAMPLE:**

```
ProCurveRS(config)# ping 192.22.2.33
```

**Syntax:** ping <ip addr> | <hostname> [source <ip addr>] [count <num>] [timeout <msec>] [ttl <num>] [size <byte>] [quiet] [numeric] [no-fragment] [verify] [data <1-to-4 byte hex>] [brief]

The only required parameter is the IP address or host name of the device.
NOTE: If the device is a ProCurve Routing Switch, you can use the host name only if you have already enabled the Domain Name Server (DNS) resolver feature on the device from which you are sending the ping. See the “Configuring IP” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The **source** `<ip addr>` specifies an IP address to be used as the origin of the ping packets.

The **count** `<num>` parameter specifies how many ping packets the device sends. You can specify from `1 – 4294967296`. The default is `1`.

The **timeout** `<msec>` parameter specifies how many milliseconds the HP device waits for a reply from the pinged device. You can specify a timeout from `1 – 4294967296` milliseconds. The default is `5000` (5 seconds).

The **ttl** `<num>` parameter specifies the maximum number of hops. You can specify a TTL from `1 – 255`. The default is `64`.

The **size** `<byte>` parameter specifies the size of the ICMP data portion of the packet. This is the payload and does not include the header. You can specify from `0 – 4000`. The default is `16`.

The **no-fragment** parameter turns on the “don’t fragment” bit in the IP header of the ping packet. This option is disabled by default.

The **quiet** parameter hides informational messages such as a summary of the ping parameters sent to the device and instead only displays messages indicating the success or failure of the ping. This option is disabled by default.

The **verify** parameter verifies that the data in the echo packet (the reply packet) is the same as the data in the echo request (the ping). By default the device does not verify the data.

The **data** `<1 – 4 byte hex>` parameter lets you specify a specific data pattern for the payload instead of the default data pattern, “abcd”, in the packet’s data payload. The pattern repeats itself throughout the ICMP message (payload) portion of the packet.

NOTE: For numeric parameter values, the CLI does not check that the value you enter is within the allowed range. Instead, if you do exceed the range for a numeric value, the software rounds the value to the nearest valid value.

The **brief** parameter causes ping test characters to be displayed. The following ping test characters are supported:

- ! Indicates that a reply was received.
- . Indicates that the network server timed out while waiting for a reply.
- U Indicates that a destination unreachable error PDU was received.
- I Indicates that the user interrupted ping.

**Possible values:** see above

**Default value:** see above

**port aps | bootp**

Closes UDP port 67 or 1972.

The software on an HP device leaves some UDP ports open by default, even when they are not in use. To enhance security, you can close the following UDP ports:

- BootP server – well known port 67

**NOTE:** Closing one of these ports will prevent the device from receiving messages for the application associated with the closed port. For example, closing the BootP server port will prevent clients from being able to use BootP to boot over the network, if they use the HP device to reach the BootP server.
EXAMPLE:
To close a UDP port, enter a command such as the following at the global CONFIG level of the CLI:

ProCurveRS(config)# no port aps
This command closes the APS port.
To re-open a UDP port, enter a command such as the following:

ProCurveRS(config)# port aps

**Syntax:** [no] port aps | bootp
The *aps | bootp* parameter indicates the UDP port you are closing or re-opening.

**Possible values:** aps or bootp
**Default value:** both UDP ports are open

**port security**
Enables the MAC port security feature globally on all interfaces

**EXAMPLE:**

**Syntax:** ProCurveRS(config-port-security)#[no] port security

**Possible values:** N/A
**Default value:** Disabled

**port-priority**
Enables ToS-based QoS on an EP device. For information about this feature, see the "EP Type of Service (ToS) Based QoS" chapter in the *Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches*.

**NOTE:** This command is supported in release 07.6.01b and later and applies only to EP devices.

**EXAMPLE:**

**Syntax:** [no] port-priority
This command enables the feature on all interfaces.

**Possible values:** N/A
**Default value:** Disabled

**privilege**
Augments the default access privileges for an access level. When you configure a user account, you can give the account one of three privilege levels: full access, port-configuration access, and read-only access. Each privilege level provides access to specific areas of the CLI by default:

- Full access provides access to all commands and displays.
- Port-configuration access gives access to:
  - The User EXEC and Privileged EXEC levels, and the port-specific parts of the CONFIG level
  - All interface configuration levels
- Read-only access gives access to:
  - The User EXEC and Privileged EXEC levels

**EXAMPLE:**
To enhance the port-configuration privilege level so users also can enter ip commands at the global CONFIG level (useful for adding IP addresses for multinetting), enter the following command:

ProCurveRS(config)# privilege configure level 4 ip
In this command, configure specifies that the enhanced access is for a command at the global CONFIG level of the CLI. The level 4 parameter indicates that the enhanced access is for privilege level 4 (port-configuration). All users with port-configuration privileges will have the enhanced access. The ip parameter indicates that the enhanced access is for the IP commands. Users who log in with valid port-configuration level user names and passwords can enter commands that begin with “ip” at the global CONFIG level.

**Syntax:** [no] privilege <cli-level> level <privilege-level> <command-string>

The <cli-level> parameter specifies the CLI level and can be one of the following values:

- **exec** – EXEC level; for example, ProCurveRS> or ProCurveRS#
- **configure** – CONFIG level; for example, ProCurveRS(config)#
- **interface** – interface level; for example, ProCurveRS(config-if-6)#
- **virtual-interface** – virtual-interface level; for example, ProCurveRS(config-vif-6)#
- **rip-router** – RIP router level; for example, ProCurveRS(config-rip-router)#
- **ospf-router** – OSPF router level; for example, ProCurveRS(config-ospf-router)#
- **dvmrp-router** – DVMRP router level; for example, ProCurveRS(config-dvmrp-router)#
- **pim-router** – PIM router level; for example, ProCurveRS(config-pim-router)#
- **bgp-router** – BGP4 router level; for example, ProCurveRS(config-bgp-router)#
- **port-vlan** – Port-based VLAN level; for example, ProCurveRS(config-vlan)#
- **protocol-vlan** – Protocol-based VLAN level

The <privilege-level> indicates the privilege level you are augmenting.

The level parameter specifies the privilege-level. You can specify one of the following:

- 0 – Full access (super-user)
- 4 – Port-configuration access
- 5 – Read-only access

The <command-string> parameter specifies the command you are allowing users with the specified privilege level to enter. To display a list of the commands at a CLI level, enter ”?” at that level’s command prompt and press Return.

**pvlan-preference**

Allows or restricts forwarding of broadcast or unknown unicast packets by a primary private VLAN to its community and isolated VLANs.

This forwarding restriction does not apply to traffic from the private VLAN. The primary port does forward broadcast and unknown unicast packets that are received from the isolated and community VLANs.

If you want to remove the forwarding restriction, you can enable the primary port to forward broadcast or unknown unicast traffic, if desired, using the following CLI method. You can enable or disable forwarding of broadcast or unknown unicast packets separately.

**NOTE:** You also can use MAC address filters to control the traffic forwarded into and out of the private VLAN.

**EXAMPLE:**

To configure the ports in the primary VLAN to forward broadcast or unknown unicast traffic received from sources outside the private VLAN, enter the following commands at the global CONFIG level of the CLI:

ProCurveRS(config)# pvlan-preference broadcast flood
ProCurveRS(config)# pvlan-preference unknown-unicast flood

These commands enable forwarding of broadcast and unknown-unicast packets to ports within the private VLAN. To again disable forwarding, enter a command such as the following:
ProCurveRS(config)# no pvlan-preference broadcast flood
This command disables forwarding of broadcast packets within the private VLAN.

Syntax: [no] pvlan-preference broadcast | unknown-unicast flood
Possible values: See above
Default value: Forwarding is disabled

qd-flow sink
Specifies the threshold values for flow control.

NOTE: To use this enhancement, 802.3x flow control must be enabled globally on the device. By default, 802.3x flow control is enabled on HP devices, but can be disabled with the no flow-control command.

EXAMPLE:
ProCurveRS(config)# qd-flow sink 75 sunk 50 slot 4 1 1 0 0

Syntax: qd-flow sink <sinking-threshold> sunk <sunk-threshold> slot <slot> <flag> <flag> <flag> <flag>
Possible values:
When the <sinking-threshold> is reached, the HP device sends out 802.3x PAUSE frames telling the sender to stop sending traffic for a period of time.
When the <sunk-threshold> is reached, the HP device drops traffic at the specified priority level.
The <slot> parameter specifies the location of the module where the thresholds are to take effect.
The <flag> parameters indicate whether to drop traffic at each priority if the number of available buffers falls below the <sunk-threshold>. Each <flag> parameter represents a priority level: 0, 1, 2, 3. To drop traffic at a priority level, set its <flag> parameter to 1. For example, to drop traffic at priority 0 and 1, enter 1 1 0 0 for the <flag> parameters. By default, the lowest priority traffic is dropped.
Default value: N/A

qos mechanism
Configures the queuing method used for QoS. Two queuing methods are available:

- Weighted (the default) – A weighted fair queuing algorithm is used to rotate service among the four queues. The rotation is based on the weights you assign to each queue. This is the default queuing method and uses a default set of queue weights. This method rotates service among the four queues, forwarding a specific number of packets in one queue before moving on to the next one.

  The number of packets serviced during each visit to a queue depends on the percentages you configure for the queues. The software automatically converts the percentages you specify into weights for the queues.

- Strict – The software assigns the maximum weights to each queue, to cause the queuing mechanism to serve as many packets in one queue as possible before moving to a lower queue. This method biases the queuing mechanism to favor the higher queues over the lower queues. For example, strict queuing processes as many packets as possible in qosp3 before processing any packets in qosp2, then processes as many packets as possible in qosp2 before processing any packets in qosp1, and so on.

EXAMPLE:
To change the queuing method from weighted fair queuing to strict queuing:

ProCurveRS(config)# qos mechanism strict

Syntax: [no] qos mechanism strict | weighted
Possible values: See above
Default value: weighted
**qos name**

Changes the QoS queue names from their defaults. The default queue names are qosp3, qosp2, qosp1, and qosp0.

**EXAMPLE:**

To rename queue qosp3 (the premium queue) to “92-octane”:

```
ProCurveRS(config)# qos name qosp3 92-octane
ProCurveRS(config)# write memory
```

**Syntax:** `qos name <old-name> <new-name>`

**Possible values:** The `<old-name>` parameter specifies the name of the queue before the change.

The `<new-name>` parameter specifies the new name of the queue. You can specify an alphanumeric string up to 32 characters long.

**qos profile**

Changes the minimum guaranteed bandwidth percentages of the queues. If you change the percentages for the queues, the software changes the weights, which changes the number of visits a queue receives during a full queue cycle and also the number of packets sent from each queue during each visit. For example, if you change the percentages so that queue qosp3 receives a weight of 5, then the system processes five packets in that queue during each visit to the queue.

**NOTE:** The weighted fair queuing method is based on packet-level scheduling. As a result, a queue’s bandwidth percentage does not necessarily reflect the exact bandwidth share the queue receives. This is due to the effects of variable size packets.

**EXAMPLE:**

To change the minimum guaranteed bandwidth percentages of the queues on a device that supports four queues:

```
ProCurveRS(config)# qos profile qosp3 75 qosp2 10 qosp1 10 qosp0 5
Profile qosp3     : PREMIUM     bandwidth requested 75% calculated 75%
Profile qosp2     : HIGH        bandwidth requested 10% calculated 13%
Profile qosp1     : NORMAL      bandwidth requested 10% calculated 8%
Profile qosp0     : BEST-EFFORT bandwidth requested 5% calculated 4%
ProCurveRS(config)# write memory
```

The following syntax applies to HP devices that support four queues:

**Syntax:** `[no] qos profile <queue> <percentage> <queue> <percentage> <queue> <percentage> <queue> <percentage>`

The following syntax applies to HP devices that support eight queues:

**Syntax:** `[no] qos profile <queue> <percentage> <queue> <percentage> <queue> <percentage> <queue> <percentage> <queue> <percentage> <queue> <percentage>`

Each `<queue>` parameter specifies the name of a queue. You can specify the queues in any order on the command line, but you must specify each queue.

The `<percentage>` parameter specifies a number for the percentage of the device’s outbound bandwidth that is allocated to the queue. Note the following:

- The total of the percentages you enter must equal 100.
- On devices that have four queues, the percentage for the premium queue (the highest priority queue) must be at least 50.
- On devices that have four queues, if you enter percentages that are less than the minimum percentages supported for a queue, the CLI recalculates the percentages to fall within the supported minimums.
**Possible values:** See above.

**Default value:**

The following table lists the default minimum guaranteed bandwidth percentages of the queues on devices that support four queues:

<table>
<thead>
<tr>
<th>Queue</th>
<th>Default Minimum Percentage of Bandwidth</th>
</tr>
</thead>
<tbody>
<tr>
<td>qos0</td>
<td>80%</td>
</tr>
<tr>
<td>qos1</td>
<td>15%</td>
</tr>
<tr>
<td>qos2</td>
<td>3.3%</td>
</tr>
<tr>
<td>qos3</td>
<td>1.7%</td>
</tr>
</tbody>
</table>

**qos tagged-priority**

Allows you to reassign 802.1p priorities to different QoS queues. Tagged priority applies to tagged packets that come in from tagged ports. These packets have a tag in the header that specifies the packet's VLAN ID and its 802.1p priority tag value, which is 3 bits long.

You can specify how the HP device interprets the 3-bit priority information by reassigning the priority levels to other queues. For example, if you want the device to disregard the 802.1p priority and instead assign the priority based on other items (VLAN, port, and so on), you can configure the device to set all the 802.1p priorities to the best-effort queue (qos0). If a tagged packet's 802.1p priority level is always in the qos0 queue, then the packet's outbound queue is affected by other items such as incoming port, VLAN, and so on.

**EXAMPLE:**

To reassign all 802.1p priority levels 2 – 7 to the best-effort queue (qos0), enter the following commands:

```
ProCurveRS(config)# qos tagged-priority 2 qos0
ProCurveRS(config)# qos tagged-priority 3 qos0
ProCurveRS(config)# qos tagged-priority 4 qos0
ProCurveRS(config)# qos tagged-priority 5 qos0
ProCurveRS(config)# qos tagged-priority 6 qos0
ProCurveRS(config)# qos tagged-priority 7 qos0
ProCurveRS(config)# write memory
```

**Syntax:** `[no] qos tagged-priority <num> <queue>

The `<num>` parameter can be from 0 – 7 and specifies the IEEE 802.1 equivalent to one of the four QoS queues.

The `<queue>` parameter specifies the queue to which you are reassigning the priority level. You must specify one of the named queues. The default names are qos0, qos1, qos2, and qos3. The example above reassigns the 802.1p levels to queue qos0. (There is no need to reassign levels 0 and 1 in this case, because they are already assigned to qos0 by default.)

**Possible values:** See above.

**Default value:** By default, an HP device interprets the prioritization information in the 3-bit priority tag as follows:

<table>
<thead>
<tr>
<th>Priority Level</th>
<th>Queue</th>
</tr>
</thead>
<tbody>
<tr>
<td>6, 7</td>
<td>qos0</td>
</tr>
<tr>
<td>4, 5</td>
<td>qos1</td>
</tr>
<tr>
<td>2, 3</td>
<td>qos2</td>
</tr>
<tr>
<td>Priority Level</td>
<td>Queue</td>
</tr>
<tr>
<td>---------------</td>
<td>-------</td>
</tr>
<tr>
<td>0, 1</td>
<td>qos0</td>
</tr>
</tbody>
</table>

**qos-tos map cos-dscp**

**NOTE:** DiffServ Control Point (DSCP)EP are used if the trust level is CoS and DSCP marking is enabled. This command is supported in release 07.6.01b and later and applies only to EP devices.

**NOTE:** ToS-based QoS must be enabled. See “port-priority” on page 6-119.

**NOTE:** To place a mapping change into effect, you must enter the `ip rebind-acl all` command at the global CONFIG level of the CLI after making the mapping change.

**EXAMPLE:**

**COS-DSCP map:**

```
COS:  0 1 2 3 4 5 6 7
     ----------------------------------------
dscp:  
```

**Possible values:** See above

**Default value:**

**qos-tos map dscp-dscp**

**NOTE:** This command is supported in release 07.6.01b and later and applies only to EP devices.

**NOTE:** ToS-based QoS must be enabled. See “port-priority” on page 6-119.

**NOTE:** To place a mapping change into effect, you must enter the `ip rebind-acl all` command at the global CONFIG level of the CLI after making the mapping change.

This command changes the mapping of DSCP value 0 from 0 to 10.

You can change up to eight DSCP values in the same commend. Make sure you enter the old values and their new values in the same order.

**Possible values:** See above

**Default value:** The device maps a packet's DSCP value to the same DSCP value. For example, if the packet has DSCP value 63 when the packet is received, the packet still has DSCP value 63 when the packet is placed in the hardware forwarding queue.

**qos-tos map dscp-priority**

**NOTE:** This command is supported in release 07.6.01b and later and applies only to EP devices.

**NOTE:** ToS-based QoS must be enabled. See “port-priority” on page 6-119.
NOTE: To place a mapping change into effect, you must enter the `ip rebind-acl all` command at the global CONFIG level of the CLI after making the mapping change.

**EXAMPLE:**
Possible values: See above
Default value:

**qos-tos map ip-prec-dscp**
T mappings are used if the trust level is IP Precedence and DSCP marking is enabled.

**NOTE:** This command is supported in release 07.6.01b and later and applies only to EP devices.

**NOTE:** ToS-based QoS must be enabled. See “port-priority” on page 6-119.

**NOTE:** To place a mapping change into effect, you must enter the `ip rebind-acl all` command at the global CONFIG level of the CLI after making the mapping change.

**EXAMPLE:**
EP
Possible values: See above
Default value:

**quit**
Returns you from any level of the CLI to the User EXEC mode.

**EXAMPLE:**
ProCurveRS(config)# quit
ProCurveRS>

**Syntax:** quit

**Possible values:** N/A

**Default value:** N/A

**radius-server**
Identifies a RADIUS server and sets other RADIUS authentication parameters for authenticating access to the HP device.

**EXAMPLE:**
ProCurveRS(config)# radius-server host 209.157.22.99

**Syntax:** radius-server host <ip-addr> | <server-name> [auth-port <number>] [acct-port <number>]

<ip-addr> | <server-name> is either an IP address or an ASCII text string.

<auth-port> is the Authentication port number; it is an optional parameter. The default is 1645.

<acct-port> is the Accounting port number; it is an optional parameter. The default is 1646.

**Syntax:** radius-server [key 0 | 1 <key-string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The key <key-string> parameter specifies the value that the HP device sends to the server when trying to authenticate user access. The RADIUS server uses the key to determine whether the HP device has authority to request authentication from the server. The key can be from 1 – 32 characters in length and cannot include any space characters.
**Syntax:** radius-server host `<ip-addr> | <server-name>` [auth-port `<number>` acct-port `<number>` default key `<string>` dot1x]

The **default key** `<string>` **dot1x** parameter indicates that this RADIUS server supports the 802.1X standard. A RADIUS server that supports the 802.1X standard can also be used to authenticate non-802.1X authentication requests.

**NOTE:** To implement 802.1X port security, at least one of the RADIUS servers identified to the HP device must support the 802.1X standard.

When you display the configuration of the HP device, the RADIUS key is encrypted. For example:

```
ProCurveRS(config)# radius-server key 1 abc
ProCurveRS(config)# write terminal
...
radius-server host 1.2.3.5
radius key 1 $!2d
```

**NOTE:** Encryption of the RADIUS keys is done by default. The 0 parameter disables encryption. The 1 parameter is not required; it is provided for backwards compatibility.

The timeout `<number>` is how many seconds to wait before declaring a RADIUS server timeout for the authentication request. The default timeout is 3 seconds. The range of possible timeout values is from 1 – 15.

The retransmit `<number>` is the maximum number of retransmission attempts. When an authentication request timeout, the HP software will retransmit the request up to the maximum number of retransmissions configured. The default retransmit value is 3 seconds. The possible retransmit value is from 1 – 5.

The **dead-time** parameter is not used in this software release. When the software allows multiple authentication servers, this parameter will specify how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

You can designate a server to handle a specific AAA task. For example, you can designate one RADIUS server to handle authorization and another RADIUS server to handle accounting. You can specify individual servers for authentication and accounting, but not for authorization. You can set the RADIUS key for each server.

**Syntax:** radius-server host `<ip-addr> | <server-name>` [authentication-only | accounting-only | default] [key 0 | 1 `<string>`]

The **default** parameter causes the server to be used for all AAA functions.

**Possible values:** see above

**Default value:** see above

rarp

Enters a static IP RARP entry for static routes on a ProCurve Routing Switch.

**EXAMPLE:**

```
ProCurveRS(config)# rarp 1 1245.7654.2348 192.53.4.2
ProCurveRS(config)# exit
ProCurveRS# write memory
```

**Syntax:** rarp `<number>` `<mac-addr>.<ip-addr>`

The `<number>` parameter identifies the RARP entry number. You can specify an unused number from 1 to the maximum number of RARP entries supported on the device.

The `<mac-addr>` parameter specifies the MAC address of the RARP client.

The `<ip-addr>` parameter specifies the IP address the Routing Switch will give the client in response to the client's RARP request.
**Possible values:** See above  
**Default value:** N/A

---

### rate-limit-arp

Limit the number of ARP packets the HP device accepts during each second.

By default, the software does not limit the number of ARP packets the device can receive. Since the device sends ARP packets to the CPU for processing, if a device in a busy network receives a high number of ARP packets in a short period of time, some CPU processing might be deferred while the CPU processes the ARP packets.

To prevent the CPU from becoming flooded by ARP packets in a busy network, you can restrict the number of ARP packets the device will accept each second. When you configure an ARP rate limit, the device accepts up to the maximum number of packets you specify, but drops additional ARP packets received during the one-second interval. When a new one-second interval starts, the counter restarts at zero, so the device again accepts up to the maximum number of ARP packets you specified, but drops additional packets received within the interval.

**EXAMPLE:**

To limit the number of ARP packets the device will accept each second, enter a command such as the following at the global CONFIG level of the CLI:

```
ProCurveRS(config)# rate-limit-arp 100
```

This command configures the device to accept up to 100 ARP packets each second. If the device receives more than 100 ARP packets during a one-second interval, the device drops the additional ARP packets during the remainder of that one-second interval.

**Syntax:** `[no] rate-limit-arp <num>`

The `<num>` parameter specifies the number of ARP packets and can be from 0 – 100. If you specify 0, the device will not accept any ARP packets.

**NOTE:** If you want to change a previously configured the ARP rate limiting policy, you must remove the previously configured policy using the `no rate-limit-arp <num>` command before entering the new policy.

---

### redundancy

Changes the CLI to the configuration level for redundant management modules.

---

### relative-utilization

Allows you to configure uplink utilization lists that display the percentage of a given uplink port's bandwidth that is used by a specific list of downlink ports. The percentages are based on 30-second intervals of RMON packet statistics for the ports. Both transmit and receive traffic is counted in each percentage.

**NOTE:** This feature is intended for ISP or collocation environments in which downlink ports are dedicated to various customers’ traffic and are isolated from one another. If traffic regularly passes between the downlink ports, the information displayed by the utilization lists does not provide a clear depiction of traffic exchanged by the downlink ports and the uplink port.

Each uplink utilization list consists of the following:

- Utilization list number (1, 2, 3, or 4)
- One or more uplink ports
- One or more downlink ports

Each list displays the uplink port and the percentage of that port's bandwidth that was utilized by the downlink ports over the most recent 30-second interval. You can configure up to four bandwidth utilization lists.
EXAMPLE:
To configure a link utilization list with port 1/1 as the uplink port and ports 1/2 and 1/3 as the downlink ports.

ProCurveRS(config)# relative-utilization 1 uplink eth 1/1 downlink eth 1/2 to 1/3

Syntax: [no] relative-utilization <num> uplink ethernet <portnum> [to <portnum> | <portnum>…] downlink ethernet <portnum> [to <portnum> | <portnum>…]

Possible values: The <num> parameter specifies the list number. You can configure up to four lists. Specify a number from 1 – 4.

The uplink ethernet parameters and the port number(s) you specify after the parameters indicate the uplink port(s).

The downlink ethernet parameters and the port number(s) you specify after the parameters indicate the downlink port(s).

Default value: N/A

remote-management rebind
Configures a Routing Switch to perform hardware filtering for remote access. When you make changes to the ACL configuration and/or make changes to the management VLAN, you must enter this command after making the configuration changes:

EXAMPLE:
ProCurveRS(config)# remote-management rebind

Syntax: remote-management rebind

Possible values: N/A

Default value: N/A

rmon alarm
Defines what MIB objects are monitored, the type of thresholds that will be monitored (falling, rising or both), the value of those thresholds, and the sample type (absolute or delta).

An alarm event will be reported each time that a threshold is exceeded. The alarm entry also defines the action (event) to take should the threshold be exceeded.

A sample CLI alarm entry and its syntax is shown below:

EXAMPLE:
ProCurveRS(config)# rmon alarm 1 ifInOctets.6 10 delta rising-threshold 100 1 falling threshold 50 1 owner nyc02

Syntax: rmon alarm <entry-number> <MIB-object.interface-number> <sampling-time> <sample-type> <threshold-type> <threshold-value> <event-number> <threshold-type> <threshold-value> owner <text>

Possible values:
- Threshold type: rising-threshold or falling threshold
- Sample type: delta or absolute

Default value: N/A

rmon event
There are two elements to the RMON event group 9, the event control table and the event log table.

The event control table defines the action to be taken when an alarm is reported. Defined events can be displayed by entering the CLI command show event.

The event log table collects and stores reported events for retrieval by an RMON application.
Global CONFIG Commands

EXAMPLE:
ProCurveRS(config)# rmon event 1 description 'testing a longer string' log-and-trap
public owner nyc02

Syntax: rmon event <event-entry> description <text-string> log | trap | log-and-trap owner <rmon-station>

Possible values: N/A
Default value: N/A

rmon history
All active ProCurve Routing Switch ports by default will generate two RMON history (group 2) control data entries. If a port becomes inactive, then the two entries will automatically be deleted.

Two history entries are generated for each device by default:

- a sampling of statistics every 30 seconds
- a sampling of statistics every 30 minutes

You can modify how many of these historical entries are saved in an event log (buckets) as well as how often these intervals are taken. The station (owner) that collects these entries can also be defined.

To review the control data entry for each port or interface, enter the show rmon history command.

EXAMPLE:
ProCurveRS(config)# rmon history 1 interface 1 buckets 10 interval 10 owner nyc02

Syntax: rmon history <entry-number> interface <portnum> buckets <number> interval <sampling-interval> owner
<text-string>

Possible values: Buckets: 1 – 50 entries.

Default value: N/A

route-map

Creates a route map and places you in the Route Map CONFIG level of the CLI. A route map is a named set of match conditions and parameter settings that the router can use to modify route attributes and to control redistribution of the routes into other protocols. See the "Configuring BGP4" chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

EXAMPLE:
To add instance 1 of a route map named "GET_ONE" with a permit action, enter the following command.

ProCurveRS(config)# route-map GET_ONE permit 1
ProCurveRS(config-routemap GET_ONE)#

Syntax: route-map <map-name> permit | deny <num>

As shown in this example, the command prompt changes to the Route Map level. You can enter the match and set statements at this level. See "Route Map Commands" on page 27-1. Also see the "Configuring BGP4" chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The <map-name> is a string of characters that names the map. Map names can be up to 32 characters in length.

The permit | deny parameter specifies the action the router will take if a route matches a match statement.

- If you specify deny, the Routing Switch does not advertise or learn the route.
- If you specify permit, the Routing Switch applies the match and set statements associated with this route map instance.

The <num> parameter specifies the instance of the route map you are defining. Each route map can have up to 50 instances. Routes are compared to the instances in ascending numerical order. For example, a route is compared to instance 1, then instance 2, and so on.
To delete a route map, enter a command such as the following. When you delete a route map, all the permit and deny entries in the route map are deleted.

ProCurveRS(config)# no route-map Map1

This command deletes a route map named “Map1”. All entries in the route map are deleted.

To delete a specific instance of a route map without deleting the rest of the route map, enter a command such as the following:

ProCurveRS(config)# no route-map Map1 permit 10

This command deletes the specified instance from the route map but leaves the other instances of the route map intact.

Possible values: N/A
Default value: N/A

route-only

Globally disables Layer 2 switching on a ProCurve Routing Switch.

**NOTE:** Make sure you really want to disable all Layer 2 switching operations before you use this option. Consult your reseller or Hewlett-Packard for information.

**NOTE:** As an alternative to disabling switching globally, you can disable it on individual interfaces. See “route-only” on page 8-73.

**EXAMPLE:**

```bash
ProCurveRS(config)# route-only
ProCurveRS(config)# exit
ProCurveRS# write memory
ProCurveRS# reload
```

**Syntax:** [no] route-only

Possible values: N/A
Default value: Enabled

router appletalk

This is a launch command that allows you to move to the AppleTalk configuration level.

**EXAMPLE:**

```bash
ProCurveRS(config)# router appletalk
ProCurveRS(config-atalk-router)# end
ProCurveRS# write memory
ProCurveRS# reload
```

**NOTE:** You must reset the system when AppleTalk is first enabled on the router using the `router appletalk` command. If you have previously reset the system and defined AppleTalk interface(s), and the interface configuration represents an addition, then no reset of the system is required.

**Syntax:** router appletalk

Possible values: N/A
Default value: disabled

router bgp

This is a launch command that allows you to move to the BGP configuration level.
NOTE: If you disable BGP4 by entering the **no router bgp** command, all BGP4 configuration information is deleted. To disable BGP4 without losing the configuration information, use the **no local-as** command to disable the local AS instead. See "local-as" on page 17-9.

**EXAMPLE:**

ProCurveRS(config)# router bgp
ProCurveRS(config-bgp-router)#

**Syntax:** [no] router bgp
**Possible values:** N/A
**Default value:** disabled

**router dvmrp**

This is a launch command that allows you to move to the DVMRP configuration level.

In releases prior to software release 07.8.00, the behavior of the **[no] router dvmrp** command was as follows:

- ProCurve Routing Switches required a software reload whenever you enabled DVMRP using the **router dvmrp** command.
- Entering a **no router dvmrp** command removed all configuration for PIM multicast on a Routing Switch (**router pim** level) and all PIM and PIM-Sparse (**ip pim** and **ip pim-sparse**) configuration on all interfaces.

Beginning with software release 07.8.00:

- Entering **router dvmrp** command to enable DVMRP does not require a software reload.
- Entering a **no router dvmrp** command removes all configuration for PIM multicast on a Routing Switch (**router pim** level) only.

**EXAMPLE:**

ProCurveRS(config)# router dvmrp
ProCurveRS(config-dvmrp-router)# write memory
ProCurveRS(config-dvmrp-router)# end
ProCurveRS# reload

**Syntax:** router dvmrp
**Possible values:** N/A
**Default value:** disabled

**router ipx**

Activates IPX routing on a Routing Switch.

**NOTE:** You must reload the software after enabling this protocol to place the change into effect.

**EXAMPLE:**

ProCurveRS(config)# router ipx
ProCurveRS(config-ipx-router)# write memory
ProCurveRS(config-ipx-router)# end
ProCurveRS# reload

**Syntax:** router ipx
**Possible values:** N/A
**Default value:** disabled
**router msdp**
Activates Multicast Source Discovery Protocol (MSDP) on a Routing Switch and places the CLI at the MSDP configuration level.

**NOTE:** You must reload the software after enabling this protocol to place the change into effect.

Also, router that run MSDP must also run BGP. The source address used by the MSDP router must be the same source address used by BGP.

**EXAMPLE:**
ProCurveRS(config)# router msdp
ProCurveRS(config-msdp-router)# write memory
ProCurveRS(config-msdp-router)# end
ProCurveRS# reload

**Syntax:** router msdp
**Possible values:** N/A
**Default value:** disabled

**router ospf**
Activates OSPF routing on a ProCurve Routing Switch and launches you into the OSPF configuration level.

**EXAMPLE:**
ProCurveRS(config)# router ospf
ProCurveRS(config-ospf-router)#

**Syntax:** router ospf
**Possible values:** N/A
**Default value:** disabled

**router pim**
Activates PIM multicast on a Routing Switch.

In releases prior to software release 07.8.00, the behavior of the [no] router pim command was as follows:

- **ProCurve Routing Switches required a software reload whenever you enabled PIM using the router pim command.**
- **Entering a no router pim command removed all configuration for PIM multicast on a Routing Switch (router pim level) and all PIM and PIM-Sparse (ip pim and ip pim-sparse) configuration on all interfaces.**

Beginning with software release 07.8.00:

- **Entering router pim command to enable PIM does not require a software reload.**
- **Entering a no router pim command removes all configuration for PIM multicast on a Routing Switch (router pim level) only.**

Use the disable-pim command if you want to disable PIM, but want to retain PIM configuration.

**EXAMPLE:**
ProCurveRS(config)# router pim
ProCurveRS(config-pim-router)# write memory
ProCurveRS(config-pim-router)# end
ProCurveRS# reload

**Syntax:** router pim
Possible values: N/A
Default value: disabled

router rip
Activates RIP routing on a Routing Switch and launches you into that configuration level to assign or modify RIP parameters.

NOTE: You must enable the protocol globally and also on individual interfaces. Globally enabling the protocol does not enable it on individual interfaces. To enable RIP on an interface, see “ip rip” on page 8-30.

EXAMPLE:
ProCurveRS(config)# router rip
ProCurveRS(config-rip-router)# write memory
ProCurveRS(config-rip-router)# end
ProCurveRS# reload

Syntax: router rip

Possible values: N/A
Default value: disabled

router vrrp
Enables VRRP.

EXAMPLE:
ProCurveRS(config)# router vrrp

Syntax: router vrrp

Possible values: N/A
Default value: disabled

router vrrp-extended
Enables VRRP Extended (VRRPE).

EXAMPLE:
ProCurveRS(config)# router vrrp-extended

Syntax: router vrrp-extended

Possible values: N/A
Default value: disabled

router vsrp
Disables or re-enables the Virtual Switch Redundancy Protocol (VSRP) on a Routing Switch. VSRP is an alternative to STP that provides Layer 2 and Layer 3 redundancy and sub-second failover in mesh topologies.

EXAMPLE:
On a Routing Switch, if you want to use VRRP or VRRPE for Layer 3 redundancy instead of VSRP, you need to disable VSRP first. To disable VSRP:
ProCurveRS(config)# no router vsrp
To re-enable VSRP:
ProCurveRS(config)# router vsrp

Syntax: [no] router vsrp

Possible values: N/A
Default value: VSRP is enabled by default on Routing Switches.

scale-timer
Changes the timer scale.

The **timer scale** is a value used by the software to calculate the timers. By default, the scale value is 1. If you increase the timer scale, each timer’s value is divided by the scale value.

To achieve sub-second failover times, you can shorten the duration of all VSRP timers by adjusting the timer scale. Using the timer scale to adjust VSRP timer values enables you to easily change all the timers while preserving the ratios among their values. Here is an example.

<table>
<thead>
<tr>
<th>Timer</th>
<th>Timer Scale</th>
<th>Timer Value</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hello interval</td>
<td>1</td>
<td>1 second</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0.5 seconds</td>
</tr>
<tr>
<td>Dead interval</td>
<td>1</td>
<td>3 seconds</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1.5 seconds</td>
</tr>
<tr>
<td>Backup Hello interval</td>
<td>1</td>
<td>60 seconds</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>30 seconds</td>
</tr>
<tr>
<td>Hold-down interval</td>
<td>1</td>
<td>2 seconds</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>1 second</td>
</tr>
</tbody>
</table>

If you configure the device to receive its timer values from the Master, the Backup also receives the timer scale value from the Master.

**NOTE:** The Backups always use the value of the timer scale received from the Master, regardless of whether the timer values that are saved in the configuration are the values configured on the Backup or the values received from the Master.

**EXAMPLE:**
To change the timer scale, enter a command such as the following at the global CONFIG level of the CLI:

```
ProCurveRS(config)# scale-timer 2
```
This command changes the scale to 2. All VSRP timer values will be divided by 2.

**Syntax:** [no] scale-timer <num>
The <num> parameter specifies the multiplier. You can specify a timer scale from 1 – 10.

**Possible values:** 1 – 10

**Default value:** 1

server port
Adds a profile for an application TCP or UDP port. This command applies only when you are using a Routing Switch for the Globally-distributed Server Load Balancing (SLB) feature. See the "Route Health Injection" chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches. When you add a profile for an application port, the health check for the port is automatically enabled.

**EXAMPLE:**
To add a profile for TCP port 80 and thus enable its health check, enter the following commands:

```
ProCurveRS(config)# server port 80
```
server real-name

Identifies a Web server for Globally-distributed Server Load Balancing (SLB). Globally-distributed SLB allows the same web site (and same IP address) to reside on multiple servers, which usually are in geographically dispersed locations. See the "Route Health Injection" chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

Use the server real-name command to identify the web sites for which the ProCurve Routing Switch is helping to provide geographically-distributed SLB.

**EXAMPLE:**

ProCurveRS(config)# server real S2 209.157.22.249
ProCurveRS(config-rs-S2)# port http keepalive

**server session-vm-limit**

Changes the maximum number of Layer 4 sessions the individual T-Flow Switching Processor (TSPs) on the T-Flow Redundant Management Module can have.

**EXAMPLE:**

ProCurveRS(config)# server session-vm-limit 1000000

**service password-encryption**

Enables password encryption. When encryption is enabled, users cannot learn the device's passwords by viewing the configuration file. Password encryption is enabled by default.
NOTE: Password encryption does not encrypt the password in Telnet packets sent to the device. This feature applies only to the configuration file.

EXAMPLE:
ProCurveRS(config)# no service password-encryption

Syntax: [no] service password-encryption
Possible values: N/A
Default value: Enabled

sflow destination
Specifies the collector for sFlow data.

EXAMPLE:
ProCurveRS(config)# sflow destination 10.10.10.1
This command specifies a collector with IP address 10.10.10.1, listening for sFlow data on UDP port 6343.

Syntax: [no] sflow destination <ip-addr> [<dest-udp-port>]
The <ip-addr> parameter specifies the collector's IP address.
The <dest-udp-port> parameter specifies the UDP port on which the sFlow collector will be listening for exported sFlow data. The default port number is 6343.

NOTE: The default UDP port is present in release 07.5.06 and later only. Earlier releases do not have a default.
Possible values: See above
Default value: UDP port 6343. There is no default for the IP address.

sflow enable
Globally enables sFlow.

NOTE: You also must enable sFlow forwarding on individual interfaces. See "sflow forwarding" on page 8-74.

EXAMPLE:
ProCurveRS(config)# sflow enable

Syntax: [no] sflow enable
Possible values: N/A
Default value: Disabled

sflow polling-interval
Changes the sFlow polling interval.

The polling interval defines how often the MIB objects for network interface statistics are polled. The interval value applies to all interfaces on which sFlow is enabled.

EXAMPLE:
To change the interval, enter a command such as the following at the global CONFIG level of the CLI:
ProCurveRS(config)# sflow polling-interval 30

Syntax: [no] sflow polling-interval <secs>
The <secs> parameter specifies the interval and can be from 1 to any higher value. The default is 20 seconds. If you specify 0, counter data sampling is disabled.
**Possible values:** 1 to any higher value

**Default value:** 20 seconds

### sflow sample

Globally changes the average packet sampling rate for sFlow.

**NOTE:** You also can specify the sampling rate for an individual interface. See “sflow sample” on page 8-74.

**EXAMPLE:**

```
ProCurveRS(config)# sflow sample 2048
```

**Syntax:** `[no] sflow sample <num>

The `<num>` parameter specifies the average number of packets from which each sample will be taken. The software rounds the value you enter to the next higher odd power of 2. This value becomes the actual default sampling rate and is one of the following. For example, if the configured sampling rate is 1000, then the actual rate is 2048 and 1 in 2048 packets are sampled by the hardware.

- 2
- 8
- 32
- 128
- 512
- 2048
- 8192
- 32768
- 131072
- 524288
- 2097152
- 8388608
- 33554432
- 134217728
- 536870912
- 2147483648

The default is 512 packets.

**Possible values:** See above

**Default value:** In releases prior to 07.6.04, the default sampling rate is 512 packets. In software releases 07.6.04 and later, the default sampling rate depends on the device being configured. The following are the new default sFlow sampling rates:

- 4-slot chassis: 2048
- 8-slot chassis: 8192
- 15-slot chassis: 8192
- ProCurve 9408sl: 2048

### sflow source

Specifies the source interface for exporting data to the sFlow collector.
NOTE: This command does not apply to release 07.6.04 or later.

By default, the HP device uses the port that is connected to a collector as the source interface for flows exported to that collector. You can specify an Ethernet port, a loopback interface, or the null interface as the source for sFlow export packets.

- **Ethernet port** – sFlow sends the export packets out the specified interface. To load balance the export of flows from the main cache to a given collector, configure multiple source interfaces for the collector.

- **Loopback interface** – sFlow sends the export packets from the specified loopback address, using a physical port connected to the collector to transmit the packet.

- **Null interface** – sFlow continues to collect flows but does not export them to the collector. Use this type of interface when you want to administratively stop flow export without stopping flow collection and without removing configuration information.

**EXAMPLE:**

```
ProCurveRS(config)# sflow source ethernet 1/1
```

This command configures port 1/1 to be the source interface for sFlow packets.

**Syntax:**

```
[no] sflow source ethernet | loopback <portnum>
```

The `ethernet | loopback <portnum>` specifies a physical port or loopback interface.

The `null` parameter discards the export packets instead of sending them to a collector. However, the sFlow agent continues to collect samples.

**Possible values:** See above

**Default value:** The interface connected to the collector

### show

Displays a variety of configuration and statistical information about the Routing Switch. See “Show Commands” on page 40-1.

### snm check-link-status

Displays the link between each of the five SXPNT ASICs on the switch fabric module and interface modules installed in the chassis.

**EXAMPLE:**

```
ProCurveRS# snm 0 check-link-status
```

```
-----------Cards Present in Slots 0-7-----------
Card in Slot 0
Card in Slot 4

-----------SXPNT Link Status-----------------------
Serdes#(0-7) 0 1 2 3 4 5 6 7
Slot#(0-7) 7 1 6 5 2 0 4 3
Device#
SXPNT #0 UP UP UP UP UP UP UP
SXPNT #1 UP UP UP UP UP UP UP
SXPNT #2 UP UP UP UP UP UP UP
SXPNT #3 UP UP UP UP UP UP UP
SXPNT #4 UP UP UP UP UP UP UP

Syntax: snm <module> check-link-status
```
**module** indicates that the switch fabric module for which you are checking the link status. Currently, you can specify 0 only, which indicates the switch fabric module in chassis slot SF.

**UP** in the SXPNT Link Status table indicates that the link between the SXPNT ASIC and the interface module is functioning properly.

**DOWN** in the SXPNT Link Status table indicates that the link between the SXPNT ASIC and the interface module is down and not functioning properly.

**Possible values:** N/A

**Default value:** N/A

### snm read-temperature

Displays the temperature of each of the five SXPNT ASICs on the switch fabric module.

**EXAMPLE:**

To display the temperature of each of the five SXPNT ASICs on the switch fabric module:

```
ProCurveRS# snm 0 read-temperature
SNM0/SXPNT0 temp is 41.87C
SNM0/SXPNT1 temp is 48.71C
SNM0/SXPNT2 temp is 43.3C
SNM0/SXPNT3 temp is 45.0C
SNM0/SXPNT4 temp is 39.40C
```

**Syntax:** snm <module> read-temperature

- `<module>` indicates that the switch fabric module for which you are checking the temperature. Currently, you can specify 0 only, which indicates the switch fabric module in chassis slot SF.

**Possible values:** N/A

**Default value:** N/A

### snmp disable

Disables SNMP management on the HP device.

**EXAMPLE:**

To disable SNMP management of the device:

```
ProCurveRS(config)# snmp disable
```

To later re-enable SNMP management of the device:

```
ProCurveRS(config)# no snmp disable
```

**Syntax:** [no] snmp disable

**Possible values:** N/A

**Default value:** N/A

### snmp-client

Restricts SNMP management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device through SNMP applications.

If you want to restrict access from Telnet or the Web, use one or both of the following commands:

- **telnet-client** – restricts Telnet access. See “telnet-client” on page 6-160.
- **web-client** – restricts Web access. See “web-client” on page 6-169.

If you want to restrict all management access, you can use the commands above and the **snmp-client** command or you can use the following command: **all-client**. See “all-client” on page 6-19.
EXAMPLE:
To restrict SNMP access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
ProCurveRS(config)# snmp-client 209.157.22.26
```

**Syntax:** `[no] snmp-client <ip-addr>

**Possible values:** A valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

**Default value:** N/A

### snmp-server community

Assigns an SNMP community string for the system:

- read-only (public)
- read-write (private)

**EXAMPLE:**

```
ProCurveRS(config)# snmp-server community planet1 ro view admin 2
```

**Syntax:**

```
snmp-server community [0 | 1] <string> ro | rw [view <viewname>]
[<standard-acl-name> | <standard-acl-id>]
```

The `<string>` parameter specifies the community string name.

The `ro` | `rw` parameter specifies whether the string has read-only (`ro`) or read-write (`rw`) privileges to the assigned view.

The `0` | `1` parameter affects encryption for display of the string in the running-config and the startup-config file. Encryption is enabled by default.

When encryption is enabled, the community string is encrypted in the CLI regardless of the access level you are using. In the Web management interface, the community string is encrypted at the read-only access level but is visible at the read-write access level.

The encryption option can be omitted (the default) or can be one of the following.

- `0` – Disables encryption for the community string you specify with the command. The community string is shown as clear text in the running-config and the startup-config file. Use this option if you do not want display of the community string to be encrypted.
- `1` – Assumes that the community string you enter is the encrypted form, and decrypts the value before using it.

**NOTE:** If you want the software to assume that the value you enter is the clear-text form, and to encrypt display of that form, do not enter `0` or `1`. Instead, omit the encryption option and allow the software to use the default behavior.

If you specify encryption option `1`, the software assumes that you are entering the encrypted form of the community string. In this case, the software decrypts the community string you enter before using the value for authentication. If you accidentally enter option `1` followed by the clear-text version of the community string, authentication will fail because the value used by the software will not match the value you intended to use.

The `view` `<viewstring>` parameter is optional. It allows you to associate a view to the members of this community string. If no view is specified, access to the full MIB is granted.

The `<standard-acl-name> | <standard-acl-id>` parameter is optional. It allows you to specify which ACL group will be used to filter incoming SNMP packets. You can enter either the ACL name or its ID.
NOTE: When `snmp-server community` is configured, all incoming SNMP packets are validated first by their community strings and then by their bound ACLs. Before software release 07.7.00, packets are denied if filters are not configured for an ACL. Beginning with software release 07.7.00, packets are permitted if no filters are configured for an ACL.

**Possible values:** See above

**Default value:** The default read-only (ro) community string is "public". HP devices do not have a default read-write (rw) community string.

### snmp-server contact

Identifies a system contact. You can designate a contact name for the Routing Switch and save it in the configuration file for later reference. You can later access contact information using the `show snmp server` command.

**EXAMPLE:**

```
ProCurveRS(config)# snmp-server contact administrator
```

**Syntax:** `snmp-server contact <text>`

**Possible values:** up to 32 alphanumeric characters for the system contact text string

**Default value:** N/A

### snmp-server enable ethernet

Allows SNMP access only to clients on a specific port.

**EXAMPLE:**

The following example configures the device to allow SNMP access only to clients connected to Ethernet port 7/11.

```
ProCurveRS(config)# snmp-server enable ethernet 7/11
```

**Syntax:** `[no] snmp-server enable ethernet <portnum>`

**Possible values:** An Ethernet port

**Default value:** N/A

### snmp-server enable traps

When the command is preceded with `no`, the command is used to stop certain traps from being generated by a system. The following SNMP traps are collected by default:

- authentication key
- bgp
- cold-start
- link-up
- link-down
- new-root
- topology-change
- power-supply-failure
- locked-address-violation

**EXAMPLE:**

To stop reporting incidences of links that are down, enter the following commands:

```
ProCurveRS(config)# no snmp-server enable traps link-down
```

**Syntax:** `[no] snmp-server enable traps <trap-type>`
Possible values: trap type (for example, cold-start, new-root, and so on)

Default value: All of the following SNMP traps are enabled and will be generated by default for a system:
- authentication key
- bgp
- cold-start
- link-up
- link-down
- new-root
- topology-change
- power-supply-failure
- locked-address-violation

`snmp-server enable traps holddown-time`
Changes the holddown time for SNMP traps.

When an HP device starts up, the software waits for Layer 2 convergence (STP) and Layer 3 convergence (OSPF) before beginning to send SNMP traps to external SNMP servers. Until convergence occurs, the device might not be able to reach the servers, in which case the messages are lost.

By default, an HP device uses a one-minute holddown time to wait for the convergence to occur before starting to send SNMP traps. After the holddown time expires, the link up trap remembers which ports are up during the holddown them and the device sends the traps, including traps such as “cold start” or “warm start” that occur before the holddown time expires.

**EXAMPLE:**

```
ProCurveRS(config)# snmp-server enable traps holddown-time 30
```

The command in this example changes the holddown time for SNMP traps to 30 seconds. The device waits 30 seconds to allow convergence in STP and OSPF before sending traps to the SNMP trap receiver.

**Syntax:** `[no] snmp-server enable traps holddown-time <secs>`

The `<secs>` parameter specifies the number of seconds and can be from 1 – 600 (ten minutes). The default is 60 seconds.

**Possible values:** 1 – 600 seconds

**Default value:** 60 seconds

`snmp-server enable vlan`
Allows SNMP access only to clients in a specific VLAN.

**EXAMPLE:**

The following example configures the device to allow SNMP access only to clients connected to ports within port-based VLAN 40. Clients connected to ports that are not in VLAN 40 are denied access.

```
ProCurveRS(config)# snmp-server enable vlan 40
```

**Syntax:** `[no] snmp-server enable vlan <vlan-id>`

**Possible values:** A VLAN ID

**Default value:** N/A

`snmp-server engineid`
Changes the default engine ID to a user-defined one. (For SNMP version 3.) An SNMP engine ID identifies an SNMP management entity.
**EXAMPLE:**

ProCurveRS(config)# snmp-server engineid local 800007c70300e05290ab60

**Syntax:** [no] snmp-server engineid local <hex-string>

The **local** parameter indicates that engine ID to be entered is the ID of this device.

**NOTE:** Since the current implementation of SNMP version 3 does not support Notification, remote engine IDs cannot be configured at this time.

The <hex-string> variable consists of 11 octets, entered as hexadecimal values. There are two hexadecimal characters in each octet. There should be an even number of hexadecimal characters in an engine ID.

The default engine ID has a maximum of 11 octets:

- Octets 1 through 4 represent the agent's SNMP management private enterprise number as assigned by the Internet Assigned Numbers Authority (IANA). The most significant bit of Octet 1 is "1".
- Octet 5 is always 03 in hexadecimal and indicates that the next set of values represent a MAC address.
- Octets 6 through 11 form the MAC address of the lowest port in the management module.

**NOTE:** Engine ID must be a unique number among the various SNMP engines in the management domain. Using the default engine ID ensures the uniqueness of the numbers.

**Possible values:** See above.

**Default value:** Default engine ID.

**snmp-server group**

Maps SNMP users to SNMP views. For each SNMP group, you can configure a read view, a write view, or both. Users who are mapped to a group will use its views for access control. (For SNMP version 3.)

**EXAMPLE:**

ProCurveRS(config)# snmp-server group admin v3 auth read v1default write v1default

**Syntax:** [no] snmp-server group <groupname> v1 | v2 | v3 auth | noauth [access <standard-acl-id>] [read <viewstring> | write <viewstring>]

**NOTE:** This command is not used for SNMP version 1 and SNMP version 2. In these versions, groups and group views are created internally using community strings. When a community string is created, two groups are created, based on the community string name. One group is for SNMP version 1 packets, while the other is for SNMP version 2 packets.

The **group** <groupname> parameter defines the name of the SNMP group to be created.

The **v1** | **v2** | **v3** parameter indicates which version of SNMP is used. In most cases, you will be using v3.

The **auth** | **noauth** parameter determines whether or not authentication will be required to access the supported views. If auth is selected, then only authenticated packets are allowed to access the view specified for the user group. Selecting **noauth** means that no authentication is not required to access the specified view.

The **access** <standard-acl-id> parameter is optional. It allows incoming SNMP packets to be filtered based on the standard ACL attached to the group.

The **read** <viewstring> | **write** <viewstring> parameter is optional. It indicates that users who belong to this group have either read or write access to the portion of the MIB specified by the <viewstring>.

The <viewstring> variable is the name of the view to which the SNMP group members have access. If no view is specified, then the group has no access to the MIB.
The value of `<viewstring>` is defined using the `snmp-server view` command. The SNMP agent comes with the "v1default" view; however, it must be specified when defining a group. The "v1default" view provides access to the entire MIB. The "v1default" view also allows SNMP version 3 to be backwards compatibility with SNMP version 1 and version 2.

**NOTE:** If you will be using a view other than the "v1default" view, that view must exist before creating the user group. See the section "snmp-server view" on page 6-146.

To delete a group, use the no parameter before the command.

**Possible values:** See above.  
**Default value:** N/A

### snmp-server host

Assigns or removes a station as an SNMP trap receiver. To assign the trap receiver, use the command `snmp-server host`. To later remove the trap receiver feature, enter `no snmp-server host`.

**EXAMPLE:**

To specify an SNMP trap receiver and change the UDP port that will be used to receive traps, enter a command such as the following:

```bash
ProCurveRS(config)# snmp-server host 2.2.2.2 0 mypublic port 200
ProCurveRS(config)# write memory
```

**Syntax:** `snmp-server host <ip-addr> [0 | 1] <string> [port <value>]`

- The `<ip-addr>` parameter specifies the IP address of the trap receiver.
- The `[0 | 1]` parameter specifies whether you want the software to encrypt the string (1) or show the string in the clear (0). The default is 0.
- The `<string>` parameter specifies an SNMP community string configured on the HP device. The string can be a read-only string or a read-write string. The string is not used to authenticate access to the trap host but is instead a useful method for filtering traps on the host. For example, if you configure each of your HP devices that use the trap host to send a different community string, you can easily distinguish among the traps from different HP devices based on the community strings.
- The command in the example above adds trap receiver 2.2.2.2 and configures the software to encrypt display of the community string. When you save the new community string to the startup-config file (using the `write memory` command), the software adds the following command to the file:

```bash
snmp-server host 2.2.2.2 1 <encrypted-string>
```

To add a trap receiver and configure the software to encrypt display of the community string in the CLI and Web management interface, enter commands such as the following:

```bash
ProCurveRS(config)# snmp-server host 2.2.2.2 0 ProCurveRS-12
ProCurveRS(config)# write memory
```

- The `port <value>` parameter allows you to specify which UDP port will be used by the trap receiver. This parameter allows you to configure several trap receivers in a system. HP devices can be configured to send copies of traps to more than one network management application.

**Possible values:** IP address of trap receiver station, community string

**Default value:** no system default

### snmp-server location

Identifies a system location for the Routing Switch. This information is saved in the configuration file for later reference. You can later access system location information using the `show snmp server` command.

**EXAMPLE:**

```bash
ProCurveRS(config)# snmp-server location Gertrude_lane
```
**Global CONFIG Commands**

### Syntax:
`snmp-server location <text>`

**Possible values:** up to 32 alphanumeric characters for the `snmp-server location` text string

**Default value:** N/A

### `snmp-server pw-check`
Disables password checking for SNMP set requests. If a third-party SNMP management application does not add a password to the password field when it sends SNMP set requests to an HP device, by default the HP device rejects the request. You can disable this password checking with the `no snmp-server pw-check` command.

**EXAMPLE:**
```
ProCurveRS(config)# no snmp-server pw-check
```

**Syntax:** `[no] snmp-server pw-check`

**Possible values:** N/A

**Default value:** N/A

### `snmp-server trap-source`
Specifies a port, loopback interface, or virtual interface whose lowest-numbered IP address the HP device must use as the source for all SNMP traps sent by the device.

**EXAMPLE:**
To specify a loopback interface as the device’s SNMP trap source, enter commands such as the following:
```
ProCurveRS(config)# int loopback 1
ProCurveRS(config-lbif-1)# ip address 10.0.0.1/24
ProCurveRS(config-lbif-1)# exit
ProCurveRS(config)# snmp-server trap-source loopback 1
```

The commands in this example configure loopback interface 1, assign IP address 10.0.0.1/24 to the loopback interface, then designate the interface as the SNMP trap source for this Routing Switch. Regardless of the port the HP device uses to send traps to the receiver, the traps always arrive from the same source IP address.

**Syntax:** `snmp-server trap-source loopback <num> | ethernet <portnum> | ve <num>`

The `<num>` parameter is a loopback interface or virtual interface number. If you specify an Ethernet, the `<portnum>` is the port’s number (including the slot number). The lowest-numbered address on the specified interface is used as the trap source.

**Possible values:** Valid Ethernet port, loopback interface, or virtual interface

**Default value:** N/A

### `snmp-server user`
Creates an SNMP user, defines the group to which the user will be associated, defines the type of authentication to be used for SNMP access by the user.

**EXAMPLE:**
```
ProCurveRS(config)# snmp-s user bob admin v3 access 2 encrypted auth md5 md5authstring
```

**Syntax:** `[no] snmp-server user <name> <groupname> v3
[[<access <standard-acl-id>]> [encrypted] [auth md5 <md5-password> | sha <sha-password>] [priv [encrypted] des <des-password>]]]
```

The `<name>` parameter defines the SNMP user name or security name used to access the management module.

The `<groupname>` parameter identifies the SNMP group to which this user is associated or mapped. All users must be mapped to an SNMP group. Groups are defined using the `snmp-server group` command.
Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches

NOTE: The SNMP group to which the user account will be mapped should be configured before creating the user accounts; otherwise, the group will be created without any views. Also, ACL groups must be configured before configuring user accounts.

The `v3` parameter is required.

The `access <standard-acl-id>` parameter is optional. It indicates that incoming SNMP packets are filtered based on the ACL attached to the user account.

NOTE: The ACL specified in a user account overrides the ACL assigned to the group to which the user is mapped. If no ACL is entered for the user account, then the ACL configured for the group will be used to filter packets.

The `encrypted` parameter means that the MD5 or SHA password will be a digest value. MD5 has 16 octets in the digest. SHA has 20. The digest string has to be entered as a hexadecimal string. In this case, the agent need not generate any explicit digest. If the `encrypted` parameter is not used, the user is expected to enter the authentication password string for MD5 or SHA. The agent will convert the password string to a digest, as described in RFC 2574.

The `auth md5 | sha` parameter is optional. It defines the type of encryption that the user must have to be authenticated. Choose between MD5 or SHA encryption. MD5 and SHA are two authentication protocols used in SNMP version 3.

The `<md5-password>` and `<sha-password>` define the password the user must use to be authenticated. These passwords must have a minimum of 8 characters. If the `encrypted` parameter is used, then the digest has 16 octets for MD5 or 20 octets for SHA.

NOTE: Once a password string is entered, the generated configuration displays the digest (for security reasons), not the actual password.

The `priv [encrypted] des <des-password>` parameter is optional. It defines the type of encryption that will be used to encrypt the privacy password. If the "encryption" keyword is used, enter a 16-octet DES key in hexadecimal format for the `des-password`. If the "encryption" keyword is not used enter a password string. The agent will generate a suitable 16-octet DES key from the password string.

Currently, DES is the only encryption type supported for priv password.

To delete a user account, use the no parameter before the command.

Possible values: See above.

Default value: N/A

**snmp-server view**

Configures an SNMP view. You can use an SNMP view as an argument with other commands.

SNMP views are named groups of MIB objects that can be associated with user accounts to allow limited access for viewing and modification of SNMP statistics and system configuration. SNMP views can also be used with other commands that take SNMP views as an argument. SNMP views reference MIB objects using object names, numbers, wildcards, or a combination of the three. The numbers represent the hierarchical location of the object in the MIB tree. You can reference individual objects in the MIB tree or a subset of objects from the MIB tree.

NOTE: The `snmp-server view` command supports the MIB objects as defined in RFC 1445.

**EXAMPLE:**

To add an SNMP view, use the following CLI method:

```
ProCurveRS(config)# snmp-server view Maynes system included
ProCurveRS(config)# snmp-server view Maynes system.2 excluded
ProCurveRS(config)# snmp-server view Maynes 2.3.*.6
ProCurveRS(config)# write mem
```
**Global CONFIG Commands**

**Syntax:** [no] snmp-server view <name> <mib_tree> included | excluded

The `<name>` parameter can be any alphanumeric name you choose to identify the view. The names cannot contain spaces.

The `<mib_tree>` parameter is the name of the MIB object or family. MIB objects and MIB sub-trees can be identified by name or by the numbers representing the position of the object or sub-tree in the MIB hierarchy. You can use a wildcard (*) in the numbers to specify a sub-tree family.

The **included | excluded** parameter specifies whether the MIB objects identified by the `<mib_family>` parameter are included in the view or excluded from the view.

**NOTE:** All MIB objects are automatically excluded from any view unless they are explicitly included; therefore, when creating views using the **snmp-server view** command, indicate which portion of the MIB you want users to access.

To delete a view, use the no parameter before the command.

**Possible values:** See above

**Default value:** N/A

**sntp poll-interval**

This parameter sets how often clock updates are requested from an SNTP server.

**EXAMPLE:**
To configure the Routing Switch to poll for clock updates from an SNTP server every 15 minutes, enter the following:

```
ProCurveRS(config)# sntp poll-interval 900
```

**Syntax:** sntp poll-interval <1 – 65535>

**Possible values:** 1 – 65535 seconds

**Default value:** 1800 seconds

**sntp server**

Allows you to define the SNTP server that will be used for clock synchronization for the HP device. You can enter the SNTP server's IP address or its host name.

Up to three SNTP server entries can be defined.

**EXAMPLE:**
To define the SNTP server (IP address 192.1.4.69) that will be polled by the Routing Switch for time updates, enter:

```
ProCurveRS(config)# sntp server 192.1.4.69
```

**Syntax:** sntp server <ip-addr> | <hostname> [<version>]

The `<version>` parameter specifies the SNTP version the server is running and can be from 1 – 4. The default is 1. You can configure up to three SNTP servers by entering three **separate sntp server** commands.

**Possible values:** See above.

**Default value:** N/A

**spanning-tree**

Enables or disables (no) Spanning Tree on the device. This change can be viewed by the **show spanning tree** command. This feature is disabled by default.

To disable this feature, enter **no spanning-tree**. To later re-enable spanning tree on the router, enter **spanning-tree**.
Also, once 802.1W has been enabled on a device (see the “spanning-tree 802-1w” on page 6-149 command), use this command to disable and re-enable 802.1W on a port.

**EXAMPLE:**
To disable spanning tree, enter the following:

```
ProCurveRS(config)# no span
```

**EXAMPLE:**
To enable spanning tree, enter the following:

```
ProCurveRS(config)# spanning-tree
```

**EXAMPLE:**
To disable 802.1W on a port, enter the following:

```
ProCurveRS(config)# interface 1/1
ProCurveRS(config-if-1/1)# no spanning-tree
```

**Syntax:** [no] spanning-tree

**Possible values:** N/A

**Default value:** Disabled.

**spanning-tree <parameter>**

Spanning Tree bridge and port parameters are configurable using one CLI command. When no port-based VLANs are active on the system, spanning tree parameters are set at the Global CONFIG Level.

When port-based VLANs are active on the system, spanning tree protocol bridge and port parameters can be configured at the VLAN Level (see “spanning-tree” on page 30-14). Additionally, you can disable or enable STP on an interface basis.

**NOTE:** If VLANs are active on a Routing Switch, spanning-tree will not be seen as an option at the Global CONFIG Level of the CLI but will be an option of the VLAN Level.

All bridge and port parameters have default values and do not need to be modified unless required to match network needs. Additionally, all values will be globally applied to the Routing Switch. By default this feature is disabled on Routing Switches.

You can modify the following STP Parameters:
- Bridge parameters—forward delay, maximum age, hello time, and priority
- Port parameters—priority and path cost

**EXAMPLE:**
To enable spanning tree on a system in which no port-based VLANs are active and change the hello-time from the default value of 2 to 8 seconds, enter the following commands.

```
ProCurveRS(config)# span hello-time 8
ProCurveRS(config)# span ethernet 1/5 path-cost 15 priority 64
```

Here is the syntax for global STP parameters.

**Syntax:** spanning-tree [forward-delay <value>] | [hello-time <value>] | [maximum-age <value>] | [priority <value>]

Here is the syntax for port STP parameters.

**Syntax:** spanning-tree ethernet <portnum> path-cost <value> | priority <value>

**Possible values:** see below

Bridge Parameters:
- **forward-delay:** Possible values: 4 – 30 seconds. Default is 15 seconds.
- **max-age:** Possible values: 6 – 40 seconds. Default is 20 seconds.
Global CONFIG Commands

- **hello-time**: Possible values: 1 – 10 seconds. Default is 2 seconds.
- **priority**: Possible values: 1 – 65535. Default is 32768. A higher numerical value means a lower priority; thus, the highest priority is 0.

Port Parameters:
- **path**: Possible values: 1 – 65535. Default: The default depends on the port type:
  - 10 Mbps – 100
  - 100 Mbps – 19
  - Gigabit – 4
  - 10 Gigabit – 2
- **priority**: possible values are 8 – 252, in increments of 4. Default is 128. A higher numerical value means a lower priority; thus, the highest priority is 8.

**NOTE:** The range in software releases earlier than 07.5.01b is 0 – 255. If you are upgrading a device that has a configuration saved under an earlier software release, and the configuration contains a value from 0 – 7 for a port's STP priority, the software changes the priority to the default when you save the configuration while running the new release.

---

**spanning-tree 802-1w**

Enables 802.1W on all ports of a device running the Spanning Tree Protocol. The 802.1W feature is HP's implementation of the IEEE 802.1W standard Rapid Spanning Tree Protocol (RSTP). HP's earlier implementation of RSTP, which was 802.1W Draft 3, provided only a subset of the IEEE 802.1W standard; whereas, this implementation provides the full standard. This new implementation of the protocol is referred to as 802.1W. The implementation of the 802.1W Draft 3 is referred to as RSTP Draft 3. (See the command "spanning-tree single rstp" on page 6-151 to enable RSTP Draft 3.)

**EXAMPLE:**
To enable 802.1W on a device, enter commands such as the following:
```
ProCurveRS(config)# spanning-tree 802-1w
```

**Syntax:** [no] spanning-tree 802-1w

**Possible Values:** N/A

**Default values:** Disabled

**spanning-tree 802-1w <parameter>**

Configures 802.1W bridge and port parameters once 802.1W has been enabled on the device. There are two versions of this command. The first one configures bridge parameters; the other configures port parameters.

**Bridge Parameters:**

Configuration changes using these parameters are applied to all ports on the bridge.

**EXAMPLE:**
To change 802.1W bridge parameters, enter commands such as the following:
```
ProCurveRS(config)# spanning-tree 802-1w forward-delay 20 hello-time 3 max-age 10 priority 10
```

The command in this example changes the parameter on a device on which you have not configured port-based VLANs. The change applies to the default VLAN. If you have configured a port-based VLAN on the device, you can configure the parameters only at the configuration level for individual VLANs. (See "spanning-tree 802-1w" on page 30-15 for an example.)

**Syntax:** spanning-tree 802-1w [forward-delay <value>] | [hello-time <value>] | [max-age <time>] | [force-version <value>] | [priority <value>]

---

June 2005
The **forward-delay** `<value>` parameter specifies how long a port waits before it forwards an RST BPDU after a topology change. This can be a value from 4 – 30 seconds. The default is 15 seconds.

The **hello-time** `<value>` parameter specifies the interval between two hello packets. This parameter can have a value from 1 – 10 seconds. The default is 2 seconds; however, set this value to at least 4 seconds to provide enough time for BPDUs to reach the root bridge from non-root bridge.

The **max-age** `<value>` parameter specifies the amount of time the device waits to receive a hello packet before it initiates a topology change. You can specify a value from 6 – 40 seconds. The default is 20 seconds.

Beginning with software release 07.6.04, the value of **max-age** must be greater than the value of **forward-delay** to ensure that the downstream bridges do not age out faster than the upstream bridges (those bridges that are closer to the root bridge).

The **force-version** `<value>` parameter forces the bridge to send BPDUs in a specific format. You can specify one of the following values:

- 0 – The STP compatibility mode. Only STP (or legacy) BPDUs will be sent.
- 2 – The default. RST BPDUs will be sent unless a legacy bridge is detected. If a legacy bridge is detected, STP BPDUs will be sent instead.

The default is 2.

The **priority** `<value>` parameter specifies the priority of the bridge. You can enter a value from 0 – 65535. A lower numerical value means a the bridge has a higher priority. Thus, the highest priority is 0. The default is 32768.

You can specify some or all of these parameters on the same command line. If you specify more than one parameter, you must specify them in the order shown above, from left to right.

**Possible values:** See above

**Default values:** See above

**Port Parameters:**

These commands can be entered on individual ports or on multiple ports, such as all ports that belong to a VLAN.

**EXAMPLE:**

You can change the following 802.1W port parameters using the following methods.

```
ProCurveRS(config)# vlan 10
ProCurveRS(config-vlan-10)# spanning-tree 802-1w ethernet 1/5 path-cost 15 priority 64
```

**Syntax:** `spanning-tree 802-1w ethernet <portnum> path-cost <value> | priority <value> | [admin-edge-port] | [admin-pt2pt-mac] | [force-migration-check]`

The **ethernet** `<portnum>` parameter specifies the interface used.

The **path-cost** `<value>` parameter specifies the cost of the port's path to the root bridge. 802.1W prefers the path with the lowest cost. You can specify a value from 1 – 20,000,000. Table 6.6 shows the recommended path cost values from the IEEE standards.

**Table 6.6: Recommended Path Cost Values of 802.1W**

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>Recommended (Default) 802.1W Path Cost Values</th>
<th>Recommended 802.1W Path Cost Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>Less than 100 kilobits per second</td>
<td>200,000,000</td>
<td>20,000,000 – 200,000,000</td>
</tr>
<tr>
<td>1 Megabit per second</td>
<td>20,000,000</td>
<td>2,000,000 – 200,000,000</td>
</tr>
<tr>
<td>10 Megabits per second</td>
<td>2,000,000</td>
<td>200,000 – 200,000,000</td>
</tr>
</tbody>
</table>
Table 6.6: Recommended Path Cost Values of 802.1W

<table>
<thead>
<tr>
<th>Link Speed</th>
<th>Recommended (Default) 802.1W Path Cost Values</th>
<th>Recommended 802.1W Path Cost Range</th>
</tr>
</thead>
<tbody>
<tr>
<td>100 Megabits per second</td>
<td>200,000</td>
<td>20,000 – 200,000,000</td>
</tr>
<tr>
<td>1 Gigabit per second</td>
<td>20,000</td>
<td>2,000 – 200,000,000</td>
</tr>
<tr>
<td>10 Gigabits per second</td>
<td>2,000</td>
<td>200 – 20,000</td>
</tr>
<tr>
<td>100 Gigabits per second</td>
<td>200</td>
<td>20 – 2,000</td>
</tr>
<tr>
<td>1 Terabits per second</td>
<td>20</td>
<td>2 – 200</td>
</tr>
<tr>
<td>10 Terabits per second</td>
<td>2</td>
<td>1 – 20</td>
</tr>
</tbody>
</table>

The `priority <value>` parameter specifies the preference that 802.1W gives to this port relative to other ports for forwarding traffic out of the topology. You can specify a value from 8 – 255. The default is 128. A higher numerical value means a lower priority. The highest priority is 8.

Set the `admin-edge-port` to enabled or disabled. If set to enabled, then the port becomes an edge port in the domain.

Set the `admin-pt2pt-mac` to enabled or disabled. If set to enabled, then a port is connected to another port through a point-to-point link. The point-to-point link increases the speed of convergence. This parameter, however, does not auto-detect whether or not the link is a physical point-to-point link.

The `force-migration-check` parameter forces the specified port to sent one RST BPDU. If only STP BPDUs are received in response to the sent RST BPDU, then the port will go return to sending STP BPDUs.

**Possible Values:** See above

**Default values:** See above

**spanning-tree single 802-1w**

Enables 802.1W on all ports of a single spanning tree.

**EXAMPLE:**
Enter a command such as the following:

```
ProCurveRS(config)# spanning-tree single 802-1w
```

**Syntax:** [no] spanning-tree single 802-1w

**Possible values:** N/A

**Default value:** Disabled

**spanning-tree single <parameter>**

Configures single spanning tree. Single spanning tree enables you to configure a single instance of the Spanning Tree Protocol (SSTP) to run on all the port-based VLANs on a device.

SSTP uses the same parameters, with the same value ranges and defaults, as the default STP on HP devices (multiple-instance STP or "MSTP"), which is described in the previous section.

When you enable SSTP, all VLANs in which STP is enabled are added to the single spanning tree. VLANs in which STP is disabled are excluded from the single spanning tree.

**spanning-tree single rstp**

Enables 802.1W Draft 3 Rapid Spanning Tree on a device that is running Single Spanning Tree.
NOTE: To enable 802.1W Draft 3 on a device that is not running Single Spanning Tree, enter the `spanning-tree rstp` command at the VLAN configuration level. See "spanning-tree rstp" on page 30-17.

802.1W Draft 3 enhances STP by providing a fast failover mechanism for a root port that fails on a non-root bridge. 802.1W Draft 3 provides a subset of the capabilities described in the 802.1W STP specification.

**EXAMPLE:**
To enable 802.1W Draft 3 on a device that is running single STP, enter the following command at the global CONFIG level of the CLI:

```bash
ProCurveRS(config)# spanning-tree single rstp
```

**Syntax:** `[no] spanning-tree single rstp`

This command enables 802.1W Draft 3 on the whole device.

**NOTE:** This command does not also enable single STP. To enable single STP, first enter the `spanning-tree single` command without the `rstp` parameter. After you enable single STP, enter the `spanning-tree single rstp` command to enable RSTP.

To disable 802.1W Draft 3 on a device that is running single STP, enter the following command:

```bash
ProCurveRS(config)# no spanning-tree single rstp
```

**Possible values:** N/A

**Default value:** Disabled

**ssh access-group**
Specifies an ACL that restricts SSH access to management functions on the device.

**EXAMPLE:**
To configure an ACL that restricts SSH access the device:

```bash
ProCurveRS(config)# access-list 12 deny host 209.157.22.98 log
ProCurveRS(config)# access-list 12 deny 209.157.23.0 ... access-list 12 permit any
ProCurveRS(config)# ssh access-group 12
ProCurveRS(config)# write memory
```

**Syntax:** `ssh access-group <num>`

The `<num>` parameter specifies the number of a standard ACL and must be from 1 – 99.

These commands configure ACL 12, then apply the ACL as the access list for SSH access. The device denies SSH access from the IP addresses listed in ACL 12 and permits SSH access from all other IP addresses. Without the last ACL entry for permitting all packets, this ACL would deny SSH access from all IP addresses.

**Possible values:** see above

**Default value:** N/A

**static-mac-address**
Allows you to define a static MAC address for a port on an HP device to ensure the device is not aged out. When defining the MAC address entry, you can also define the port's priority and whether or not it is a router-type or host-type.

**NOTE:** HP recommends that you configure a static ARP entry to match the static MAC entry. In fact, the software automatically creates a static MAC entry when you create a static ARP entry. See "arp" on page 6-21.
NOTE: The location of the `static-mac-address` command in the CLI depends on whether you configure port-based VLANs on the device. If the device does not have more than one port-based VLAN (VLAN 1, which is the default VLAN that contains all the ports), the static-mac-address command is at the global CONFIG level of the CLI. If the device has more than one port-based VLAN, then the `static-mac-address` command is not available at the global CONFIG level. In this case, the command is available at the configuration level for each port-based VLAN.

**EXAMPLE:**

```
ProCurveRS(config)# static 1145.5563.67FF e12 2/7 router-type
```

**Syntax:** `[no] static-mac-address <mac-addr> ethernet <portnum> [to <portnum> ethernet <portnum>] [priority <number>] [host-type | router-type | fixed-host]

priority <number>Chassis device A large number of MAC entries in the MAC table could increase CPU utilization. To alleviate the load on the CPU, use this feature with the Control Plane Security option.

The priority can be 0 – 7 (0 is lowest and 7 is highest).

**Default value:** host-type; 0 or normal priority

**stp-group**

Begins configuration of an STP group. An STP group enables you to manage multiple port-based VLANs in the same spanning tree, without using the Single Span feature. When you enter this command, the CLI changes to the STP group configuration level. (See “STP Group Commands” on page 35-1.)

**EXAMPLE:**

```
ProCurveRS(config)# stp-group 1
ProCurveRS(config)# stp-group 1 master-vlan 2
ProCurveRS(config-stp-group-1)# member-vlan 3 to 4
ProCurveRS(config-stp-group-1)# exit
ProCurveRS(config)# stp-group 2
ProCurveRS(config-stp-group-2)# master-vlan 12
ProCurveRS(config-stp-group-2)# member-vlan 13 to 14
```

These commands configure two STP groups and add VLANs to those groups. All the VLANs in an STP group are managed in the same spanning tree. For information about the commands at the STP group configuration level, see “STP Group Commands” on page 35-1.

**Syntax:** `[no] stp-group <num>

The `<num>` parameter specifies the STP group ID and can be from 1 – 32.

**Possible values:** 1 – 32

**Default value:** N/A

**super-span**

Globally enables the SuperSpan™ feature on the ProCurve 9408sl.

NOTE: Use the `super-span-global` command to enable SuperSpan on devices other than the ProCurve 9408sl.

Use this command after you configure the SuperSpan boundary interfaces. (See “stp-boundary” on page 8-76.) You can enable SuperSpan globally or on an individual VLAN level. If you enable the feature globally, the feature is enabled on all VLANs. To enable or disable SuperSpan in an individual VLAN, see “super-span” on page 30-18.

NOTE: If you enable the feature globally, then create a new VLAN, the new VLAN inherits the global SuperSpan state. For example, if SuperSpan is globally enabled when you create a VLAN, SuperSpan also is enabled in the new VLAN.

For information about this feature, see the “SuperSpan™” section in the “Configuring Spanning Tree Protocol (STP)” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches.*
EXAMPLE:
ProCurveRS(config)# super-span

**Syntax:** [no] super-span [preforward-delay <secs>]

The `<secs>` parameter specifies the length of the Preforwarding state. You can specify from 3 – 30 seconds. The default is 5 seconds.

**Possible values:** 3 – 30 seconds for the Preforwarding state

**Default value:** Disabled; when SuperSpan is enabled, the default length for the Preforwarding state is 5 seconds.

### super-span-global

Globally enables the SuperSpan™ feature.

**NOTE:** Use the `super-span` command to enable SuperSpan on the ProCurve 9408sl.

Use this command after you configure the SuperSpan boundary interfaces. (See “stp-boundary” on page 8-76.) You can enable SuperSpan globally or on an individual VLAN level. If you enable the feature globally, the feature is enabled on all VLANs. To enable or disable SuperSpan in an individual VLAN, see “super-span” on page 30-18.

**NOTE:** If you enable the feature globally, then create a new VLAN, the new VLAN inherits the global SuperSpan state. For example, if SuperSpan is globally enabled when you create a VLAN, SuperSpan also is enabled in the new VLAN.

For information about this feature, see the “SuperSpan™” section in the “Configuring Spanning Tree Protocol (STP)” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches*.

EXAMPLE:
ProCurveRS(config)# super-span-global

**Syntax:** [no] super-span-global [preforward-delay <secs>]

The `<secs>` parameter specifies the length of the Preforwarding state. You can specify from 3 – 30 seconds. The default is 5 seconds.

**Possible values:** 3 – 30 seconds for the Preforwarding state

**Default value:** Disabled; when SuperSpan is enabled, the default length for the Preforwarding state is 5 seconds.

### system hash-per-server-trunk

**NOTE:** This feature applies to software releases 07.7.00 and later.

Specifies the maximum number of hash buckets per server trunk.

Increasing the number of hash buckets per server trunk enhances the speed and efficiency at which the HP device forwards and load balances IP packets on server trunk ports.

**EXAMPLE:**
ProCurveRS(config)# system hash-per-server-trunk 64
ProCurveRS(config)# write mem
ProCurveRS(config)# end
ProCurveRS# reload

**NOTE:** You must reload the software to place this configuration in effect.

**Syntax:** [no] system hash-per-server-trunk <max number of hash buckets>

**Possible values:**

<max number of hash buckets> can be 32, 64, 128, or 256.
Default values:
- On the 9315M, the default is 16.
- On the 9304M and 9308M, the default is 256.

**system-max**

Allows you to modify the default settings for parameters that use system memory. The configurable parameters and their defaults and maximums differ depending on the device. To display the configurable parameters, their defaults, and the maximum configurable values for each, enter the following command at any level of the CLI: `show default values`. See “show default” on page 40-23.

**NOTE:** You must save the configuration (write memory), then reload the software to place this command into effect.

**NOTE:** You do not need to reload the software for the `pim-max-int-group` or `dvmrp-max-int-group` option.

**NOTE:** Beginning with software release 07.6.04, there is no longer a limit to the number of interface groups that can be configured for PIM and DVMRP; therefore, the `system-max pim-max-int-group` and the `system-max dvmrp-max-int-group` commands have been removed from the CLI.

**EXAMPLE:**
To define the maximum number of repeated DVMRP traffic being sent from the same source address and being received by the same destination address, enter a command such as the following:

```
ProCurveRS(config)# system-max dvmrp-mcache 500
```

**Syntax:** `system-max dvmrp-mcache <num>`

**Possible values:** The `<num>` parameter specifies the maximum number of multicast cache entries for DVMRP. Enter a number from 128 – 2048.

**Default value:** The default is 512.

**EXAMPLE:**
To increase the system capacity of an 9300 series for IP routes from the default 10000 to 50000, enter the following command:

```
ProCurveRS(config)# system-max ip-route 50000
```

**Syntax:** `system-max <parameter> <value>`

**Possible values:** These depend on the device you are configuring. See the System Parameters section in the show default values display. The CLI will display the acceptable range if you enter a value that is outside the range.

**Default value:** These depend on the device you are configuring. See the System Parameters section in the show default values display. The CLI will display the acceptable range if you enter a value that is outside the range.

**EXAMPLE:**
On EP and 10-Gigabit Ethernet devices running software release 07.8.00 or later Routing Switch code, you can increase the maximum number of ACL entries from 4096 to 8192. Enter a command such as the following:

```
9300 series(config)# system-max ip-filter-sys 8192
```

**Syntax:** `[no] system-max ip-filter-sys <num>`

**Possible values:** `<num>` is a value from 64 to 8192

**Default value:** 4096
EXAMPLE:
To define the maximum number of entries for the Multicast Flow table, enter a command such as the following:

ProCurveRS(config)# system-max multicast-flow 2048

**Syntax:** system-max multicast-flow <num>

**Possible values:** The `<num>` parameter specifies the maximum number of PIM and DVMRP multicast cache flows that can be stored in the CAM. Enter a number from 512 – 2048.

**Default value:** The default is 1024.

**NOTE:** Do not set this maximum too high since you may run out of resources in the CAM.

EXAMPLE:
To define the maximum number of repeated PIM traffic being sent from the same source address and being received by the same destination address, enter a command such as the following:

ProCurveRS(config)# system-max pim-mcache 999

**Syntax:** system-max pim-mcache <num>

**Possible values:** The `<num>` parameter specifies the maximum number of multicast cache entries for PIM. Enter a number from 256 – 4096.

**Default:** The default is 1024.

EXAMPLE:
To increase the number of SNMP views available on an HP device:

ProCurveRS(config)# system-max view 15

**Syntax:** system-max view <number-of-views>

This command specifies the maximum number of SNMPv2 and v3 views that can be configured on a device.

**Possible values:** The number of views can be from 10 – 65536.

**Default value:** The default is 10 views.

A view can be configured using command “snmp-server view” on page 6-146.

EXAMPLE:
To specify the amount of Content Addressable Memory (CAM) space to reserve with hardware multicasting:

**NOTE:** This parameter is supported on the ProCurve 9408sl only.

1. Enter the required CAM space, save it to the startup-up config file, then reload the device:

   ProCurveRS(config-vlan-2)# system-max vlan-multicast-flooding 200
   ProCurveRS(config-vlan-2)# exit
   ProCurveRS(config)# write mem
   ProCurveRS(config)# end
   ProCurveRS# reload

   **NOTE:** After entering the `system-max vlan-multicast-flooding` command, you must reboot the HP device to place the configuration change into effect.

2. Enable multicast flooding on the VLAN:

   ProCurveRS(config)# vlan 2
   ProCurveRS(config-vlan-2)# multicast-flooding

   **Syntax:** system-max vlan-multicast-flooding <value>

   **Possible values:** The `<value>` can be from 0 – 4095.
**Default value:** The default is 0.

**tacacs-server**

Identifies a TACACS or TACACS+ server and sets other TACACS/TACACS+ parameters for authenticating access to the HP device.

**EXAMPLE:**

ProCurveRS(config)# tacacs-server host 209.157.22.99

**Syntax:** tacacs-server host <ip-addr> | <server-name> [auth-port <number>]

The only required parameter is the IP address or host name of the server. You can enter this command up to three times, to add up to three servers. During authentication, the device tries to reach the servers in the order you add them.

**NOTE:** To specify the server's host name instead of its IP address, you must first identify a DNS server using the `ip dns server-address <ip-addr>` command at the global CONFIG level. See the “Configuring IP” chapter of the Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches.

The `auth-port` parameter specifies the UDP port number of the authentication port on the server. The default port number is 49.

**Syntax:** tacacs-server [key 0 | 1 <string>] [timeout <number>] [retransmit <number>] [dead-time <number>]

The `key` parameter specifies the value that the HP device sends to the server when trying to authenticate user access. The TACACS+ server uses the key to determine whether the HP device has authority to request authentication from the server. The key can be from 1 – 32 characters in length and cannot include any space characters.

**NOTE:** Encryption of the TACACS+ keys is done by default. The 0 parameter disables encryption. The 1 parameter is not required; it is provided for backwards compatibility.

The `timeout` parameter specifies how many seconds the HP device waits for a response from the TACACS/TACACS+ server before either retrying the authentication request or determining that the TACACS/TACACS+ server is unavailable and moving on to the next authentication method in the authentication-method list. The timeout can be from 1 – 15 seconds. The default is 3 seconds.

The `retransmit` parameter specifies how many times the HP device will resend an authentication request when the TACACS/TACACS+ server does not respond. The retransmit value can be from 1 – 5 times. The default is 3 times.

The dead-time parameter specifies how long the HP device waits for the primary authentication server to reply before deciding the server is dead and trying to authenticate using the next server. The dead-time value can be from 1 – 5 seconds. The default is 3.

In a TACACS+ configuration, you can designate a server to handle a specific AAA task. For example, you can designate one TACACS+ server to handle authorization and another TACACS+ server to handle accounting. You can set the TACACS+ key for each server.

For example, to specify different TACACS+ servers for authentication, authorization, and accounting:

ProCurveRS(config)# tacacs-server host 1.2.3.4 auth-port 49 authentication-only key abc
ProCurveRS(config)# tacacs-server host 1.2.3.5 auth-port 49 authorization-only key def
ProCurveRS(config)# tacacs-server host 1.2.3.6 auth-port 49 accounting-only key ghi

**Syntax:** tacacs-server host <ip-addr> | <server-name> [authentication-only | authorization-only | accounting-only | default] [key <string>]

The `default` parameter causes the server to be used for all AAA functions.
After authentication takes place, the server that performed the authentication is used for authorization and/or accounting. If the authenticating server cannot perform the requested function, then the next server in the configured list of servers is tried; this process repeats until a server that can perform the requested function is found, or every server in the configured list has been tried.

Possible values: see above
Default value: see above

tag-type
This parameter defines the value that will be sent out on a packet to indicate it is part of a tagged VLAN port. The 802.1p/q standard recognizes the value of 8100 for this purpose. Other values can be assigned to this parameter but are not recommended, unless you are configuring 802.1q tag-type translation (for more information about this feature, see the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches).

EXAMPLE:
ProCurveRS(config)# tag-type 8100

Syntax: [no] tag-type <hex-value> [e <slot number>/<port number> to <port number>]

Possible values:

<hex value> is a hexadecimal value from 0 – ffff. If you are configuring 802.1q tag-type translation (available on the ProCurve 9408sl Switch), you must specify a value other than 8100.

The <slot number> parameter specifies the slot number on an HP Chassis device. This parameter is available on the ProCurve 9408sl. This parameter is used to configure 802.1q tag-type translation.

The <port number> to <port number> parameter specifies the interface(s) that will use the defined tag type. This parameter is available on the ProCurve 9408sl. This parameter is used to configure 802.1q-in-q tagging and 802.1q tag-type translation.

The <port number> to <port number> parameter operates with the following rule:

- If the interfaces specified in the command <port number> to <port number> are part of a multi-slot trunk, all of the interfaces that are part of the multi-slot trunk will be configured with the specified tag-type.

- If you specify a single port number, the 802.1Q tag-type applies to all ports within the port region. For example, if you enter the command tag-type 9100 e 1, the HP device automatically applies the 802.1Q tag to ports 1 – 8 since all of these ports are in the same port region (controlled by the same DMA). Use the show running-config command at any level of the CLI to view port regions. Note that on Gigabit Ethernet modules, ports 1 and 2 belong to the same port region.

- On the ProCurve 9408sl. If you do not specify a port or range of ports, the 802.1Q tag-type applies to all Ethernet ports on the device.

Default value: 8100

telnet access-group
Specifies an ACL that restricts Telnet access to management functions on the device.

EXAMPLE:
To configure an ACL that restricts Telnet access the device:

ProCurveRS(config)# access-list 12 deny host 209.157.22.98 log
ProCurveRS(config)# access-list 12 deny host 209.157.23.0 0.0.0.255 log
ProCurveRS(config)# access-list 12 deny host 209.157.24.0/24 log
ProCurveRS(config)# access-list 12 permit any
ProCurveRS(config)# telnet access-group 12
ProCurveRS(config)# write memory

Syntax: telnet access-group <num>

The <num> parameter specifies the number of a standard ACL and must be from 1 – 99.
These commands configure ACL 12, then apply the ACL as the access list for Telnet access. The device denies Telnet access from the IP addresses listed in ACL 12 and permits Telnet access from all other IP addresses. Without the last ACL entry for permitting all packets, this ACL would deny Telnet access from all IP addresses.

**Possible values:** see above

**Default value:** N/A

**telnet login-retries**

Specifies the maximum number of login attempts for Telnet access.

If you are connecting to the HP device using Telnet, the device prompts you for a username and password. By default, you have up to 4 chances to enter a correct username and password. If you do not enter a correct username or password after 4 attempts, the HP device disconnects the Telnet session.

Starting with release 07.8.00, you can use this command to specify the number of attempts a Telnet user has to enter a correct username and password before the device disconnects the Telnet session.

**EXAMPLE:**

To allow a Telnet user up to 5 chances to enter a correct username and password, enter the following command:

```
ProCurveRS(config)# telnet login-retries 5
```

**Syntax:** [no] `telnet login-retries <number>`

**Possible values:** You can specify from 0 – 5 attempts.

**Default value:** 4 attempts

**telnet login-timeout**

Changes the login timeout period for Telnet sessions.

**EXAMPLE:**

To change the login timeout period for Telnet sessions to 5 minutes:

```
ProCurveRS(config)# telnet login-timeout 5
```

**Syntax:** [no] `telnet login-timeout <minutes>`

**Possible values:** 1 – 10 minutes

**Default value:** 1 minute

**telnet server enable ethernet**

**NOTE:** This command is supported in software releases 07.8.00 and later.

Allows Telnet access only to a specific interface.

**EXAMPLE:**

The following command configures the device to allow Telnet management access only to a client connected to port 1 in slot 1:

```
ProCurveRS(config)# telnet server enable e1/1
```

**Syntax:** [no] `telnet server enable ethernet <slot>/<port>`

**Possible values:** N/A

**Default value:** N/A

**telnet server enable vlan**

Allows Telnet access only to clients in a specific VLAN.
**EXAMPLE:**
The following command configures the device to allow Telnet management access only to clients connected to ports within port-based VLAN 10. Clients connected to ports that are not in VLAN 10 are denied management access.

```
ProCurveRS(config)# telnet server enable vlan 10
```

**Syntax:** [no] telnet server enable vlan <vlan-id>

**Possible values:** N/A

**Default value:** N/A

**telnet server suppress-reject-message**
Suppresses the rejection message the device sends in response to a denied Telnet client.

If you enable suppression of the connection rejection message, a denied Telnet client does not receive a message from the HP device. Instead, the denied client simply does not gain access.

**EXAMPLE:**
To suppress the connection rejection message sent by the device to a denied Telnet client, enter the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# telnet server suppress-reject-message
```

**Syntax:** [no] telnet server suppress-reject-message

**Possible values:** N/A

**Default value:** Disabled

**telnet-client**
Restricts Telnet management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device's CLI through Telnet.

If you want to restrict access from SNMP or the Web, use one or two of the following commands:

- **snmp-client** – restricts SNMP access. See “snmp-client” on page 6-139.
- **web-client** – restricts web access. See “web-client” on page 6-169.

If you want to restrict all management access, you can use the commands above and the **telnet-client** command or you can use the following command: **all-client**. See “all-client” on page 6-19.

**EXAMPLE:**
To restrict Telnet access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
ProCurveRS(config)# telnet-client 209.157.22.26
```

**Syntax:** [no] telnet-client <ip-addr>

Starting in release 07.8.00, you can restrict Telnet access to the HP device based on the MAC address of a connecting client. For example, the following command allows Telnet access to the HP device only to the host with IP address 209.157.22.39 and MAC address 0007.e90f.e9a0:

```
ProCurveRS(config)# telnet-client 209.157.22.39 0007.e90f.e9a0
```

**Syntax:** [no] telnet-client <ip-addr> <mac-addr>

The following command allows Telnet access to the HP device to a host with any IP address and MAC address 0007.e90f.e9a0:

```
ProCurveRS(config)# telnet-client any 0007.e90f.e9a0
```

**Syntax:** [no] telnet-client any <mac-addr>

**Possible values:** A valid address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.
Global CONFIG Commands

Default value: N/A

telnet-server
Enables or disables Telnet access to an HP device. By default, Telnet access is allowed on a system.

EXAMPLE:
To disable Telnet access to an HP device, enter the following:
ProCurveRS(config)# no telnet-server

Syntax: [no] telnet-server
Possible values: Enabled or disabled
Default value: Enabled

telnet-timeout
Defines how many minutes a Telnet session can remain idle before it is timed out. An idle Telnet session is a session that is still sending TCP ACKs in response to keepalive messages from the HP device, but is not being used to send data.

By default, the Telnet timeout is zero (which means Telnet sessions do not time out).

NOTE: HP devices also have another, non-configurable Telnet timer used to close sessions that have ended abnormally. This mechanism is enabled regardless of the setting of the Telnet timeout. The HP device sends TCP keepalive messages to the Telnet client once a minute. If the client fails to respond to two consecutive keepalive messages, the HP device concludes that the TCP session has ended abnormally and immediately ends the session. A typical cause of a session ending abnormally is the client rebooting during the TCP session.

EXAMPLE:
ProCurveRS(config)# telnet-timeout 120

Syntax: telnet-timeout <0 – 240>
Possible values: 0 – 240 minutes
Default value: 0 minutes (no timeout)

temp-poll-period
Changes the interval at which the system reads the temperature sensors on each module.

EXAMPLE:
The following command sets the temp-poll-period to 120 seconds.
ProCurveRS(config)# temp-poll-period 120

Syntax: temp-poll-period <seconds>
Possible values: 30 – 120 seconds. Setting this parameter to 0 disables the system from polling the temperature sensor on each module.
Default value: 60 seconds

terminal length
Specifies how many lines to display on the screen during the current CLI session. This command is useful when reading multiple lines of displayed information, especially those that do not fit on one screen.

EXAMPLE:
To specify the maximum number of lines displayed on one page, enter a command such as the following:
ProCurveRS(config)# terminal length 15

Syntax: terminal length <number-of-lines>
Possible values: The <number-of-lines> parameter indicates the maximum number of lines that will display on a full screen of text during the current session. If the displayed information requires more than one page, the terminal pauses. Pressing the space bar displays the next page.

Default: The default <number-of-lines> is 24. Entering a value of 0 prevents the terminal from pausing between multiple output pages.

tftp client enable vlan

Allows TFTP access only to clients in a specific VLAN.

EXAMPLE:
The following example configures the device to allow TFTP access only to clients connected to ports within port-based VLAN 40. Clients connected to ports that are not in VLAN 40 are denied access.

ProCurveRS(config)# tftp client enable vlan 40

Syntax: [no] tftp client enable vlan <vlan-id>

Possible values: N/A

Default value: N/A

topology-group

Creates a topology group.

A topology group is a named set of VLANs that share a Layer 2 topology. Topology groups simplify configuration and enhance scalability of Layer 2 protocols by allowing you to run a single instance of a Layer 2 protocol on multiple VLANs.

You can use topology groups with the following Layer 2 protocols:

• STP
• MRP
• VSRP
• 802.1W

EXAMPLE:

ProCurveRS(config)# topology-group 2
ProCurveRS(config-topo-group-2)# master-vlan 2
ProCurveRS(config-topo-group-2)# member-vlan 3
ProCurveRS(config-topo-group-2)# member-vlan 4
ProCurveRS(config-topo-group-2)# member-vlan 5
ProCurveRS(config-topo-group-2)# member-group 2

Syntax: [no] topology-group <group-id>

The <group-id> parameter specifies the topology group ID and can be from 1 – 256.

For information about the other commands in this example, see “Topology Group Commands” on page 33-1.

Possible values: See above

Default value: N/A

trunk

Allows you to add a trunk group and connect the ports in the group to a router or server for high-speed connections.

See the "Configuring Trunk Groups and Dynamic Link Aggregation" chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches for trunk configuration rules and more examples.
NOTE: The ports in a trunk group make a single logical link. Therefore, all the ports in a trunk group must be connected to the same device at the other end.

NOTE: You can trunk two 10 Gigabit Ethernet ports together. The first port must be in an odd-numbered chassis slot and the second port must be in the following even-numbered slot.

NOTE: If you are running a software release earlier than 07.5.04, you must save the configuration (write memory), then reload the software to place this command into effect. On devices running 07.5.04 or later, you can dynamically place trunk configuration changes into effect by entering the trunk deploy command at the global CONFIG level of the CLI. The ProCurve 9408sl automatically places a trunk configuration command into effect without the trunk deploy command.

EXAMPLE:
To assign ports 1 and 2 to a trunk group, enter the following command:

```
ProCurveRS(config)# trunk switch e 1/1 to 1/2
```

A trunk group must then also be configured on the connecting Routing Switch at the other end of the trunk group. The switch parameter in this command can refer to another ProCurve Routing Switch.

If you are going to connect to a server, then enter the following command:

```
ProCurveRS(config)# trunk server e 1/1 to 1/2
```

This will connect a trunk group of ports 1 and 2 to a server.

Syntax: [no] trunk [server | switch] ethernet <primary-portnum> to <portnum>

The server | switch parameter specifies whether the trunk ports will be connected to a server or to another Routing Switch. This parameter affects the type of load balancing performed by the device. See the “Configuring Trunk Groups and Dynamic Link Aggregation” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches. The default is switch.

Each ethernet parameter introduces a port group.

The <primary-portnum> to <portnum> parameters specify the ports. The first port must be a primary port and the remaining ports must be the ports that follow it. The primary port is always the lowest number in the port range.

EXAMPLE:
To configure a trunk group consisting of two groups of ports, 1/1 – 1/4 on module 1 and 4/5 – 5/8 on module 4, enter the following commands:

```
ProCurveRS(config)# trunk ethernet 1/1 to 1/4 ethernet 4/5 to 4/8
ProCurveRS(config)# write memory
ProCurveRS(config)# trunk deploy
```

Syntax: trunk [server | switch] ethernet <primary-portnum> to <portnum> ethernet <primary-portnum> to <portnum>

The server | switch parameter specifies whether the trunk ports will be connected to a server or to another Routing Switch. This parameter affects the type of load balancing performed by the HP device. See the “Configuring Trunk Groups and Dynamic Link Aggregation” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches. The default is switch.

Each ethernet parameter introduces a port group.

The <primary-portnum> to <portnum> parameters specify a port group. Notice that each port group in this example begins with a primary port. After you enter this command, the primary port of the first port group specified (which must be the group with the lower port numbers) becomes the primary port for the entire trunk group. For Gigabit Ethernet modules, the primary ports are 1, 3, 5, and 7.
Possible values: see above
Default value: N/A

**trunk deploy**
Dynamically places trunk configuration changes into effect.

NOTE: You still need to save the trunk configuration changes to the startup-config file in order for the changes to be retained following a software reload.

NOTE: You do not need to enter this command on the ProCurve 9408sl, which automatically places the trunk configuration into effect with the **trunk ethernet** command.

**EXAMPLE:**
ProCurveRS(config)# trunk ethernet 1/1 to 1/8
ProCurveRS(config-trunk-1/1-1/8)# write memory
ProCurveRS(config-trunk-1/1-1/8)# exit
ProCurveRS(config)# trunk deploy

**Syntax:** trunk deploy

**Possible values:** N/A

**Default value:** N/A

**unknown-unicast limit**
Specifies the maximum number of unknown-unicast packets the device can forward each second. By default the device sends unknown unicasts and all other traffic at wire speed and is limited only by the capacities of the hardware. However, if other devices in the network cannot handle unlimited unknown-unicast traffic, this command allows you to relieve those devices by throttling the unknown unicasts at the HP device.

NOTE: The unknown-unicast limit does not affect broadcast or multicast traffic. However, you can use the **broadcast limit** and **multicast limit** commands to control these types of traffic. See “broadcast limit” on page 6-25 and “multicast limit” on page 6-116.

**EXAMPLE:**
ProCurveRS(config)# unknown-unicast limit 30000

**Syntax:** unknown-unicast limit <num>

**Possible values:** 0 – 4294967295; if you specify 0, limiting is disabled.

**Default value:** N/A

**username**
Configures a local user account. For each user account, you specify the user name. You also can specify the following parameters:

- A password
- The privilege level, which can be one of the following:
  - Full access (super-user). This is the default.
  - Port-configuration access
  - Read-only access

**EXAMPLE:**
To configure a user account, enter a command such as the following at the global CONFIG level of the CLI.

ProCurveRS(config)# username wanda password willy
This command adds a user account for a super-user with the user name "wanda" and the password "willy", with privilege level super-user. This user has full access to all configuration and display features.

**NOTE:** If you configure user accounts, you must add a user account for super-user access before you can add accounts for other access levels. You will need the super-user account to make further administrative changes.

```plaintext
ProCurveRS(config)# username waldo privilege 5 password staff11
```

This command adds a user account for user name "waldo", password "staff11", with privilege level read-only. Waldo can look for information but cannot make configuration changes.

**Syntax:** `[no] username <user-string> privilege <privilege-level> password | nopassword <password-string>`

The `privilege` parameter specifies the privilege-level. You can specify one of the following:

- 0 – Full access (super-user)
- 4 – Port-configuration access
- 5 – Read-only access

The default privilege level is 0. If you want to assign full access to the user account, you can enter the command without "privilege 0", as shown in the command example above.

The `password | nopassword` parameter indicates whether the user must enter a password. If you specify `password`, enter the string for the user's password.

**NOTE:** You must be logged on with super-user access (privilege level 0, or with a valid Enable password for super-user access) to add user accounts or configure other access parameters.

---

**virtual-interface-mac**

Specifies the MAC address for virtual routing interfaces.

By default, an HP device uses the MAC address of the first port (1 or 1/1) as the MAC address for all virtual routing interfaces configured on the device. You can specify a different MAC address for the virtual routing interfaces. If you specify another MAC address for the virtual routing interfaces, the address applies to all the virtual routing interfaces configured on the device.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# virtual-interface-mac aaaa.bbbb.cccc
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] virtual-interface-mac <mac-addr>`

Enter the MAC address in the following format: HHHH,HHHH,HHHH

**NOTE:** You must save the configuration and reload the software to place the change into effect.

**Possible values:** A MAC address belonging to one of the device’s ports

**Default value:** The MAC address of the first port on the device

---

**vlan**

Creates or changes the CLI focus to a port-based VLAN.

**EXAMPLE:**

```plaintext
ProCurveRS(config)# vlan 200 by port
ProCurveRS(config)# vlan 200 name Prod Marketing
```

**Syntax:** `vlan <num> by port`
**Syntax:** vlan <num> name <string>

**NOTE:** The second command is optional and also creates the VLAN if the VLAN does not already exist. You can enter the first command after you enter the second command if you first exit to the global CONFIG level of the CLI.

**Possible values:** VLAN ID 1 – 4096; VLAN name can be a string up to 16 characters. You can use blank spaces in the name if you enclose the name in double quotes (for example, “Prod Marketing”).

**Default value:** n/a

**vlan-dynamic-discovery**

Disables or re-enables dynamic discovery of protocol VLANs on switch-to-switch links. This feature enables switch-to-switch links to be automatically included in protocol VLANs that have dynamic port membership.

**EXAMPLE:**

To disable the feature, enter the following command:

`ProCurveRS(config)# no vlan-dynamic-discovery`

**Syntax:** [no] vlan-dynamic-discovery

**Possible values:** Enabled or disabled

**Default value:** Enabled

**vlan-group**

Configures a VLAN group. A VLAN group enables you to easily configure multiple VLANs that have identical parameters.

You can add a virtual interface group to each VLAN group. See “interface group-ve” on page 6-47.

**EXAMPLE:**

To configure a VLAN group, enter commands such as the following:

`ProCurveRS(config)# vlan-group 1 vlan 2 to 1000`

`ProCurveRS(config-vlan-group-1)# tagged 1/1 to 1/2`

The first command in this example begins configuration for VLAN group 1, and assigns VLANs 2 through 1000 to the group. The second command adds ports 1/1 and 1/2 as tagged ports. Since all the VLANs in the group share the ports, you must add the ports as tagged ports.

**Syntax:** vlan-group <num> vlan <vlan-id> to <vlan-id>

**Syntax:** tagged ethernet <portnum> [to <portnum> | ethernet <portnum>]

The <num> parameter with the vlan-group command specifies the VLAN group ID and can be from 1 – 32. The vlan <vlan-id> to <vlan-id> parameters specify a contiguous range (a range with no gaps) of individual VLAN IDs. Specify the low VLAN ID first and the high VLAN ID second. The command adds all the specified VLANs to the VLAN group.

**NOTE:** The device’s memory must be configured to contain at least the number of VLANs you specify for the higher end of the range. For example, if you specify 2048 as the VLAN ID at the high end of the range, you first must increase the memory allocation for VLANs to 2048 or higher. Additionally, on Routing Switches, if you allocate additional memory for VLANs, you also need to allocate the same amount of memory for virtual interfaces, before you configure the VLAN groups. This is true regardless of whether you use the virtual interface groups. The memory allocation is required because the VLAN groups and virtual interface groups have a one-to-one mapping.

If a VLAN within the range you specify is already configured, the CLI does not add the group but instead displays an error message. In this case, create the group by specifying a valid contiguous range. Then add more VLANs to the group after the CLI changes to the configuration level for the group. See the following example.
You can add and remove individual VLANs or VLAN ranges from at the VLAN group configuration level. For example, if you want to add VLANs 1001 and 1002 to VLAN group 1 and remove VLANs 900 through 1000, enter the following commands:

```
ProCurveRS(config-vlan-group-1)# add-vlan 1001 to 1002
ProCurveRS(config-vlan-group-1)# remove-vlan 900 to 1000
```

**Syntax:** add-vlan <vlan-id> [to <vlan-id>]

**Syntax:** remove-vlan <vlan-id> [to <vlan-id>]

**Possible values:** See above

**Default value:** n/a

### vlan max-vlans

Allows you to assign a set number of VLANs to be supported on a Routing Switch. This allows you to set a smaller value than the default to preserve memory on the system.

**EXAMPLE:**

```
ProCurveRS(config)# vlan max-vlans 200
```

**Syntax:** vlan max-vlans <value>

**Possible values:** 1 – 1,024

**Default value:** 32

### vlan-l3jumbo

Activates per-VLAN forwarding of jumbo packets on the device.

When you configure the MTU on a port, the port is capable of transmitting jumbo packets. However, on a tagged port, there may be a need to treat packets for one VLAN differently from packets for another VLAN. Starting with release 07.8.00, you can configure the device to forward jumbo packets based on the packets' VLAN membership. Jumbo-sized packets can be forwarded on one VLAN, while another VLAN can be restricted to forwarding standard-sized packets.

**EXAMPLE:**

```
ProCurveRS(config)# vlan-l3jumbo
```

**Syntax:** [no] vlan-l3jumbo

**Possible values:** N/A

**Default value:** Disabled

### vm boot

Changes the default boot source for a T-Flow Redundant Management Module.

**EXAMPLE:**

```
ProCurveRS(config)# vm boot secondary
ProCurveRS(config)# write memory
```

This command configures the module to boot from the secondary flash by default.

To configure the module to pause during booting to allow you to specify the boot source, enter the following command:

```
ProCurveRS(config)# vm boot interactive
```

**NOTE:** The **write memory** command saves the change to the startup-config file. You must save the configuration change for the change to remain in effect after you reboot.

**Syntax:** vm boot primary | secondary | interactive
The **primary** and **secondary** parameters specify a flash memory location. The **interactive** parameter causes the device to pause during bootup to allow you to specify the boot source for the TSPs. You must use this method if you want to boot the TSPs from a TFTP server. Otherwise, the **interactive** parameter is used for troubleshooting.

**Possible values:** See above

**Default value:** primary

### vm vm-map
Maps a forwarding module to a specific T-Flow Switching Processor (TSP) on the T-Flow Redundant Management Module.

**EXAMPLE:**
```
ProCurveRS(config)# vm vm-map slot 3 vm-slot 2 vm-cpu 1
```
This command remaps processing for the modules in slot 3 to TSP CPU 1 on the T-Flow in slot 2.

**Syntax:** `vm vm-map <from-slotnum> vm-slot <to-slotnum> vm-cpu <cpunum>`

The `<from-slotnum>` parameter specifies the slot that contains the forwarding module.

The `<to-slotnum>` parameter specifies the slot that contains the T-Flow.

The `<cpunum>` parameter specifies the TSP CPU on `<to-slotnum>` that will perform the processing. The VSM CPUs are numbered from 1 – 3.

**Possible values:** See above

**Default value:** Allocations are based on module weight and occur during software reload.

### vm vm-map per-port-dma
Configures the T-Flow to use per-DMA TSP load sharing. This command allows the T-Flow to assign DMAs to TSPs dynamically. When the device is started or reset, the T-Flow load balances processing by assigning DMAs to the TSPs according to the total bandwidth of the DMAs. See "TSP Load Sharing on a Per-DMA Basis" in the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* for more information.

**EXAMPLE:**
```
ProCurveRS(config)# vm vm-map per-port-dma
```

**Syntax:** `[no] vm vm-map per-port-dma`

**Possible values:** N/A

**Default value:** If the `vm vm-map per-port-dma` command is in the HP device’s configuration when the device is started or reset, the T-Flow uses per-DMA TSP load sharing. Otherwise, the T-Flow uses per-module TSP load sharing to balance forwarding among the TSPs.

If any ports or modules are statically assigned to TSPs, then those assignments are made prior to any dynamic assignments. You can have both per-module static assignments and per-DMA static assignments in a configuration.

### vm vm-map port-dma
Assigns ports to individual TSPs statically. Forwarding for all of the ports controlled by the specified port’s DMA are handled by the specified TSP. See "TSP Load Sharing on a Per-DMA Basis" in the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* for more information.

**EXAMPLE:**
```
ProCurveRS(config)# vm vm-map port-dma 2/1 vm-slot 1 vm-cpu 1
```
This command assigns the DMA that controls port 2/1 to TSP 1 on the T-Flow in slot 1:

**Syntax:** `[no] vm vm-map port-dma <port> vm-slot <slot> vm-cpu <tsp-cpu>`

**Possible values:**
Global CONFIG Commands

The <port> parameter is one of the ports controlled by the DMA that you want to assign to a TSP. To assign a DMA to a TSP, you specify any of the ports controlled by the DMA as the <port> parameter. Forwarding for all of the ports controlled by the DMA is then handled by the specified TSP.

The <slot> parameter specifies the slot that contains the T-Flow.

The <tsp-cpu> parameter specifies the TSP CPU on <slot> that will perform the processing. The VSM CPUs are numbered from 1 – 3.

**Default value:** Allocations are based on module weight and occur during software reload.

**web access-group**

Specifies an ACL that restricts Web management access to management functions on the device.

**EXAMPLE:**

To configure an ACL that restricts Web management access the device:

```
ProCurveRS(config)# access-list 12 deny host 209.157.22.98 log
ProCurveRS(config)# access-list 12 deny 209.157.23.0 0.0.0.255 log
ProCurveRS(config)# access-list 12 deny 209.157.24.0/24 log
ProCurveRS(config)# access-list 12 permit any
ProCurveRS(config)# web access-group 12
ProCurveRS(config)# write memory
```

**Syntax:** `web access-group <num>`

The <num> parameter specifies the number of a standard ACL and must be from 1 – 99.

These commands configure ACL 12, then apply the ACL as the access list for Web management access. The device denies Web management access from the IP addresses listed in ACL 12 and permits Web management access from all other IP addresses. Without the last ACL entry for permitting all packets, this ACL would deny Web management access from all IP addresses.

**Possible values:** see above

**Default value:** N/A

**web-client**

Restricts Web management access to the HP device to the host whose IP address you specify. No other device except the one with the specified IP address can access the HP device’s Web management interface.

If you want to restrict access from SNMP or Telnet, use one or two of the following commands:

- **snmp-client** – restricts SNMP access. See “snmp-client” on page 6-139.
- **telnet-client** – restricts Telnet access to the CLI. See “telnet-client” on page 6-160.

If you want to restrict all management access, you can use the commands above and the **web-client** command or you can use the following command: **all-client**. See “all-client” on page 6-19.

**EXAMPLE:**

To restrict Web access to the HP device to the host with IP address 209.157.22.26, enter the following command:

```
ProCurveRS(config)# web-client 209.157.22.26
```

**Syntax:** `[no] web-client <ip-addr>`

**Possible values:** a valid IP address. You can enter one IP address with the command. You can use the command up to ten times for up to ten IP addresses.

**Default value:** N/A

**web-management**

Sets configuration options on the Web management interface. By default the Web management interface is enabled.
EXAMPLE:
To disable the Web management interface on an HP device, enter the following:

```
ProCurveRS(config)# no web-management
```

You can also enter the following command:

```
ProCurveRS(config)# web-management tcp-port 168
```

Syntax: `[no] web-management [allow-no-password | enable [vlan <vlan-id>] | front-panel | hp-top-tools | list-menu] [tcp-port <port-number>]`

Possible values:
The `allow-no-password` option disables password authentication for the Web management interface.
The `enable` option enables the Web management interface on the HP device.
The `front-panel` option causes the front panel frame, which contains a graphic depicting the Routing Switch, to be displayed on the Web management interface.
The `hp-top-tools` parameter disables TCP port 280. By default, TCP ports 80 and 280 are enabled on the HP device. TCP port 80 (HTTP) allows access to the device’s Web management interface. TCP port 280 allows access to the device by ProCurve Manager.
The `list-menu` option causes the List (pre-06.0.00) menu to be displayed on the Web management interface, instead of the Tree menu.
The `tcp-port`, `port-number` option specifies the port to be used to access the device’s Web management interface.

Default value: Password authentication and the front panel are enabled by default. The List menu is disabled by default. (This means the Tree menu is enabled by default.)

web-management enable vlan

Allows Web management access only to clients in a specific VLAN.

EXAMPLE:
The following example configures the device to allow Web management access only to clients connected to ports within port-based VLAN 10. Clients connected to ports that are not in VLAN 10 are denied management access.

```
ProCurveRS(config)# web-management enable vlan 10
```

Syntax: `[no] web-management enable vlan <vlan-id>`

Possible values: N/A

Default value: N/A

web-management https

Enables the SSL server on the HP device for Web management.

Starting with release 07.8.00, HP devices support Secure Sockets Layer (SSL) for configuring the device using the Web Management interface. When enabled, the SSL protocol uses digital certificates and public-private key pairs to establish a secure connection to the HP device. Digital certificates serve to prove the identity of a connecting client, and public-private key pairs provide a means to encrypt data sent between the device and the client.

EXAMPLE:
To enable the SSL server on the HP device, enter the following command:

```
ProCurveRS(config)# web-management https
```

Syntax: `[no] web-management http | https`

You can enable either the HTTP or HTTPS servers with this command. You can disable both the HTTP and HTTPS servers by entering the following command:

```
ProCurveRS(config)# no web-management
```
**Syntax:** no web-management  
**Possible values:** See above  
**Default value:** N/A

**write memory**  
Saves the running configuration into the startup-config file.  
**EXAMPLE:**  
ProCurveRS(config)# write memory  
**Syntax:** write memory  
**Possible values:** N/A  
**Default value:** N/A

**write terminal**  
Displays the running configuration of the HP device on the terminal screen. In software releases 07.6.04 and later, this command also displays the size of the running-config file.  
**NOTE:** This command is equivalent to the **show running-config** command.  
**EXAMPLE:**  
ProCurveRS(config)# write terminal  
**Syntax:** write terminal  
**Possible values:** N/A  
**Default value:** N/A