This chapter describes the Internet Protocol (IP) parameters on ProCurve Routing Switches and how to configure them. After you add IP addresses and configure other IP parameters, see the following chapters for configuration information for the IP routing protocols:

- “Configuring RIP” on page 10-1
- “Configuring OSPF” on page 12-1
- “Configuring BGP4” on page 13-1

To configure and monitor IP, see the following sections:

- “Basic IP Parameters and Defaults” on page 9-8
- “The following sections describe how to configure IP parameters. Some parameters can be configured globally while others can be configured on individual interfaces. Some parameters can be configured globally and overridden for individual interfaces.” on page 9-15
- “Displaying IP Configuration Information and Statistics” on page 9-80

**Basic Configuration**

IP is enabled by default. Basic configuration consists of adding IP addresses and enabling a route exchange protocol, such as Routing Information Protocol (RIP).

- See “Configuring IP Addresses” on page 9-15 to add IP addresses, then see one or more of the following to enable and configure the route exchange protocols:
  - “Configuring RIP” on page 10-1
  - “Configuring OSPF” on page 12-1
  - “Configuring BGP4” on page 13-1

The rest of this chapter describes IP and how to configure it in more detail. Use the information in this chapter if you need to change some of the IP parameters from their default values or you want to view configuration information or statistics.

**Overview**

ProCurve 9300 series Routing Switches support Internet Protocol (IP) version 4. IP support on ProCurve Routing Switches includes all of the following, in addition to a highly configurable implementation of basic IP services...
including Address Resolution Protocol (ARP), ICMP Router Discovery Protocol (IRDP), and Reverse ARP (RARP):

- Route exchange protocols
  - Routing Information Protocol (RIP)
  - Open Shortest Path First (OSPF)
  - Border Gateway Protocol version 4 (BGP4)
- Multicast protocols (9300 series only)
  - Internet Group Membership Protocol (IGMP)
  - Protocol Independent Multicast Dense (PIM-DM)
  - Protocol Independent Multicast Sparse (PIM-SM)
  - Distance Vector Multicast Routing Protocol (DVMRP)
- Router redundancy protocols
  - Virtual Router Redundancy Protocol Extended (VRRPE) (9300 series only)
  - Virtual Router Redundancy Protocol (VRRP)

**IP Interfaces**

ProCurve Routing Switches allow you to configure IP addresses. IP addresses are associated with individual interfaces.

All ProCurve Routing Switches support configuration and display of IP address in classical sub-net format (example: 192.168.1.1 255.255.255.0) and Classless Interdomain Routing (CIDR) format (example: 192.168.1.1/24). You can use either format when configuring IP address information. IP addresses are displayed in classical sub-net format by default but you can change the display format to CIDR. See “Changing the Network Mask Display to Prefix Format” on page 9-80.

ProCurve Routing Switches allow you to configure IP addresses on the following types of interfaces:

- Ethernet ports
- Virtual routing interfaces (used by VLANs to route among one another)
- Loopback interfaces

Each IP address on a Routing Switch must be in a different sub-net. You can have only one interface that is in a given sub-net. For example, you can configure IP addresses 192.168.1.1/24 and 192.168.2.1/24 on the same Routing Switch, but you cannot configure 192.168.1.1/24 and 192.168.1.2/24 on the same Routing Switch.

You can configure multiple IP addresses on the same interface.

The number of IP addresses you can configure on an individual interface depends on the Routing Switch model. To display the maximum number of IP addresses and other system parameters you can configure on a Routing Switch, see the “Displaying and Modifying System Parameter Default Settings” section in the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* or the *Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch*.

You can use any of the IP addresses you configure on the Routing Switch for Telnet, Web management, or SNMP access.

**IP Packet Flow Through a Routing Switch**

Figure 9.1 shows how an IP packet moves through a ProCurve Routing Switch.
Figure 9.1 shows the following packet flow:

1. When the Routing Switch receives an IP packet, the Routing Switch checks for filters on the receiving interface. If a deny filter on the interface denies the packet, the Routing Switch discards the packet and performs no further processing, except generating a Syslog entry and SNMP message, if logging is enabled for the filter.

2. If the packet is not denied at the incoming interface, the Routing Switch looks in the session table for an entry that has the same source IP address and TCP or UDP port as the packet. If the session table contains a matching entry, the Routing Switch immediately forwards the packet, by addressing it to the destination IP address and TCP or UDP port listed in the session table entry and sending the packet to a queue on the outgoing port(s) listed in the session table. The Routing Switch selects the queue based on the Quality of Service (QoS) level associated with the session table entry.

3. If the session table does not contain an entry that matches the packet's source address and TCP or UDP port, the Routing Switch looks in the IP forwarding cache for an entry that matches the packet's destination IP address. If the forwarding cache contains a matching entry, the Routing Switch forwards the packet to the IP address in the entry. The Routing Switch sends the packet to a queue on the outgoing port(s) listed in the forwarding cache. The Routing Switch selects the queue based on the Quality of Service (QoS) level associated with the forwarding cache entry.

1. The filter can be an Access Control List (ACL) or an IP access policy.
4. If the IP forwarding cache does not have an entry for the packet, the Routing Switch checks the IP route table for a route to the packet's destination. If the IP route table has a route, the Routing Switch makes an entry in the session table or the forwarding cache, and sends the route to a queue on the outgoing port(s).

   • If the running-config contains a Policy-Based Routing (PBR) definition or an IP access policy for the packet, the software makes an entry in the session table. The Routing Switch uses the new session table entry to forward subsequent packets from the same source to the same destination.

   • If the running-config does not contain a PBR definition or an IP access policy for the packet, the software creates a new entry in the forwarding cache. The Routing Switch uses the new cache entry to forward subsequent packets to the same destination.

The following sections describe the IP tables and caches:

• ARP cache and static ARP table
• IP route table
• IP forwarding cache
• IP session table

The software enables you to display these tables. You also can change the capacity of the tables on an individual basis if needed by changing the memory allocation for the table.

**ARP Cache and Static ARP Table**

The ARP cache contains entries that map IP addresses to MAC addresses. Generally, the entries are for devices that are directly attached to the Routing Switch.

An exception is an ARP entry for an interface-based static IP route that goes to a destination that is one or more router hops away. For this type of entry, the MAC address is either the destination device's MAC address or the MAC address of the router interface that answered an ARP request on behalf of the device, using proxy ARP.

**ARP Cache**

The ARP cache can contain dynamic (learned) entries and static (user-configured) entries. The software places a dynamic entry in the ARP cache when the Routing Switch learns a device's MAC address from an ARP request or ARP reply from the device.

The software can learn an entry when the Routing Switch receives an ARP request from another IP forwarding device or an ARP reply. Here is an example of a dynamic entry:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Age</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>207.95.6.102</td>
<td>0800.5afc.ea21</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>

Each entry contains the destination device's IP address and MAC address.

**Static ARP Table**

In addition to the ARP cache, Routing Switches have a static ARP table. Entries in the static ARP table are user-configured. You can add entries to the static ARP table regardless of whether the device the entry is for is connected to the Routing Switch.

The software places an entry from the static ARP table into the ARP cache when the entry's interface comes up.

Here is an example of a static ARP entry:

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>207.95.6.111</td>
<td>0800.093b.d210</td>
<td>1/1</td>
</tr>
</tbody>
</table>

Each entry lists the information you specified when you created the entry.

To display ARP entries, see the following:

• “Displaying the ARP Cache” on page 9-88
• “Displaying the Static ARP Table” on page 9-90
To configure other ARP parameters, see the following:

- “Configuring ARP Parameters” on page 9-29

To increase the size of the ARP cache and static ARP table, see the following:

- For dynamic entries, see the “Displaying and Modifying System Parameter Default Settings” section in the “Configuring Basic Features” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches or the Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch. The ip-arp parameter controls the ARP cache size.

- Static entries, “Changing the Maximum Number of Entries the Static ARP Table Can Hold” on page 9-33. The ip-static-arp parameter controls the static ARP table size.

### IP Route Table

The IP route table contains paths to IP destinations. The IP route table can receive the paths from the following sources:

- A directly-connected destination, which means there are no router hops to the destination
- A static IP route, which is a user-configured route
- A route learned through RIP
- A route learned through OSPF
- A route learned through BGP4

The IP route table contains the best path to a destination.

- When the software receives paths from more than one of the sources listed above, the software compares the administrative distance of each path and selects the path with the lowest administrative distance. The administrative distance is a protocol-independent value from 1 – 255.
- When the software receives two or more best paths from the same source and the paths have the same metric (cost), the software can load share traffic among the paths based on destination host or network address (based on the configuration and the Routing Switch model).

Here is an example of an entry in the IP route table:

<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>1.1.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
</tbody>
</table>

Each IP route table entry contains the destination’s IP address and sub-net mask and the IP address of the next-hop router interface to the destination. Each entry also indicates the port attached to the destination or the next-hop to the destination, the route’s IP metric (cost), and the type. The type indicates how the IP route table received the route.

To display the IP route table, see the following:

- “Displaying the IP Route Table” on page 9-93

To configure a static IP route, see the following:

- “Configuring Static Routes” on page 9-39

To clear a route from the IP route table, see the following:

- “Clearing IP Routes” on page 9-96

To increase the size of the IP route table for learned and static routes, see the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches or the Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch.

- For learned routes, modify the ip-route parameter.
• For static routes, modify the ip-static-route parameter.

**IP Forwarding Cache**

The IP forwarding cache provides a fast-path mechanism for forwarding IP packets. The cache contains entries for IP destinations. When an ProCurve Routing Switch has completed processing and addressing for a packet and is ready to forward the packet, the device checks the IP forwarding cache for an entry to the packet’s destination.

• If the cache contains an entry with the destination IP address, the device uses the information in the entry to forward the packet out the ports listed in the entry. The destination IP address is the address of the packet’s final destination. The port numbers are the ports through which the destination can be reached.

• If the cache does not contain an entry and the traffic does not qualify for an entry in the session table instead, the software can create an entry in the forwarding cache.

Each entry in the IP forwarding cache has an age timer. If the entry remains unused for ten minutes, the software removes the entry. The age timer is not configurable.

Here is an example of an entry in the IP forwarding cache:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Next Hop</th>
<th>MAC Type</th>
<th>Port</th>
<th>VLAN</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.11</td>
<td>DIRECT</td>
<td>0000.0000.0000</td>
<td>PU</td>
<td>n/a</td>
<td>0</td>
</tr>
</tbody>
</table>

Each IP forwarding cache entry contains the IP address of the destination, and the IP address and MAC address of the next-hop router interface to the destination. If the destination is actually an interface configured on the Routing Switch itself, as shown here, then next-hop information indicates this. The port through which the destination is reached is also listed, as well as the VLAN and Layer 4 QoS priority associated with the destination if applicable.

To display the IP forwarding cache, see “Displaying the Forwarding Cache” on page 9-91.

**NOTE:** You cannot add static entries to the IP forwarding cache, although Chassis Routing Switches do have options to optimize the cache and increase the number of entries the cache can contain. See “Optimizing the IP Forwarding Cache” on page 9-63 and the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* or the *Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch*.

To increase the size of the IP forwarding cache, see the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* or the *Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch*. The ip-cache parameter controls the size of the IP forwarding cache.

**Layer 4 Session Table**

The Layer 4 session provides a fast path for forwarding packets. A session is an entry that contains complete Layer 3 and Layer 4 information for a flow of traffic. Layer 3 information includes the source and destination IP addresses. Layer 4 information includes the source and destination TCP and UDP ports. For comparison, the IP forwarding cache contains the Layer 3 destination address but does not contain the other source and destination address information of a Layer 4 session table entry.

The Routing Switch selects the session table instead of the IP forwarding table for fast-path forwarding for the following features:

• Policy-Based Routing (PBR)

• Layer 4 Quality-of-Service (QoS) policies

• IP access policies

To increase the size of the session table, see the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve*.
9300 Series Routing Switches or the Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch. The ip-qos-session parameter controls the size of the session table.

**IP Route Exchange Protocols**
ProCurve Routing Switches support the following IP route exchange protocols:

- Routing Information Protocol (RIP)
- Open Shortest Path First (OSPF)
- Border Gateway Protocol version 4 (BGP4)

All these protocols provide routes to the IP route table. You can use one or more of these protocols, in any combination. The protocols are disabled by default. For configuration information, see the following:

- “Configuring RIP” on page 10-1
- “Configuring OSPF” on page 12-1
- “Configuring BGP4” on page 13-1

**IP Multicast Protocols**
ProCurve Routing Switches also support the following Internet Group Membership Protocol (IGMP) based IP multicast protocols:

- Protocol Independent Multicast – Dense mode (PIM-DM)
- Protocol Independent Multicast – Sparse mode (PIM-SM)
- Distance Vector Multicast Routing Protocol (DVMRP)

For configuration information, see “Configuring IP Multicast Protocols (9300 Series Only)” on page 11-1.

**IP Interface Redundancy Protocols**
You can configure a ProCurve Routing Switch to back up an IP interface configured on another ProCurve Routing Switch. If the link for the backed up interface becomes unavailable, the other Routing Switch can continue service for the interface. This feature is especially useful for providing a backup to a network's default gateway.

ProCurve Routing Switches support the following IP interface redundancy protocols:

- Virtual Router Redundancy Protocol (VRRP) – A standard router redundancy protocol based on RFC 2338. You can use VRRP to configure ProCurve Routing Switches and third-party routers to back up IP interfaces on other ProCurve Routing Switches or third-party routers.
- Virtual Router Redundancy Protocol Extended (VRRPE) – An HP extension to standard VRRP that adds additional features and overcomes limitations in standard VRRP. You can use VRRPE only on ProCurve Routing Switches.

For configuration information, see the following:

- Virtual Router Redundancy Protocol Extended (VRRPE) – see “Configuring VRRP and VRRPE” on page 16-1.
- Virtual Router Redundancy Protocol (VRRP) – see “Configuring VRRP and VRRPE” on page 16-1.

**Network Address Translation (9300 Series Only)**
HP’s Chassis Routing Switches support Network Address Translation (NAT). NAT enables private IP networks that use nonregistered IP addresses to connect to the Internet. Configure NAT on a ProCurve Routing Switch that is placed at the border of an inside network and an outside network (such as the Internet). NAT translates the internal local addresses to globally unique IP addresses before sending packets to the outside network.

For configuration information, see “Network Address Translation (9300 Series Only)” on page 15-1.
Access Control Lists and IP Access Policies

ProCurve Routing Switches provide two mechanisms for filtering IP traffic:

- Access Control Lists (ACLs)
- IP access policies

Both methods allow you to filter packets based on Layer 3 and Layer 4 source and destination information.

ACLs also provide great flexibility by providing the input to various other filtering mechanisms such as route maps, which are used by BGP4. ACLs also provide the input for Policy-Based Routing (PBR), which allows you to selectively modify and route IP packets based on their source IP address.

IP access policies allow you to configure QoS based on sessions (Layer 4 traffic flows).

Only one of these filtering mechanisms can be enabled on an HP device at a time. HP devices can store forwarding information for both methods of filtering in the session table.

For configuration information, see the following:

- “Software-Based IP Access Control Lists (ACLs)” on page 4-1
- “Policies and Filters” on page B-1

Basic IP Parameters and Defaults

IP is enabled by default. The following IP-based protocols are all disabled by default:

- Routing protocols
  - Routing Information Protocol (RIP) – see “Configuring RIP” on page 10-1
  - Open Shortest Path First (OSPF) – see “Configuring OSPF” on page 12-1
  - Border Gateway Protocol version 4 (BGP4) – see “Configuring BGP4” on page 13-1
- Multicast protocols
  - Internet Group Membership Protocol (IGMP) – see “Changing Global IP Multicast Parameters” on page 11-2
  - Protocol Independent Multicast Dense (PIM-DM) – see “PIM Dense” on page 11-11
  - Protocol Independent Multicast Sparse (PIM-SM) – see “PIM Sparse” on page 11-22
  - Distance Vector Multicast Routing Protocol (DVMRP) – see “DVMRP Overview” on page 11-62
- Router redundancy protocols
  - Virtual Router Redundancy Protocol Extended (VRRPE) – see “Configuring VRRP and VRRPE” on page 16-1.
  - Virtual Router Redundancy Protocol (VRRP) – see “Configuring VRRP and VRRPE” on page 16-1.

The following tables list the Routing Switch IP parameters, their default values, and where to find configuration information.

**NOTE:** For information about parameters in other protocols based on IP, such as RIP, OSPF, and so on, see the configuration chapters for those protocols.

**When Parameter Changes Take Effect**

Most IP parameters described in this chapter are dynamic. They take effect immediately, as soon as you enter the CLI command or select the Web management interface option. You can verify that a dynamic change has taken effect by displaying the running-config. To display the running-config, enter the `show running-config` or `write terminal` command at any CLI prompt. (You cannot display the running-config from the Web management interface.)
To save a configuration change permanently so that the change remains in effect following a system reset or software reload, save the change to the startup-config file.

- To save configuration changes to the startup-config file, enter the `write memory` command from the Privileged EXEC level of any configuration level of the CLI.

- To save the configuration changes using the Web management interface, select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory. You also can access the dialog for saving configuration changes by clicking on Command in the tree view, then clicking on Save to Flash.

Changes to memory allocation require you to reload the software after you save the changes to the startup-config file. When reloading the software is required to complete a configuration change described in this chapter, the procedure that describes the configuration change includes a step for reloading the software.

**IP Global Parameters**

Table 9.1 lists the IP global parameters for Routing Switches.

### Table 9.1: IP Global Parameters

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP state</strong></td>
<td>The Internet Protocol, version 4</td>
<td>Enabled</td>
<td>n/a</td>
</tr>
<tr>
<td><strong>Note</strong>: You cannot disable IP.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>IP address and mask notation</strong></td>
<td>Format for displaying an IP address and its network mask information. You can enable one of the following:</td>
<td>Class-based</td>
<td>9-80</td>
</tr>
<tr>
<td><strong>Note</strong>: Changing this parameter affects the display of IP addresses, but you can enter addresses in either format regardless of the display setting.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Class-based format; example: 192.168.1.1 255.255.255.0</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• Classless Interdomain Routing (CIDR) format; example: 192.168.1.1/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Router ID</strong></td>
<td>The value that routers use to identify themselves to other routers when exchanging route information. OSPF and BGP4 use router IDs to identify routers. RIP does not use the router ID.</td>
<td>The IP address configured on the lowest-numbered loopback interface. If no loopback interface is configured, then the lowest-numbered IP address configured on the device.</td>
<td>9-26</td>
</tr>
<tr>
<td><strong>Maximum Transmission Unit (MTU)</strong></td>
<td>The maximum length an Ethernet packet can be without being fragmented.</td>
<td>1500 bytes for Ethernet II encapsulation 1492 bytes for SNAP encapsulation</td>
<td>9-22</td>
</tr>
</tbody>
</table>
### Table 9.1: IP Global Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Address Resolution Protocol (ARP)</strong></td>
<td>A standard IP mechanism that routers use to learn the Media Access Control (MAC) address of a device on the network. The router sends the IP address of a device in the ARP request and receives the device's MAC address in an ARP reply.</td>
<td>Enabled</td>
<td>9-29</td>
</tr>
<tr>
<td><strong>ARP rate limiting</strong></td>
<td>Lets you specify a maximum number of ARP packets the device will accept each second. If the device receives more ARP packets than you specify, the device drops additional ARP packets for the remainder of the one-second interval.</td>
<td>Disabled</td>
<td>9-30</td>
</tr>
<tr>
<td><strong>ARP age</strong></td>
<td>The amount of time the device keeps a MAC address learned through ARP in the device's ARP cache. The device resets the timer to zero each time the ARP entry is refreshed and removes the entry if the timer reaches the ARP age. <strong>Note</strong>: You also can change the ARP age on an individual interface basis. See Table 9.2 on page 9-14.</td>
<td>Ten minutes</td>
<td>9-31</td>
</tr>
<tr>
<td><strong>Proxy ARP</strong></td>
<td>An IP mechanism a router can use to answer an ARP request on behalf of a host, by replying with the router's own MAC address instead of the host's.</td>
<td>Disabled</td>
<td>9-31</td>
</tr>
<tr>
<td><strong>Static ARP entries</strong></td>
<td>An ARP entry you place in the static ARP table. Static entries do not age out.</td>
<td>No entries</td>
<td>9-32</td>
</tr>
<tr>
<td><strong>Time to Live (TTL)</strong></td>
<td>The maximum number of routers (hops) through which a packet can pass before being discarded. Each router decreases a packet's TTL by 1 before forwarding the packet. If decreasing the TTL causes the TTL to be 0, the router drops the packet instead of forwarding it.</td>
<td>64 hops</td>
<td>9-35</td>
</tr>
<tr>
<td><strong>Directed broadcast forwarding</strong></td>
<td>A directed broadcast is a packet containing all ones (or in some cases, all zeros) in the host portion of the destination IP address. When a router forwards such a broadcast, it sends a copy of the packet out each of its enabled IP interfaces. <strong>Note</strong>: You also can enable or disable this parameter on an individual interface basis. See Table 9.2 on page 9-14.</td>
<td>Disabled</td>
<td>9-35</td>
</tr>
</tbody>
</table>
| **Directed broadcast mode**      | The packet format the router treats as a directed broadcast. The following formats can be directed broadcast:  
  - All ones in the host portion of the packet's destination address.  
  - All zeroes in the host portion of the packet's destination address.  
  **Note**: If you enable all-zeroes directed broadcasts, all-ones directed broadcasts remain enabled. | All ones  | 9-37        |
### Table 9.1: IP Global Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Source-routed packet forwarding</td>
<td>A source-routed packet contains a list of IP addresses through which the packet must pass to reach its destination.</td>
<td>Enabled</td>
<td>9-36</td>
</tr>
</tbody>
</table>
| Internet Control Message Protocol (ICMP) messages | The ProCurve Routing Switch can send the following types of ICMP messages:  
  • Echo messages (ping messages)  
  • Destination Unreachable messages  
  • Redirect messages  
  **Note**: You also can enable or disable ICMP Redirect messages on an individual interface basis. See Table 9.2 on page 9-14. | Enabled          | 9-37, 9-39 |
| ICMP Router Discovery Protocol (IRDP)          | An IP protocol a router can use to advertise the IP addresses of its router interfaces to directly attached hosts. You can enable or disable the protocol, and change the following protocol parameters:  
  • Forwarding method (broadcast or multicast)  
  • Hold time  
  • Maximum advertisement interval  
  • Minimum advertisement interval  
  • Router preference level  
  **Note**: You also can enable or disable IRDP and configure the parameters on an individual interface basis. See Table 9.2 on page 9-14. | Disabled         | 9-70        |
| Reverse ARP (RARP)                             | An IP mechanism a host can use to request an IP address from a directly attached router when the host boots. | Enabled          | 9-72        |
| Static RARP entries                            | An IP address you place in the RARP table for RARP requests from hosts.  
  **Note**: You must enter the RARP entries manually. The Routing Switch does not have a mechanism for learning or dynamically generating RARP entries. | No entries       | 9-73        |
<p>| Maximum BootP relay hops                       | The maximum number of hops away a BootP server can be located from a router and still be used by the router’s clients for network booting. | Four             | 9-79        |
| Domain name for Domain Name Server (DNS) resolver | A domain name (example: hp.router.com) you can use in place of an IP address for certain operations such as IP pings, trace routes, and Telnet management connections to the router. | None configured  | 9-19        |
| DNS default gateway addresses                  | A list of gateways attached to the router through which clients attached to the router can reach DNSs. | None configured  | 9-19        |</p>
<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP unicast cache performance mode</td>
<td>The amount of available IP cache that is set aside for IP unicast entries. When the router caches unicast forwarding entries, the cached entries provide an optimal path through the router because the router CPU does not need to process the packets for forwarding. Once a packet is processed, the forwarding information is placed in the cache for reuse. ProCurve Routing Switches provide an optional high-performance mode for allocating additional cache space for unicast forwarding entries. Use this option when the router is handling a very large number of unicast flows (source plus destination pairs) and you want to ensure that more flows can remain in the cache at one time.</td>
<td>High-performance mode enabled</td>
<td>9-64</td>
</tr>
<tr>
<td>IP load sharing</td>
<td>An HP feature that enables the router to balance traffic to a specific destination across multiple equal-cost paths. Load sharing uses a simple round-robin mechanism and is based on destination address. <strong>Note</strong>: Load sharing is sometimes called Equal Cost Multi Path (ECMP).</td>
<td>Enabled</td>
<td>9-51</td>
</tr>
<tr>
<td>IP load sharing aggregation</td>
<td>A feature that increases the capacity of the load sharing cache by aggregating destination addresses into networks. When IP load sharing aggregation is enabled, each cache entry is an aggregate network for multiple destination hosts. If IP load sharing aggregation not enabled, the device creates a separate load sharing cache entry for each destination host address.</td>
<td>Aggregated by network</td>
<td>9-61</td>
</tr>
<tr>
<td>Maximum IP load sharing paths</td>
<td>The maximum number of equal-cost paths across which the Routing Switch is allowed to distribute traffic.</td>
<td>Four</td>
<td>9-62</td>
</tr>
<tr>
<td>CAM programming</td>
<td>Whether the device programs separate route entries into the CAM for individual route destinations or programs single aggregate entries for multiple destinations.</td>
<td>Separate entries are programmed for each destination</td>
<td>9-63</td>
</tr>
<tr>
<td>Origination of default routes</td>
<td>You can enable a router to originate default routes for the following route exchange protocols, on an individual protocol basis: • RIP • OSPF • BGP4</td>
<td>Disabled</td>
<td>10-11, 12-39, 13-32</td>
</tr>
</tbody>
</table>
### Table 9.1: IP Global Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Default network route</td>
<td>The router uses the default network route if the IP route table does not contain a route to the destination and also does not contain an explicit default route (0.0.0.0 0.0.0.0 or 0.0.0.0/0).</td>
<td>None configured</td>
<td>9-49</td>
</tr>
<tr>
<td>Static route</td>
<td>An IP route you place in the IP route table.</td>
<td>No entries</td>
<td>9-39</td>
</tr>
</tbody>
</table>
| Source interface     | The IP address the router uses as the source address for Telnet, RADIUS, or TACACS/TACACS+ packets originated by the router. The router can select the source address based on either of the following:  
  • The lowest-numbered IP address on the interface the packet is sent on.  
  • The lowest-numbered IP address on a specific interface. The address is used as the source for all packets of the specified type regardless of interface the packet is sent on. | The lowest-numbered IP address on the interface the packet is sent on. | 9-27        |
## IP Interface Parameters

Table 9.2 lists the interface-level IP parameters for Routing Switches.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP state</td>
<td>The Internet Protocol, version 4</td>
<td>Enabled</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> You cannot disable IP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>A Layer 3 network interface address</td>
<td>None configured¹</td>
<td>9-15</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> a single IP address used for management access to the entire device. Routing Switches have separate IP addresses on individual interfaces.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Encapsulation type</td>
<td>The format of the packets in which the router encapsulates IP datagrams. The encapsulation format can be one of the following:</td>
<td>Ethernet II</td>
<td>9-21</td>
</tr>
<tr>
<td></td>
<td>• Ethernet II</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>• SNAP</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Maximum Transmission Unit (MTU)</td>
<td>The maximum length (number of bytes) of an encapsulated IP datagram the router can forward.</td>
<td>1500 for Ethernet II encapsulated packets</td>
<td>9-23</td>
</tr>
<tr>
<td></td>
<td>1492 for SNAP encapsulated packets</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP age</td>
<td>Locally overrides the global setting. See Table 9.1 on page 9-9.</td>
<td>Ten minutes</td>
<td>9-31</td>
</tr>
<tr>
<td>Metric</td>
<td>A numeric cost the router adds to RIP routes learned on the interface. This parameter applies only to RIP routes.</td>
<td>1 (one)</td>
<td>10-4</td>
</tr>
<tr>
<td>Directed broadcast forwarding</td>
<td>Locally overrides the global setting. See Table 9.1 on page 9-9.</td>
<td>Disabled</td>
<td>9-35</td>
</tr>
<tr>
<td>ICMP Router Discovery Protocol (IRDP)</td>
<td>Locally overrides the global IRDP settings. See Table 9.1 on page 9-9.</td>
<td>Disabled</td>
<td>9-71</td>
</tr>
<tr>
<td>ICMP Redirect messages</td>
<td>Locally overrides the global setting. See Table 9.1 on page 9-9.</td>
<td>Enabled</td>
<td>9-39</td>
</tr>
</tbody>
</table>
Table 9.2: IP Interface Parameters (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>DHCP gateway stamp</td>
<td>The router can assist DHCP/BootP Discovery packets from one sub-net to reach DHCP/BootP servers on a different sub-net by placing the IP address of the router interface that receives the request in the request packet's Gateway field. You can override the default and specify the IP address to use for the Gateway field in the packets. <strong>Note:</strong> UDP broadcast forwarding for client DHCP/BootP requests (bootpc) must be enabled and you must configure an IP helper address (the server's IP address or a directed broadcast to the server's sub-net) on the port connected to the client.</td>
<td>The lowest-numbered IP address on the interface that receives the request</td>
<td>9-79</td>
</tr>
<tr>
<td>UDP broadcast forwarding</td>
<td>The router can forward UDP broadcast packets for UDP applications such as BootP. By forwarding the UDP broadcasts, the router enables clients on one sub-net to find servers attached to other sub-nets. <strong>Note:</strong> To completely enable a client's UDP application request to find a server on another sub-net, you must configure an IP helper address consisting of the server's IP address or the directed broadcast address for the sub-net that contains the server. See the next row.</td>
<td>The router helps forward broadcasts for the following UDP application protocols: • bootps • dns • netbios-dgm • netbios-ns • tacs • tftp • time</td>
<td>9-75</td>
</tr>
<tr>
<td>IP helper address</td>
<td>The IP address of a UDP application server (such as a BootP or DHCP server) or a directed broadcast address. IP helper addresses allow the router to forward requests for certain UDP applications from a client on one sub-net to a server on another sub-net.</td>
<td>None configured</td>
<td>9-76</td>
</tr>
</tbody>
</table>

1. Some devices have a factory default, such as 209.157.22.154, used for troubleshooting during installation. For Routing Switches, the address is on module 1 port 1 (or 1/1).

### Configuring IP Parameters – Routing Switches

The following sections describe how to configure IP parameters. Some parameters can be configured globally while others can be configured on individual interfaces. Some parameters can be configured globally and overridden for individual interfaces.

### Configuring IP Addresses

You can configure an IP address on the following types of Routing Switch interfaces:

- Ethernet port
- Virtual routing interface (also called a Virtual Ethernet or “VE”)
- Loopback interface
By default, you can configure up to 24 IP addresses on each interface. On Routing Switches, you can increase this amount to up to 64 IP sub-net addresses per port by increasing the size of the subnet-per-interface table. See the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches or the Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch.

NOTE: Once you configure a virtual routing interface on a VLAN, you cannot configure Layer 3 interface parameters on individual ports in the VLAN. Instead, you must configure the parameters on the virtual routing interface itself.

HP devices support both classical IP network masks (Class A, B, and C sub-net masks, and so on) and Classless Interdomain Routing (CIDR) network prefix masks.

- To enter a classical network mask, enter the mask in IP address format. For example, enter "209.157.22.99 255.255.255.0" for an IP address with a Class-C sub-net mask.
- To enter a prefix network mask, enter a forward slash (/) and the number of bits in the mask immediately after the IP address. For example, enter "209.157.22.99/24" for an IP address that has a network mask with 24 significant bits (ones).

By default, the CLI displays network masks in classical IP address format (example: 255.255.255.0). You can change the display to prefix format. See “Changing the Network Mask Display to Prefix Format” on page 9-80.

### Assigning an IP Address to an Ethernet Port

To assign an IP address to an Ethernet port, use either of the following methods.

**USING THE CLI**

To assign an IP address to port 1/1, enter the following commands:

```bash
ProCurveRS(config)# interface ethernet 1/1
ProCurveRS(config-if-1/1)# ip address 192.45.6.1 255.255.255.0
```

**Syntax:** `[no] ip address <ip-addr> <ip-mask> [ospf-ignore | ospf-passive | secondary]`  

or

**Syntax:** `[no] ip address <ip-addr>/<mask-bits> [ospf-ignore | ospf-passive | secondary]`

The `ospf-ignore` and `ospf-passive` parameters modify the Routing Switch defaults for adjacency formation and interface advertisement. Use one of these parameters if you are configuring multiple IP sub-net addresses on the interface but you want to prevent OSPF from running on some of the sub-nets.

- `ospf-passive` – This option disables adjacency formation with OSPF neighbors. By default, when OSPF is enabled on an interface, the software forms OSPF router adjacencies between each primary IP address on the interface and the OSPF neighbor attached to the interface.
- `ospf-ignore` – This option disables OSPF adjacency formation and also disables advertisement of the interface into OSPF. The sub-net is completely ignored by OSPF.

**NOTE:** The `ospf-passive` option disables adjacency formation but does not disable advertisement of the interface into OSPF. To disable advertisement in addition to disabling adjacency formation, you must use the `ospf-ignore` option.

Use the `secondary` parameter if you have already configured an IP address within the same sub-net on the interface.
NOTE: When you configure more than one address in the same sub-net, all but the first address are secondary addresses and do not form OSPF adjacencies.

USING THE WEB MANAGEMENT INTERFACE
To assign an IP address and mask to a router interface:

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration dialog is displayed.
2. Select the IP Address link. The IP addresses already configured on the device are listed in a table. To add a new IP address link, select Add IP Address to display the following panel.

<table>
<thead>
<tr>
<th>Slot</th>
<th>Port</th>
<th>IP Address</th>
<th>Subset Mask</th>
<th>Type</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>10.187.14.69</td>
<td>255.255.255.0</td>
<td>Secondary</td>
</tr>
</tbody>
</table>

   Add      Disable      Reset

   (Save)

3. Select the port (and slot if applicable) on which you want to configure the address.
4. Enter the IP address and network mask.
5. If the port already has an IP address configured, select the Secondary checkbox.
6. Click the Add button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

   NOTE: You also can access the dialog for saving configuration changes by clicking on Command in the tree view, then clicking on Save to Flash.

Assigning an IP Address to a Loopback Interface
Loopback interfaces are always up, regardless of the states of physical interfaces. They can add stability to the network because they are not subject to route flap problems that can occur due to unstable links between a Routing Switch and other devices. You can configure up to eight loopback interfaces on a Chassis Routing Switch and up to four loopback interfaces on.

You can add up to 24 IP addresses to each loopback interface.

   NOTE: If you configure the ProCurve Routing Switch to use a loopback interface to communicate with a BGP4 neighbor, you also must configure a loopback interface on the neighbor and configure the neighbor to use that loopback interface to communicate with the ProCurve Routing Switch. See “Adding a Loopback Interface” on page 13-12.

To add a loopback interface, use one of the following methods.

USING THE CLI
To add a loopback interface, enter commands such as those shown in the following example:
Syntax: interface loopback <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.

See the syntax description in “Assigning an IP Address to an Ethernet Port” on page 9-16.

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the IP Address link to display a table listing the configured IP addresses.
3. Select the Loop Back link.

   NOTE: If the device already has loopback interfaces, a table listing the interfaces is displayed. Click the Modify button to the right of the row describing an interface to change its configuration, or click the Add Loop Back link to display the Router Loop Back configuration panel.

4. Select the loopback interface number from the Loopback field’s pulldown menu. You can select from 1 – 8.
5. Select the status. The interface is enabled by default.
6. Click Add to add the new interface.
7. Click on Configure in the tree view to display the configuration options.
8. Click on IP to display the IP configuration options.
9. Select the Add IP Address link to display the Router IP Address panel.
10. Select the loopback interface from the Port field’s pulldown menu. For example, to select loopback interface 1, select “lb1”. (You can have any slot number in the Slot field. Loopback interfaces are not associated with particular slots or physical ports.)
11. Enter the loopback interface’s IP address in the IP Address field.
12. Enter the network mask in the Subnet Mask field.
13. Click the Add button to save the change to the device’s running-config file.
14. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Assigning an IP Address to a Virtual Interface

A virtual interface is a logical port associated with a Layer 3 Virtual LAN (VLAN) configured on a Routing Switch. You can configure routing parameters on the virtual interface to enable the Routing Switch to route protocol traffic from one Layer 3 VLAN to the other, without using an external router.

You can configure IP, IPX, or AppleTalk routing interface parameters on a virtual interface. This section describes how to configure an IP address on a virtual interface. Other sections in this chapter that describe how to configure interface parameters also apply to virtual interfaces.

NOTE: The Routing Switch uses the lowest MAC address on the device (the MAC address of port 1 or 1/1) as the MAC address for all ports within all virtual interfaces you configure on the device.

USING THE CLI

To add a virtual interface to a VLAN and configure an IP address on the interface, enter commands such as the following:
ProCurveRS(config)# vlan 2 name IP-Subnet_1.1.2.0/24
ProCurveRS(config-vlan-2)# untag e1 to 4
ProCurveRS(config-vlan-2)# router-interface ve1
ProCurveRS(config-vlan-2)# interface ve1
ProCurveRS(config-vif-1)# ip address 1.1.2.1/24

The first two commands in this example create a Layer 3 protocol-based VLAN name “IP-Subnet_1.1.2.0/24” and add a range of untagged ports to the VLAN. The router-interface command creates virtual interface 1 as the routing interface for the VLAN. The last two commands change to the interface configuration level for the virtual interface and assign an IP address to the interface.

Syntax: router-interface ve <num>

Syntax: interface ve <num>

See the syntax description in “Assigning an IP Address to an Ethernet Port” on page 9-16.

Deleting an IP Address

To delete an IP address, enter a command such as the following:
ProCurveRS(config-if-1/1)# no ip address 1.1.2.1

This command deletes IP address 1.1.2.1. You do not need to enter the subnet mask.

To delete all IP addresses from an interface, enter the following command:
ProCurveRS(config-if-1/1)# no ip address *

Syntax: no ip address <ip-addr> | *

Configuring Domain Name Server (DNS) Resolver

The Domain Name Server (DNS) resolver feature lets you use a host name to perform Telnet, ping, and traceroute commands. You can also define a DNS domain on a ProCurve Routing Switch and thereby recognize all hosts within that domain. After you define a domain name, the ProCurve Routing Switch automatically appends the appropriate domain to the host and forwards it to the domain name server.

For example, if the domain “newyork.com” is defined on a ProCurve Routing Switch and you want to initiate a ping to host “NYC01” on that domain, you need to reference only the host name in the command instead of the host name and its domain name. For example, you could enter either of the following commands to initiate the ping:
ProCurveRS# ping nyc01
ProCurveRS# ping nyc01.newyork.com

Defining a DNS Entry

You can define up to four DNS servers for each DNS entry. The first entry serves as the primary default address. If a query to the primary address fails to be resolved after three attempts, the next gateway address is queried (also up to three times). This process continues for each defined gateway address until the query is resolved. The order in which the default gateway addresses are polled is the same as the order in which you enter them.

USING THE CLI

Suppose you want to define the domain name of newyork.com on a Routing Switch and then define four possible default DNS gateway addresses. To do so, enter the following commands:
ProCurveRS(config)# ip dns domain-name newyork.com
ProCurveRS(config)# ip dns server-address 209.157.22.199 205.96.7.15 208.95.7.25 201.98.7.15

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

In this example, the first IP address in the ip dns server-address... command becomes the primary gateway address and all others are secondary addresses. Because IP address 201.98.7.15 is the last address listed, it is also the last address consulted to resolve a query.
**USING THE WEB MANAGEMENT INTERFACE**

To map a domain name server to multiple IP addresses:

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Configure in the tree view, then click on the plus sign next to IP, then select DNS to display the DNS panel.

3. Enter the domain name in the Domain Name field.

4. Enter an IP address for each device that will serve as a gateway to the domain name server.

**NOTE:** The first address entered will be the primary DNS gateway address. The other addresses will be used in chronological order, left to right, if the primary address is available.

5. Click the Apply button to save the change to the device’s running-config file.

6. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Using a DNS Name To Initiate a Trace Route**

Suppose you want to trace the route from a ProCurve Routing Switch to a remote server identified as NYC02 on domain newyork.com. Because the newyork.com domain is already defined on the Routing Switch, you need to enter only the host name, NYC02, as noted below.

**USING THE CLI**

ProCurveRS# traceroute nyc02

**Syntax:** traceroute <host-ip-addr> [maxttl <value>] [minttl <value>] [numeric] [timeout <value>] [source-ip <ip addr>]

The only required parameter is the IP address of the host at the other end of the route. See the Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches for information about the parameters.

After you enter the command, a message indicating that the DNS query is in process and the current gateway address (IP address of the domain name server) being queried appear on the screen:

Type Control-c to abort

Sending DNS Query to 209.157.22.199
Tracing Route to IP node 209.157.22.80
To ABORT Trace Route, Please use stop-traceroute command.

Traced route to target IP node 209.157.22.80:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Round Trip Time1</th>
<th>Round Trip Time2</th>
</tr>
</thead>
<tbody>
<tr>
<td>207.95.6.30</td>
<td>93 msec</td>
<td>121 msec</td>
</tr>
</tbody>
</table>

**NOTE:** In the above example, 209.157.22.199 is the IP address of the domain name server (default DNS gateway address), and 209.157.22.80 represents the IP address of the NYC02 host.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Command in the tree view to list the command options.

3. Select the Trace Route link to display the Trace Route panel.

4. Enter the host name or IP address in the Target Address field.
5. Optionally change the minimum and maximum TTLs and the Timeout.

6. Click on Start to begin the trace. The trace results are displayed below the Start and Abort buttons.

**Configuring Packet Parameters**

You can configure the following packet parameters on Routing Switches. These parameters control how the Routing Switch sends IP packets to other devices on an Ethernet network. The Routing Switch always places IP packets into Ethernet packets to forward them on an Ethernet port.

- **Encapsulation type** – The format for the Layer 2 packets within which the Routing Switch sends IP packets.
- **Maximum Transmission Unit (MTU)** – The maximum length of IP packet that a Layer 2 packet can contain. IP packets that are longer than the MTU are fragmented and sent in multiple Layer 2 packets. You can change the MTU globally or an individual ports.
  - Global MTU (configurable on EP devices only) – The default MTU value depends on the encapsulation type on a port and is 1500 bytes for Ethernet II encapsulation and 1492 bytes for SNAP encapsulation. On EP devices, you can set the global MTU up to 14336 bytes.
  - Port MTU (configurable on devices with EP and Standard modules) – A port's default MTU depends on the encapsulation type enabled on the port.

**Changing the Encapsulation Type**

The Routing Switch encapsulates IP packets into Layer 2 packets, to send the IP packets on the network. (A Layer 2 packet is also called a MAC layer packet or an Ethernet frame.) The source address of a Layer 2 packet is the MAC address of the Routing Switch interface sending the packet. The destination address can be one of the following:

- The MAC address of the IP packet's destination. In this case, the destination device is directly connected to the Routing Switch.
- The MAC address of the next-hop gateway toward the packet's destination.
- An Ethernet broadcast address.

The entire IP packet, including the source and destination address and other control information and the data, is placed in the data portion of the Layer 2 packet. Typically, an Ethernet network uses one of two different formats of Layer 2 packet:

- Ethernet II
- Ethernet SNAP (also called IEEE 802.3)

The control portions of these packets differ slightly. All IP devices on an Ethernet network must use the same format. ProCurve Routing Switches use Ethernet II by default. You can change the IP encapsulation to Ethernet SNAP on individual ports if needed.

**NOTE:** All devices connected to the Routing Switch port must use the same encapsulation type.

To change the IP encapsulation type on a Routing Switch port, use either of the following methods.

**USING THE CLI**

To change the IP encapsulation type on interface 1/5 to Ethernet SNAP, enter the following commands:

ProCurveRS(config)# int e 1/5
ProCurveRS(config-if-5)# ip encapsulation ethernet_snap

**Syntax:** ip encapsulation ethernet_snap | ethernet_ii
**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the Interface link to display the interface table.
5. Click on the Modify button in the row for the port.
6. Select the encapsulation type from the Encapsulation pulldown menu.
7. Click the Add button to save the change to the device’s running-config file.
8. To configure settings for another port, select the port (and slot, if applicable) and go to step 6.
9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Changing the Maximum Transmission Unit (MTU)**

The Maximum Transmission Unit (MTU) is the maximum length of IP packet that a Layer 2 packet can contain. IP packets that are longer than the MTU are fragmented and sent in multiple Layer 2 packets. You can change the MTU globally or an individual ports.

The default MTU is 1500 bytes for Ethernet II packets and 1492 for Ethernet SNAP packets.

On Chassis devices with EP modules that has 1 Gigabit and 10 Gigabit ports, you can configure an MTU up to 14336 bytes, on a global or individual interface basis.

On Standard devices, the maximum supported MTU is 1500 bytes for Ethernet II packets and 1492 for Ethernet SNAP packets. You can configure a lower MTU on an individual port basis. You cannot configure a higher MTU.

**EP MTU Enhancements**

Software release 07.6.04 and later contain the following enhancements to EP jumbo packet support:

- Hardware forwarding of Layer 3 jumbo packets – Layer 3 IP unicast jumbo packets received on a port that supports the frame’s MTU size and forwarded to another port that also supports the frame’s MTU size are forwarded in hardware. Previous releases support hardware forwarding of Layer 2 jumbo frames only.

- ICMP unreachable message if a frame is too large to be forwarded – If a jumbo packet has the Don’t Fragment (DF) bit set, and the outbound interface does not support the packet’s MTU size, the HP device sends an ICMP unreachable message to the device that sent the packet.

**NOTE:** These enhancements apply only to transit traffic forwarded through the HP device.

**Configuration Considerations for Increasing the EP MTU**

- When you increase the MTU size of a port, the increase uses system resources. Increase the MTU size only on the ports that need it. For example, if you have one port connected to a server that uses jumbo frames and two other ports connected to clients that can support the jumbo frames, increase the MTU only on those three ports. Leave the MTU size on the other ports at the default value (1500 bytes). Globally increase the MTU size only if needed.

- Use the same MTU size on all ports that will be supporting jumbo frames. If the device needs to fragment a jumbo frame (and the frame does not have the DF bit set), the device fragments the frame into 1500-byte fragments, even if the outbound port has a larger MTU. For example, if a port has an MTU setting of 8000 and receives an 8000-byte frame, then must forward the frame onto a port with an MTU of 4000, the device does not fragment the 8000-byte frame into two 4000-byte frames. Instead, the device fragments the 8000-byte frame into six fragments (five 1500-byte fragments and a final, smaller fragment.)

**Globally Changing the Maximum Transmission Unit (MTU) – EP**

The Maximum Transmission Unit (MTU) is the maximum size an IP packet can be when encapsulated in a Layer 2 packet. If an IP packet is larger than the MTU allowed by the Layer 2 packet, the Routing Switch fragments the IP...
packet into multiple parts that will fit into the Layer 2 packets, and sends the parts of the fragmented IP packet separately, in different Layer 2 packets. The device that receives the multiple fragments of the IP packet reassembles the fragments into the original packet.

You can increase the MTU size to accommodate jumbo packet sizes.

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

ProCurveRS(config)# default-mtu 14336
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, as follows:

- If the 802.1X authentication is used and 802.1X supplicant will be sending packet that is greater than 1500 MTU, then default-mtu must be set to 1700 bytes. You can specify from 64 – 14336 bytes, on a global or individual interface basis. The default is 1518 bytes. If the 802.1X authentication is used and 802.1X supplicant will be sending packet that is greater than 1500 MTU, then default-mtu must be set to 1700 bytes.

**NOTE:**

Changing the Maximum Transmission Unit on an Individual Port – EP

To change the MTU on individual ports, enter commands such as the following:

ProCurveRS(config)# interface ethernet 1/1 to 1/2
ProCurveRS(config-mif-1/1-1/2)# mtu 14336
ProCurveRS(config-mif-1/1-1/2)# write memory
ProCurveRS(config-mif-1/1-1/2)# end
ProCurveRS# reload

**Syntax:** [no] mtu <num>

These commands change the MTU on ports 1/1 and 1/2 to 14336. When you set the MTU on an individual port or group of ports, this setting overrides the global MTU setting.

**NOTE:**

Changing the Maximum Transmission Unit on an Individual Port – Standard

By default, the maximum Ethernet MTU sizes are as follows:

- 1500 bytes – The maximum for Ethernet II encapsulation
- 1492 bytes – The maximum for SNAP encapsulation

**NOTE:** If you set the MTU of a port to a value lower than the global MTU and from 576 – 1499, the port fragments the packets. However, if the port’s MTU is exactly 1500 and this is larger than the global MTU, the port drops the packets.

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

**NOTE:** If the 802.1X authentication is used and the 802.1X supplicant will be sending packet that is greater than 1500 MTU, then the following MTU on devices with Standard modules using the jumbo 1920 command.

To change the MTU for a port, use either of the following methods.
USING THE CLI

To change the MTU for interface 1/5 to 1000, enter the following commands:

ProCurveRS(config)# int e 1/5
ProCurveRS(config-if-5)# ip mtu 1000
ProCurveRS(config-if-5)# write memory
ProCurveRS(config-if-5)# end
ProCurveRS# reload

Syntax: [no] ip mtu <num>

The <num> parameter specifies the MTU. Ethernet II packets can hold IP packets from 572 – 1500 bytes long. Ethernet SNAP packets can hold IP packets from 572 – 1492 bytes long. The default MTU for Ethernet II packets is 1500. The default MTU for SNAP packets is 1492.

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the Interface link to display the interface table.
5. Click on the Modify button in the row for the port.
6. Enter an MTU value from 572 – 1492 if the interface is operating with Ethernet SNAP encapsulation. If the interface is operating with Ethernet II, enter a value from 572 – 1500.
7. Click the Add button to save the change to the device’s running-config file.
8. To configure settings for another port, select the port (and slot, if applicable) and go to step 6.
9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Path MTU Discovery (RFC 1191) Support

Starting in release 07.6.04, HP devices support the path MTU discovery method described in RFC 1191. When the HP device receives an IP packet that has its Don’t Fragment (DF) bit set, and the packet size is greater than the MTU value of the outbound interface, then the HP device returns an ICMP Destination Unreachable message to the source of the packet, with the Code indicating “fragmentation needed and DF set”. The ICMP Destination Unreachable message includes the MTU of the outbound interface. The source host can use this information to help determine the maximum MTU of a path to a destination.

RFC 1191 is supported on all interfaces.

No Fragmentation for Jumbo Packets Sent to the CPU (Release 07.8.00 and Higher)

In releases prior to 07.8.00, EP devices support forwarding of Layer 2 and Layer 3 jumbo packets for transit traffic passing through the device (that is, forwarded in hardware). However, jumbo packets originated or received by the CPU are divided into fragments no larger than 1500 bytes each. These kinds of packets include jumbo-sized control packets for IP protocols.

Starting in release 07.8.00, you can configure the HP device to send unfragmented jumbo-sized control packets from the CPU. The HP device can send IP packets to the CPU that are up to the maximum MTU of the port on which the packet was received. This improves throughput and forwarding efficiency for jumbo-sized control packets.

When jumbo-sized control packets are not fragmented, routing protocols can exchange routing table information with neighboring routers using fewer packets. For example, OSPF can send packets at the MTU size during the negotiation phase of forming an adjacency. In addition, DVMRP control packets can include more routes in a single route update, resulting in a faster convergence of the DVMRP route table.

This performance enhancement is activated by default. In order for an interface to receive jumbo packets, you must configure a large enough MTU on the interface.
Specifying an MTU for IP Control Packets

By default, the MTU used for IP control packets is the configured MTU for the interface, minus 18 bytes. For example, if the configured MTU on the interface is 9018 bytes, the maximum MTU for IP control packets is 9000 bytes. (The other 18 bytes is used for 14 bytes of MAC header, and 4 bytes of CRC.)

You can optionally specify an alternate MTU for IP control packets. The MTU specified for IP control packets overrides the interface's configured MTU. For example, the following commands set the MTU for IP control packets on interface 3/11 to 4096 bytes:

```plaintext
ProCurveRS(config)# interface e 3/11
ProCurveRS(config-if-3/11)# ip jumbo-mtu 4096
```

**Syntax:** `[no] ip jumbo-mtu <length>`

In this example, the maximum MTU for IP control packets is 4078 bytes (4096 bytes minus 18 bytes).

You can specify a value that is between 1500 bytes and the MTU configured for the interface.

**NOTE:** To set an IP MTU smaller than 1500 bytes, use the `ip mtu` command instead of the `ip jumbo-mtu` command. The `ip mtu` command is intended for use only when you want to configure an MTU smaller than 1500 bytes.

Notes Regarding OSPF Adjacencies

By default, the HP device compares the MTU in an OSPF database description packet received from another OSPF router with the MTU on the HP device. The HP device allows formation of an adjacency with the other router only if the MTU in the other router's packet matches the MTU on the HP device.

The following applies when the `ip jumbo-mtu` command is configured:

- If the HP device is connected to another HP device, the MTU used is the MTU configured on the interface, minus 18 bytes. For example, if two devices each have an MTU of 9018 bytes, the OSPF adjacency is established with an MTU of 9000 bytes.
- If the HP device is connected to a Cisco router, add 18 bytes to the MTU setting. For example, if the MTU of the Cisco router is 9000 bytes, the MTU of the HP device should be set to 9018 bytes.
- If the HP device is connected to a Juniper router, add 4 bytes to the MTU setting. For example, if the MTU of the Juniper router is 9000 bytes, the MTU of the HP device should be set to 9004 bytes.
- If the two routers have an MTU mismatch, you can configure the `ip ospf mtu-ignore` command at the interface CONFIG level to disable the MTU negotiation.

Per-VLAN Forwarding of Jumbo Packets (Release 07.8.00 and Higher)

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.

To activate per-VLAN forwarding on the HP device, enter the following command:

```plaintext
ProCurveRS(config)# vlan-l3jumbo
```

**Syntax:** `[no] vlan-l3jumbo`

The following commands set the MTU on port 1/1 9018 bytes:

```plaintext
ProCurveRS(config)# int e 1/1
ProCurveRS(config-if-e1000-1/1)# mtu 9018
ProCurveRS(config-if-e1000-1/1)# exit
```

The following commands set up two VLANs consisting of port 1/1, and enable jumbo packet forwarding for one of the VLANs.

```plaintext
ProCurveRS(config)# vlan 10
```
ProCurveRS(config-vlan-10)# tagged e 1/1
ProCurveRS(config-vlan-10)# permit-l3jumbo
ProCurveRS(config-vlan-10)# router-interface ve 10
ProCurveRS(config-vlan-10)# exit

ProCurveRS(config)# vlan 20
ProCurveRS(config-vlan-20)# tagged e 1/1
ProCurveRS(config-vlan-20)# router-interface ve 10
ProCurveRS(config-vlan-20)# exit

**Syntax:** [no] permit-l3jumbo

The following commands create two virtual routing interfaces

ProCurveRS(config)# int ve 10
ProCurveRS(config-vif-10)# ip address 10.10.10.1/24
ProCurveRS(config-vif-10)# exit

ProCurveRS(config)# int ve 20
ProCurveRS(config-vif-20)# ip address 20.20.20.1/24
ProCurveRS(config-vif-20)# exit

In this sample configuration, packets forwarded out virtual interface ve 10 are forward as jumbo, while packets forwarded out virtual interface ve 20 are fragmented.

**Notes:**
- The 10/100 ports on EP modules do not support the jumbo MTU setting. If 10/100 ports are part of the virtual routing interface, the effective MTU is the lowest MTU of all the ports in the VLAN.
- This enhancement applies only to EP devices.

### Changing the Router ID

In most configurations, a Routing Switch has multiple IP addresses, usually configured on different interfaces. As a result, a Routing Switch’s identity to other devices varies depending on the interface to which the other device is attached. Some routing protocols, including Open Shortest Path First (OSPF) and Border Gateway Protocol version 4 (BGP4), identify a Routing Switch by just one of the IP addresses configured on the Routing Switch, regardless of the interfaces that connect the Routing Switches. This IP address is the router ID.

**NOTE:** If you change the router ID, all current BGP4 sessions are cleared.

By default, the router ID on a ProCurve Routing Switch is one of the following:

- If the router has loopback interfaces, the default router ID is the IP address configured on the lowest numbered loopback interface configured on the Routing Switch. For example, if you configure loopback interfaces 1, 2, and 3 as follows, the default router ID is 9.9.9.9/24:
  - Loopback interface 1, 9.9.9.9/24
  - Loopback interface 2, 4.4.4.4/24
  - Loopback interface 3, 1.1.1.1/24
- If the device does not have any loopback interfaces, the default router ID is the lowest numbered IP interface configured on the device.

If you prefer, you can explicitly set the router ID to any valid IP address. The IP address cannot be in use on another device in the network.

**NOTE:** ProCurve Routing Switches use the same router ID for both OSPF and BGP4. If the router is already configured for OSPF, you may want to use the router ID that is already in use on the router rather than set a new one. To display the router ID, enter the `show ip` CLI command at any CLI level or select the [IP->General](#) links from the Configure tree in the Web management interface.

9 - 26 June 2005
**USING THE CLI**

To change the router ID, enter a command such as the following:

```
ProCurveRS(config)# ip router-id 209.157.22.26
```

**Syntax:** `ip router-id <ip-addr>`

The `<ip-addr>` can be any valid, unique IP address.

**NOTE:** You can specify an IP address used for an interface on the ProCurve Routing Switch, but do not specify an IP address in use by another device.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Edit the value in the Router ID field. Specify a valid IP address that is not in use on another device in the network.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Specifying a Single Source Interface for Telnet, TACACS/TACACS+, or RADIUS Packets**

When the Routing Switch originates a Telnet, TACACS/TACACS+, or RADIUS packet, the source address of the packet is the lowest-numbered IP address on the interface that sends the packet. You can configure the Routing Switch to always use the lowest-numbered IP address on a specific interface as the source addresses for these types of packets. When you configure the Routing Switch to use a single source interface for all Telnet, TACACS/TACACS+, or RADIUS packets, the Routing Switch uses the same IP address as the source for all packets of the specified type, regardless of the port(s) that actually sends the packets.

Identifying a single source IP address for Telnet, TACACS/TACACS+, or RADIUS packets provides the following benefits:

- If your Telnet, TACACS/TACACS+, or RADIUS server is configured to accept packets only from specific IP addresses, you can use this feature to simplify configuration of the server by configuring the HP device to always send the packets from the same link or source address.
- If you specify a loopback interface as the single source for Telnet, TACACS/TACACS+, or RADIUS packets, servers can receive the packets regardless of the states of individual links. Thus, if a link to the server becomes unavailable but the client or server can be reached through another link, the client or server still receives the packets, and the packets still have the source IP address of the loopback interface.

The software contains separate CLI commands for specifying the source interface for Telnet, TACACS/TACACS+, or RADIUS packets. You can configure a source interface for one or more of these types of packets separately.

To specify an Ethernet or a loopback or virtual interface as the source for all TACACS/TACACS+ packets from the device, use the following CLI method. The software uses the lowest-numbered IP address configured on the port or interface as the source IP address for TACACS/TACACS+ packets originated by the device.

**USING THE CLI**

The following sections show the syntax for specifying a single source IP address for Telnet, TACACS/TACACS+, and RADIUS packets.
### Telnet Packets

To specify the lowest-numbered IP address configured on a virtual interface as the device's source for all Telnet packets, enter commands such as the following:

```bash
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 `<num>` parameter is a loopback interface or virtual interface number. If you specify an Ethernet port, the `<portnum>` is the port's number (including the slot number).

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.

```bash
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
```
**TACACS/TACACS+ Packets**

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>`

The `<num>` parameter is a loopback interface or virtual interface number. If you specify an Ethernet port, the `<portnum>` is the port's number (including the slot number).

**RADIUS Packets**

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>`

The `<num>` parameter is a loopback interface or virtual interface number. If you specify an Ethernet port, the `<portnum>` is the port's number (including the slot number).

**Using the Web Management Interface**

You cannot configure a single source interface for Telnet, TACACS/TACACS+, or RADIUS using the Web management interface.

**Configuring ARP Parameters**

Address Resolution Protocol (ARP) is a standard IP protocol that enables an IP Routing Switch to obtain the MAC address of another device's interface when the Routing Switch knows the IP address of the interface. ARP is enabled by default and cannot be disabled.

**How ARP Works**

A Routing Switch needs to know a destination's MAC address when forwarding traffic, because the Routing Switch encapsulates the IP packet in a Layer 2 packet (MAC layer packet) and sends the Layer 2 packet to a MAC interface on a device directly attached to the Routing Switch. The device can be the packet's final destination or the next-hop router toward the destination.

The Routing Switch encapsulates IP packets in Layer 2 packets regardless of whether the ultimate destination is locally attached or is multiple router hops away. Since the Routing Switch's IP route table and IP forwarding cache contain IP address information but not MAC address information, the Routing Switch cannot forward IP packets based solely on the information in the route table or forwarding cache. The Routing Switch needs to know the MAC address that corresponds with the IP address of either the packet's locally attached destination or the next-hop router that leads to the destination.

For example, to forward a packet whose destination is multiple router hops away, the Routing Switch must send the packet to the next-hop router toward its destination, or to a default route or default network route if the IP route table does not contain a route to the packet's destination. In each case, the Routing Switch must encapsulate the packet and address it to the MAC address of a locally attached device, the next-hop router toward the IP packet's destination.

To obtain the MAC address required for forwarding a datagram, the Routing Switch does the following:
• First, the Routing Switch looks in the ARP cache (not the static ARP table) for an entry that lists the MAC address for the IP address. The ARP cache maps IP addresses to MAC addresses. The cache also lists the port attached to the device and, if the entry is dynamic, the age of the entry. A dynamic ARP entry enters the cache when the Routing Switch receives an ARP reply or receives an ARP request (which contains the sender’s IP address and MAC address). A static entry enters the ARP cache from the static ARP table (which is a separate table) when the interface for the entry comes up.

To ensure the accuracy of the ARP cache, each dynamic entry has its own age timer. The timer is reset to zero each time the Routing Switch receives an ARP reply or ARP request containing the IP address and MAC address of the entry. If a dynamic entry reaches its maximum allowable age, the entry times out and the software removes the entry from the table. Static entries do not age out and can be removed only by you.

• If the ARP cache does not contain an entry for the destination IP address, the Routing Switch broadcasts an ARP request out all its IP interfaces. The ARP request contains the IP address of the destination. If the device with the IP address is directly attached to the Routing Switch, the device sends an ARP response containing its MAC address. The response is a unicast packet addressed directly to the Routing Switch. The Routing Switch places the information from the ARP response into the ARP cache.

ARP requests contain the IP address and MAC address of the sender, so all devices that receive the request learn the MAC address and IP address of the sender and can update their own ARP caches accordingly.

NOTE: The ARP request broadcast is a MAC broadcast, which means the broadcast goes only to devices that are directly attached to the Routing Switch. A MAC broadcast is not routed to other networks. However, some routers, including ProCurve Routing Switches, can be configured to reply to ARP requests from one network on behalf of devices on another network. See “Enabling Proxy ARP” on page 9-31.

NOTE: If the router receives an ARP request packet that it is unable to deliver to the final destination because of the ARP timeout and no ARP response is received (the Routing Switch knows of no route to the destination address), the router sends an ICMP Host Unreachable message to the source.

**Rate Limiting ARP Packets**

You can 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.

**USING THE CLI**

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.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure ARP rate limiting using the Web management interface.

**Changing the ARP Aging Period**

When the Routing Switch places an entry in the ARP cache, the Routing Switch also starts an aging timer for the entry. The aging timer ensures that the ARP cache does not retain learned entries that are no longer valid. An entry can become invalid when the device with the MAC address of the entry is no longer on the network.

The ARP age affects dynamic (learned) entries only, not static entries. The default ARP age is ten minutes. On Routing Switches, you can change the ARP age to a value from 0 – 240 minutes. If you set the ARP age to zero, aging is disabled and entries do not age out.

To change the ARP age on a Routing Switch, use either of the following methods.

**USING THE CLI**

To globally change the ARP aging parameter to 20 minutes, enter the following command:

```
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.

To override the globally configured IP ARP age on an individual interface, enter a command such as the following at the interface configuration level:

```
ProCurveRS(config-if-eth0-1/1)# ip arp-age 30
```

**Syntax:** [no] ip arp-age <num>

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

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the General link to display the IP configuration panel.
5. Enter a value from 0 – 240 into the ARP Age field.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Enabling Proxy ARP**

Proxy ARP allows a Routing Switch to answer ARP requests from devices on one network on behalf of devices in another network. Since ARP requests are MAC-layer broadcasts, they reach only the devices that are directly connected to the sender of the ARP request. Thus, ARP requests do not cross routers.

For example, if Proxy ARP is enabled on a Routing Switch connected to two sub-nets, 10.10.10.0/24 and 20.20.20.0/24, the Routing Switch can respond to an ARP request from 10.10.10.69 for the MAC address of the device with IP address 20.20.20.69. In standard ARP, a request from a device in the 10.10.10.0/24 sub-net cannot reach a device in the 20.20.20.0 sub-net if the sub-nets are on different network cables, and thus is not answered.
NOTE: An ARP request from one sub-net can reach another sub-net when both sub-nets are on the same physical segment (Ethernet cable), since MAC-layer broadcasts reach all the devices on the segment.

Proxy ARP is disabled by default on ProCurve Routing Switches.

To enable Proxy ARP, use either of the following methods.

**USING THE CLI**

To enable IP proxy ARP, enter the following command:

```
ProCurveRS(config)# ip proxy-arp
```

To again disable IP proxy ARP, enter the following command:

```
ProCurveRS(config)# no ip proxy-arp
```

**Syntax:** `[no] ip proxy-arp`

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the **General** link to display the IP configuration panel.
5. Select the Enable or Disable radio button next to Proxy ARP.
6. Click the **Apply** button to save the change to the device's running-config file.
7. Select the **Save** link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Creating Static ARP Entries**

ProCurve Routing Switches have a static ARP table, in addition to the regular ARP cache. The static ARP table contains entries that you configure.

Static entries are useful in cases where you want to pre-configure an entry for a device that is not connected to the Routing Switch, or you want to prevent a particular entry from aging out. The software removes a dynamic entry from the ARP cache if the ARP aging interval expires before the entry is refreshed. Static entries do not age out, regardless of whether the HP device receives an ARP request from the device that has the entry's address.

The maximum number of static ARP entries you can configure depends on the product. See “Changing the Maximum Number of Entries the Static ARP Table Can Hold” on page 9-33.

To display the ARP cache and static ARP table, see the following:

- To display the ARP table, see “Displaying the ARP Cache” on page 9-88.
- To display the static ARP table, see “Displaying the Static ARP Table” on page 9-90.

To configure a static ARP entry, use either of the following methods.

**USING THE CLI**

To create a static ARP entry on a ProCurve Routing Switch, enter a command such as the following:

```
ProCurveRS(config)# arp 1 192.53.4.2 1245.7654.2348 e 1/2
```

**Syntax:** `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.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Click the Static ARP link.
   - If the device does not have any static ARP entries, the Static ARP configuration panel is displayed, as shown in the following example.
   - If a static ARP entry is already configured and you are adding a new entry, click on the Add Static ARP link to display the Static ARP configuration panel, as shown in the following example.
   - If you are modifying an existing static ARP entry, click on the Modify button to the right of the row describing the entry to display the Static ARP configuration panel, as shown in the following example.

<table>
<thead>
<tr>
<th>Static ARP</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address: 192.168.4.2</td>
</tr>
<tr>
<td>MAC Address: 00:25:53:45:23:67:21:70</td>
</tr>
<tr>
<td>Slot: 1 Port: 2</td>
</tr>
</tbody>
</table>

6. Enter the IP address. The address must be for a device that is directly connected to the Routing Switch.
7. Enter the MAC address.
8. Select the port that the static ARP entry is to be assigned to from the pull down menu.
9. Click the Add button to save the change to the device's running-config file.
10. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Changing the Maximum Number of Entries the Static ARP Table Can Hold**

Table 9.3 on page 9-34 lists the default maximum and configurable maximum number of entries in the static ARP table that are supported on each type of ProCurve Routing Switch. If you need to change the maximum number of entries supported on a Routing Switch, use either of the following methods.

**NOTE:** You must save the configuration to the startup-config file and reload the software after changing the static ARP table size to place the change into effect.

**NOTE:** The basic procedure for changing the static ARP table size is the same as the procedure for changing other configurable cache or table sizes. See the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* or the *Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch*. 
**USING THE CLI**

To increase the maximum number of entries in the static ARP table you can configure on a ProCurve Routing Switch using a 512MB Management 4 module, enter commands such as the following at the global CONFIG level of the CLI:

```
ProCurveRS(config)# system-max ip-static-arp 8000
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

To increase the maximum number of entries in the static ARP table you can configure on an 9308M Routing Switch using a 128MB management module, enter commands such as the following at the global CONFIG level of the CLI:

```
ProCurveRS(config)# system-max ip-static-arp 2048
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `system-max ip-static-arp <num>`

The `<num>` parameter indicates the maximum number of static ARP entries and can be a number in one of the following ranges, depending on the device you are configuring. The table below lists the default maximum and range of configurable maximums for static ARP table entries supported on each type of ProCurve Routing Switch.

<table>
<thead>
<tr>
<th>Product</th>
<th>Default Maximum</th>
<th>Configurable Minimum</th>
<th>Configurable Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>256MB Management 4 module</td>
<td>2048</td>
<td>2048</td>
<td>10,000</td>
</tr>
<tr>
<td>128MB management module (Management 2)</td>
<td>1024</td>
<td>1024</td>
<td>2048</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To modify a table size using the Web management interface:

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the Max-Parameter link to display the Configure System Parameter Maximum Value table. This table lists the settings and valid ranges for all the configurable table sizes on the device.
3. Click the Modify button next to the ip-static-arp row.
4. Enter the new value for the cache size. The value you enter specifies the maximum number of entries the cache can hold.
5. Click Apply to save the changes to the device's running-config.
6. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.
7. Click on the plus sign next to Command in the tree view to list the command options.
8. Select the Reload link and select Yes when the Web management interface asks you whether you really want to reload the software. Changes to cache and table sizes do not take effect until you reload the software.

**Configuring Forwarding Parameters**

The following configurable parameters control the forwarding behavior of ProCurve Routing Switches:

- Time-To-Live (TTL) threshold
• Forwarding of directed broadcasts
• Forwarding of source-routed packets
• Ones-based and zero-based broadcasts

All these parameters are global and thus affect all IP interfaces configured on the Routing Switch.

To configure these parameters, use the procedures in the following sections.

**Changing the TTL Threshold**

The TTL threshold prevents routing loops by specifying the maximum number of router hops an IP packet originated by the Routing Switch can travel through. Each device capable of forwarding IP that receives the packet decrements (decreases) the packet's TTL by one. If a device receives a packet with a TTL of 1 and reduces the TTL to zero, the device drops the packet.

The default TTL is 64. You can change the TTL to a value from 1–255.

To modify the TTL, use either of the following methods.

**USING THE CLI**

To modify the TTL threshold to 25, enter the following commands:

```
ProCurveRS(config)# ip ttl 25
```

**Syntax:** ip ttl <1-255>

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the General link to display the IP configuration panel.
5. Enter a value from 1–255 into the TTL field.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Enabling Forwarding of Directed Broadcasts**

A directed broadcast is an IP broadcast to all devices within a single directly-attached network or sub-net. A net-directed broadcast goes to all devices on a given network. A sub-net-directed broadcast goes to all devices within a given sub-net.

**NOTE:** A less common type, the all-sub-nets broadcast, goes to all directly-attached sub-nets. Forwarding for this broadcast type also is supported, but most networks use IP multicasting instead of all-sub-net broadcasting.

Forwarding for all types of IP directed broadcasts is disabled by default. You can enable forwarding for all types if needed. You cannot enable forwarding for specific broadcast types.

To enable forwarding of IP directed broadcasts, use either of the following methods.

**USING THE CLI**

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

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

HP software makes the forwarding decision based on the router’s knowledge of the destination network prefix. Routers cannot determine that a message is unicast or directed broadcast apart from the destination network prefix. The decision to forward or not forward the message is by definition only possible in the last hop router.
To disable the directed broadcasts, enter the following command in the CONFIG mode:

```
ProCurveRS(config)# no ip directed-broadcast
```

To enable directed broadcasts on an individual interface instead of globally for all interfaces, enter commands such as the following:

```
ProCurveRS(config)# interface ethernet 1/1
ProCurveRS(config-if-1/1)# ip directed-broadcast
```

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

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the General link to display the IP configuration panel.
5. Select Enable or Disable next to Directed Broadcast Forward.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Disabling Forwarding of IP Source-Routed Packets**

A source-routed packet specifies the exact router path for the packet. The packet specifies the path by listing the IP addresses of the router interfaces through which the packet must pass on its way to the destination. The Routing Switch supports both types of IP source routing:

- **Strict source routing** – requires the packet to pass through only the listed routers. If the Routing Switch receives a strict source-routed packet but cannot reach the next hop interface specified by the packet, the Routing Switch discards the packet and sends an ICMP Source-Route-Failure message to the sender.

**NOTE:** The Routing Switch allows you to disable sending of the Source-Route-Failure messages. See “Disabling ICMP Messages” on page 9-37.

- **Loose source routing** – requires that the packet pass through all of the listed routers but also allows the packet to travel through other routers, which are not listed in the packet.

The Routing Switch forwards both types of source-routed packets by default. To disable the feature, use either of the following methods. You cannot enable or disable strict or loose source routing separately.

**USING THE CLI**

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
```

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Select the Disable or Enable radio button next to Source Route.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Enabling 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. For example, the Routing Switch treats IP packets with 209.157.22.255/24 as the destination IP address as IP broadcast packets and forwards the packets to all IP hosts within the 209.157.22.x sub-net (except the host that sent the broadcast packet to the Routing Switch).

Most IP hosts are configured to receive IP sub-net broadcast packets with all ones in the host portion of the address. However, some older IP hosts instead expect IP sub-net broadcast packets that have all zeros instead of all ones in the host portion of the address. To accommodate this type of host, you can enable the Routing Switch to treat IP packets with all zeros in the host portion of the destination IP address as broadcast packets.

**NOTE:** When you enable the Routing Switch for zero-based sub-net broadcasts, the Routing Switch 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.

**NOTE:** This feature applies only to IP sub-net broadcasts, not to local network broadcasts. The local network broadcast address is still expected to be all ones.

To enable the Routing Switch for zero-based IP broadcasts, use either of the following methods.

**USING THE CLI**

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`

**USING THE WEB MANAGEMENT INTERFACE**

You cannot enable zero-based IP sub-net broadcasting using the Web management interface.

**Disabling ICMP Messages**

HP devices are enabled to reply to ICMP echo messages and send ICMP Destination Unreachable messages by default.

You can selectively disable the following types of Internet Control Message Protocol (ICMP) messages:

- Echo messages (ping messages) – The Routing Switch replies to IP pings from other IP devices.
- Destination Unreachable messages – If the Routing Switch receives an IP packet that it cannot deliver to its destination, the Routing Switch discards the packet and sends a message back to the device that sent the packet to the Routing Switch. The message informs the device that the destination cannot be reached by the Routing Switch.

**Disabling Replies to Broadcast Ping Requests**

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 using the following CLI method.

**USING THE CLI**

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

**USING THE WEB MANAGEMENT INTERFACE**

You cannot disable ICMP Echo replies using the Web management interface.

**Disabling 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.

You can disable the HP device from sending these types of ICMP messages on an individual basis. To do so, use the following CLI method.

**NOTE:** Disabling an ICMP Unreachable message type does not change the HP device’s ability to forward packets. Disabling ICMP Unreachable messages prevents the device from generating or forwarding the Unreachable messages.

**USING THE CLI**

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.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot disable ICMP Destination Unreachable messages using the Web management interface.

## Disabling ICMP Redirect Messages

You can disable or re-enable ICMP redirect messages. By default, a ProCurve Routing Switch sends an ICMP redirect message to the source of a misdirected packet in addition to forwarding the packet to the appropriate router. You can disable ICMP redirect messages on a global basis or on an individual port basis.

**NOTE:** The device forwards misdirected traffic to the appropriate router, even if you disable the redirect messages.

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`

To disable ICMP redirect messages on a specific interface, enter the following command at the configuration level for the interface:

```
ProCurveRS(config)# int e 3/11
ProCurveRS(config-if-e100-3/11)# no ip redirect
```

**Syntax:** `[no] ip redirect`

## Configuring Static Routes

The IP route table can receive routes from the following sources:

- **Directly-connected networks** – When you add an IP interface, the Routing Switch automatically creates a route for the network the interface is in.
- **RIP** – If RIP is enabled, the Routing Switch can learn about routes from the advertisements other RIP routers send to the Routing Switch. If the route has a lower administrative distance than any other routes from different sources to the same destination, the Routing Switch places the route in the IP route table.
- **OSPF** – See RIP, but substitute “OSPF” for “RIP”.
- **BGP4** – See RIP, but substitute “BGP4” for “RIP”.
- **Default network route** – A statically configured default route that the Routing Switch uses if other default routes to the destination are not available. See “Configuring a Default Network Route” on page 9-49.
- **Statically configured route** – You can add routes directly to the route table. When you add a route to the IP route table, you are creating a static IP route. This section describes how to add static routes to the IP route table.

### Static Route Types

You can configure the following types of static IP routes:
advanced configuration and management guide for procurve 9300/9400 series routing switches

- standard – the static route consists of the destination network address and network mask, and the IP address of the next-hop gateway. You can configure multiple standard static routes with the same metric for load sharing or with different metrics to provide a primary route and backup routes.

- interface-based – the static route consists of the destination network address and network mask, and the routing switch interface through which you want the routing switch to send traffic for the route. Typically, this type of static route is for directly attached destination networks.

- null – the static route consists of the destination network address and network mask, and the “null0” parameter. Typically, the null route is configured as a backup route for discarding traffic if the primary route is unavailable.

static ip route parameters

when you configure a static ip route, you must specify the following parameters:

- the ip address and network mask for the route’s destination network.

- the route’s path, which can be one of the following:
  - the ip address of a next-hop gateway
  - an ethernet port
  - a virtual interface (a routing interface used by vlans for routing layer 3 protocol traffic among one another)
  - a “null” interface. the routing switch drops traffic forwarded to the null interface.

you also can specify the following optional parameters:

- the route’s metric – the value the routing switch uses when comparing this route to other routes in the ip route table to the same destination. the metric applies only to routes that the routing switch has already placed in the ip route table. the default metric for static ip routes is 1.

- the route’s administrative distance – the value that the routing switch uses to compare this route with routes from other route sources to the same destination before placing a route in the ip route table. this parameter does not apply to routes that are already in the ip route table. the default administrative distance for static ip routes is 1.

the default metric and administrative distance values ensure that the routing switch always prefers static ip routes over routes from other sources to the same destination.

multiple static routes to the same destination provide load sharing and redundancy

you can add multiple static routes for the same destination network to provide one or more of the following benefits:

- ip load balancing – when you add multiple ip static routes for the same destination to different next-hop gateways, and the routes each have the same metric and administrative distance, the routing switch can load balance traffic to the routes’ destination. for information about ip load balancing, see “configuring ip load sharing” on page 9-51.

- path redundancy – when you add multiple static ip routes for the same destination, but give the routes different metrics or administrative distances, the routing switch uses the route with the lowest administrative distance by default, but uses another route to the same destination of the first route becomes unavailable.

see the following sections for examples and configuration information:

- “configuring load balancing and redundancy using multiple static routes to the same destination” on page 9-44
- “configuring standard static ip routes and interface or null static routes to the same destination” on page 9-46

static route states follow port states

ip static routes remain in the ip route table only so long as the port or virtual interface used by the route is available. if the port or virtual routing interface becomes unavailable, the software removes the static route from
the IP route table. If the port or virtual routing interface becomes available again later, the software adds the route back to the route table.

This feature allows the Routing Switch to adjust to changes in network topology. The Routing Switch does not continue trying to use routes on unavailable paths but instead uses routes only when their paths are available.

Figure 9.2 shows an example of a network containing a static route. The static route is configured on Router A, as shown in the CLI example following the figure.

**Figure 9.2  Example of a static route**

![Diagram of network with static routes](image)

The following command configures a static route to 207.95.7.0, using 207.95.6.157 as the next-hop gateway.

```
ProCurveRS(config)# ip route 207.95.7.0/24 207.95.6.157
```

When you configure a static IP route, you specify the destination address for the route and the next-hop gateway or Routing Switch interface through which the Routing Switch can reach the route. The Routing Switch adds the route to the IP route table. In this case, Router A knows that 207.95.6.157 is reachable through port 1/2, and also assumes that local interfaces within that sub-net are on the same port. Router A deduces that IP interface 207.95.7.188 is also on port 1/2.

The software automatically removes a static IP route from the IP route table if the port used by that route becomes unavailable. When the port becomes available again, the software automatically re-adds the route to the IP route table.

**Configuring a Static IP Route**

To configure an IP static route, use either of the following methods.

**USING THE CLI**

To configure an IP static route with a destination address of 192.0.0.0 255.0.0.0 and a next-hop router IP address of 195.1.1.1, enter the following commands:

```
ProCurveRS(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1
```

To configure a static IP route with an Ethernet port instead of a next-hop address, enter a command such as the following.

```
ProCurveRS(config)# ip route 192.128.2.69 255.255.255.0 ethernet 4/1
```

The command in the example above configures a static IP route for destination network 192.128.2.69/24. Since an Ethernet port is specified instead of a gateway IP address as the next hop, the Routing Switch always forwards traffic for the 192.128.2.69/24 network to port 4/1. The command in the following example configures an IP static route that uses virtual interface 3 as its next hop.

```
ProCurveRS(config)# ip route 192.128.2.71 255.255.255.0 ve 3
```

**Syntax:**

```
ip route <dest-ip-addr> <dest-mask>
<next-hop-ip-addr> |
eternet <portnum> | ve <num>
[<metric>] [distance <num>]
```

or
**Syntax:** ip route <dest-ip-addr>/<mask-bits> | ethernet <portnum> | ve <num> [metric] [distance <num>]

The `<dest-ip-addr>` is the route’s destination. The `<mask-bits>` 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.

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’s next hop 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.

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:** The Routing Switch will replace the static route if it receives a route with a lower administrative distance. See “Changing Administrative Distances” on page 13-36 for a list of the default administrative distances for all types of routes.

**NOTE:** You can also assign the default router as the destination by entering 0.0.0.0 0.0.0.0 xxx.xxx.xxx.xxx.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Click the Static Route link.
   • If the device does not have any IP static routes, the Static Route configuration panel is displayed.
   • If a static route is already configured and you are adding a new route, click on the Add Static Route link to display the Static Route configuration panel.
   • If you are modifying an existing static route, click on the Modify button to the right of the row describing the static route to display the Static Route configuration panel.
6. Enter the network address for the route in the Network field.
7. Enter the network mask in the Mask field.
8. Select the next-hop type. You can select one of the following:
   • Address – The next-hop is the IP address of a gateway router.
Configuring IP

• Interface – The next hop is a port or virtual interface on the Routing Switch.

9. Enter the next-hop IP address (if you selected the Address method) or select the interface (if you selected the Interface method).

• Address – Enter the IP address of the next-hop gateway in the Next Hop (by Address) field.

• Interface – Select the port, loopback interface, or virtual interface from the Next Hop (by Interface) field’s pulldown menu(s). Loopback interfaces and virtual interfaces are listed in the Port pulldown menu, not in the Slot pulldown menu. Ignore the Slot pulldown menu and select the interface from the Port pulldown menu.

10. Optionally change the metric by editing the value in the Metric field. You can specify 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.

11. Optionally change the administrative distance by editing the value in the Distance field. 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.

12. Click the Add button to save the change to the device's running-config file.

13. Repeat steps 8 – 12 for each static route to the same destination.

14. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

Configuring a “Null” Route

You can configure the Routing Switch to drop IP packets to a specific network or host address by configuring a “null” (sometimes called “null0”) static route for the address. When the Routing Switch receives a packet destined for the address, the Routing Switch drops the packet instead of forwarding it.

To configure a null static route, use the following CLI method.

To configure a null static route to drop packets destined for network 209.157.22.x, enter the following commands.

ProCurveRS(config)# ip route 209.157.22.0 255.255.255.0 null0
ProCurveRS(config)# write memory

Syntax: ip route <ip-addr> <ip-mask> null0 [<metric>] [distance <num>]

or

Syntax: ip route <ip-addr>/<mask-bits> null0 [<metric>] [distance <num>]

To display the maximum value for your device, enter the show default values command. The maximum number of static IP routes the system can hold is listed in the ip-static-route row in the System Parameters section of the display. To change the maximum value, use the system-max ip-static-route <num> command at the global CONFIG level.

The <ip-addr> parameter specifies the network or host address. The Routing Switch will drop packets that contain this address in the destination field instead of forwarding them.

The <ip-mask> parameter specifies the network mask. Ones are significant bits and zeros allow any value. For example, the mask 255.255.255.0 matches on all hosts within the Class C sub-net address specified by <ip-addr>. Alternatively, you can specify the number of bits in the network mask. For example, you can enter 209.157.22.0/24 instead of 209.157.22.0 255.255.255.0.

The null0 parameter indicates that this is a null route. You must specify this parameter to make this a null route.

The <metric> parameter adds a cost to the route. You can specify from 1 – 16. The default is 1.

The distance <num> parameter configures the administrative distance for the route. You can specify a value from 1 – 255. The default is 1. The value 255 makes the route unusable.
**NOTE:** The last two parameters are optional and do not affect the null route, unless you configure the administrative distance to be 255. In this case, the route is not used and the traffic might be forwarded instead of dropped.

**Dropping Traffic Sent to the Null0 Interface In Hardware**

In releases prior to 07.7.00, traffic sent to the null0 interface was done in software; that is, by sending the traffic to the CPU. Starting in release 07.7.00, this is now done in hardware; that is, by programming the CAM to discard traffic sent to the null0 interface. This improves forwarding efficiency and reduces the burden on the HP device's CPU.

Hardware dropping for IP traffic sent to the null0 interface is supported on devices with Standard and EP modules. Note that this enhancement applies only when you are configuring a null static route. On Standard devices, when you configure ACLs and route-maps with Policy-Based Routing (PBR) to send traffic to the null0 interface, the traffic is still dropped in software.

This feature applies to traffic not using the default IP route (0.0.0.0/0). If you define a null static route to drop traffic sent to the default IP route address, the traffic is still dropped by software. You can optionally configure the HP device to drop traffic sent to the default IP route address in hardware. To do this, enter the following commands:

```
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`

Configuring the HP device to drop traffic sent to the default IP route address in hardware causes the device to program 32-bit host CAM entries for each destination address using the default route, which could consume the CAM space. To prevent this from happening, you can enable the CAM Default Route Aggregation feature. To do this, enter the following command:

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

**Syntax:** `ip dr-aggregate`

See “CAM Default Route Aggregation” on page 9-68 for more information.

**Configuring Load Balancing and Redundancy Using Multiple Static Routes to the Same Destination**

You can configure multiple static IP routes to the same destination, for the following benefits:

- **IP load sharing** – If you configure more than one static route to the same destination, and the routes have different next-hop gateways but have the same metrics, the Routing Switch load balances among the routes using basic round-robin. For example, if you configure two static routes with the same metrics but to different gateways, the Routing Switch alternates between the two routes. For information about IP load balancing, see “Configuring IP Load Sharing” on page 9-51.

- **Backup Routes** – If you configure multiple static IP routes to the same destination, but give the routes different next-hop gateways and different metrics, the Routing Switch will always use the route with the lowest metric. If this route becomes unavailable, the Routing Switch will fail over to the static route with the next-lowest metric, and so on.

**NOTE:** You also can bias the Routing Switch to select one of the routes by configuring them with different administrative distances. However, make sure you do not give a static route a higher administrative distance than other types of routes, unless you want those other types to be preferred over the static route. For a list of the default administrative distances, see “Changing Administrative Distances” on page 13-36.

The steps for configuring the static routes are the same as described in the previous section. The following sections provide examples.

**USING THE CLI**

To configure multiple static IP routes, enter commands such as the following.

```
ProCurveRS(config)# ip route 192.128.2.69 255.255.255.0 209.157.22.1
```

June 2005
The commands in the example above configure two static IP routes. The routes go to different next-hop gateways but have the same metrics. These commands use the default metric value (1), so the metric is not specified. These static routes are used for load sharing among the next-hop gateways.

The following commands configure static IP routes to the same destination, but with different metrics. The route with the lowest metric is used by default. The other routes are backups in case the first route becomes unavailable. The Routing Switch uses the route with the lowest metric if the route is available.

In this example, each static route has a different metric. The metric is not specified for the first route, so the default (1) is used. A metric is specified for the second and third static IP routes. The second route has a metric of two and the third route has a metric of 3. Thus, the second route is used only of the first route (which has a metric of 1) becomes unavailable. Likewise, the third route is used only if the first and second routes (which have lower metrics) are both unavailable.

For complete syntax information, see “Configuring a Static IP Route” on page 9-41.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Click the Static Route link.
   - If the device does not have any IP static routes, the Static Route configuration panel is displayed, as shown in the following example.
   - If a static route is already configured and you are adding a new route, click on the Add Static Route link to display the Static Route configuration panel, as shown in the following example.
   - If you are modifying an existing static route, click on the Modify button to the right of the row describing the static route to display the Static Route configuration panel, as shown in the following example.

6. Enter the network address for the route in the Network field.
7. Enter the network mask in the Mask field.
8. Enter the IP address of the next hop gateway in the Next Hop field.
9. Optionally change the metric by editing the value in the Metric field. You can specify 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.

10. Optionally change the administrative distance by editing the value in the Distance field. 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.

11. Click the Add button to save the change to the device’s running-config file.

12. Repeat steps 8 – 11 for each static route to the same destination.

13. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

### Configuring Standard Static IP Routes and Interface or Null Static Routes to the Same Destination

You can configure a null0 or interface-based static route to a destination and also configure a normal static route to the same destination, so long as the route metrics are different.

When the Routing Switch has multiple routes to the same destination, the Routing Switch always prefers the route with the lowest metric. Generally, when you configure a static route to a destination network, you assign the route a low metric so that the Routing Switch prefers the static route over other routes to the destination.

This feature is especially useful for the following configurations. These are not the only allowed configurations but they are typical uses of this enhancement.

- When you want to ensure that if a given destination network is unavailable, the Routing Switch drops (forwards to the null interface) traffic for that network instead of using alternate paths to route the traffic. In this case, assign the normal static route to the destination network a lower metric than the null route.

- When you want to use a specific interface by default to route traffic to a given destination network, but want to allow the Routing Switch to use other interfaces to reach the destination network if the path that uses the default interface becomes unavailable. In this case, give the interface route a lower metric than the normal static route.

**NOTE:** You cannot add a null or interface-based static route to a network if there is already a static route of any type with the same metric you specify for the null or interface-based route.

Figure 9.3 shows an example of two static routes configured for the same destination network. In this example, one of the routes is a standard static route and has a metric of 1. The other static route is a null route and has a higher metric than the standard static route. The Routing Switch always prefers the static route with the lower metric. In this example, the Routing Switch always uses the standard static route for traffic to destination network 192.168.7.0/24, unless that route becomes unavailable, in which case the Routing Switch sends traffic to the null route instead.
**Figure 9.3 Standard and null static routes to the same destination network**

Two static routes to 192.168.7.0/24:

- Standard static route through gateway 192.168.6.157, with metric 1
- Null route, with metric 2

When standard static route is good, Router A uses that route.

If standard static route is unavailable, Router A uses the null route (in effect dropping instead of forwarding the packets).

**Figure 9.4** shows another example of two static routes. In this example, a standard static route and an interface-based static route are configured for destination network 192.168.6.0/24. The interface-based static route has a lower metric than the standard static route. As a result, the Routing Switch always prefers the interface-based route when the route is available. However, if the interface-based route becomes unavailable, the Routing Switch still forwards the traffic toward the destination using an alternate route through gateway 192.168.8.11/24.
Two static routes to 192.168.7.0/24:

--Interface-based route through port 1/1, with metric 1.

--Standard static route through gateway 192.168.8.11, with metric 3.

Router A

When route through interface 1/1 is available, Router A always uses that route.

Router B

If route through interface 1/1 becomes unavailable, Router A uses alternate route through gateway 192.168.8.11/24.

Router C

Router D

To configure the multiple static routes of different types to the same destination, use either of the following methods.

**USING THE CLI**

To configure a standard static IP route and a null route to the same network as shown in Figure 9.3 on page 9-47, enter commands such as the following:

```
ProCurveRS(config)# ip route 192.168.7.0/24 192.168.6.157/24 1
ProCurveRS(config)# ip route 192.168.7.0/24 null0 3
```

The first command configures a standard static route, which includes specification of the next-hop gateway. The command also gives the standard static route a metric of 1, which causes the Routing Switch to always prefer this route when the route is available.

The second command configures another static route for the same destination network, but the second route is a null route. The metric for the null route is 3, which is higher than the metric for the standard static route. If the standard static route is unavailable, the software uses the null route.

For complete syntax information, see “Configuring a Static IP Route” on page 9-41.

To configure a standard static route and an interface-based route to the same destination, enter commands such as the following:

```
ProCurveRS(config)# ip route 192.168.6.0/24 ethernet 1/1 1
ProCurveRS(config)# ip route 192.168.6.0/24 192.168.8.11/24 3
```

The first command configured an interface-based static route through Ethernet port 1/1. The command assigns a metric of 1 to this route, causing the Routing Switch to always prefer this route when it is available. If the route becomes unavailable, the Routing Switch uses an alternate route through the next-hop gateway 192.168.8.11/24.
**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.

3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.

4. Click on the General link to display the IP configuration panel.

5. Click the Static Route link.
   - If the device does not have any IP static routes, the Static Route configuration panel is displayed.
   - If a static route is already configured and you are adding a new route, click on the Add Static Route link to display the Static Route configuration panel.
   - If you are modifying an existing static route, click on the Modify button to the right of the row describing the static route to display the Static Route configuration panel.

6. Enter the network address for the route in the Network field.

7. Enter the network mask in the Mask field.

8. Select the next-hop type. You can select one of the following:
   - Address – The next-hop is the IP address of a gateway router.
   - Interface – The next hop is a port, loopback interface, or virtual interface on the Routing Switch.

9. Enter the next-hop IP address (if you selected the Address method) or select the interface (if you selected the Interface method).
   - Address – Enter the IP address of the next-hop gateway in the Next Hop (by Address) field.
   - Interface – Select the port, loopback interface, or virtual interface from the Next Hop (by Interface) field’s pulldown menu(s). Loopback interfaces and virtual interfaces are listed in the Port pulldown menu, not in the Slot pulldown menu. Ignore the Slot pulldown menu and select the interface from the Port pulldown menu.

**NOTE:** You cannot configure a null IP static route using the Web management interface.

10. Optionally change the metric by editing the value in the Metric field. You can specify 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.

11. Optionally change the administrative distance by editing the value in the Distance field. 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.

12. Click the Add button to save the change to the device’s running-config file.

13. Repeat steps 8 – 12 for each static route to the same destination.

14. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Configuring a Default Network Route**

The Routing Switch enables you to specify a candidate default route without the need to specify the next hop gateway. If the IP route table does not contain an explicit default route (for example, 0.0.0.0/0) or propagate an explicit default route through routing protocols, the software can use the default network route as a default route instead.
When the software uses the default network route, it also uses the default network route's next hop gateway as the gateway of last resort.

This feature is especially useful in environments where network topology changes can make the next hop gateway unreachable. This feature allows the Routing Switch to perform default routing even if the default network route's default gateway changes.

The feature thus differs from standard default routes. When you configure a standard default route, you also specify the next hop gateway. If a topology change makes the gateway unreachable, the default route becomes unusable.

For example, if you configure 10.10.10.0/24 as a candidate default network route, if the IP route table does not contain an explicit default route (0.0.0.0/0), the software uses the default network route and automatically uses that route's next hop gateway as the default gateway. If a topology change occurs and as a result the default network route's next hop gateway changes, the software can still use the default network route. To configure a default network route, use the following CLI method.

If you configure more than one default network route, the Routing Switch uses the following algorithm to select one of the routes:

1. Use the route with the lowest administrative distance.
2. If the administrative distances are equal:
   - Are the routes from different routing protocols (RIP, OSPF, or BGP4)? If so, use the route with the lowest IP address.
   - If the routes are from the same routing protocol, use the route with the best metric. The meaning of "best" metric depends on the routing protocol:
     - RIP – The metric is the number of hops (additional routers) to the destination. The best route is the route with the fewest hops.
     - OSPF – The metric is the path cost associated with the route. The path cost does not indicate the number of hops but is instead a numeric value associated with each route. The best route is the route with the lowest path cost.
     - BGP4 – The metric is the Multi-exit Discriminator (MED) associated with the route. The MED applies to routes that have multiple paths through the same AS. The best route is the route with the lowest MED.

### Configuring a Default Network Route

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

**USING THE CLI**

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
```

```
Total number of IP routes: 2
Start index: 1  B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default
<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>1 209.157.20.0</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>2 209.157.22.0</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.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure a default network route using the Web management interface. In addition, the IP route table display in the Web management interface does not indicate routes that are candidate default network routes. The routes are listed but are not flagged with an asterisk.

### Configuring IP Load Sharing

The IP route table can contain more than one path to a given destination. When this occurs, the Routing Switch selects the path with the lowest cost as the path for forwarding traffic to the destination. If the IP route table contains more than one path to a destination and the paths each have the lowest cost, then the Routing Switch uses **IP load sharing** to select a path to the destination.\(^1\)

IP load sharing is based on the destination address of the traffic. Chassis Routing Switches support load sharing based on individual host addresses or on network addresses. Support load sharing based on host addresses.

You can enable a Routing Switch to load balance across up to eight equal-cost paths. The default maximum number of equal-cost load sharing paths is four.

**NOTE:** IP load sharing is not based on source routing, only on next-hop routing.

**NOTE:** The term “path” refers to the next-hop router to a destination, not to the entire route to a destination. Thus, when the software compares multiple equal-cost paths, the software is comparing paths that use different next-hop routers, with equal costs, to the same destination.

In many contexts, the terms “route” and “path” mean the same thing. Most of the user documentation uses the term “route” throughout. The term “path” is used in this section to refer to an individual next-hop router to a destination, while the term “route” refers collectively to the multiple paths to the destination. Load sharing applies when the IP route table contains multiple, equal-cost paths to a destination.

**NOTE:** HP devices also perform load sharing among the ports in aggregate links. See the “Trunk Group Load Sharing” section in the “Configuring Trunk Groups and Dynamic Link Aggregation” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches*.

### How Multiple Equal-Cost Paths Enter the IP Route Table

IP load sharing applies to equal-cost paths in the IP route table. Routes that are eligible for load sharing can enter the table from any of the following sources:

- IP static routes
- Routes learned through RIP
- Routes learned through OSPF
- Routes learned through BGP4

**Administrative Distance**

The administrative distance is a unique value associated with each type (source) of IP route. Each path has an administrative distance. The administrative distance is not used when performing IP load sharing, but the administrative distance is used when evaluating multiple equal-cost paths to the same destination from different sources, such as RIP, OSPF and so on.

---

\(^1\)IP load sharing is also called “Equal-Cost Multi-Path (ECMP)” load sharing or just “ECMP”
The value of the administrative distance is determined by the source of the route. The Routing Switch is configured with a unique administrative distance value for each IP route source.

When the software receives multiple paths to the same destination and the paths are from different sources, the software compares the administrative distances of the paths and selects the path with the lowest distance. The software then places the path with the lowest administrative distance in the IP route table. For example, if the Routing Switch has a path learned from OSPF and a path learned from RIP for a given destination, only the path with the lower administrative distance enters the IP route table.

Here are the default administrative distances on the ProCurve Routing Switch:

- Directly connected – 0 (this value is not configurable)
- Static IP route – 1 (applies to all static routes, including default routes and default network routes)
- Exterior Border Gateway Protocol (EBGP) – 20
- OSPF – 110
- RIP – 120
- Interior Gateway Protocol (IBGP) – 200
- Local BGP – 200
- Unknown – 255 (the router will not use this route)

Lower administrative distances are preferred over higher distances. For example, if the router receives routes for the same network from OSPF and from RIP, the router will prefer the OSPF route by default.

Since the software selects only the path with the lowest administrative distance, and the administrative distance is determined by the path's source, IP load sharing does not apply to paths from different route sources. IP load sharing applies only when the IP route table contains multiple paths to the same destination, from the same IP route source.

IP load sharing does not apply to paths that come from different sources.

**Path Cost**

The cost parameter provides a common basis of comparison for selecting from among multiple paths to a given destination. Each path in the IP route table has a cost. When the IP route table contains multiple paths to a destination, the Routing Switch chooses the path with the lowest cost. When the IP route table contains more than one path with the lowest cost to a destination, the Routing Switch uses IP load sharing to select one of the lowest-cost paths.

The source of a path's cost value depends on the source of the path.

- IP static route – The value you assign to the metric parameter when you configure the route. The default metric is 1. See "Configuring Load Balancing and Redundancy Using Multiple Static Routes to the Same Destination" on page 9-44.
- RIP – The number of next-hop routers to the destination.
- OSPF – The Path Cost associated with the path. The paths can come from any combination of inter-area, intra-area, and external Link State Advertisements (LSAs).
- BGP4 – The path's Multi-Exit Discriminator (MED) value.

**NOTE:** If the path is redistributed between two or more of the above sources before entering the IP route table, the cost can increase during the redistribution due to settings in redistribution filters.

**Static Route, OSPF, and BGP4 Load Sharing**

IP load sharing and load sharing for static routes, OSPF routes, and BGP4 routes are individually configured. Multiple equal-cost paths for a destination can enter the IP route table only if the source of the paths is configured to support multiple equal-cost paths. For example, if BGP4 allows only one path with a given cost for a given destination, the BGP4 route table cannot contain equal-cost paths to the destination. Consequently, the IP route table will not receive multiple equal-cost paths from BGP4.
Table 9.4 lists the default and configurable maximum numbers of paths for each IP route source that can provide equal-cost paths to the IP route table. The table also lists where to find configuration information for the route source's load sharing parameters.

The load sharing state for all the route sources is based on the state of IP load sharing. Since IP load sharing is enabled by default on all ProCurve Routing Switches, load sharing for static IP routes, RIP routes, OSPF routes, and BGP4 routes also is enabled by default.

### Table 9.4: Default Load Sharing Parameters for Route Sources

<table>
<thead>
<tr>
<th>Route Source</th>
<th>Default Maximum Number of Paths</th>
<th>Maximum Number of Paths</th>
<th>See...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static IP route</td>
<td>4&lt;sup&gt;1&lt;/sup&gt;</td>
<td>8&lt;sup&gt;a&lt;/sup&gt;</td>
<td>9-62</td>
</tr>
<tr>
<td>RIP</td>
<td>4&lt;sup&gt;a&lt;/sup&gt;</td>
<td>8&lt;sup&gt;a&lt;/sup&gt;</td>
<td>9-62</td>
</tr>
<tr>
<td>OSPF</td>
<td>4</td>
<td>8</td>
<td>9-62</td>
</tr>
<tr>
<td>BGP4</td>
<td>1</td>
<td>4</td>
<td>13-27</td>
</tr>
</tbody>
</table>

<sup>1</sup>This value depends on the value for IP load sharing, and is not separately configurable.

### How IP Load Sharing Works

When the Routing Switch receives traffic for a destination and the IP route table contains multiple, equal-cost paths to that destination, the device checks the IP forwarding cache for a forwarding entry for the destination. The IP forwarding cache provides fast path for forwarding IP traffic, including load-balanced traffic. The cache contains entries that associate a destination host or network with a path (next-hop router).

- If the IP forwarding sharing cache contains a forwarding entry for the destination, the device uses the entry to forward the traffic.
- If the IP load forwarding cache does not contain a forwarding entry for the destination, the software selects a path from among the available equal-cost paths to the destination, then creates a forwarding entry in the cache based on the calculation. Subsequent traffic for the same destination uses the forwarding entry.

ProCurve Routing Switches support the following IP load sharing methods:

- Host-based – The Routing Switch uses a simple round-robin mechanism to distribute traffic across the equal-cost paths based on destination host IP address. This is the only method supported by and also is supported on Chassis Routing Switches.
- Network-based – The Routing Switch distributes traffic across equal-cost paths based on destination network address. The software selects a path based on a calculation involving the maximum number of load-sharing paths allowed and the actual number of paths to the destination network. This method is available only on Chassis Routing Switches and is the default.

In addition, on Chassis Routing Switches you can use network-based load sharing as the default while configuring host-based load sharing for specific destination networks. 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:** Regardless of the method of load sharing that is enabled, the Routing Switch always load shares paths for default routes and the network default route based on destination host address.
NOTE: The T-Flow uses hash-based load-balancing of equal-cost entries instead of host-based or network-based load balancing. 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. Hash-based load sharing applies to traffic forwarded by software, not to traffic forwarded by hardware. Normally, traffic is forwarded in software when you configure a CPU-based feature such as ACLs, rate limiting, or NetFlow. Traffic also is forwarded by software if the CAM (used for hardware forwarding) becomes full.

Path Redundancy

If a path to a given destination becomes unavailable, the Routing Switch provides redundancy by using another available equal-cost path to the destination, as described in the following sections.

NOTE: The following sections do not apply to the T-Flow. See the note above.

Response to Path State Changes

If one of the load-balanced paths to a cached destination becomes unavailable, or the IP route table receives a new equal-cost path to a cached destination, the software removes the unavailable path from the IP route table. Then the software selects a new path:

- For host-based IP load sharing, the next load-balancing cache entry uses the first path to the destination. The first path is the path that entered the IP route table first. "Host-Based IP Load Sharing" on page 9-54 describes the host-based load-sharing mechanism.

- For network-based IP load sharing, the next load-balancing cache entry uses the next available path that is then calculated based on the current number of paths and the maximum number of paths allowed. "Network-Based IP Load Sharing" on page 9-56 describes the network-based load-sharing mechanism.

Host-Based IP Load Sharing

The host-based load sharing method uses a simple round-robin mechanism to select an equal-cost path for traffic to a destination host. When the Routing Switch receives traffic for a destination host and the IP route table has multiple equal-cost paths to the host, the Routing Switch checks the IP forwarding cache for a forwarding entry to the destination.

- If the IP forwarding cache contains a forwarding entry for the destination, the device uses the entry to forward the traffic.

- If the IP forwarding cache does not contain a forwarding entry for the destination, the software selects the next path in the rotation (the path after the one the software used for the previous load sharing selection). The software then creates an IP forwarding cache entry that associates the destination host IP address with the selected path (next-hop IP address).

A cache entry for host-based IP load sharing has an age time of ten minutes. If a cache entry is not used before the age time expires, the device deletes the cache entry. The age time for IP load sharing cache entries is not configurable.

Figure 9.5 shows an example of host-based IP load sharing. In this example, the Routing Switch has two equal-cost paths to hosts H1 – H9. For simplicity, this example assumes that the Routing Switch does not have any entries in its IP forwarding cache to begin with, and receives traffic for the destination hosts (H1 – H9) in ascending numerical order, beginning with H1 and ending with H9.
Figure 9.5  Host-based IP load sharing – basic example

The cache entries in this example are based on the assumption that R1 receives traffic for hosts H1 - H9 in that order.

Once a packet for host H1 is received, the cache entry applies to all traffic for H1. Thus, R2 is always used.

As shown in this example, when the Routing Switch receives traffic for a destination and the IP route table has multiple equal-cost paths to that destination, the Routing Switch selects the next equal-cost path (next-hop router) in the rotation and assigns that path to destination. The path rotation is determined by the order in which the IP route table receives the paths.

Since the configuration in this example contains two paths to hosts H1 – H9, the software alternates between the two paths when creating new load sharing cache entries for hosts H1 – H9. So long as the cache entry for a destination remains in the cache, the Routing Switch always uses the same path for the traffic to the destination. In this example, the Routing Switch always uses R2 as the next hop for forwarding traffic to H1.

Figure 9.6 shows another example of IP forwarding cache entries for the configuration shown in Figure 9.5. The network and load sharing configurations are the same, but the order in which R1 receives traffic for the host is different. The paths differ due to the order in which the Routing Switch receives the traffic for the destination hosts.
Figure 9.6 Host-based IP load sharing – additional example

Network-Based IP Load Sharing

Network-based load sharing distributes traffic across multiple equal-cost paths based on the destination network. This method of load sharing optimizes system resources by aggregating the forwarding cache entries used for load sharing. Host-based load sharing contains a separate cache entry for each destination host, whereas network-based load sharing contains a single entry for each destination network.

The network-based load sharing method is available only on Chassis Routing Switches and is the default.

When the Routing Switch receives traffic for a device on a destination network for which the IP route table has multiple equal-cost paths, the Routing Switch checks the IP forwarding cache for a forwarding entry to the destination network:

- If the IP forwarding cache contains a forwarding entry for the destination network, the device uses the entry to forward the traffic.
- If the IP forwarding cache does not contain a forwarding entry for the destination network, the software selects the next path in the rotation (the path after the one the software used for the previous load sharing selection). The software then creates an IP forwarding cache entry that associates the destination network address with the selected path. IP forwarding cache entries for network-based load sharing do not age out. Once the software creates a cache entry for a destination network, traffic for all hosts on the network uses the same path. The cache entries remain in effect until the state of one of the paths changes or the software is reloaded.

Figure 9.7 shows an example of IP load sharing cache entries for network-based IP load sharing. The network in this example is the same as the network in Figure 9.5 and Figure 9.6. Notice that the cache contains one entry for...
each destination network, instead of a separate entry for each destination host. Based on the cache entries, traffic for all hosts (H1, H2, and H3) on network N1 uses the path through R2.

Figure 9.7 Network-based IP load sharing – basic example

R1 is configured with four IP load sharing paths, and has two paths to networks N1 - N3, attached to R4.

The cache entries in this example are based on the assumption that R1 receives traffic for hosts in N1 - N3 in that order.

Once a packet for a host on N1 is received, the cache entry applies to all hosts on N1. The same applies for N2 and N3.

Notice that network-based load sharing does not use a simple round-robin method. The path rotation starts with path 2, then proceeds in ascending numerical order through the remaining paths and ends with path 1. In Figure 9.7, the first cache entry uses path 2 instead of path 1. The algorithm evenly distributes the load among the available paths, but starts with the second path instead of the first path.

For optimal results, set the maximum number of paths to a value at least as high as the maximum number of equal-cost paths your network typically contains. For example, if the Routing Switch you are configuring for IP load sharing has six next-hop routers, set the maximum paths value to six. See “Changing the Maximum Number of Load Sharing Paths” on page 9-62.

**NOTE:** If the setting for the maximum number of paths is lower than the actual number of equal-cost paths, the software does not use all the paths for load sharing.

The network-based IP load sharing mechanism selects a path based on the following calculation, which involves the maximum number of paths allowed on the Routing Switch and the number of equal-cost paths available to the destination network.

\[ M \text{ modulo } P + 1 = S \]

where:

\[ M = \text{A number from 1 to the maximum number of load-sharing paths. This value increases by 1 until it reaches the maximum, then reverts to 1.} \]
P = Number of equal-cost paths to destination network
S = Selected path

For reference, the following table lists the path that the network-based IP load sharing algorithm will select for each combination of maximum number of paths and number of actual paths to the destination network. The software orders the available paths based on when they enter the IP route table. The first path to enter the table is path 1, and so on.

The rows with maximum path value 4 list the path selections that occur using the default maximum number of load sharing paths, which is four.

<table>
<thead>
<tr>
<th>Number of Paths</th>
<th>Maximum Paths</th>
<th>Path Counter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>1  2  3  4  5  6  7  8</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2  1  2  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2  1  2  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  1  2  1  2  1  2  1</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>2  3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1  2  3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1  2  3  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1  2  3  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  1  2  3  1  2  3</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>2  3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4  1</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4  1  2</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4  1  2  3</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4  1  2  3  4</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>2  3  4  1  2  3  4  1</td>
<td></td>
</tr>
</tbody>
</table>
Table 9.5: Path Selection for Network-Based IP Load Sharing (Continued)

<table>
<thead>
<tr>
<th>Number of Paths</th>
<th>Maximum Paths</th>
<th>Path Counter Value</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>1 2 3 4 5 6 7 8</td>
</tr>
<tr>
<td>5</td>
<td>2</td>
<td>2 3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 3 4</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 3 4 5</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 4 5 1</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 4 5 1 2</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 4 5 1 2 3</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 4 5 1 2 3 4</td>
</tr>
<tr>
<td>6</td>
<td>2</td>
<td>2 3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 3 4</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 3 4 5</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 4 5 6</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 4 5 6 1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 4 5 6 1 2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 4 5 6 1 2 3</td>
</tr>
<tr>
<td>7</td>
<td>2</td>
<td>2 3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 3 4</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 3 4 5</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 4 5 6</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 4 5 6 7</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 4 5 6 7 1</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 4 5 6 7 1 2</td>
</tr>
<tr>
<td>8</td>
<td>2</td>
<td>2 3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 3 4</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 3 4 5</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 4 5 6</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 4 5 6 7</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 4 5 6 7 8</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 4 5 6 7 8 1</td>
</tr>
</tbody>
</table>
As shown in Table 9.5, the results of the network-based IP load sharing algorithm provide evenly-distributed load sharing. Figure 9.8 shows a network where a Routing Switch has eight equal-cost paths to destination networks N1 – N8. The Routing Switch (R1) has been enabled to support up to eight IP load sharing paths.

**Figure 9.8  Network-based IP load sharing – example with eight equal-cost paths and eight destination networks**

As shown in this example, the algorithm for network-based IP load-sharing does not select the paths beginning with the first path, but the algorithm nonetheless results in an evenly distributed selection of paths.

**Disabling or Re-Enabling Load Sharing**

If you do not use IP load sharing and you want to disable the feature, use either of the following methods.

**USING THE CLI**

To disable IP load sharing, enter the following commands:

```
ProCurveRS(config)# no ip load-sharing
```

**Syntax:** `[no] ip load-sharing`
**Configuring IP**

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Click the Disable radio button next to Load Sharing.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Changing the Load Sharing Method on Chassis Routing Switches**

Chassis Routing Switches can perform IP load sharing based on destination host address or destination network address. The default for all Chassis Routing Switches is network-based IP load sharing. If you want to enable a Chassis Routing Switch to perform host-based IP load sharing instead, use either of the following methods.

**NOTE:** Regardless of the method of load sharing that is enabled on a Routing Switch, the Routing Switch always load shares paths for default routes and the network default route based on destination host address.

**NOTE:** The T-Flow uses hash-based load balancing instead of host-based or network-based load balancing. 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.

**USING THE CLI**

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 at the same time.

**Syntax:** `[no] ip load-sharing by-host`

To disable host-based IP load sharing and re-enable network-based IP load sharing, enter the following command:

```
ProCurveRS(config)# 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**).

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

**Enabling Host-Based Load-Sharing for a Specific Destination Network**

Chassis Routing Switches can perform IP load sharing on a network basis or an individual host basis. The default on these devices is network-based load sharing. You can take advantage of the forwarding-cache optimization provided by network-based load sharing while using the more granular host-based load sharing for specific destination networks.

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 destination networks.

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 contains 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.

To enable host-based load sharing for a specific destination network, use the following CLI method.

**USING THE CLI**

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

```
[no] ip load-sharing route-by-host <ip-addr>/<mask-bits>
```

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

**Disabling Host-Based Load-Sharing**

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.

Use either of the following methods to disable host-based load sharing for destination networks for which you have configured the feature.

**USING 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.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

**Changing the Maximum Number of Load Sharing Paths**

By default, IP load sharing allows IP traffic to be balanced across up to four equal paths. You can change the maximum number of paths the Routing Switch supports to a value from 2 – 8.

For optimal results, set the maximum number of paths to a value at least as high as the maximum number of equal-cost paths your network typically contains. For example, if the Routing Switch you are configuring for IP load sharing has six next-hop routers, set the maximum paths value to six.
NOTE: If the setting for the maximum number of paths is lower than the actual number of equal-cost paths, the software does not use all the paths for load sharing.

To change the number of paths, use either of the following methods.

**USING THE CLI**

To change the number of IP load sharing paths, enter a command such as the following:

```
ProCurveRS(config)# ip load-sharing 8
```

**Syntax:** `[no] ip load-sharing [<num>]`

The `<num>` parameter specifies the number of paths and can be from 2 – 8.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Edit the value in the # of Paths field. You can enter a number from 2 – 8.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

**Optimizing the IP Forwarding Cache**

Chassis Routing Switches use *Content Addressable Memory (CAM)* as a fast lookup cache to optimize IP forwarding. The CAM contains an IP route’s destination and the IP address of the next-hop gateway, as well as pointers to packet information in various system buffers. When the Routing Switch is ready to forward a packet to its destination, the Routing Switch checks the CAM for a forwarding entry for the packet.

- If the CAM contains an entry, the Routing Switch uses the entry to forward the packet.
- If the CAM does not contain an entry, the Routing Switch searches the IP route table for a route to the packet’s destination, then programs an entry into the CAM for the destination and its next-hop gateway. The Routing Switch uses the CAM entry to forward the next packet to this destination.

By default, the CAM is optimized for environments with a lot of routes to different destination networks. Each CAM entry provides fast-path information for a different destination sub-net.

You can configure the following cache and CAM optimization options:

- **ip hi-perf** – Enables the cache to contain more unique host route entries for unicast traffic.

**NOTE:** This feature is enabled by default in software release 07.5.04 and later.

- The following features optimize 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.
  - **ip net-aggregate** – Divides the IP address space into 4096 (2^12) aggregate entries and applies a 12-bit prefix to each aggregate entry.
  - **ip net-aggregate premium** – Divides the IP address space into 8192 (2^13) aggregate entries and applies a 13-bit prefix to each aggregate entry. This feature is supported in software releases 07.8.00 and later. See “Increased CAM Network Aggregation in Release 07.8.00 (9300 Series Only)” on page 9-65.
• **ip net-aggregate supreme** – Divides the IP address space into 16,384 ($2^{14}$) aggregate entries and applies a 14-bit prefix to each aggregate entry. This feature is supported in software releases 07.8.00 and later. See “Increased CAM Network Aggregation in Release 07.8.00 (9300 Series Only)” on page 9-65.

• **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.

Regardless of whether one of the CAM optimization options described above is enabled, the Routing Switch uses the IP cache to store forwarding information, then uses the forwarding information in the IP cache to program the CAM. The IP cache can contain host route entries, network route entries, and aggregate entries (aggregate routes of varying prefix lengths or fixed-size portions of the default route). However, regardless of the CAM optimization options, the `show ip cache` command displays only the host route entries.

### Disabling Unicast High-Performance Mode

By default, the unicast high-performance mode is enabled. This mode increases the device's capacity for unicast entries. To disable or re-enable the feature, use the following CLI method.

**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.

**NOTE:** The feature is disabled by default in software releases earlier than 07.5.04.

**USING THE CLI**

To disable the high-performance mode, enter the following commands:

```
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:

```
ProCurveRS(config)# ip high-perf
ProCurveRS(config)# write memory
ProCurveRS(config)# end
ProCurveRS# reload
```

**Syntax:** `[no] ip high-perf`

### CAM Optimization Options

By default, the device programs a separate route entry for each destination network. For example, if the device forwards traffic to 10.0.0.0/24, 10.0.10.0/24, and 10.10.0.20/24, the device programs a separate CAM entry for each of the three destination networks.

In many cases, the default behavior provides optimal routing performance. However, you may want to enable a CAM optimization option if either of the following conditions is true:

- The device has a very large IP route table (100,000 routes or more). For example, this can occur if the device is a BGP4 router and contains a full set of BGP4 routes. If most of the BGP4 routes actually go to the same set of next hops as the default route, enable the CAM network aggregation feature.
- The device has relatively few explicit routes in the IP route table and uses the default route for all other traffic. In this case, enable the CAM default route aggregation feature.

With CAM network aggregation enabled, the device forward 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 aggregate (for example, /12) 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 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 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.

Increased CAM Network Aggregation in Release 07.8.00 (9300 Series Only)

NOTE: This feature applies to EP and 10-Gigabit Ethernet devices.

• In releases prior to 07.8.00, when you enable CAM network aggregation (ip net-aggregate command), the maximum number of aggregate entries is 4096 and each aggregate entry has a 12-bit prefix (/12).

• Starting in release 07.8.00, on EP and 10-Gigabit Ethernet devices, you can increase the number of aggregate entries on an HP device from a maximum of 4096 (the default), to a maximum of 8192 or 16,384 entries, depending on the Layer 3 CAM space available on the device. The device automatically adjusts the prefix for each aggregate entry, according to the maximum number of aggregate entries allowed on the device, as shown in Table 9.6.

The following table shows the CAM network aggregation support in releases 07.8.00 and above on EP and 10-Gigabit Ethernet devices.

<table>
<thead>
<tr>
<th>Description</th>
<th>Maximum Number of Aggregate Entries</th>
<th>Prefix</th>
</tr>
</thead>
<tbody>
<tr>
<td>Standard CAM optimization (default)</td>
<td>4096</td>
<td>/12</td>
</tr>
<tr>
<td>Premium CAM optimization</td>
<td>8192</td>
<td>/13</td>
</tr>
<tr>
<td>Supreme CAM optimization</td>
<td>16,384</td>
<td>/14</td>
</tr>
</tbody>
</table>

One advantage to an increased number of aggregate entries is better load balancing for outgoing traffic, since most of the routes use the default route's set of next hops rather than a single next hop destination. In addition, since EP and 10-Gigabit Ethernet modules have extensive Layer 3 CAM space, the software can allocate more aggregate entries without compromising the space needed for entries that cannot be aggregated.

Configuration Notes

• Premium and Supreme CAM optimization features are supported in software releases 07.8.00 and later.

• Premium and Supreme CAM optimization features are supported on devices with EP and 10-Gigabit Ethernet only.

• Before configuring Premium and Supreme CAM optimization features, you must check the Layer 3 CAM on all interface modules to ensure there is enough space to hold as many routes (aggregate as well as non-aggregate routes) as possible. To check the Layer 3 CAM, use the show cam-partition command. To increase the Layer 3 CAM partition, use the cam-partition command.
• If you have a mixture of modules in an HP chassis device, the software uses the lowest common denominator to determine the maximum number of supported CAM network aggregate entries.

**Maximum Number of Aggregate Entries per Module**

The maximum number of CAM network aggregate entries supported on your device depends on the availability of, and the constraints on, the Layer 3 CAM. When you enable CAM network aggregation, the device will increase the number of CAM network aggregate entries up to a maximum of 50% of the IP route (Layer 3) CAM space, excluding IP supernet and IPX networks.

For example, as shown in Table 9.7, in order to increase the number of aggregate entries to 8000 on a 9300 series device, the device must have a minimum of 16,000 CAM entries available in Layer 3 CAM, excluding the IPX partition and the IP supernet areas. Similarly, in order to increase the number of CAM network aggregate entries to 16,000 on an 9300 series EP-based device, the IP Layer 3 CAM must be capable of holding at least 32,000 aggregate entries.

Note that CAM space on Standard modules is limited and is also shared between two or more DMAs. Adversely, CAM space on EP modules is larger because these devices use Ternary CAM (TCAM), which is capable of being partitioned. The CAM space on 10-Gigabit Ethernet modules is similar to that on EP and the overall space is even larger.

Table 9.7 shows the maximum number of supported aggregate entries per HP module.

<table>
<thead>
<tr>
<th>Module</th>
<th>Device</th>
<th>Minimum Number of CAM Entries Available in Layer 3 CAM</th>
<th>Maximum Supported CAM Network Aggregate Entries</th>
</tr>
</thead>
<tbody>
<tr>
<td>EP</td>
<td>9300 series</td>
<td>32K</td>
<td>16K</td>
</tr>
<tr>
<td>Standard</td>
<td>9300 series</td>
<td>16K</td>
<td>8K</td>
</tr>
<tr>
<td>10 Gigabit Ethernet</td>
<td>9300 series</td>
<td>64K</td>
<td>16K</td>
</tr>
</tbody>
</table>

1. The numbers shown are per DMA.

**Enabling Standard Optimization for CAM Network Aggregation**

When you enable standard optimization of CAM network aggregation, the software divides the IP address space into 4096 ($2^{12}$) aggregate entries and applies a 12-bit prefix to each aggregate entry.

To enable standard CAM network aggregation, enter the following command at the global CONFIG level of the CLI:

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

**Syntax:** `[no] ip net-aggregate [<secs>]`

**Enabling Premium Optimization for CAM Network Aggregation**

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.

**NOTE:** This feature is supported in releases 07.8.00 and later.

To enable premium optimization for CAM network aggregation, enter the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# ip net-aggregate premium
```

**Syntax:** `[no] ip net-aggregate premium`
Enabling Supreme Optimization for CAM Network Aggregation

When you enable supreme optimization of CAM network aggregation, the software divides the IP address space into 16,384 \(2^{14}\) aggregate entries and applies a 14-bit prefix to each aggregate entry.

NOTE: This feature is supported in releases 07.8.00 and later.

To enable supreme CAM network aggregation, enter the following command at the global CONFIG level of the CLI:

```
ProCurveRS(config)# ip net-aggregate supreme
```

**Syntax:** [no] ip net-aggregate supreme

Displaying CAM Network Aggregation Entries

To display the CAM network aggregation entries, enter the following command at any level of the CLI:

```
ProCurveRS(config)# show ip net-aggregate
```

This example shows that premium optimization for CAM network aggregation is enabled. The default-route optimization feature divides the default route into individual networks with 13-bit prefixes. The first entry is network 0.0.0.0/13, the second entry is network 0.16.0.0/13, and so on.

**Syntax:** show ip net-aggregate [<starting-entry-num> | <ip-addr> | not-eligible]

The `<starting-entry-num>` specifies the entry number you want the command’s output to start with. By default, the display begins with the first entry.

The `<ip-addr>` parameter specifies the IP address of a destination. The CAM entry that contains the specified address is displayed.

The `not-eligible` parameter displays only the entries that are ineligible for use because they contain a destination network that the Routing Switch uses a route other than the default route to reach.
The `show ip net-aggregate` command displays the following information.

### Table 9.8: CLI Display of CAM

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Total prefixes</td>
<td>The total number of entries in the CAM.</td>
</tr>
<tr>
<td>CAM Ineligible</td>
<td>The number of entries that cannot be used for fast-path forwarding because the IP route table contains a route whose destination network is contained in the entry’s aggregate network, but does not use the default route.</td>
</tr>
<tr>
<td>Setups</td>
<td>The number of times the entire CAM has been reprogrammed during the current power cycle. Generally, this occurs when the default route changes.</td>
</tr>
<tr>
<td>Updates</td>
<td>The number of individual entries that have been updated due during the current power cycle to a route change.</td>
</tr>
<tr>
<td>Start index</td>
<td>The entry number of the first entry in the display. If you specify a starting entry number when you enter the <code>show ip net-aggregate</code> command, then this field shows that number. Otherwise, the starting number is 1.</td>
</tr>
<tr>
<td>Destination address</td>
<td>An aggregate network address. If a route’s destination is contained in this aggregate address, then this CAM entry is applicable to the destination.</td>
</tr>
<tr>
<td>Gateway</td>
<td>The IP address of the next-hop gateway reached through the default route.</td>
</tr>
<tr>
<td>CAM Entry Flag</td>
<td>A value used by HP Technical Support for troubleshooting.</td>
</tr>
<tr>
<td>CIDXn</td>
<td>A value used by HP Technical Support for troubleshooting.</td>
</tr>
</tbody>
</table>

### CAM Default Route Aggregation

The CAM default route aggregation feature optimizes CAM use in environments that have relatively few explicit routes in the route table and use a default route heavily.

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.

**Enabling CAM Default Route Aggregation**

To enable CAM default route optimization, enter the following command at the global CONFIG level of the CLI:

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

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

To disable the default-route aggregation mode, enter the following command:

```bash
ProCurveRS(config)# no ip dr-aggregate
```

**Displaying the CAM Default Route Aggregation CAM Entries**

To display the CAM default route aggregation entries, enter the following command at any level of the CLI:

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

**Syntax:** `show ip dr-aggregate [<ip-addr>]`

If you specify an IP address, only the entries for that destination are displayed.

Here is an example of the information displayed by this command.

```bash
ProCurveRS(config)# show ip dr-aggregate
Total number of cache entries: 2
Start index: 1  D:Dynamic  P:Permanent  F:Forward  U:Us  C:Complex Filter
W:Wait ARP  I:ICMP Deny  K:Drop  R:Fragment  S:Snap Encap
   IP Address      Next Hop       MAC          Type  Port  Vlan  Pri
 1  22.22.22.22     /8  207.95.6.60   0044.052e.4302  DF  1/1  1  0
 2  207.96.7.7      /12 207.95.6.60   0044.052e.4302  DF  1/1  1  0
```

This example shows two entries. The prefix associated with each entry is displayed. Notice that the prefix lengths in this example are different for each entry. The software selects a prefix length long enough to make the default network route entry unambiguous, so that is does not conflict with other cache entries.

To display the entry for a specific destination, enter the destination address, as shown in the following example.

```bash
ProCurveRS(config)# show ip dr-aggregate 207.96.7.7
Total number of cache entries: 2
Start index: 1  D:Dynamic  P:Permanent  F:Forward  U:Us  C:Complex Filter
W:Wait ARP  I:ICMP Deny  K:Drop  R:Fragment  S:Snap Encap
   IP Address      Next Hop       MAC          Type  Port  Vlan  Pri
 1  207.96.7.7      /12 207.95.6.60   0044.052e.4302  DF  1/1  1  0
```

June 2005
This example shows the second entry from the previous example, but the entry row number is 1. The row number identifies the row number in the displayed output. In addition, notice that the Total number of cache entries field shows 2, as in the previous example. The number in this field indicates the total number of default route aggregation entries in the forwarding cache.

**Clearing the Forwarding Cache Entries for Default Routes**

To clear the entries, enter the following command from the Privileged EXEC level of the CLI:

```
ProCurveRS# clear ip dr-aggregate
```

*Syntax:* clear ip dr-aggregate

*NOTE:* This command does not affect other types of forwarding cache entries.

---

## Configuring 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. You can enable the feature on a global basis or on an individual port basis.

- If you enable the feature globally, all ports use the default values for the IRDP parameters.
- If you leave the feature disabled globally but enable it on individual ports, you also can configure the IRDP parameters on an individual port basis.

*NOTE:* You can configure IRDP parameters only on an individual port basis. To do so, IRDP must be disabled globally and enabled only on individual ports. You cannot configure IRDP parameters if the feature is globally enabled.

When IRDP is enabled, the Routing Switch periodically sends Router Advertisement messages out the IP interfaces on which the feature is enabled. 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 the Router Solicitation messages to discover their default gateway. When IRDP is enabled on the ProCurve Routing Switch, the Routing Switch 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.

IRDP uses the following parameters. If you enable IRDP on individual ports instead of enabling the feature globally, you can configure these parameters on an individual port basis.

- **Packet type** – The Routing Switch can send Router Advertisement messages as IP broadcasts or as IP multicasts addressed to IP multicast group 224.0.0.1. The packet type is IP broadcast.

- **Maximum message interval and minimum message interval** – When IRDP is enabled, the Routing Switch sends the Router Advertisement messages every 450 – 600 seconds by default. The time within this interval that the Routing Switch selects is random for each message and is not affected by traffic loads or other network factors. The random interval minimizes the probability that a host will receive Router Advertisement messages from other routers at the same time. The interval on each IRDP-enabled Routing Switch interface is independent of the interval on other IRDP-enabled interfaces. The default maximum message interval is 600 seconds. The default minimum message interval is 450 seconds.

- **Hold time** – Each Router Advertisement message contains a hold time value. This value specifies the maximum amount of time the host should consider an advertisement to be valid until a newer advertisement arrives. When a new advertisement arrives, the hold time is reset. The hold time is always longer than the maximum advertisement interval. Therefore, if the hold time for an advertisement expires, the host can reasonably conclude that the router interface that sent the advertisement is no longer available. The default hold time is three times the maximum message interval.
• Preference – If a host receives multiple Router Advertisement messages from different routers, the host selects the router that sent the message with the highest preference as the default gateway. The preference can be a number from -2,147,483,648 to 2,147,483,647. The default is 0.

Enabling IRDP Globally
To enable IRDP globally, use either of the following methods.

USING THE CLI
To globally enable IRDP, enter the following command:

ProCurveRS(config)# ip irdp

This command enables IRDP on the IP interfaces on all ports. Each port uses the default values for the IRDP parameters. The parameters are not configurable when IRDP is globally enabled.

USING THE WEB MANAGEMENT INTERFACE
1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the General link to display the IP configuration panel.
5. Select Enable next to IRDP.
6. Click the Apply button to save the change to the device’s running-config.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Enabling IRDP on an Individual Port
To enable IRDP on an individual port and configure IRDP parameters, use either of the following methods.

USING THE CLI
To enable IRDP on an individual interface and change IRDP parameters, enter commands such as the following:

ProCurveRS(config)# interface ethernet 1/3
ProCurveRS(config-if-1/3)# ip irdp maxadvertinterval 400

This example shows how to enable IRDP on a specific port and change the maximum advertisement interval for Router Advertisement messages to 400 seconds.

NOTE: To enable IRDP on individual ports, you must leave the feature globally disabled.

Syntax: [no] ip irdp [broadcast | multicast] [holdtime <seconds>] [maxadvertinterval <seconds>] [minadvertinterval <seconds>] [preference <number>]

The broadcast | multicast parameter specifies the packet type the Routing Switch uses to send Router Advertisement.

• broadcast – The Routing Switch sends Router Advertisement as IP broadcasts. This is the default.

• multicast – The Routing Switch sends Router Advertisement as multicast packets addressed to IP multicast group 224.0.0.1.

The holdtime <seconds> parameter specifies how long a host that receives a Router Advertisement from the Routing Switch should consider the advertisement to be valid. When a host receives a new Router Advertisement message from the Routing Switch, the host resets the hold time for the Routing Switch to the hold time specified in the new advertisement. If the hold time of an advertisement expires, the host discards the advertisement, concluding that the router interface that sent the advertisement is no longer available. The value must be greater than the value of the maxadvertinterval parameter and cannot be greater than 9000. The default is three times the value of the maxadvertinterval parameter.
The `maxadvertinterval` parameter specifies the maximum amount of time the Routing Switch waits between sending Router Advertisements. You can specify a value from 1 to the current value of the `holdtime` parameter. The default is 600 seconds.

The `minadvertinterval` parameter specifies the minimum amount of time the Routing Switch can wait between sending Router Advertisements. The default is three-fourths (0.75) the value of the `maxadvertinterval` parameter. If you change the `maxadvertinterval` parameter, the software automatically adjusts the `minadvertinterval` parameter to be three-fourths the new value of the `maxadvertinterval` parameter. If you want to override the automatically configured value, you can specify an interval from 1 to the current value of the `maxadvertinterval` parameter.

The `preference <number>` parameter specifies the IRDP preference level of this Routing Switch. If a host receives Router Advertisements from multiple routers, the host selects the router interface that sent the message with the highest interval as the host's default gateway. The valid range is -2^32 to 2^32-1. The default is 0.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure these options using the Web management interface.

**Configuring RARP**

The Reverse Address Resolution Protocol (RARP) provides a simple mechanism for directly-attached IP hosts to boot over the network. RARP allows an IP host that does not have a means of storing its IP address across power cycles or software reloads to query a directly-attached router for an IP address.

RARP is enabled by default. However, you must create a RARP entry for each host that will use the Routing Switch for booting. A RARP entry consists of the following information:

- The entry number – the entry’s sequence number in the RARP table.
- The MAC address of the boot client.
- The IP address you want the Routing Switch to give to the client.

When a client sends a RARP broadcast requesting an IP address, the Routing Switch responds to the request by looking in the RARP table for an entry that contains the client's MAC address:

- If the RARP table contains an entry for the client, the Routing Switch sends a unicast response to the client that contains the IP address associated with the client's MAC address in the RARP table.
- If the RARP table does not contain an entry for the client, the Routing Switch silently discards the RARP request and does not reply to the client.

**How RARP Differs from BootP/DHCP**

RARP and BootP/DHCP are different methods for providing IP addresses to IP hosts when they boot. These methods differ in the following ways:

- **Location of configured host addresses**
  - RARP requires static configuration of the host IP addresses on the Routing Switch. The Routing Switch replies directly to a host's request by sending an IP address you have configured in the RARP table.
  - The Routing Switch forwards BootP and DHCP requests to a third-party BootP/DHCP server that contains the IP addresses and other host configuration information.
- **Connection of host to boot source (Routing Switch or BootP/DHCP server):**
  - RARP requires the IP host to be directly attached to the Routing Switch.
  - An IP host and the BootP/DHCP server can be on different networks and on different routers, so long as the routers are configured to forward (“help”) the host’s boot request to the boot server.
  - You can centrally configure other host parameters on the BootP/DHCP server, in addition to the IP address, and supply those parameters to the host along with its IP address.
To configure the Routing Switch to forward BootP/DHCP requests when boot clients and the boot servers are on different sub-nets on different Routing Switch interfaces, see “Configuring BootP/DHCP Forwarding Parameters” on page 9-78.

**Disabling RARP**

RARP is enabled by default. If you want to disable the feature, you can do so using either of the following methods.

**USING THE CLI**

To disable RARP, enter the following command at the global CONFIG level:

ProCurveRS(config)# no ip rarp

*Syntax:* [no] ip rarp

To re-enable RARP, enter the following command:

ProCurveRS(config)# ip rarp

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Select the Disable or Enable radio button next to RARP.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**Creating Static RARP Entries**

You must configure the RARP entries for the RARP table. The Routing Switch can send an IP address in reply to a client's RARP request only if create a RARP entry for that client.

To configure static RARP entries, use the following methods.

**USING THE CLI**

To assign a static IP RARP entry for static routes on an HP router, enter a command such as the following:

ProCurveRS(config)# rarp 1 1245.7654.2348 192.53.4.2

This command creates a RARP entry for a client with MAC address 1245.7654.2348. When the Routing Switch receives a RARP request from this client, the Routing Switch replies to the request by sending IP address 192.53.4.2 to the client.

*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. To determine the maximum number of entries supported on the device, see the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the *Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches* or the *Installation and Basic Configuration Guide for the ProCurve 9408si Routing Switch*.

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.
Advanced Configuration and Management Guide for ProCurve 9300/9400 Series Routing Switches

USING THE WEB MANAGEMENT INTERFACE

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.

2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.

3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.

4. Click on the General link to display the IP configuration panel.

5. Click the Static RARP link.

   • If the device does not have any static RARP entries, the Static RARP configuration panel is displayed, as shown in the following example.

   • If a static RARP entry is already configured and you are adding a new entry, click on the Add Static RARP link to display the Static RARP configuration panel, as shown in the following example.

   • If you are modifying an existing static RARP entry, click on the Modify button to the right of the row describing the entry to display the Static RARP configuration panel, as shown in the following example.

<table>
<thead>
<tr>
<th>Static RARP</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC Address:</td>
</tr>
<tr>
<td>IP Address:</td>
</tr>
</tbody>
</table>

6. Enter the MAC address.

7. Enter the IP address.

8. Click the Add button to save the change to the device’s running-config file.

9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Changing the Maximum Number of Static RARP Entries Supported

The number of RARP entries the Routing Switch supports depends on how much memory the Routing Switch has. To determine how many RARP entries your Routing Switch can have, display the system default information using the procedure in the “Displaying and Modifying System Parameter Default Settings” section of the “Configuring Basic Features” chapter of the Installation and Basic Configuration Guide for ProCurve 9300 Series Routing Switches or the Installation and Basic Configuration Guide for the ProCurve 9408sl Routing Switch.

If your Routing Switch allows you to increase the maximum number of RARP entries, you can use a procedure in the same section to do so.

NOTE: You must save the configuration to the startup-config file and reload the software after changing the RARP cache size to place the change into effect.

Configuring UDP Broadcast and IP Helper Parameters

Some applications rely on client requests sent as limited IP broadcasts addressed to the UDP’s application port. If a server for the application receives such a broadcast, the server can reply to the client. Routers do not forward subnet directed broadcasts, so the client and server must be on the same network for the broadcast to reach the server. If the client and server are on different networks (on opposite sides of a router), the client’s request cannot reach the server.
You can configure the Routing Switch to forward clients' requests to UDP application servers. To do so:

- Enable forwarding support for the UDP application port, if forwarding support is not already enabled.
- Configure a helper address on the interface connected to the clients. Specify the helper address to be the IP address of the application server or the subnet directed broadcast address for the IP sub-net the server is in. A helper address is associated with a specific interface and applies only to client requests received on that interface. The Routing Switch forwards client requests for any of the application ports the Routing Switch is enabled to forward to the helper address.

Forwarding support for the following application ports is enabled by default.

- bootps (port 67)
- dns (port 53)
- tftp (port 69)
- time (port 37)
- netbios-ns (port 137)
- netbios-dgm (port 138)
- tacacs (port 65)

**NOTE:** The application names are the names for these applications that the Routing Switch software recognizes, and might not match the names for these applications on some third-party devices. The numbers listed in parentheses are the UDP port numbers for the applications. The numbers come from RFC 1340.

**NOTE:** As shown above, forwarding support for BootP/DHCP is enabled by default. If you are configuring the Routing Switch to forward BootP/DHCP requests, see "Configuring BootP/DHCP Forwarding Parameters" on page 9-78.

You can enable forwarding for other applications by specifying the application port number.

You also can disable forwarding for an application.

**NOTE:** If you disable forwarding for a UDP application, forwarding of client requests received as broadcasts to helper addresses is disabled. Disabling forwarding of an application does not disable other support for the application. For example, if you disable forwarding of Telnet requests to helper addresses, other Telnet support on the Routing Switch is not also disabled.

### Enabling Forwarding for a UDP Application

If you want the Routing Switch to forward client requests for UDP applications that the Routing Switch does not forward by default, you can enable forwarding support for the port. To enable forwarding support for a UDP application, use either of the following methods. You also can disable forwarding for an application using these methods.

**NOTE:** You also must configure a helper address on the interface that is connected to the clients for the application. The Routing Switch cannot forward the requests unless you configure the helper address. See "Configuring an IP Helper Address" on page 9-79.

#### USING THE CLI

To enable the forwarding of SNMP trap broadcasts, enter the following command:

```
ProCurveRS(config)# ip forward-protocol udp snmp-trap
```

**Syntax:** `[no] ip forward-protocol udp <udp-port-name> | <udp-port-num>

The `<udp-port-name>` parameter can have one of the following values. For reference, the corresponding port numbers from RFC 1340 are shown in parentheses. If you specify an application name, enter the name only, not the parentheses or the port number shown here.
In addition, you can specify any UDP application by using the application's UDP port number.

The `<udp-port-num>` parameter specifies the UDP application port number. If the application you want to enable is not listed above, enter the application port number. You also can list the port number for any of the applications listed above.

To disable forwarding for an application, enter a command such as the following:

```
ProCurveRS(config)# no ip forward-protocol udp snmp
```

This command disables forwarding of SNMP requests to the helper addresses configured on Routing Switch interfaces.

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the General link to display the IP configuration panel.
5. Select the Disable or Enable radio button next to Broadcast Forward.
6. Click the Apply button to save the change to the device's running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

**NOTE:** To define the ports to be forwarded, select the UDP Helper link from the IP configuration sheet.

**Configuring an IP Helper Address**

To forward a client's broadcast request for a UDP application when the client and server are on different networks, you must configure a helper address on the interface connected to the client. Specify the server's IP address or the subnet directed broadcast address of the IP sub-net the server is in as the helper address.

You can configure up to 16 helper addresses on each interface. You can configure a helper address on an Ethernet port or a virtual interface. To configure a helper address, use either of the following methods.
**USING THE CLI**

To configure a helper address on interface 2 on chassis module 1, enter the following commands:

ProCurveRS(config)# interface e 1/2
ProCurveRS(config-if-1/2)# ip helper-address 1 207.95.7.6

The commands in this example change the CLI to the configuration level for port 1/2, then add a helper address for server 207.95.7.6 to the port. If the port receives a client request for any of the applications that the Routing Switch is enabled to forward, the Routing Switch forwards the client's request to the server.

**Syntax:** `ip helper-address <num> <ip-addr>`

The `<num>` parameter specifies the helper address number and can be from 1 – 16.

The `<ip-addr>` command specifies the server's IP address or the subnet directed broadcast address of the IP subnet the server is in.

**USING THE WEB MANAGEMENT INTERFACE**

To configure a helper address on an interface:

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to RIP in the tree view to expand the list of RIP option links.
4. Click on the UDP Helper link.
   - If the device does not have any UDP helper assignments, the UDP Helper configuration panel is displayed, as shown in the following example.
   - If a UDP helper assignment is already configured and you are adding a new one, click on the Add UDP Helper link to display the UDP Helper configuration panel, as shown in the following example.
   - If you are modifying an existing UDP helper assignment, click on the Modify button to the right of the row describing the assignment to display the UDP Helper configuration panel, as shown in the following example.

   ![UDP Helper Panel](image)

5. Select the port (and slot if applicable) on behalf of which the UDP helper packets will be forwarded.
6. Enter the IP address of the remote server for which the router will be relaying the packets.
7. Click the Add button to save the change to the device's running-config file.
8. To configure settings for another port, select the port (and slot, if applicable) and go to step 6.
9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device's flash memory.

To select an application to be forwarded to the server by the Routing Switch:

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to expand the list of configuration options.
3. Click on the plus sign next to RIP in the tree view to expand the list of RIP option links.
4. Click on the UDP Helper link.
5. Click on the Modify button to the right of the row describing the UDP helper assignment to display the UDP Helper configuration panel.
6. Click on the System Broadcast Forward or User Broadcast Forward link.
   • The System Broadcast Forward link displays a panel that lets you select a well-known UDP port.
   • The User Broadcast Forward link displays a panel that lets you enter any port number.
7. Select the port or enter a port number from 1 – 65535.
8. Click the Add button to save the change to the device's running-config file.
9. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Configuring BootP/DHCP Forwarding Parameters

A host on an IP network can use BootP/DHCP to obtain its IP address from a BootP/DHCP server. To obtain the address, the client sends a BootP/DHCP request. The request is a subnet directed broadcast and is addressed to UDP port 67. A limited IP broadcast is addressed to IP address 255.255.255.255 and is not forwarded by the ProCurve Routing Switch or other IP routers.

When the BootP/DHCP client and server are on the same network, the server receives the broadcast request and replies to the client. However, when the client and server are on different networks, the server does not receive the client's request, because the Routing Switch does not forward the request.

You can configure the Routing Switch to forward BootP/DHCP requests. To do so, configure a helper address on the interface that receives the BootP/DHCP requests from the client. Instead of the server's IP address, you can specify the subnet directed broadcast address of the IP sub-net the server is in.

BootP/DHCP Forwarding Parameters

The following parameters control the Routing Switch's forwarding of BootP/DHCP requests:

- Helper address – The BootP/DHCP server’s IP address. You must configure the helper address on the interface that receives the BootP/DHCP requests from the client. The Routing Switch cannot forward a request to the server unless you configure a helper address for the server.

- Gateway address – The Routing Switch places the IP address of the interface that received the BootP/DHCP request in the request packet's Gateway Address field (sometimes called the Router ID field). When the server responds to the request, the server sends the response as a unicast packet to the IP address in the Gateway Address field. (If the client and server are directly attached, the Gateway ID field is empty and the server replies to the client using a unicast or broadcast packet, depending on the server.)

By default, the Routing Switch uses the lowest-numbered IP address on the interface that receives the request as the Gateway address. You can override the default by specifying the IP address you want the Routing Switch to use.

- Hop Count – Each router that forwards a BootP/DHCP packet increments the hop count by 1. Routers also discard a forwarded BootP/DHCP request instead of forwarding the request if the hop count is greater than the maximum number of BootP/DHCP hops allows by the router. By default, a ProCurve Routing Switch forwards a BootP/DHCP request if its hop count is four or less, but discards the request if the hop count is greater than four. You can change the maximum number of hops the Routing Switch will allow to a value from 1 – 15.

NOTE: The BootP/DHCP hop count is not the TTL parameter.
Configuring IP Helper Address

The procedure for configuring a helper address for BootP/DHCP requests is the same as the procedure for configuring a helper address for other types of UDP broadcasts. See “Configuring an IP Helper Address” on page 9-76.

Changing the IP Address Used for Stamping BootP/DHCP Requests

When the Routing Switch forwards a BootP/DHCP request, the Routing Switch “stamps” the Gateway Address field. The default value the Routing Switch uses to stamp the packet is the lowest-numbered IP address configured on the interface that received the request. If you want the Routing Switch to use a different IP address to stamp requests received on the interface, use either of the following methods to specify the address.

The BootP/DHCP stamp address is an interface parameter. Change the parameter on the interface that is connected to the BootP/DHCP client.

**USING THE CLI**

To change the IP address used for stamping BootP/DHCP requests received on interface 1/1, enter commands such as the following:

```
ProCurveRS(config)# int e 1/1
ProCurveRS(config-if-1/1)# ip bootp-gateway 109.157.22.26
```

These commands change the CLI to the configuration level for port 1/1, then change the BootP/DHCP stamp address for requests received on port 1/1 to 192.157.22.26. The Routing Switch will place this IP address in the Gateway Address field of BootP/DHCP requests that the Routing Switch receives on port 1/1 and forwards to the BootP/DHCP server.

**Syntax:** `ip bootp-gateway <ip-addr>`

**USING THE WEB MANAGEMENT INTERFACE**

You cannot change the IP address used for stamping BootP/DHCP requests using the Web management interface.

Changing the Maximum Number of Hops to a BootP Relay Server

Each BootP/DHCP request includes a field Hop Count field. The Hop Count field indicates how many routers the request has passed through. When the Routing Switch receives a BootP/DHCP request, the Routing Switch looks at the value in the Hop Count field.

- If the hop count value is equal to or less than the maximum hop count the Routing Switch allows, the Routing Switch increments the hop count by one and forwards the request.
- If the hop count is greater than the maximum hop count the Routing Switch allows, the Routing Switch discards the request.

To change the maximum number of hops the Routing Switch allows for forwarded BootP/DHCP requests, use either of the following methods.

**NOTE:** The BootP/DHCP hop count is not the TTL parameter.

**USING THE CLI**

To modify the maximum number of BootP/DHCP hops, enter the following command:

```
ProCurveRS(config)# bootp-relay-max-hops 10
```

This command allows the Routing Switch to forward BootP/DHCP requests that have passed through up to ten previous hops before reaching the Routing Switch.

**Syntax:** `bootp-relay-max-hops <1-15>`
USING THE WEB MANAGEMENT INTERFACE

To modify the maximum number of hops supported:

1. Log on to the Routing Switch using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view to display the list of configuration options.
3. Click on the plus sign next to IP to display the list of IP configuration options.
4. Select the General link to display the IP configuration panel.
5. Enter a value from 1 – 15 in the BootP Relay Maximum Hop field.
6. Click the Apply button to save the change to the device’s running-config file.
7. Select the Save link at the bottom of the dialog. Select Yes when prompted to save the configuration change to the startup-config file on the device’s flash memory.

Displaying IP Configuration Information and Statistics

The following sections describe IP display options for Routing Switches.

Changing the Network Mask Display to Prefix Format

By default, the CLI displays network masks in classical IP address format (example: 255.255.255.0). You can change the displays to prefix format (example: /18) on a Routing Switch using the following CLI method.

NOTE: This option does not affect how information is displayed in the Web management interface.

USING THE CLI

To enable CIDR format for displaying network masks, entering the following command at the global CONFIG level of the CLI:

ProCurveRS(config)# ip show-subnet-length

Syntax: [no] ip show-subnet-length

USING THE WEB MANAGEMENT INTERFACE

You cannot configure this option using the Web management interface.

Displaying IP Information

You can display the following IP configuration information statistics on Routing Switches:

- Global IP parameter settings and IP access policies – see “Displaying Global IP Configuration Information” on page 9-81.
- IP interfaces – see “Displaying IP Interface Information” on page 9-85.
- ARP entries – see “Displaying ARP Entries” on page 9-88.
- Static ARP entries – see “Displaying ARP Entries” on page 9-88.
- IP forwarding cache – see “Displaying the Forwarding Cache” on page 9-91.
- IP route table – see “Displaying the IP Route Table” on page 9-93.

The sections below describe how to display this information.

In addition to the information described below, you can display the following IP information. This information is described in other parts of this guide.
Configuring IP

- RIP information – see “Displaying RIP Filters” on page 10-17.
- OSPF information – see “Displaying OSPF Information” on page 12-47.
- BGP4 information – see “Displaying BGP4 Information” on page 13-96.
- DVMRP information – see the “Show Commands” chapter in the Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches.
- PIM information – see the “Show Commands” chapter in the Command Line Interface Reference for ProCurve 9300/9400 Series Routing Switches.
- VRRP or VRRPE information – see “Displaying VRRP and VRRPE Information” on page 16-19.

Displaying Global IP Configuration Information

To display global IP configuration information for the router, use one of the following methods.

USING THE CLI

To display IP configuration information, enter the following command at any CLI level:

ProCurveRS> show ip

Global Settings
  ttl: 64, arp-age: 10, bootp-relay-max-hops: 4
  router-id: 207.95.11.128
  enabled: UDP-Broadcast-Forwarding, IRDP, Proxy-ARP, RARP, OSPF
  disabled: BGP4 Load-Sharing, RIP, DVMRP, VRRP

Static Routes
  Index  IP Address        Subnet Mask       Next Hop Router   Metric  Distance
  1     0.0.0.0           0.0.0.0           209.157.23.2     1      1

Policies
  Index  Action  Source  Destination  Protocol  Port  Operator
  1     deny    209.157.22.34  209.157.22.26  tcp       http =
  64    permit  any     any

Syntax: show ip

NOTE: This command has additional options, which are explained in other sections in this guide, including the sections below this one.
This display shows the following information.

### Table 9.9: CLI Display of Global IP Configuration Information

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Global settings</strong></td>
<td></td>
</tr>
<tr>
<td>ttl</td>
<td>The Time-To-Live (TTL) for IP packets. The TTL specifies the maximum number of router hops a packet can travel before reaching the HP router. If the packet's TTL value is higher than the value specified in this field, the HP router drops the packet.  To change the maximum TTL, see “Changing the TTL Threshold” on page 9-35.</td>
</tr>
<tr>
<td>arp-age</td>
<td>The ARP aging period. This parameter specifies how many minutes an inactive ARP entry remains in the ARP cache before the router ages out the entry.  To change the ARP aging period, see “Changing the ARP Aging Period” on page 9-31.</td>
</tr>
<tr>
<td>bootp-relay-max-hops</td>
<td>The maximum number of hops away a BootP server can be located from the HP router and still be used by the router's clients for network booting.  To change this value, see “Changing the Maximum Number of Hops to a BootP Relay Server” on page 9-79.</td>
</tr>
<tr>
<td>router-id</td>
<td>The 32-bit number that uniquely identifies the HP router.  By default, the router ID is the numerically lowest IP interface configured on the router.  To change the router ID, see “Changing the Router ID” on page 9-26.</td>
</tr>
<tr>
<td>enabled</td>
<td>The IP-related protocols that are enabled on the router.</td>
</tr>
<tr>
<td>disabled</td>
<td>The IP-related protocols that are disabled on the router.</td>
</tr>
<tr>
<td><strong>Static routes</strong></td>
<td></td>
</tr>
<tr>
<td>Index</td>
<td>The row number of this entry in the IP route table.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the route’s destination.</td>
</tr>
<tr>
<td>Subnet Mask</td>
<td>The network mask for the IP address.</td>
</tr>
<tr>
<td>Next Hop Router</td>
<td>The IP address of the router interface to which the HP router sends packets for the route.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost of the route. Usually, the metric represents the number of hops to the destination.</td>
</tr>
<tr>
<td>Distance</td>
<td>The administrative distance of the route. The default administrative distance for static IP routes in HP routers is 1.  To list the default administrative distances for all types of routes or to change the administrative distance of a static route, see “Changing Administrative Distances” on page 13-36.</td>
</tr>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
</tbody>
</table>
Table 9.9: CLI Display of Global IP Configuration Information (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The policy number. This is the number you assigned the policy when you configured it.</td>
</tr>
</tbody>
</table>
| Action        | The action the router takes if a packet matches the comparison values in the policy. The action can be one of the following:  
|               | • deny – The router drops packets that match this policy.  
|               | • permit – The router forwards packets that match this policy. |
| Source        | The source IP address the policy matches. |
| Destination   | The destination IP address the policy matches. |
| Protocol      | The IP protocol the policy matches. The protocol can be one of the following:  
|               | • ICMP  
|               | • IGMP  
|               | • IGRP  
|               | • OSPF  
|               | • TCP  
|               | • UDP  
| Port          | The Layer 4 TCP or UDP port the policy checks for in packets. The port can be displayed by its number or, for port types the router recognizes, by the well-known name. For example, TCP port 80 can be displayed as HTTP.  
|               | **Note:** This field applies only if the IP protocol is TCP or UDP. |
| Operator      | The comparison operator for TCP or UDP port names or numbers.  
|               | **Note:** This field applies only if the IP protocol is TCP or UDP. |

**USING THE WEB MANAGEMENT INTERFACE**

You cannot display global IP configuration information using the Web management interface.

**Displaying CPU Utilization Statistics**

You can display CPU utilization statistics for IP protocols using the `show process cpu` command.

Beginning with software release 07.6.04, the `show process cpu` command includes CPU utilization statistics for ACL, NAT, 802.1x, and L2VLAN. L2VLAN contains any packet transmitted to a VLAN by the CPU, including unknown unicast, multicast, broadcast, and CPU forwarded Layer 2 traffic.
**USING THE CLI**

To display CPU utilization statistics for the previous one-second, one-minute, five-minute, and fifteen-minute intervals, enter the following command at any level of the CLI:

```
ProCurveRS# show process cpu
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>5Sec(%)</th>
<th>1Min(%)</th>
<th>5Min(%)</th>
<th>15Min(%)</th>
<th>Runtime (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>714</td>
</tr>
<tr>
<td>BGP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>DOT1X</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>GVRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>L2VLAN</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.01</td>
<td>673</td>
</tr>
<tr>
<td>NAT</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>RIP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>9</td>
</tr>
<tr>
<td>STP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>7</td>
</tr>
<tr>
<td>VRRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
</tbody>
</table>

If the software has been running less than 15 minutes (the maximum interval for utilization statistics), the command indicates how long the software has been running. Here is an example:

```
ProCurveRS# show process cpu
The system has only been up for 6 seconds.
```

<table>
<thead>
<tr>
<th>Process Name</th>
<th>5Sec(%)</th>
<th>1Min(%)</th>
<th>5Min(%)</th>
<th>15Min(%)</th>
<th>Runtime (ms)</th>
</tr>
</thead>
<tbody>
<tr>
<td>ACL</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ARP</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>0.01</td>
<td>714</td>
</tr>
<tr>
<td>BGP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>DOT1X</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>GVRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>ICMP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>IP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>L2VLAN</td>
<td>0.01</td>
<td>0.00</td>
<td>0.00</td>
<td>0.01</td>
<td>673</td>
</tr>
<tr>
<td>NAT</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>OSPF</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
<tr>
<td>RIP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>9</td>
</tr>
<tr>
<td>STP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>7</td>
</tr>
<tr>
<td>VRRP</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0.00</td>
<td>0</td>
</tr>
</tbody>
</table>
To display utilization statistics for a specific number of seconds, enter a command such as the following:

```plaintext
ProCurveRS# show process cpu 2
Statistics for last 1 sec and 80 ms
Process Name  Sec(%)  Time(ms)
ACL          0     0.00
ARP          1     0.01
BGP          0     0.00
DOT1X        0     0.00
GVRP         0     0.00
ICMP         0     0.00
IP           0     0.00
L2VLAN       1     0.01
NAT          0     0.00
OSPF         0     0.00
RIP           0     0.00
STP           0     0.00
VRRP         0     0.00
```

When you specify how many seconds' worth of statistics you want to display, the software selects the sample that most closely matches the number of seconds you specified. In this example, statistics are requested for the previous two seconds. The closest sample available is actually for the previous 1 second plus 80 milliseconds.

**Syntax:** `show process cpu [<num>]`

The `<num>` parameter specifies the number of seconds and can be from 1 – 900. If you use this parameter, the command lists the usage statistics only for the specified number of seconds. If you do not use this parameter, the command lists the usage statistics for the previous one-second, one-minute, five-minute, and fifteen-minute intervals.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot display this information using the Web management interface.

**Displaying IP Interface Information**

To display IP interface information, use one of the following methods.

**USING THE CLI**

To display IP interface information, enter the following command at any CLI level:

```plaintext
ProCurveRS(config)# show ip interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK? Method</th>
<th>Status</th>
<th>Protocol</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ethernet 1/1</td>
<td>207.95.6.173</td>
<td>YES NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet 1/2</td>
<td>3.3.3.3</td>
<td>YES manual</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Loopback 1</td>
<td>1.2.3.4</td>
<td>YES NVRAM</td>
<td>down</td>
<td>down</td>
</tr>
</tbody>
</table>

**Syntax:** `show ip interface [ethernet <portnum>] | [loopback <num>] | [ve <num>]`
This display shows the following information.

### Table 9.10: CLI Display of Interface IP Configuration Information

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Interface</td>
<td>The type and the slot and port number of the interface.</td>
</tr>
</tbody>
</table>
| IP-Address    | The IP address of the interface.  
**Note:** If an “s” is listed following the address, this is a secondary address. When the address was configured, the interface already had an IP address in the same sub-net, so the software required the “secondary” option before the software could add the interface. |
| OK?           | Whether the IP address has been configured on the interface. |
| Method        | Whether the IP address has been saved in NVRAM. If you have set the IP address for the interface in the CLI or Web Management interface, but have not saved the configuration, the entry for the interface in the Method field is “manual”. |
| Status        | The link status of the interface. If you have disabled the interface with the `disable` command, the entry in the Status field will be “administratively down”. Otherwise, the entry in the Status field will be either “up” or “down”. |
| Protocol      | Whether the interface can provide two-way communication. If the IP address is configured, and the link status of the interface is up, the entry in the protocol field will be “up”. Otherwise the entry in the protocol field will be “down”. |

To display detailed IP information for a specific interface, enter a command such as the following:

```
ProCurveRS# show ip interface ethernet 1/1
Interface Ethernet 1/1
  port state: UP
  ip address: 192.168.9.51     subnet mask: 255.255.255.0
  encapsulation: ETHERNET, mtu: 1500, metric: 1
  directed-broadcast-forwarding: disabled
  proxy-arp: disabled
  ip arp-age: 10 minutes
  Ip Flow switching is disabled
  No Helper Addresses are configured.
  No inbound ip access-list is set
  No outgoing ip access-list is set
```

### USING THE WEB MANAGEMENT INTERFACE

To display IP interface information:

1. Log on to the using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Configure in the tree view.
3. Click on the plus sign next to IP in the tree view to expand the list of IP option links.
4. Click on the Interface link to display the IP interface table.
Configuring IP

Table 9.11: Web Display of IP Interface Information

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port #</td>
<td>The physical port number or virtual interface (VE) number. VEs are shown as “v&lt;num&gt;”, where &lt;num&gt; is the number you assigned to the VE when you configured it. For example, VE 1 is shown as “v1”. If a range of ports is listed in this field, the interface is a trunk group. If two ranges of ports are listed, the interface is a trunk group that spans multiple chassis modules.</td>
</tr>
<tr>
<td>Encapsulation</td>
<td>The frame type used to encapsulate packets on this interface. The frame type is always Ethernet II.</td>
</tr>
<tr>
<td>MTU</td>
<td>The Maximum Transmission Unit (MTU), which specifies the maximum packet size for packets sent and received on this interface.</td>
</tr>
<tr>
<td>Metric</td>
<td>The cost associated with this interface.</td>
</tr>
</tbody>
</table>
| Directed Broadcast Forward | The state of the directed broadcast forwarding feature. The state can be one of the following:  
  • Disable  
  • Enable  
  To change the state of this feature, see “Enabling Forwarding of Directed Broadcasts” on page 9-35.                                    |

Displaying Interface Name in Syslog

By default an interface's slot number (if applicable) and port number are displayed when you display Syslog messages. Beginning with release 07.6.04, you can display the name of the interface instead of its number by entering a command such as the following:

ProCurveRS(config)# ip show-portname

This command is applied globally to all interfaces on Routing Switches.

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" displayed as in the example below:

ProCurveRS>$ show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Buffer logging: level ACDMEINW, 3 messages logged
  level code: A=alert C=critical D=debugging M=emergency E=error
  I=informational N=notification W=warning

Static Log Buffer:
Dec 15 19:04:14:A:Fan 1, fan on right connector, failed

Dynamic Log Buffer (50 entries):
Dec 15 18:46:17:I:Interface ethernet Lab2, state up
Dec 15 18:45:15:I:Warm start
Displaying ARP Entries

You can display the ARP cache and the static ARP table. The ARP cache contains entries for devices attached to the Routing Switch. The static ARP table contains the user-configured ARP entries. An entry in the static ARP table enters the ARP cache when the entry's interface comes up.

The tables require separate display commands or Web management options.

Displaying the ARP Cache

To display the ARP cache, use one of the following methods.

**Using the CLI**

To display the contents of the ARP cache, enter the following command at any CLI level:

```text
ProCurveRS# show arp
```

```
Total number of ARP entries: 5

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Age</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>207.95.6.102</td>
<td>0800.5afc.ea21</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>207.95.6.18</td>
<td>00a0.24d2.04ed</td>
<td>Dynamic</td>
<td>3</td>
<td>6</td>
</tr>
<tr>
<td>207.95.6.54</td>
<td>00a0.24ab.cd2b</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>207.95.6.101</td>
<td>0800.207c.a7fa</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
</tr>
<tr>
<td>207.95.6.211</td>
<td>00c0.2638.ac9c</td>
<td>Dynamic</td>
<td>0</td>
<td>6</td>
</tr>
</tbody>
</table>
```

**Syntax:**`show arp [ethernet <portnum> | mac-address <xxxx.xxxx.xxxx> [<mask>] | <ip-addr> [<ip-mask>]] [<num>]`

The `ethernet <portnum>` parameter lets you restrict the display to entries for a specific port. The `mac-address <xxxx.xxxx.xxxx>` parameter lets you restrict the display to entries for a specific MAC address. The `<mask>` parameter lets you specify a mask for the `mac-address <xxxx.xxxx.xxxx>` parameter, to display entries for multiple MAC addresses. Specify the MAC address mask as “f”s and “0”s, where “f”s are significant bits.

The `<ip-addr>` and `<ip-mask>` parameters let you restrict the display to entries for a specific IP address and network mask. Specify the IP address masks in standard decimal mask format (for example, 255.255.0.0).

**NOTE:** The `<ip-mask>` parameter and `<mask>` parameter perform different operations. The `<ip-mask>` parameter specifies the network mask for a specific IP address, whereas the `<mask>` parameter provides a filter for displaying multiple MAC addresses that have specific values in common.

The `<num>` parameter lets you display the table beginning with a specific entry number.

**NOTE:** The entry numbers in the ARP cache are not related to the entry numbers for static ARP table entries.

This display shows the following information. The number in the left column of the CLI display is the row number of the entry in the ARP cache. This number is not related to the number you assign to static MAC entries in the static ARP table.

**Table 9.12: CLI Display of ARP Cache**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the device.</td>
</tr>
</tbody>
</table>
Table 9.12: CLI Display of ARP Cache (Continued)

<table>
<thead>
<tr>
<th>This Field</th>
<th>Displays</th>
</tr>
</thead>
</table>
| Type       | The type, which can be one of the following:  
|            | • Dynamic – The Routing Switch learned the entry from an incoming packet.  
|            | • Static – The Routing Switch loaded the entry from the static ARP table when the device for the entry was connected to the Routing Switch. |
| Age        | The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the table.  
|            | To display the ARP aging period, see “Displaying Global IP Configuration Information” on page 9-81. To change the ARP aging interval, see “Changing the ARP Aging Period” on page 9-31.  
|            | **Note**: Static entries do not age out. |
| Port       | The port on which the entry was learned. |

**USING THE WEB MANAGEMENT INTERFACE**

To display the IP ARP cache:

1. Log on to the using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to list the monitoring options.
3. Click on the ARP Cache link to display the IP ARP cache.

This display shows the following information.

Table 9.13: Web Display of ARP Cache

<table>
<thead>
<tr>
<th>This Field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td>Node</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the device.</td>
</tr>
</tbody>
</table>
| Type       | The type, which can be one of the following:  
|            | • Dynamic – The Routing Switch learned the entry from an incoming packet.  
|            | • Static – The Routing Switch loaded the entry from the static ARP table when the device for the entry was connected to the Routing Switch. |
| Age        | The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the cache.  
|            | To display the ARP aging period, see “Displaying Global IP Configuration Information” on page 9-81. To change the ARP aging interval, see “Changing the ARP Aging Period” on page 9-31.  
|            | **Note**: Static entries do not age out. |
### Table 9.13: Web Display of ARP Cache (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Port</td>
<td>The port attached to the device the entry is for. For dynamic entries, this is the port on which the entry was learned.</td>
</tr>
</tbody>
</table>

### Displaying the Static ARP Table

To display the static ARP table instead of the ARP cache, use either of the following methods.

**USING THE CLI**

To display the static ARP table, enter the following command at any CLI level:

```
ProCurveRS# show ip static-arp
```

Static ARP table size: 512, configurable from 512 to 1024

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>MAC Address</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>207.95.6.111</td>
<td>0800.093b.d210</td>
<td>1/1</td>
</tr>
<tr>
<td>3</td>
<td>207.95.6.123</td>
<td>0800.093b.d211</td>
<td>1/1</td>
</tr>
</tbody>
</table>

This example shows two static entries. Note that since you specify an entry’s index number when you create the entry, it is possible for the range of index numbers to have gaps, as shown in this example.

**NOTE:** The entry number you assign to a static ARP entry is not related to the entry numbers in the ARP cache.

**Syntax:** `show ip static-arp [ethernet <portnum> | mac-address <xxxx.xxxx.xxxx> [<mask>] | <ip-addr> [<ip-mask>] [<num>]]`

The `ethernet <portnum>` parameter lets you restrict the display to entries for a specific port.

The `mac-address <xxxx.xxxx.xxxx>` parameter lets you restrict the display to entries for a specific MAC address.

The `<mask>` parameter lets you specify a mask for the `mac-address <xxxx.xxxx.xxxx>` parameter, to display entries for multiple MAC addresses. Specify the MAC address mask as "f"s and "0"s, where "f"s are significant bits.

The `<ip-addr>` and `<ip-mask>` parameters let you restrict the display to entries for a specific IP address and network mask. Specify the IP address masks in standard decimal mask format (for example, 255.255.0.0).

**NOTE:** The `<ip-mask>` parameter and `<mask>` parameter perform different operations. The `<ip-mask>` parameter specifies the network mask for a specific IP address, whereas the `<mask>` parameter provides a filter for displaying multiple MAC addresses that have specific values in common.

The `<num>` parameter lets you display the table beginning with a specific entry number.

### Table 9.14: CLI Display of Static ARP Table

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Static ARP table size</td>
<td>The maximum number of static entries that can be configured on the device using the current memory allocation. The range of valid memory allocations for static ARP entries is listed after the current allocation. To change the memory allocation for static ARP entries, see “Changing the Maximum Number of Entries the Static ARP Table Can Hold” on page 9-33.</td>
</tr>
</tbody>
</table>
Table 9.14: CLI Display of Static ARP Table (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Index</td>
<td>The number of this entry in the table. You specify the entry number when you create the entry.</td>
</tr>
<tr>
<td>IP Address</td>
<td>The IP address of the device.</td>
</tr>
<tr>
<td>MAC Address</td>
<td>The MAC address of the device.</td>
</tr>
<tr>
<td>Port</td>
<td>The port attached to the device the entry is for.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**
You cannot display the static ARP table using the Web management interface.

**Displaying the Forwarding Cache**
To display the IP forwarding cache, use one of the following methods.

**NOTE:** To display only the forwarding cache entries for aggregated default network routes, see “CAM Default Route Aggregation” on page 9-68.

**USING THE CLI**
To display the IP forwarding cache, enter the following command at any CLI level:

ProCurveRS> show ip cache

Total number of cache entries: 3
D:Dynamic P:Permanent F:Forward U:Us C:Complex Filter
W:Wait ARP I:ICMP Deny K:Drop R:Fragment S:Snap Encap

<table>
<thead>
<tr>
<th>IP Address</th>
<th>Next Hop</th>
<th>MAC</th>
<th>Type</th>
<th>Port</th>
<th>Vlan</th>
<th>Pri</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 192.168.1.11</td>
<td>DIRECT</td>
<td>0000.0000.0000</td>
<td>PU</td>
<td>n/a</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>2 192.168.1.255</td>
<td>DIRECT</td>
<td>0000.0000.0000</td>
<td>PU</td>
<td>n/a</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>3 255.255.255.255</td>
<td>DIRECT</td>
<td>0000.0000.0000</td>
<td>PU</td>
<td>n/a</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**Syntax:** show ip cache [<ip-addr>] [<num>]
The <ip-addr> parameter displays the cache entry for the specified IP address.
The <num> parameter displays the cache beginning with the row following the number you enter. For example, to begin displaying the cache at row 10, enter the following command: **show ip cache 9**.

The **show ip cache** command displays the following information.

Table 9.15: CLI Display of IP Forwarding Cache

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the destination.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The IP address of the next-hop router to the destination. This field contains either an IP address or the value DIRECT. DIRECT means the destination is either directly attached or the destination is an address on this HP device. For example, the next hop for loopback addresses and broadcast addresses is shown as DIRECT.</td>
</tr>
</tbody>
</table>
### Table 9.15: CLI Display of IP Forwarding Cache (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
</table>
| MAC           | The MAC address of the destination.  
                **Note:** If the entry is type U (indicating that the destination is this HP device), the address consists of zeroes. |
| Type          | The type of host entry, which can be one or more of the following:  
                - D – Dynamic  
                - P – Permanent  
                - F – Forward  
                - U – Us  
                - C – Complex Filter  
                - W – Wait ARP  
                - I – ICMP Deny  
                - K – Drop  
                - R – Fragment  
                - S – Snap Encap |
| Port          | The port through which this device reaches the destination. For destinations that are located on this device, the port number is shown as “n/a”. |
| VLAN          | Indicates the VLAN(s) the listed port is in. |
| Pri           | The QoS priority of the port or VLAN. |

### USING THE WEB MANAGEMENT INTERFACE

To display the IP forwarding cache:

1. Log on to the using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to list the monitoring options.
3. Click on the plus sign next to IP to list the IP monitoring options.
4. Click on the Cache link to display the IP cache.

This display shows the following information.

### Table 9.16: Web Display of IP Forwarding Cache Information

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address</td>
<td>The IP address of the destination.</td>
</tr>
<tr>
<td>Next Hop</td>
<td>The IP address of the next-hop router to the destination. This field contains either an IP address or the value DIRECT. DIRECT means the destination is either directly attached or the destination is an address on this HP device. For example, the next hop for loopback addresses and broadcast addresses is shown as DIRECT.</td>
</tr>
</tbody>
</table>
Table 9.16: Web Display of IP Forwarding Cache Information (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>MAC</td>
<td>The MAC address of the destination. Note: If the entry is type U (indicating that the destination is this HP device), the address consists of zeroes.</td>
</tr>
</tbody>
</table>
| Type          | The type of host entry, which can be one or more of the following:  
• D – Dynamic  
• I – ICMP Deny  
• P – Permanent  
• F – Forward  
• U – Us  
• C – Complex Filter  
• K – Drop  
• W – Wait ARP  
• R – Fragment  
• S – Snap Encap |
| Action        | This information is used by HP customer support. |
| Flag Check    | This information is used by HP customer support. |
| Snap          | This information is used by HP customer support. |
| Port          | The port through which this device reaches the destination. For destinations that are located on this device, the port number is shown as “n/a”. |
| VLAN          | Indicates the VLAN(s) the listed port is in. |
| Priority      | The QoS priority of the port or VLAN. |

**Displaying the IP Route Table**

To display the IP route table, use one of the following methods.
**USING THE CLI**

To display the IP route table, enter the following command at any CLI level:

```
ProCurveRS> show ip route
```

Total number of IP routes: 514
Start index: 1  B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default

<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>1.1.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.2.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.3.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.4.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.5.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.6.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.7.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.8.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.9.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>R</td>
</tr>
<tr>
<td>1.10.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>1/1</td>
<td>2</td>
<td>S</td>
</tr>
</tbody>
</table>

**Syntax:** show ip route [<ip-addr>] [<ip-mask>] [longer] [none-bgp] | <num> | bgp | direct | ospf | rip | static

The `<ip-addr>` parameter displays the route to the specified IP address.

The `<ip-mask>` parameter lets you specify a network mask or, if you prefer CIDR format, the number of bits in the network mask. If you use CIDR format, enter a forward slash immediately after the IP address, then enter the number of mask bits (for example: 209.157.22.0/24 for 209.157.22.0 255.255.255.0).

The `longer` parameter applies only when you specify an IP address and mask. This option displays only the routes for the specified IP address and mask. See the example below.

The `none-bgp` parameter displays only the routes that did not come from BGP4.

The `<num>` option display the route table entry whose row number corresponds to the number you specify. For example, if you want to display the tenth row in the table, enter “10”.

The `bgp` option displays the BGP4 routes.

The `direct` option displays only the IP routes that are directly attached to the Routing Switch.

The `ospf` option displays the OSPF routes.

The `rip` option displays the RIP routes.

The `static` option displays only the static IP routes.

The default routes are displayed first.

Here is an example of how to use the `direct` option. To display only the IP routes that go to devices directly attached to the Routing Switch:

```
ProCurveRS(config)# show ip route direct
Start index: 1  B:BGP D:Connected  R:RIP  S:Static  O:OSPF *:Candidate default

Destination     NetMask       Gateway   Port | Cost | Type |
------------------------------------------|------|------|------|
209.157.22.0     255.255.255.0 0.0.0.0   4/11 | 1    | D    |
```

Notice that the route displayed in this example has “D” in the Type field, indicating the route is to a directly connected device.
Here is an example of how to use the **static** option. To display only the static IP routes:

```
ProCurveRS(config)# show ip route static
Start index: 1  B:BGP D:Connected R:RIP S:Static O:OSPF *:Candidate default
```

<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>192.144.33.11</td>
<td>255.255.255.0</td>
<td>209.157.22.12</td>
<td>1/1</td>
<td>2</td>
<td>S</td>
</tr>
</tbody>
</table>

Notice that the route displayed in this example has “S” in the Type field, indicating the route is static.

Here is an example of how to use the **longer** option. To display only the routes for a specified IP address and mask, enter a command such as the following:

```
ProCurveRS(config)# show ip route 209.159.0.0/16 longer
Starting index: 1 B:BGP D:Directly-Connected R:RIP S:Static O:OSPF
```

<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>52 209.159.38.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>53 209.159.39.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>54 209.159.40.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>55 209.159.41.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>56 209.159.42.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>57 209.159.43.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>58 209.159.44.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>59 209.159.45.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
<tr>
<td>60 209.159.46.0</td>
<td>255.255.255.0</td>
<td>207.95.6.101</td>
<td>1/1</td>
<td>1</td>
<td>S</td>
</tr>
</tbody>
</table>

This example shows all the routes for networks beginning with 209.159. The mask value and **longer** parameter specify the range of network addresses to be displayed. In this example, all routes within the range 209.159.0.0 – 209.159.255.255 are listed.

The **summary** option displays a summary of the information in the IP route table. The following is an example of the output from this command:

```
ProCurveRS# show ip route summary
```

**IP Routing Table - 35 entries:**

- 6 connected, 28 static, 0 RIP, 1 OSPF, 0 BGP
- Number of prefixes:
  - /0: 1 /16: 27 /22: 1 /24: 5 /32: 1

**Syntax:** **show ip route summary**

In this example, the IP route table contains 35 entries. Of these entries, 6 are directly connected devices, 28 are static routes, and 1 route was calculated through OSPF. One of the routes has a zero-bit mask (this is the default route), 27 have a 22-bit mask, 5 have a 24-bit mask, and 1 has a 32-bit mask.

The following table lists the information displayed by the **show ip route** command.

<p>| <strong>Table 9.17: CLI Display of IP Route Table</strong> |</p>
<table>
<thead>
<tr>
<th><strong>This Field...</strong></th>
<th><strong>Displays...</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>Destination</td>
<td>The destination network of the route.</td>
</tr>
<tr>
<td>NetMask</td>
<td>The network mask of the destination address.</td>
</tr>
</tbody>
</table>
**Table 9.17: CLI Display of IP Route Table (Continued)**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Gateway</td>
<td>The next-hop router.</td>
</tr>
<tr>
<td>Port</td>
<td>The port through which this router sends packets to reach the route's destination.</td>
</tr>
<tr>
<td>Cost</td>
<td>The route's cost.</td>
</tr>
<tr>
<td>Type</td>
<td>The route type, which can be one of the following:</td>
</tr>
</tbody>
</table>

- **B** – The route was learned from BGP.
- **D** – The destination is directly connected to this Routing Switch.
- **R** – The route was learned from RIP.
- **S** – The route is a static route.
- ***** – The route is a candidate default route.
- **O** – The route is an OSPF route. Unless you use the `ospf` option to display the route table, “O” is used for all OSPF routes. If you do use the `ospf` option, the following type codes are used:
  - **O** – OSPF intra area route (within the same area).
  - **IA** – The route is an OSPF inter area route (a route that passes from one area into another).
  - **E1** – The route is an OSPF external type 1 route.
  - **E2** – The route is an OSPF external type 2 route.

---

**Using The Web Management Interface**

To display the IP route table:

1. Log on to the system using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to list the monitoring options.
3. Click on the plus sign next to IP to list the IP monitoring options.
4. Click on the Routing Table link to display the table.

**Clearing IP Routes**

If needed, you can clear the entire route table or specific individual routes. To do so, use one of the following procedures.

**Using The CLI**

To clear all routes from the IP route table:

```
ProCurveRS# clear ip route
```

To clear route 209.157.22.0/24 from the IP routing table:

```
ProCurveRS# clear ip route 209.157.22.0/24
```

**Syntax:** `clear ip route [<ip-addr> <ip-mask>]`

or

**Syntax:** `clear ip route [<ip-addr>/<mask-bits>]`
**USING THE WEB MANAGEMENT INTERFACE**

The Web management interface does not allow you to selectively clear routes in the IP routing table, but does allow you to clear all routes from the IP routing table.

To clear all routes from the IP route table:

1. Log on to the using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Command in the tree view to expand the list of command options.
3. Click on the **Clear** link to display the Clear panel.
4. Select the box next to IP Route.
5. Click Apply.

**Displaying IP Traffic Statistics**

To display IP traffic statistics, use one of the following methods.

**USING THE CLI**

To display IP traffic statistics, enter the following command at any CLI level:

```
ProCurveRS> show ip traffic
```

**IP Statistics**

139 received, 145 sent, 0 forwarded
0 filtered, 0 fragmented, 0 reassembled, 0 bad header
0 no route, 0 unknown proto, 0 no buffer, 0 other errors

**ICMP Statistics**

Received:
0 total, 0 errors, 0 unreachable, 0 time exceed
0 parameter, 0 source quench, 0 redirect, 0 echo,
0 echo reply, 0 timestamp, 0 timestamp reply, 0 addr mask
0 addr mask reply, 0 irdp advertisement, 0 irdp solicitation

Sent:
0 total, 0 errors, 0 unreachable, 0 time exceed
0 parameter, 0 source quench, 0 redirect, 0 echo,
0 echo reply, 0 timestamp, 0 timestamp reply, 0 addr mask
0 addr mask reply, 0 irdp advertisement, 0 irdp solicitation

**UDP Statistics**

1 received, 0 sent, 1 no port, 0 input errors

**TCP Statistics**

0 active opens, 0 passive opens, 0 failed attempts
0 active resets, 0 passive resets, 0 input errors
138 in segments, 141 out segments, 4 retransmission

**RIP Statistics**

0 requests sent, 0 requests received
0 responses sent, 0 responses received
0 unrecognized, 0 bad version, 0 bad addr family, 0 bad req format
0 bad metrics, 0 bad resp format, 0 resp not from rip port
0 resp from loopback, 0 packets rejected
The `show ip traffic` command displays the following information.

**Table 9.18: CLI Display of IP Traffic Statistics**

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>received</td>
<td>The total number of IP packets received by the device.</td>
</tr>
<tr>
<td>sent</td>
<td>The total number of IP packets originated and sent by the device.</td>
</tr>
<tr>
<td>forwarded</td>
<td>The total number of IP packets received by the device and forwarded to other devices.</td>
</tr>
<tr>
<td>filtered</td>
<td>The total number of IP packets filtered by the device.</td>
</tr>
<tr>
<td>fragmented</td>
<td>The total number of IP packets fragmented by this device to accommodate the MTU of this device or of another device.</td>
</tr>
<tr>
<td>reassembled</td>
<td>The total number of fragmented IP packets that this device reassembled.</td>
</tr>
<tr>
<td>bad header</td>
<td>The number of IP packets dropped by the device due to a bad packet header.</td>
</tr>
<tr>
<td>no route</td>
<td>The number of packets dropped by the device because there was no route.</td>
</tr>
<tr>
<td>unknown proto</td>
<td>The number of packets dropped by the device because the value in the Protocol field of the packet header is unrecognized by this device.</td>
</tr>
<tr>
<td>no buffer</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>other errors</td>
<td>The number of packets that this device dropped due to error types other than the types listed above.</td>
</tr>
<tr>
<td><strong>ICMP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>total</td>
<td>The total number of ICMP messages sent or received by the device.</td>
</tr>
<tr>
<td>errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>unreachable</td>
<td>The number of Destination Unreachable messages sent or received by the device.</td>
</tr>
<tr>
<td>time exceed</td>
<td>The number of Time Exceeded messages sent or received by the device.</td>
</tr>
<tr>
<td>parameter</td>
<td>The number of Parameter Problem messages sent or received by the device.</td>
</tr>
<tr>
<td>source quench</td>
<td>The number of Source Quench messages sent or received by the device.</td>
</tr>
<tr>
<td>redirect</td>
<td>The number of Redirect messages sent or received by the device.</td>
</tr>
<tr>
<td>echo</td>
<td>The number of Echo messages sent or received by the device.</td>
</tr>
</tbody>
</table>
### Table 9.18: CLI Display of IP Traffic Statistics (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo reply</td>
<td>The number of Echo Reply messages sent or received by the device.</td>
</tr>
<tr>
<td>timestamp</td>
<td>The number of Timestamp messages sent or received by the device.</td>
</tr>
<tr>
<td>timestamp reply</td>
<td>The number of Timestamp Reply messages sent or received by the device.</td>
</tr>
<tr>
<td>addr mask</td>
<td>The number of Address Mask Request messages sent or received by the device.</td>
</tr>
<tr>
<td>addr mask reply</td>
<td>The number of Address Mask Replies messages sent or received by the device.</td>
</tr>
<tr>
<td>irdp advertisement</td>
<td>The number of ICMP Router Discovery Protocol (IRDP) Advertisement messages sent or received by the device.</td>
</tr>
<tr>
<td>irdp solicitation</td>
<td>The number of IRDP Solicitation messages sent or received by the device.</td>
</tr>
</tbody>
</table>

### UDP statistics

<table>
<thead>
<tr>
<th>received</th>
<th>The number of UDP packets received by the device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>sent</td>
<td>The number of UDP packets sent by the device.</td>
</tr>
<tr>
<td>no port</td>
<td>The number of UDP packets dropped because the packet did not contain a valid UDP port number.</td>
</tr>
<tr>
<td>input errors</td>
<td>This information is used by HP customer support.</td>
</tr>
</tbody>
</table>

### TCP statistics

The TCP statistics are derived from RFC 793, “Transmission Control Protocol”.

<table>
<thead>
<tr>
<th>active opens</th>
<th>The number of TCP connections opened by this device by sending a TCP SYN to another device.</th>
</tr>
</thead>
<tbody>
<tr>
<td>passive opens</td>
<td>The number of TCP connections opened by this device in response to connection requests (TCP SYNs) received from other devices.</td>
</tr>
<tr>
<td>failed attempts</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>active resets</td>
<td>The number of TCP connections this device reset by sending a TCP RESET message to the device at the other end of the connection.</td>
</tr>
<tr>
<td>passive resets</td>
<td>The number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.</td>
</tr>
<tr>
<td>input errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>in segments</td>
<td>The number of TCP segments received by the device.</td>
</tr>
<tr>
<td>out segments</td>
<td>The number of TCP segments sent by the device.</td>
</tr>
<tr>
<td>retransmission</td>
<td>The number of segments that this device retransmitted because the retransmission timer for the segment had expired before the device at the other end of the connection had acknowledged receipt of the segment.</td>
</tr>
</tbody>
</table>
### Table 9.18: CLI Display of IP Traffic Statistics (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>RIP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>requests sent</td>
<td>The number of requests this device has sent to another RIP router for all or part of its RIP routing table.</td>
</tr>
<tr>
<td>requests received</td>
<td>The number of requests this device has received from another RIP router for all or part of this device's RIP routing table.</td>
</tr>
<tr>
<td>responses sent</td>
<td>The number of responses this device has sent to another RIP router's request for all or part of this device's RIP routing table.</td>
</tr>
<tr>
<td>responses received</td>
<td>The number of responses this device has received to requests for all or part of another RIP router's routing table.</td>
</tr>
<tr>
<td>unrecognized</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>bad version</td>
<td>The number of RIP packets dropped by the device because the RIP version was either invalid or is not supported by this device.</td>
</tr>
<tr>
<td>bad addr family</td>
<td>The number of RIP packets dropped because the value in the Address Family Identifier field of the packet's header was invalid.</td>
</tr>
<tr>
<td>bad req format</td>
<td>The number of RIP request packets this router dropped because the format was bad.</td>
</tr>
<tr>
<td>bad metrics</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>bad resp format</td>
<td>The number of responses to RIP request packets this router dropped because the format was bad.</td>
</tr>
<tr>
<td>resp not from rip port</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>resp from loopback</td>
<td>The number of RIP responses received from loopback interfaces.</td>
</tr>
<tr>
<td>packets rejected</td>
<td>This information is used by HP customer support.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To display IP traffic statistics:

1. Log on to the  using a valid user name and password for read-only or read-write access. The System configuration panel is displayed.
2. Click on the plus sign next to Monitor in the tree view to list the monitoring options.
3. Click on the plus sign next to IP to list the IP monitoring options.
4. Click on the Traffic link to display the table.

This display shows the following information.

### Table 9.19: Web Display of IP Traffic Statistics

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Packets Received</td>
<td>The number of IP packets received by the device.</td>
</tr>
</tbody>
</table>
### Table 9.19: Web Display of IP Traffic Statistics (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Packets Sent</td>
<td>The number of IP packets originated and sent by the device.</td>
</tr>
<tr>
<td>Packets Forwarded</td>
<td>The number of IP packets received from another device and forwarded by this device.</td>
</tr>
<tr>
<td>Filtered</td>
<td>The number of IP packets filtered by this device.</td>
</tr>
<tr>
<td>Fragmented</td>
<td>The number of IP packets fragmented by this device before sending or forwarding them.</td>
</tr>
<tr>
<td>Reassembled</td>
<td>The number of fragmented IP packets received and re-assembled by the device.</td>
</tr>
<tr>
<td>Bad Header</td>
<td>The number of packets dropped because they had a bad header.</td>
</tr>
<tr>
<td>No Route</td>
<td>The number of packets dropped because they had no route information.</td>
</tr>
<tr>
<td>Unknown Protocols</td>
<td>The number of packets dropped because they were using an unknown protocol.</td>
</tr>
<tr>
<td>No Buffer</td>
<td>The number of packets dropped because the device ran out of buffer space.</td>
</tr>
<tr>
<td>Other Errors</td>
<td>The number of packets dropped due to errors other than the ones listed above.</td>
</tr>
</tbody>
</table>

#### ICMP statistics

| Total Received         | The number of ICMP packets received by the device.                        |
| Total Sent             | The number of ICMP packets sent by the device.                             |
| Received Errors        | This information is used by HP customer support.                          |
| Sent Errors            | This information is used by HP customer support.                          |
| Received Unreachable   | The number of Destination Unreachable messages received by the device.    |
| Sent Unreachable       | The number of Destination Unreachable messages sent by the device.        |
| Received Time Exceed   | The number of Time Exceeded messages received by the device.              |
| Sent Time Exceed       | The number of Time Exceeded messages sent by the device.                  |
| Received Parameter     | The number of Parameter Problem messages received by the device.          |
| Sent Parameter         | The number of Parameter Problem messages sent by the device.              |
| Received Source Quench | The number of Source Quench messages received by the device.              |
| Sent Source Quench     | The number of Source Quench messages sent by the device.                  |
| Received Redirect      | The number of Redirect messages received by the device.                   |
| Sent Redirect          | The number of Redirect messages sent by the device.                       |
| Received Echo          | The number of Echo messages received by the device.                       |
### Table 9.19: Web Display of IP Traffic Statistics (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Sent Echo</td>
<td>The number of Echo messages sent by the device.</td>
</tr>
<tr>
<td>Received Echo Reply</td>
<td>The number of Echo messages received by the device.</td>
</tr>
<tr>
<td>Sent Echo Reply</td>
<td>The number of Echo messages sent by the device.</td>
</tr>
<tr>
<td>Received Timestamp</td>
<td>The number of Timestamp messages received by the device.</td>
</tr>
<tr>
<td>Sent Timestamp</td>
<td>The number of Timestamp messages sent by the device.</td>
</tr>
<tr>
<td>Received Timestamp Reply</td>
<td>The number of Timestamp Reply messages received by the device.</td>
</tr>
<tr>
<td>Sent Timestamp Reply</td>
<td>The number of Timestamp Reply messages sent by the device.</td>
</tr>
<tr>
<td>Received Address Mask</td>
<td>The number of Address Mask Request messages received by the device.</td>
</tr>
<tr>
<td>Sent Address Mask</td>
<td>The number of Address Mask Request messages sent by the device.</td>
</tr>
<tr>
<td>Received Address Mask Reply</td>
<td>The number of Address Mask Replies messages received by the device.</td>
</tr>
<tr>
<td>Sent Address Mask Reply</td>
<td>The number of Address Mask Replies messages sent by the device.</td>
</tr>
<tr>
<td>Received IRDP Advertisement</td>
<td>The number of ICMP Router Discovery Protocol (IRDP) Advertisement messages received by the device.</td>
</tr>
<tr>
<td>Sent IRDP Advertisement</td>
<td>The number of IRDP Advertisement messages sent by the device.</td>
</tr>
<tr>
<td>Received IRDP Solicitation</td>
<td>The number of IRDP Solicitation messages received by the device.</td>
</tr>
<tr>
<td>Sent IRDP Solicitation</td>
<td>The number of IRDP Solicitation messages sent by the device.</td>
</tr>
</tbody>
</table>

**UDP statistics**

- **Received**
  - The number of UDP packets received by the device.
- **Sent**
  - The number of UDP packets sent by the device.
- **No Port**
  - The number of UDP packets dropped because the packet did not contain a valid UDP port number.
- **Input Errors**
  - This information is used by HP customer support.

**TCP statistics**

The TCP statistics are derived from RFC 793, “Transmission Control Protocol”.

- **Active Opens**
  - The number of TCP connections opened by this device by sending a TCP SYN to another device.
- **Passive Opens**
  - The number of TCP connections opened by this device in response to connection requests (TCP SYN)s received from other devices.
- **Failed Attempts**
  - This information is used by HP customer support.
- **Active Resets**
  - The number of TCP connections this device reset by sending a TCP RESET message to the device at the other end of the connection.
- **Passive Resets**
  - The number of TCP connections this device reset because the device at the other end of the connection sent a TCP RESET message.
<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Input Errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>In Segments</td>
<td>The number of TCP segments received by the device.</td>
</tr>
<tr>
<td>Out Segments</td>
<td>The number of TCP segments sent by the device.</td>
</tr>
<tr>
<td>Retransmission</td>
<td>The number of segments that this device retransmitted because the retransmission timer for the segment had expired before the device at the other end of the connection had acknowledged receipt of the segment.</td>
</tr>
</tbody>
</table>

**RIP statistics**

The RIP statistics are derived from RFC 1058, “Routing Information Protocol”.

<table>
<thead>
<tr>
<th>Requests Sent</th>
<th>The number of requests this device has sent to another RIP router for all or part of its RIP routing table.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Requests Received</td>
<td>The number of requests this device has received from another RIP router for all or part of this device's RIP routing table.</td>
</tr>
<tr>
<td>Responses Sent</td>
<td>The number of responses this device has sent to another RIP router's request for all or part of this device's RIP routing table.</td>
</tr>
<tr>
<td>Responses Received</td>
<td>The number of responses this device has received to requests for all or part of another RIP router's routing table.</td>
</tr>
<tr>
<td>Unrecognized</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Bad Version</td>
<td>The number of RIP packets dropped by the device because the RIP version was either invalid or is not supported by this device.</td>
</tr>
<tr>
<td>Bad Address Family</td>
<td>The number of RIP packets dropped because the value in the Address Family Identifier field of the packet's header was invalid.</td>
</tr>
<tr>
<td>Bad Request Format</td>
<td>The number of RIP request packets this router dropped because the format was bad.</td>
</tr>
<tr>
<td>Bad Metrics</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Bad Response Format</td>
<td>The number of responses to RIP request packets this router dropped because the format was bad.</td>
</tr>
<tr>
<td>Resp Not From RIP Port</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Response From Loopback</td>
<td>The number of RIP responses received from loopback interfaces.</td>
</tr>
<tr>
<td>Packets Rejected</td>
<td>This information is used by HP customer support.</td>
</tr>
</tbody>
</table>