This chapter describes the Internet Protocol (IP) parameters on HP ProCurve routing switches and 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 7-1
- “Configuring OSPF” on page 8-1
- “Configuring BGP4” on page 10-1

To configure and monitor IP, see the following sections:

- “Basic IP Parameters and Defaults – Routing Switches” on page 6-9
- “Basic IP Parameters and Defaults – HP 6208M-SX” on page 6-16
- “Configuring IP Parameters – Routing Switches” on page 6-18
- “Configuring IP Parameters – HP 6208M-SX” on page 6-73
- “Displaying IP Configuration Information and Statistics” on page 6-80

Basic Configuration

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

- If you are configuring a routing switch, see “Configuring IP Addresses” on page 6-18 to add IP addresses, then see one or more of the following to enable and configure the route exchange protocols:
  - “Configuring RIP” on page 7-1
  - “Configuring OSPF” on page 8-1
  - “Configuring BGP4” on page 10-1
- If you are configuring a switch, see “Configuring the Management IP Address and Specifying the Default Gateway” on page 6-73 to add an IP address for management access through the network and to specify the default gateway.

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

The HP Procurve 6208M-SX switch and HP 9304M, HP 9308M, and HP 6308M-SX routing switches support Internet Protocol (IP) version 4. IP support on the HP 6208M-SX consists of basic services to support management access and access to a default gateway. IP support on the 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**
  - 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)
  - Virtual Router Redundancy Protocol (VRRP)
  - Standby Router Protocol (SRP)

**IP Interfaces**

HP ProCurve devices allow you to configure IP addresses. On the routing switches, IP addresses are associated with individual interfaces. On the HP 6208M-SX, a single IP address serves as the management access address for the entire device.

All HP ProCurve devices 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 6-80.

**Routing Switches**

HP 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 “Configuring Basic Features” chapter of the Installation and Getting Started Guide.

You can use any of the IP addresses you configure on the routing switch for Telnet, Web management, or SNMP access.
The HP 6208M-SX Switch

You can configure an IP address on the HP 6208M-SX for management access to the switch. An IP address is required for Telnet access, Web management access, and SNMP access.

You also can specify the default gateway for forwarding traffic to other sub-nets.

IP Packet Flow Through a Routing Switch

Figure 6.1 shows how an IP packet moves through an HP routing switch.

Figure 6.1 IP Packet flow through an HP routing switch

Figure 6.1 shows the following packet flow:

1. When the routing switch receives an IP packet, the routing switch checks for filters on the receiving interface.¹ 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

¹ The filter can be an Access Control List (ACL) or an IP access policy.
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.

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 switch or 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.

**NOTE:** The routing switches have a static ARP table but the HP 6208M-SX does not.

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 6-85 – routing switch
- “Displaying the Static ARP Table” on page 6-87 – routing switch only
- “Displaying ARP Entries” on page 6-101 – switch

To configure other ARP parameters, see the following:
- “Configuring ARP Parameters” on page 6-27 – routing switch only

To increase the size of the ARP cache and static ARP table, see the following:
- For dynamic entries, see the “Configuring Basic Features” chapter of the Installation and Getting Started Guide. 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 6-31 – routing switches only. The ip-static-arp parameter controls the static ARP table size.

**IP Route Table**

The IP route table contains paths to IP destinations.

**NOTE:** The HP 6208M-SX does not have an IP route table. The switch sends all packets addressed to another sub-net to the default gateway, which you specify when you configure the basic IP information on the switch.

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).

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 6-90 – routing switch only

To configure a static IP route, see the following:

- “Configuring Static Routes” on page 6-36 – routing switch only

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

- “Clearing IP Routes” on page 6-93 – routing switch only

To increase the size of the IP route table for learned and static routes, see the “Configuring Basic Features” chapter of the Installation and Getting Started Guide:

- 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 HP 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.

**NOTE:** The HP 6208M-SX does not have an IP forwarding cache.

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</th>
<th>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>
<td></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 6-88.

**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 6-60 and the “Configuring Basic Features” chapter of the Installation and Getting Started Guide.

To increase the size of the IP forwarding cache, see the “Configuring Basic Features” chapter of the Installation and Getting Started Guide. 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 switch or 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 “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*. The ip-qos-session parameter controls the size of the session table.

**IP Route Exchange Protocols**

HP 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 7-1
- “Configuring OSPF” on page 8-1
- “Configuring BGP4” on page 10-1

**IP Multicast Protocols**

HP 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” on page 9-1.

**NOTE:** The HP 6208M-SX supports IGMP and can forward IP multicast packets. See the “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*.

**IP Interface Redundancy Protocols**

You can configure an HP ProCurve routing switch to back up an IP interface configured on another HP 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.

HP 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 HP routing switches and third-party routers to back up IP interfaces on other HP 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 HP routing switches.
- Standby Router Protocol (SRP) – An HP router redundancy protocol developed before VRRP and VRRPE that provides some of the features of VRRP and some of the features of VRRPE. You can use SRP only on the HP 9304M, HP 9308M, and HP 6308M-SX routing switches.
For configuration information, see the following:

- Virtual Router Redundancy Protocol Extended (VRRPE) – see “Configuring VRRP and VRRPE” on page 12-1.
- Virtual Router Redundancy Protocol (VRRP) – see “Configuring VRRP and VRRPE” on page 12-1.
- Standby Router Protocol (SRP) – see “Configuring SRP” on page 13-1

**Network Address Translation**

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 an HP 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” on page 11-1.

**Access Control Lists and IP Access Policies**

HP 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:

- “Using Access Control Lists (ACLs)” on page 3-1
- “Policies and Filters” on page C-1
Basic IP Parameters and Defaults – Routing Switches

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

- Route exchange protocols
  - Routing Information Protocol (RIP) – see “Configuring RIP” on page 7-1
  - Open Shortest Path First (OSPF) – see “Configuring OSPF” on page 8-1
  - Border Gateway Protocol version 4 (BGP4) – see “Configuring BGP4” on page 10-1
- Multicast protocols
  - Internet Group Membership Protocol (IGMP) – see “Changing Global IP Multicast Parameters” on page 9-2
  - Protocol Independent Multicast Dense (PIM-DM) – see “PIM Dense Overview” on page 9-4
  - Protocol Independent Multicast Sparse (PIM-SM) – see “PIM Sparse Overview” on page 9-12
  - Distance Vector Multicast Routing Protocol (DVMRP) – see “DVMRP Overview” on page 9-39
- Router redundancy protocols
  - Virtual Router Redundancy Protocol Extended (VRRPE) – see “Configuring VRRP and VRRPE” on page 12-1
  - Virtual Router Redundancy Protocol (VRRP) – see “Configuring VRRP and VRRPE” on page 12-1.
  - Standby Router Protocol (SRP) – see “Configuring SRP” on page 13-1

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 – Routing Switches

Table 6.1 lists the IP global parameters for routing switches.

#### Table 6.1: IP Global Parameters – 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 and mask notation</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>6-80</td>
</tr>
<tr>
<td></td>
<td>- Class-based format; example: 192.168.1.1 255.255.255.0</td>
<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>
</tr>
<tr>
<td></td>
<td>- Classless Interdomain Routing (CIDR) format; example: 192.168.1.1/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Router ID</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 lowest-numbered IP address configured on the lowest-numbered virtual routing interface (VE). If no VE is configured, then the lowest-numbered IP address configured on the device.</td>
<td>6-24</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</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>6-27</td>
</tr>
<tr>
<td>ARP age</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.</td>
<td>Ten minutes</td>
<td>6-28</td>
</tr>
<tr>
<td>Proxy ARP</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>6-29</td>
</tr>
<tr>
<td>Static ARP entries</td>
<td>An ARP entry you place in the static ARP table. Static entries do not age out.</td>
<td>No entries</td>
<td>6-29</td>
</tr>
<tr>
<td>Time to Live (TTL)</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>6-32</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
<td>See page...</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
<td>----------------</td>
<td>-------------</td>
</tr>
<tr>
<td>Directed broadcast forwarding</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 6.2 on page 6-14.</td>
<td>Disabled</td>
<td>6-32</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       | 6-34        |
| Source-routed packet forwarding   | A source-routed packet contains a list of IP addresses through which the packet must pass to reach its destination. | Enabled        | 6-33        |
| 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 6.2 on page 6-14. | Disabled       | 6-62        |
| Reverse ARP (RARP)                | A IP mechanism a host can use to request an IP address from a directly attached router when the host boots. | Enabled       | 6-64        |
| 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     | 6-66        |
| 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           | 6-72        |
## Table 6.1: IP Global Parameters – routing switches (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name for Domain Name Server (DNS) resolver</td>
<td>A domain name (example: amaynes.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.</td>
<td>None configured</td>
<td>6-21</td>
</tr>
<tr>
<td>DNS default gateway addresses</td>
<td>A list of gateways attached to the router through which clients attached to the router can reach DNSs.</td>
<td>None configured</td>
<td>6-21</td>
</tr>
<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. Chassis devices 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>Standard</td>
<td>6-60</td>
</tr>
<tr>
<td>IP load sharing</td>
<td>A 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>6-48</td>
</tr>
<tr>
<td>IP load sharing aggregation</td>
<td>A feature on Chassis devices 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. <strong>Note:</strong> Load sharing aggregation is not available on Fixed-port devices. Fixed-port devices cache load sharing entries based on destination host addresses.</td>
<td>On Chassis devices, aggregated by network On Fixed-port devices, single host entries</td>
<td>6-58</td>
</tr>
<tr>
<td>Maximum IP load sharing paths</td>
<td>The maximum number of equal-cost paths across which the router is allowed to distribute traffic.</td>
<td>Four</td>
<td>6-59</td>
</tr>
<tr>
<td>Parameter</td>
<td>Description</td>
<td>Default</td>
<td>See page...</td>
</tr>
<tr>
<td>---------------------------------</td>
<td>-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
<td>---------------------------</td>
<td>-------------</td>
</tr>
</tbody>
</table>
| Origination of default routes   | You can enable a router to originate default routes for the following route exchange protocols, on an individual protocol basis:  
• RIP  
• OSPF  
• BGP4                                                                                                                                      | Disabled                  | 7-10  
8-32  
10-29 |
| Default route aggregation       | Optimizes forwarding cache space by aggregating cache entries for destinations to which the router forwards traffic using a default route. When you enable default route aggregation, the router makes a single cache entry for a destination network instead of multiple entries for the hosts on the network. | Separate cache entry for each destination host | 6-61        |
| Default network route           | 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).                                           | None configured           | 6-46        |
| Static route                    | An IP route you place in the IP route table.                                                                                                                                                                 | No entries                | 6-36        |
| 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. | 6-25        |
### IP Interface Parameters – Routing Switches

Table 6.2 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 configured(^a)</td>
<td>6-18</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> The HP 6208M-SX has a single IP address used for management access to the entire device. The 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>6-23</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</td>
<td>6-24</td>
</tr>
<tr>
<td></td>
<td>1492 for SNAP.</td>
<td>1492 for SNAP encapsulated packets</td>
<td></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>7-5</td>
</tr>
<tr>
<td>Directed broadcast forwarding</td>
<td>Locally overrides the global setting.  See Table 6.1 on page 6-10.</td>
<td>Disabled</td>
<td>6-32</td>
</tr>
<tr>
<td>ICMP Router Discovery Protocol (IRDP)</td>
<td>Locally overrides the global IRDP settings. See Table 6.1 on page 6-10.</td>
<td>Disabled</td>
<td>6-64</td>
</tr>
<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>6-71</td>
</tr>
</tbody>
</table>
**Table 6.2: IP Interface Parameters – routing switches (Continued)**

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<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 • tacacs • tftp • time</td>
<td>6-68</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>6-69</td>
</tr>
</tbody>
</table>

a. Some devices have a factory default, such as 209.157.22.154, used for troubleshooting during installation. For routing switches, the address is on port 1 (or 1/1).
Basic IP Parameters and Defaults – HP 6208M-SX

IP is enabled by default. The following tables list the switch IP parameters, their default values, and where to find configuration information.

NOTE: The HP 6208M-SX also provides IP multicast forwarding, which is enabled by default. For information about this feature, see the “Configuring Basic Features” chapter of the Installation and Getting Started Guide.

IP Global Parameters – HP 6208M-SX

Table 6.3 lists the IP global parameters for the switch.

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP address and mask notation</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>6-80</td>
</tr>
<tr>
<td></td>
<td>• Class-based format; example: 192.168.1.1 255.255.255.0</td>
<td>Note: 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>
</tr>
<tr>
<td></td>
<td>• Classless Interdomain Routing (CIDR) format; example: 192.168.1.1/24</td>
<td></td>
<td></td>
</tr>
<tr>
<td>IP address</td>
<td>A Layer 3 network interface address</td>
<td>None configureda</td>
<td>6-73</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: The HP 6208M-SX has 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>Default gateway</td>
<td>The IP address of a locally attached router (or a router attached to the switch by bridges or other switches). The switch and clients attached to it use the default gateway to communicate with devices on other sub-nets.</td>
<td>None configured</td>
<td>6-73</td>
</tr>
<tr>
<td>Address Resolution Protocol (ARP)</td>
<td>A standard IP mechanism that networking devices use to learn the Media Access Control (MAC) address of another device on the network. The switch 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>n/a</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You cannot disable ARP.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>ARP age</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.</td>
<td>Ten minutes</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td><strong>Note</strong>: You cannot change the ARP age on switches.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Time to Live (TTL)</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>6-76</td>
</tr>
</tbody>
</table>
### Table 6.3: IP Global Parameters – switch (Continued)

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Domain name for Domain Name Server (DNS) resolver</td>
<td>A domain name (example: amaynes.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.</td>
<td>None configured</td>
<td>6-74</td>
</tr>
<tr>
<td>DNS default gateway addresses</td>
<td>A list of gateways attached to the router through which clients attached to the router can reach DNSs.</td>
<td>None configured</td>
<td>6-74</td>
</tr>
<tr>
<td>Source interface</td>
<td>The IP address the switch uses as the source address for Telnet, RADIUS, or TACACS/TACACS+ packets originated by the router. The switch uses its management IP address as the source address for these packets.</td>
<td>The management IP address of the switch.</td>
<td>n/a</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> This parameter is not configurable on the HP 6208M-SX.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>DHCP gateway stamp</td>
<td>The device 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 forwards the packet in the packet’s Gateway field.</td>
<td>None configured</td>
<td>6-79</td>
</tr>
<tr>
<td></td>
<td>You can specify up to 32 gateway lists. A gateway list contains up to eight gateway IP addresses. You activate DHCP assistance by associating a gateway list with a port.</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>When you configure multiple IP addresses in a gateway list, the switch inserts the addresses into the DHCP Discovery packets in a round robin fashion.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

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

### Interface IP Parameters – HP 6208M-SX

Table 6.4 lists the interface-level IP parameters for the HP 6208M-SX.

### Table 6.4: Interface IP Parameters – switch

<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>You can configure a list of DHCP stamp addresses for a port. When the port receives a DHCP/BootP Discovery packet from a client, the port places the IP address(es) in the gateway list into the packet’s Gateway field.</td>
<td>None configured</td>
<td>6-79</td>
</tr>
</tbody>
</table>
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.

NOTE: This section describes how to configure IP parameters for routing switches. For IP configuration information for the HP 6208M-SX, see “Configuring IP Parameters – HP 6208M-SX” on page 6-73.

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 the HP 6308M-SX, 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 “Configuring Basic Features” chapter of the Installation and Getting Started Guide.

HP ProCurve 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 6-80.

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:

```
HP9300(config)# interface ethernet 1/1
HP9300(config-if-1/1)# ip address 192.45.6.1 255.255.255.0
```

Syntax: ip address <ip-addr> <ip-mask> [secondary]

or

Syntax: ip address <ip-addr> <mask-bits> [secondary]

Use the secondary parameter if you have already configured an IP address within the same sub-net on the interface.

NOTE: You also can enter the IP address and mask in CIDR format, as follows:

```
HP9300(config-if-1/1)# ip address 192.45.6.1/24
```
USING THE WEB MANAGEMENT INTERFACE

To assign an IP address and mask to a router interface:

1. Log on to the device 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. Select Add IP Address to display the following panel.

3. Select the port (and slot if applicable) on which you want to configure the address.

   **NOTE:** This example shows the panel for configuring an address on a routing switch. On the HP 6208M-SX, the IP address is global and applies to all the switch’s ports. Thus, you do not need to select a port.

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 routing switch.

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

   **NOTE:** If you configure the HP 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 HP routing switch. See “Adding a Loopback Interface” on page 10-13.

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:

```
HP9300(config-bgp-router)# exit
HP9300(config)# int loopback 1
```
Syntax: interface loopback <num>
The <num> value can be from 1 – 8.

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

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

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device 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”. (If you are configuring a Chassis device, 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.1

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.

1. HP’s feature that allows routing between VLANs within the same device, without the need for external routers, is called Integrated Switch Routing (ISR). See “Integrated Switch Routing (ISR)” on page 16-3.
For more information about VLANs and how to configure them, see “Configuring VLANs” on page 16-1.

**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:

```
HP9300(config)# vlan 2 name IP-Subnet_1.1.2.0/24
HP9300(config-vlan-2)# untag e1 to 4
HP9300(config-vlan-2)# router-interface ve1
HP9300(config-vlan-2)# interface ve1
HP9300(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>`
- `interface ve <num>`
- The `<num>` value can be from 1 – 8.
- `ip address <ip-addr> <ip-mask> [secondary]`
  
  or
  
  `ip address <ip-addr>/<mask-bits> [secondary]`

### 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 the device and thereby recognize all hosts within that domain. After you define a domain name, the device 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 device 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:

```
HP9300# ping nyc01
HP9300# 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:

```
HP9300(config)# ip dns domain-name newyork.com
HP9300(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 device using a valid user name and password for read-write access. The System configuration panel is displayed.

2. Do one of the following:
   - On the HP 6208M-SX – Select the **DNS** link to display the DNS panel.
   - On a routing switch – 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 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**

HP9300# 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 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:
  IP Address  Round Trip Time1  Round Trip Time2
  207.95.6.30  93 msec           121 msec
```

   **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.
Configuring IP

NOTE: You can use the host name only if you have already configured the DNS resolver for the domain that contains the host.

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.

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. HP 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 encapsulation type on a routing switch port, use either of the following methods.

USING THE CLI

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

HP9300(config)# int e 1/5
HP9300(config-if-5)# ip encapsulation ethernet_snap

Syntax: ip encapsulation ethernet_snap | ethernet_ii

USING THE WEB MANAGEMENT INTERFACE

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 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 Size of the Maximum Transmission Unit (MTU)**

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.

Since the MTU depends on the encapsulation type, and the encapsulation type can be configured on an individual port basis, the MTU also can be configured on an individual port basis.

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

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:

```
HP9300(config)# int e 1/5
HP9300(config-if-5)# ip mtu 1000
```

**Syntax:** `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 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 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.

**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: Routing Information Protocol (RIP) does not use the router ID.

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

By default, the router ID on an HP routing switch is one of the following:

• If the routing switch 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: HP routing switches use the same router ID for both OSPF and BGP4. If the routing switch is already configured for OSPF, you may want to use the router ID that is already in use on the routing switch 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.

**USING THE CLI**

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

```plaintext
HP9300(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 HP routing switch, but do not specify an IP address in use by another device.

**USING THE WEB MANAGEMENT INTERFACE**

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 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 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 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 port 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:

```
HP9300(config)# int loopback 2
HP9300(config-lbif-2)# ip address 10.0.0.2/24
HP9300(config-lbif-2)# exit
HP9300(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, if you are configuring a chassis device).

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.

```
HP9300(config)# interface ethernet 1/4
HP9300(config-if-1/4)# ip address 209.157.22.110/24
HP9300(config-if-1/4)# exit
HP9300(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:

```
HP9300(config)# int ve 1
HP9300(config-vif-1)# ip address 10.0.0.3/24
HP9300(config-vif-1)# exit
HP9300(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>`
Configuring IP

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, if you are configuring a chassis device).

**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:

```
HP9300(config)# int ve 1
HP9300(config-vif-1)# ip address 10.0.0.3/24
HP9300(config-vif-1)# exit
HP9300(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, if you are configuring a chassis device).

### 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.

**NOTE:** The HP 6208M-SX also supports ARP. The description in “How ARP Works” also applies to ARP on the HP 6208M-SX. However, the configuration options described later in this section apply only to routing switches, not to the HP 6208M-SX.

**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 HP 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 6-29.

NOTE: If the routing switch 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 routing switch sends an ICMP Host Unreachable message to the source.

### 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. You cannot change the ARP age on switches. 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 modify the ARP aging parameter to 20 minutes, enter the following command:

```
HP9300(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.

**USING THE WEB MANAGEMENT INTERFACE**

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 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 HP routing switches. The feature is not supported on the HP 6208M-SX.

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

USING THE CLI
To enable IP proxy ARP, enter the following command:

```
HP9300(config)# ip proxy-arp
```

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

```
HP9300(config)# no ip proxy-arp
```

Syntax: [no] ip proxy-arp

USING THE WEB MANAGEMENT INTERFACE
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 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

HP 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.

NOTE: You cannot create static ARP entries on a switch.

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 6-31.

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

- To display the ARP table, see “Displaying the ARP Cache” on page 6-85.
- To display the static ARP table, see “Displaying the Static ARP Table” on page 6-87.
To configure a static ARP entry, use either of the following methods.

**USING THE CLI**

To create a static ARP entry, enter a command such as the following:

```
HP9300(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 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 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 on 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.

![Static ARP Configuration Panel](image)

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 6.5 on page 6-31 lists the default maximum and configurable maximum number of entries in the static ARP table that are supported on each type of HP 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 "Configuring Basic Features" chapter of the *Installation and Getting Started Guide*.

**USING THE CLI**

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

```
HP9300(config)# system-max ip-static-arp 2048
HP9300(config)# write memory
HP9300(config)# end
HP9300# 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. Table 6.5 lists the default maximum and range of configurable maximums for static ARP table entries supported on each type of HP routing switch.

**USING THE WEB MANAGEMENT INTERFACE**

To modify a table size using the Web management interface:

1. Log on to the device 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.

---

**Table 6.5: Static ARP Entry Support**

<table>
<thead>
<tr>
<th>Product</th>
<th>Default Maximum</th>
<th>Configurable Minimum</th>
<th>Configurable Maximum</th>
</tr>
</thead>
<tbody>
<tr>
<td>HP 9304M or HP 9308M with 128MB management module</td>
<td>1024</td>
<td>1024</td>
<td>2048</td>
</tr>
<tr>
<td>HP 9304M or HP 9308M with 32MB management module (Management I module)</td>
<td>512</td>
<td>512</td>
<td>1024</td>
</tr>
<tr>
<td>HP ProCurve 6308M-SX routing switch with 32MB memory</td>
<td>512</td>
<td>512</td>
<td>1024</td>
</tr>
</tbody>
</table>
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 HP 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:

```
HP9300(config)# ip ttl 25
```

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

**USING THE WEB MANAGEMENT INTERFACE**

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 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**

HP9300(config)# ip directed-broadcast

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

HP software makes the forwarding decision based on the routing switch’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:

HP9300(config)# no ip directed-broadcast

**USING THE WEB MANAGEMENT INTERFACE**

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 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 6-34.

- **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:

HP9300(config)# no ip source-route

**Syntax:** [no] ip source-route

To re-enable forwarding of source-routed packets, enter the following command:
**HP9300(config)# ip source-route**

**USING THE WEB MANAGEMENT INTERFACE**

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 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.

```bash
HP9300(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:

```
HP9300(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:

```
HP9300(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:

```
HP9300(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:

```
HP9300(config)# no ip icmp unreachable host
HP9300(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:

```
HP9300(config)# ip icmp unreachable host
HP9300(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 Redirects**

You can disable ICMP redirects on a global basis or on an individual port basis. To disable ICMP redirects globally, enter the following command at the global CONFIG level of the CLI:

```
HP9300(config)# no ip icmp redirects
```

**Syntax:** `[no] ip icmp redirects`

To disable ICMP redirects on a specific interface, enter the same command at the configuration level for the interface:

```
HP9300(config)# int e 3/11
HP9300(config-if-e100-3/11)# no ip icmp redirects
```

**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 6-46.
- 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:

- **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 6-48.

- **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 6-41
- “Configuring Standard Static IP Routes and Interface or Null Static Routes to the Same Destination” on page 6-43
Static Route States Follow Port States

IP static routes remain in the IP route table only so long as the next-hop gateway, port, or virtual interface used by the route is available. If the gateway or port becomes unavailable, the software removes the static route from the IP route table. If the gateway or port later becomes available again, 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 6.2 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 6.2 Example of a static route](image)

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

```
HP9300(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:

```
HP9300(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.

```
HP9300(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.

```
HP9300(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>
Configuring IP

```
eternet <portnum> | ve <num>
[<metric>] [distance <num>]
```

or

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

The `<dest-ip-addr>` is the route's destination. The `<dest-mask>` is the network mask for the route's destination IP address. Alternatively, you can specify the network mask information by entering a forward slash followed by the number of bits in the network mask. For example, you can enter `192.0.0.0 255.255.255.0` as `192.0.0.0/24`.

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, if you are configuring an HP 9304M or HP 9308M). 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 the routing switch receives a route with a lower administrative distance. See "Changing Administrative Distances" on page 10-30 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`.

**USING THE WEB MANAGEMENT INTERFACE**

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 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. To select a loopback interface or a virtual interface on a Chassis device, 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.

**USING THE CLI**

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

HP9300(config)# ip route 209.157.22.0 255.255.255.0 null0
HP9300(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 it.

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.

**USING THE WEB MANAGEMENT INTERFACE**

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

**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 6-48.

- **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 10-30.

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.

```
HP9300(config)# ip route 192.128.2.69 255.255.255.0 209.157.22.1
HP9300(config)# ip route 192.128.2.69 255.255.255.0 192.111.10.1
```

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.

```
HP9300(config)# ip route 192.128.2.69 255.255.255.0 209.157.22.1
HP9300(config)# ip route 192.128.2.69 255.255.255.0 192.111.10.1 2
HP9300(config)# ip route 192.128.2.69 255.255.255.0 201.1.1.1 3
```

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 6-38.

**USING THE WEB MANAGEMENT INTERFACE**

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 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.

![Static Route](image)

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 6.3 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.
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

Router A
192.168.6.188/24

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

192.168.6.157/24

Router B
192.168.7.7/24

192.168.7.69/24

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

Figure 6.3 Standard and null static routes to the same destination network

Figure 6.4 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

192.168.6.188/24
Port 1/1

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

192.168.6.12/24
Port 4/4

192.168.8.11/24

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

Router B

192.168.6.188/24
Port 1/1

Router C

192.168.6.80/24

Router D

192.168.6.69/24

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 6.3 on page 6-44, enter commands such as the following:

```
HP9300(config)# ip route 192.168.7.0/24 192.168.6.157/24 1
HP9300(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 6-38.

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

```
HP9300(config)# ip route 192.168.6.0/24 ethernet 1/1 1
HP9300(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.
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 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. To select a loopback interface or a virtual interface on a Chassis device, 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:

```
HP9300(config)# ip default-network 209.157.22.0
HP9300(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:

```
HP9300(config)# show ip route
```

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

This example shows two routes. Both of the routes are directly attached, as indicated in the Type column. However, one of the routes is shown as type “D”, with an asterisk (*). The asterisk indicates that this route is a candidate default network route.
**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. The HP 6308M-SX routing switch supports 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.

---

**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.

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.

---

1. IP load sharing is also called “Equal-Cost Multi-Path (ECMP)” load sharing or just “ECMP”
Here are the default administrative distances on the HP 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 routing switch will not use this route)

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

**NOTE:** You can change the administrative distances individually. See the configuration chapter for the route source for information.

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 6-41.
- 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 6.6 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 HP routing switches, load sharing for static IP routes, RIP routes, OSPF routes, and BGP4 routes also is enabled by default.

<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^a)</td>
<td>(8^a)</td>
<td>6-59</td>
</tr>
<tr>
<td>RIP</td>
<td>(4^a)</td>
<td>(8^a)</td>
<td>6-59</td>
</tr>
<tr>
<td>OSPF</td>
<td>4</td>
<td>8</td>
<td>6-59</td>
</tr>
<tr>
<td>BGP4</td>
<td>1</td>
<td>4</td>
<td>10-25</td>
</tr>
</tbody>
</table>

\(^a\) 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.

**HP 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 the HP 6308M-SX routing switch. This method is an option 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.

**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.
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 6-51 describes the host-based load-sharing mechanism.

- For network-based IP load sharing, the next load-balancing cache entry uses the next available path is then calculated based on the current number of paths and the maximum number of paths allowed. “Network-Based IP Load Sharing” on page 6-53 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 6.5 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.
### IP Forwarding Cache

<table>
<thead>
<tr>
<th>Destination Host</th>
<th>Next-Hop</th>
</tr>
</thead>
<tbody>
<tr>
<td>192.168.1.170 (H1)</td>
<td>192.168.6.2 (R2)</td>
</tr>
<tr>
<td>192.168.1.234 (H2)</td>
<td>192.168.5.1 (R3)</td>
</tr>
<tr>
<td>192.168.1.218 (H3)</td>
<td>192.168.6.2 (R2)</td>
</tr>
<tr>
<td>192.168.2.175 (H4)</td>
<td>192.168.5.1 (R3)</td>
</tr>
<tr>
<td>192.168.2.193 (H5)</td>
<td>192.168.6.2 (R2)</td>
</tr>
<tr>
<td>192.168.2.155 (H6)</td>
<td>192.168.5.1 (R3)</td>
</tr>
<tr>
<td>192.168.3.209 (H7)</td>
<td>192.168.6.2 (R2)</td>
</tr>
<tr>
<td>192.168.3.159 (H8)</td>
<td>192.168.5.1 (R3)</td>
</tr>
<tr>
<td>192.168.3.111 (H9)</td>
<td>192.168.5.1 (R2)</td>
</tr>
</tbody>
</table>

R1 is configured with four IP load sharing paths, and has two paths to hosts H1 - H9, attached to R4.

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

---

**Figure 6.5  Host-based IP load sharing – basic example**

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 6.6 shows another example of IP forwarding cache entries for the configuration shown in Figure 6.5. 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.
**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 6.7 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 6.5 and Figure 6.6. 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.

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.

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 6-59.

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 = 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></td>
<td>1 2 3 4 5 6 7 8</td>
</tr>
<tr>
<td>2</td>
<td>2</td>
<td>2 1</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 1 2</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 1 2 1</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 1 2 1 2</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 1 2 1 2 1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 1 2 1 2 1 2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 1 2 1 2 1 2 1</td>
</tr>
<tr>
<td>3</td>
<td>2</td>
<td>2 3</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>2 3 1</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>2 3 1 2</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 1 2 3</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 1 2 3 1</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 1 2 3 1 2</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 1 2 3 1 2 3</td>
</tr>
<tr>
<td>4</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 1</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>2 3 4 1 2</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>2 3 4 1 2 3</td>
</tr>
<tr>
<td></td>
<td>7</td>
<td>2 3 4 1 2 3 4</td>
</tr>
<tr>
<td></td>
<td>8</td>
<td>2 3 4 1 2 3 4 1</td>
</tr>
</tbody>
</table>
### Table 6.7: 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 6.7, the results of the network-based IP load sharing algorithm provide evenly-distributed load sharing. Figure 6.8 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.

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:

`HP9300(config)# no ip load-sharing`

**Syntax:** `[no] ip load-sharing`
**USING THE WEB MANAGEMENT INTERFACE**

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 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:** The HP 6308M-SX routing switch supports host-based IP load sharing only.

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

**USING THE CLI**

To enable host-based IP load sharing, enter the following command:

```
HP9300(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:

```
HP9300(config)# no ip load-sharing by-host
```

**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.

**NOTE:** This feature applies only to chassis routing switches. The HP 6308M-SX routing switch performs host-based load sharing for all destinations and cannot be configured for network-based load sharing. Use this feature only when network-based load sharing is enabled.

When you configure host-based load sharing for a specific destination network, the routing switch distributes traffic to hosts on the network evenly across the available paths. For other networks, the routing switch uses a single path for all traffic to hosts on a given network.
NOTE: The host-based load sharing for the destination takes effect only if the IP route table 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:

```
HP9300(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:

```
HP9300(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:

```
HP9300(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:

```
HP9300(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 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 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

**NOTE:** This section applies only to routing switches that are running software release 07.1.X or higher.

The IP forwarding cache provides fast-path forwarding for IP traffic. The entries in the cache contain the following information:

- Source IP address and TCP or UDP port
- Destination IP address and TCP or UDP port

The default cache settings are adequate for most situations. However, if the routing switch forwards traffic to a very large number of destination hosts or uses default routes to send traffic to a large number of destinations, you may need to adjust the cache settings.

The software on chassis routing switches allows you to adjust the following forwarding cache settings:

- **Cache capacity for unicast forwarding entries** – The forwarding cache contains a unique entry for each host destination. You can set the cache to allow more unicast forwarding entries by enabling the **high-performance mode**. This option enables the cache to contain more unique entries for unicast traffic.
- **Cache format for default route entries** – The forwarding cache contains a unique entry for each host destination of a default route. You can increase the cache’s capacity for default route entries by enabling the **default-route aggregation mode**. This option increases the cache’s capacity for default routes by aggregating forwarding information for multiple destinations into single default-route entries.

These optimization options are disabled by default. To enable them, use the following procedures.

**Enabling Unicast High-Performance Mode**

To increase the capacity of the forwarding cache for unicast entries, 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.

**USING THE CLI**

To enable the high-performance mode, enter the following command:

HP9300(config)# ip high-perf
HP9300(config)# write memory
HP9300(config)# end
HP9300# reload

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

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

HP9300(config)# no ip high-perf
HP9300(config)# write memory
HP9300(config)# end
HP9300# reload

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

**Enabling the Default-Route Aggregation Mode**

By default, the IP forwarding cache of a routing switch contains a unique entry for each host destination of a default route. You can increase the cache’s capacity for default route entries by enabling the default-route aggregation mode. This option increases the cache’s capacity for default routes by aggregating forwarding information for multiple destinations into single default-route entries.

When you enable default route aggregation, the routing switch associates a network prefix length with each forwarding cache entry that is based on a default network route.

The routing switch reprograms the default route cache entries if external events cause a conflict between entries.

To configure the forwarding cache to aggregate entries for default route destinations, use the following CLI method.

**NOTE:** You do not need to reload the software to place a change to default-route aggregation into effect.

**USING THE CLI**

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

HP9300(config)# ip dr-aggregate

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

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

HP9300(config)# no ip dr-aggregate

**USING THE WEB MANAGEMENT INTERFACE**

You cannot configure this option using the Web management interface.

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

To display the default route entries in the IP forwarding cache, use the following CLI method. This method enables you to display the default route entries without displaying other types of forwarding entries.

**NOTE:** To display other types of forwarding cache entries, see “Displaying the Forwarding Cache” on page 6-88.

**USING THE CLI**

To display the default route cache entries, enter the following command at any level of the CLI:
HP9300(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.

HP9300(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 it 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.

HP9300(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

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.

**USING THE WEB MANAGEMENT INTERFACE**

You cannot display the default-route cache entries using the Web management interface.

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

You can clear the default route entries from the IP forwarding cache. To do so, use the following CLI method.

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

**USING THE CLI**

To clear the default-route cache entries, enter the following command from the Privileged EXEC level of the CLI:

HP9300# clear ip dr-aggregate

**Syntax:** clear ip dr-aggregate

**USING THE WEB MANAGEMENT INTERFACE**

You cannot clear the entries using the Web management interface.

**Configuring IRDP**

The ICMP Router Discovery Protocol (IRDP) is used by HP 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.
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 HP 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 HP 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 -4294967296 to 4294967295. 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:

```bash
HP9300(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 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 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:

```
HP9300(config)# interface ethernet 1/3
HP9300(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 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 -4294967296 to 4294967295. 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 6-70.

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:

```
HP9300(config)# no ip rarp
```

**Syntax:** [no] ip rarp

To re-enable RARP, enter the following command:

```
HP9300(config)# ip rarp
```

**USING THE WEB MANAGEMENT INTERFACE**

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 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 you 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 routing switch, enter a command such as the following:

```
HP9300(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 “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*.

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.

**USING THE WEB MANAGEMENT INTERFACE**

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 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 on 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.

```
Static RARP

<table>
<thead>
<tr>
<th>MAC Address:</th>
<th>12-45-23-67-21-78</th>
</tr>
</thead>
<tbody>
<tr>
<td>IP Address:</td>
<td>192.53.4.2</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 “Configuring Basic Features” chapter of the *Installation and Getting Started Guide*.

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 limited 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 limited 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 6-70.

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 6-71.

USING THE CLI

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

```
HP9300(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.

- bootpc (port 68)
- bootps (port 67)
- discard (port 9)
- dns (port 53)
- dnsix (port 90)
- echo (port 7)
- mobile-ip (port 434)
- netbios-dgm (port 138)
- netbios-ns (port 137)
- ntp (port 123)
- tacacs (port 65)
- talk (port 517)
- time (port 37)
- tftp (port 69)

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:

```
HP9300(config)# no ip forward-protocol udp snmp
```

This command disables forwarding of SNMP requests to the helper addresses configured on routing switch interfaces.
Configuring IP

USING THE WEB MANAGEMENT INTERFACE

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 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 limited broadcast address of the IP sub-net the server is in as the helper address.

You can configure up to four 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:

```
HP9300(config)# interface e 1/2
HP9300(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 – 4. Thus, an interface can have up to four helper addresses.

The `<ip-addr>` command specifies the server’s IP address or the limited broadcast address of the IP sub-net the server is in.

USING THE WEB MANAGEMENT INTERFACE

To configure a helper address on an interface:

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.
   - 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.
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 routing switch 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 limited 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 HP 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 client requests, and specify the BootP/DHCP server's IP address as the address you are helping the BootP/DHCP requests to reach. Instead of the server's IP address, you can specify the limited broadcast address of the IP sub-net the server is in.
Configuring IP 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 allowed by the router. By default, an HP 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 an 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 6-69.

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:

```plaintext
HP9300(config)# int e 1/1
HP9300(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 109.157.22.26. 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:

```
HP9300(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 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 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.
Configuring IP Parameters – HP 6208M-SX

The following sections describe how to configure IP parameters on the HP 6208M-SX.

NOTE: This section describes how to configure IP parameters for the HP 6208M-SX switch. For IP configuration information for routing switches, see “Configuring IP Parameters – Routing Switches” on page 6-18.

Configuring the Management IP Address and Specifying the Default Gateway

To manage the switch using Telnet or Secure Shell (SSH) CLI connections or the Web management interface, you must configure an IP address for the switch. Optionally, you also can specify the default gateway.

HP ProCurve 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 6-80.

To configure an IP address and specify the default gateway, use the following CLI method.

USING THE CLI

To assign an IP address to the HP 6208M-SX, enter a command such as the following at the global CONFIG level:

```
HP6208(config)# ip address 192.45.6.110 255.255.255.0
```

Syntax: `ip address <ip-addr> <ip-mask>`

or

```
Syntax: `ip address <ip-addr>/<mask-bits>`
```

NOTE: You also can enter the IP address and mask in CIDR format, as follows:

```
HP6208(config)# ip address 192.45.6.1/24
```

To specify the switch’s default gateway, enter a command such as the following:

```
HP6208(config)# ip default-gateway 192.45.6.1 255.255.255.0
```

Syntax: `ip default-gateway <ip-addr>`

or

```
Syntax: `ip default-gateway <ip-addr>/<mask-bits>`
```

USING THE WEB MANAGEMENT INTERFACE

You cannot perform initial configuration of the management IP address using the Web management interface, but you can change an address you already configured. You also can configure the default gateway. Use the following procedure.

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 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 IP Address link to display the IP address configuration panel.
5. Enter the IP address in the IP address field.
6. Enter the sub-net mask in the Subnet Mask field.
7. Enter the default gateway's IP address in the Default Gateway field.
8. Click the Apply 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 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 the device and thereby recognize all hosts within that domain. After you define a domain name, the device 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 device 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:

HP6208# ping nyc01
HP6208# 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 the HP 6208M-SX and then define four possible default DNS gateway addresses. To do so, enter the following commands:

```
HP6208(config)# ip dns domain-name newyork.com
HP6208(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 device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Do one of the following:
   • On the HP 6208M-SX – Select the DNS link to display the DNS panel.
   • On a routing switch – 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**

**EXAMPLE:**

Suppose you want to trace the route from the HP 6208M-SX to a remote server identified as NYC02 on domain newyork.com. Because the newyork.com domain is already defined on the switch, you need to enter only the host name, NYC02, as noted below.

**USING THE CLI**

HP6208# 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 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.

---

**Domain Name Server**

![Diagram of domain name server](image)

**Figure 6.9 Querying a host on the newyork.com domain**

**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.

**NOTE:** You can use the host name only if you have already configured the DNS resolver for the domain that contains the host.

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.

### Changing the TTL Threshold

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

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

To modify the TTL, use the following CLI method.

**USING THE CLI**

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

```
HP6208(config)# ip ttl 25
HP6208(config)# exit
```

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

**USING THE WEB MANAGEMENT INTERFACE**

You cannot change the TTL on the HP 6208M-SX using the Web management interface.

### Configuring DHCP Assist

DHCP Assist allows the HP 6208M-SX to assist a routing switch that is performing multi-netting on its interfaces as part of its DHCP relay function.

DHCP Assist ensures that a DHCP server that manages multiple IP sub-nets can readily recognize the requester’s IP sub-net, even when that server is not on the client’s local LAN segment. The switch does so by stamping each request with its IP gateway address in the DHCP discovery packet.

**NOTE:** HP ProCurve routing switches provide BootP/DHCP assistance by default on an individual port basis. See “Changing the IP Address Used for Stamping BootP/DHCP Requests” on page 6-71.

By allowing multiple sub-net DHCP requests to be sent on the same wire, you can reduce the number of router ports required to support secondary addressing as well as reduce the number of DHCP servers required, by allowing a server to manage multiple sub-net address assignments.
Configuring IP

Step 3:
DHCP Server generates IP addresses for Hosts 1, 2, 3, and 4. All IP addresses are assigned in the 192.95.5.1 range.

DHCP requests for the other sub-nets were not recognized by the non-DHCP assist router, causing incorrect address assignments to occur.

Step 2:
Router assumes the lowest IP address (192.95.5.1) is the gateway address.

IP addresses configured on the router interface:
- 192.95.5.1
- 200.95.6.1
- 202.95.1.1
- 202.95.5.1

Step 1:
DHCP IP address requests for Hosts 1, 2, 3, and 4 in Sub-nets 1, 2, 3, and 4.

Host 1
- 200.95.6.x
- Sub-net 1

Host 2
- 192.95.5.x
- Sub-net 2

Host 3
- 202.95.1.x
- Sub-net 3

Host 4
- 202.95.5.x
- Sub-net 4

Hub

HP Switch 4000

Router

DHCP Server
- 207.95.7.6

192.95.5.5
192.95.5.10
192.95.5.35
192.95.5.30

Figure 6.10  DHCP requests in a network without DHCP Assist on the switch

In a network operating without DHCP Assist, hosts can be assigned IP addresses from the wrong sub-net range because a routing switch with multiple sub-nets configured on an interface cannot distinguish among DHCP discovery packets received from different sub-nets.

For example, in Figure 6.10 a host from each of the four sub-nets supported on a switch requests an IP address from the DHCP server. These requests are sent transparently to the router. Because the router is unable to determine the origin of each packet by sub-net, it assumes the lowest IP address or the ‘primary address’ is the gateway for all ports on the switch and stamps the request with that address.

When the DHCP request is received at the server, it assigns all IP addresses within that range only.

With DHCP Assist enabled on the HP 6208M-SX, correct assignments are made because the switch provides the stamping service.

How DHCP Assist Works

Upon initiation of a DHCP session, the client sends out a DHCP discovery packet for an address from the DHCP server as seen in Figure 6.11. When the DHCP discovery packet is received at an HP 6208M-SX with the DHCP Assist feature enabled, the gateway address configured on the receiving interface is inserted into the packet. This address insertion is also referred to as stamping.
Step 1:
DHCP IP address requests for Hosts 1,2,3 and 4 in Sub-nets 1, 2, 3 and 4

Step 2:
The HP 6208M-SX stamps each DHCP request with the gateway address of the corresponding sub-net of the receiving port.

Step 3:
Router forwards the DHCP request to the server without touching the gateway address inserted in the packet by the switch.

Figure 6.11  DHCP requests in a network with DHCP Assist operating on the HP 6208M-SX

When the stamped DHCP discovery packet is then received at the router, it is forwarded to the DHCP server. The DHCP server then extracts the gateway address from each request and assigns an available IP address within the corresponding IP sub-net (Figure 6.12). The IP address is then forwarded back to the workstation that originated the request.

NOTE: The DHCP relay function of the connecting router needs to be turned on.
Configuring IP

Step 4: DHCP Server extracts the gateway address from each packet and assigns IP addresses for each host within the appropriate range.

DHCP response with IP addresses for sub-nets 1, 2, 3, and 4:
- 192.95.5.10
- 200.95.6.15
- 202.95.1.35
- 202.95.5.25

Step 5: IP addresses are distributed to the appropriate hosts.

 USING THE CLI

EXAMPLE:
To create the configuration indicated in Figure 6.11 and Figure 6.12:

HP6208(config)# dhcp-gateway-list 1 192.95.5.1
HP6208(config)# dhcp-gateway-list 2 200.95.6.1
HP6208(config)# dhcp-gateway-list 3 202.95.1.35 202.95.5.25
HP6208(config)# int e 2
HP6208(config-if-2)# dhcp-gateway-list 1
HP6208(config-if-2)# dhcp-gateway-list 2
HP6208(config-if-2)# dhcp-gateway-list 3
**Syntax:** dhcp-gateway-list <num> <ip-addr>

**USING THE WEB MANAGEMENT INTERFACE**

1. Log on to the device using a valid user name and password for read-write access. The System configuration panel is displayed.
2. Select the **DHCP Gateway** link to display the DHCP Gateway configuration panel.
3. Enter the list ID in the List ID field. You can specify a number from 1 – 32.
4. Enter up to eight gateway IP address in the IP address fields.
5. Click the Add button to save the change to the device’s running-config file.
6. Select the **Save** link at the bottom of the dialog, then 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 HP ProCurve routing switches and the HP 6208M-SX switch.

- To display IP information on a routing switch, see “Displaying IP Information – Routing Switches” on page 6-80.
- To display IP information on a switch, see “Displaying IP Information – HP 6208M-SX” on page 6-100.

**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 or 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:

```
HP9300(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 – Routing Switches**

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 6-81.
- IP interfaces – see “Displaying IP Interface Information” on page 6-83.
- ARP entries – see “Displaying ARP Entries” on page 6-85.
- Static ARP entries – see “Displaying ARP Entries” on page 6-85.
- IP forwarding cache – see “Displaying the Forwarding Cache” on page 6-88.
- IP route table – see “Displaying the IP Route Table” on page 6-90.

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.

- RIP information – see “Displaying RIP Filters” on page 7-16.
- OSPF information – see “Displaying OSPF Information” on page 8-39.
- BGP4 information – see “Displaying BGP4 Information” on page 10-84.
- DVMRP information – see the “Show Commands” chapter in the Command Line Interface Reference.
- PIM information – see the “Show Commands” chapter in the Command Line Interface Reference.
- VRRP or VRRPE information – see “Displaying VRRP and VRRPE Information” on page 12-19.
- SRP information – see the “Show Commands” chapter in the Command Line Interface Reference.

Displaying Global IP Configuration Information

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

**USING THE CLI**

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

```
HP9300> 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 SRP VRRP
```

**Static Routes**

<table>
<thead>
<tr>
<th>Index</th>
<th>IP Address</th>
<th>Subnet Mask</th>
<th>Next Hop Router</th>
<th>Metric</th>
<th>Distance</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>0.0.0.0</td>
<td>0.0.0.0</td>
<td>209.157.23.2</td>
<td>1</td>
<td>1</td>
</tr>
</tbody>
</table>

**Policies**

<table>
<thead>
<tr>
<th>Index</th>
<th>Action</th>
<th>Source</th>
<th>Destination</th>
<th>Protocol</th>
<th>Port</th>
<th>Operator</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>deny</td>
<td>209.157.22.34</td>
<td>209.157.22.26</td>
<td>tcp</td>
<td>http</td>
<td>=</td>
</tr>
<tr>
<td>64</td>
<td>permit</td>
<td>any</td>
<td>any</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**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>
<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 routing switch. If the packet's TTL value is higher than the value specified in this field, the HP routing switch drops the packet. To change the maximum TTL, see “Changing the TTL Threshold” on page 6-32.</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 routing switch ages out the entry. To change the ARP aging period, see “Changing the ARP Aging Period” on page 6-28.</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 routing switch and still be used by the routing switch’s clients for network booting. To change this value, see “Changing the Maximum Number of Hops to a BootP Relay Server” on page 6-72.</td>
</tr>
<tr>
<td>router-id</td>
<td>The 32-bit number that uniquely identifies the HP routing switch. By default, the router ID is the numerically lowest IP interface configured on the routing switch. To change the router ID, see “Changing the Router ID” on page 6-24.</td>
</tr>
<tr>
<td>enabled</td>
<td>The IP-related protocols that are enabled on the routing switch.</td>
</tr>
<tr>
<td>disabled</td>
<td>The IP-related protocols that are disabled on the routing switch.</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 routing switch 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 routing switches 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 10-30.</td>
</tr>
</tbody>
</table>
### Table 6.8: CLI Display of Global IP Configuration Information – routing switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Policies</strong></td>
<td></td>
</tr>
<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 routing switch takes if a packet matches the comparison values in the policy. The action can be one of the following:  
  - deny – The routing switch drops packets that match this policy.  
  - permit – The routing switch 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 routing switch 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 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:

```
HP9300(config)# show ip interface
```

<table>
<thead>
<tr>
<th>Interface</th>
<th>IP-Address</th>
<th>OK?</th>
<th>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</td>
<td>NVRAM</td>
<td>up</td>
<td>up</td>
</tr>
<tr>
<td>Ethernet 1/2</td>
<td>3.3.3.3</td>
<td>YES</td>
<td>manual</td>
<td>up</td>
<td>up</td>
</tr>
</tbody>
</table>
Loopback 1 1.2.3.4 YES NVRAM down down

Syntax: show ip interface [ethernet <portnum>] | [loopback <num>] | [ve <num>]

This display shows the following 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>
<tr>
<td>IP-Address</td>
<td>The IP address of the interface.</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
<tr>
<td>OK?</td>
<td>Whether the IP address has been configured on the interface.</td>
</tr>
<tr>
<td>Method</td>
<td>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”.</td>
</tr>
<tr>
<td>Status</td>
<td>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”.</td>
</tr>
<tr>
<td>Protocol</td>
<td>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”.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To display IP interface information:

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 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.
This display shows the following information.

Table 6.10: 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 6-32.                                                                                                                  |

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:

```
HP9300# 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.xxx.xxx> [<mask>] | <ip-addr> [<ip-mask>]]

The ethernet <portnum> parameter lets you restrict the display to entries for a specific port.

The mac-address <xxxx.xxx.xxx> 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>
<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>
<tr>
<td>Type</td>
<td>The type, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Dynamic – The routing switch learned the entry from an incoming packet.</td>
</tr>
<tr>
<td></td>
<td>• Static – The routing switch loaded the entry from the static ARP table when the device for the entry was connected to the routing switch.</td>
</tr>
<tr>
<td>Age</td>
<td>The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the table.</td>
</tr>
<tr>
<td></td>
<td>To display the ARP aging period, see &quot;Displaying Global IP Configuration Information&quot; on page 6-81. To change the ARP aging interval, see &quot;Changing the ARP Aging Period&quot; on page 6-28.</td>
</tr>
<tr>
<td></td>
<td><strong>Note:</strong> Static entries do not age out.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the entry was learned.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To display the IP ARP cache:

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 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 6.12: Web Display of ARP Cache – routing switch

<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>
<tr>
<td>Type</td>
<td>The type, which can be one of the following:</td>
</tr>
<tr>
<td></td>
<td>• Dynamic – The routing switch learned the entry from an incoming packet.</td>
</tr>
<tr>
<td></td>
<td>• Static – The routing switch loaded the entry from the static ARP table when the device for the entry was connected to the routing switch.</td>
</tr>
<tr>
<td>Age</td>
<td>The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the cache.</td>
</tr>
<tr>
<td></td>
<td>To display the ARP aging period, see “Displaying Global IP Configuration Information” on page 6-81. To change the ARP aging interval, see “Changing the ARP Aging Period” on page 6-28.</td>
</tr>
<tr>
<td>Note:</td>
<td>Static entries do not age out.</td>
</tr>
<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:

```
HP9300# 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 6.13: 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 6-31.</td>
</tr>
<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 “Displaying the Forwarding Cache Entries for Default Routes” on page 6-61.

USING THE CLI
To display the IP forwarding cache, enter the following command at any CLI level:

HP9300> 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 6.14: CLI Display of IP Forwarding Cache – routing switch

<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>
<tr>
<td>MAC</td>
<td>The MAC address of the destination.</td>
</tr>
<tr>
<td>Note:</td>
<td>If the entry is type U (indicating that the destination is this HP device), the address consists of zeroes.</td>
</tr>
<tr>
<td>Type</td>
<td>The type of host entry, which can be one or more of the following:</td>
</tr>
<tr>
<td></td>
<td>• D – Dynamic</td>
</tr>
<tr>
<td></td>
<td>• P – Permanent</td>
</tr>
<tr>
<td></td>
<td>• F – Forward</td>
</tr>
<tr>
<td></td>
<td>• U – Us</td>
</tr>
<tr>
<td></td>
<td>• C – Complex Filter</td>
</tr>
<tr>
<td></td>
<td>• W – Wait ARP</td>
</tr>
<tr>
<td></td>
<td>• I – ICMP Deny</td>
</tr>
<tr>
<td></td>
<td>• K – Drop</td>
</tr>
<tr>
<td></td>
<td>• R – Fragment</td>
</tr>
<tr>
<td></td>
<td>• S – Snap Encap</td>
</tr>
<tr>
<td>Port</td>
<td>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”.</td>
</tr>
<tr>
<td>VLAN</td>
<td>Indicates the VLAN(s) the listed port is in.</td>
</tr>
<tr>
<td>Pri</td>
<td>The QoS priority of the port or VLAN.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To display the IP forwarding cache:

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 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 6.15: Web Display of IP Forwarding Cache Information – routing switch

<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>
<tr>
<td>MAC</td>
<td>The MAC address of the destination. <strong>Note:</strong> 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  
• P – Permanent  
• F – Forward  
• U – Us  
• C – Complex Filter  
• W – Wait ARP  
• I – ICMP Deny  
• K – Drop  
• 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:

```plaintext
HP9300> show ip route
Total number of IP routes: 514
```
Configuring IP

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]] | <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 <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.

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:

HP9300(config)# show ip route direct
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>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>

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:

HP9300(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:

HP9300(config)# show ip route 209.159.0.0/16 longer
Starting index: 1  B:BGP  D:Directly-Connected  R:RIP  S:Static  O:OSPF

Destination NetMask Gateway Port Cost Type
52 209.159.38.0 255.255.255.0 207.95.6.101 1/1 1 S
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 following table lists the information displayed by the `show ip route` command.

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</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>
<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>
<tr>
<td></td>
<td>• B – The route was learned from BGP.</td>
</tr>
<tr>
<td></td>
<td>• D – The destination is directly connected to this routing switch.</td>
</tr>
<tr>
<td></td>
<td>• R – The route was learned from RIP.</td>
</tr>
<tr>
<td></td>
<td>• S – The route is a static route.</td>
</tr>
<tr>
<td></td>
<td>• * – The route is a candidate default route.</td>
</tr>
<tr>
<td></td>
<td>• O – The route is an OSPF route. Unless you use the ospf option to display the route table, &quot;O&quot; is used for all OSPF routes. If you do use the ospf option, the following type codes are used:</td>
</tr>
<tr>
<td></td>
<td>• O – OSPF intra area route (within the same area).</td>
</tr>
<tr>
<td></td>
<td>• IA – The route is an OSPF inter area route (a route that passes from one area into another).</td>
</tr>
<tr>
<td></td>
<td>• E1 – The route is an OSPF external type 1 route.</td>
</tr>
<tr>
<td></td>
<td>• E2 – The route is an OSPF external type 2 route.</td>
</tr>
</tbody>
</table>

**USING THE WEB MANAGEMENT INTERFACE**

To display the IP route table:

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 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:

HP9300# clear ip route

To clear route 209.157.22.0/24 from the IP routing table:

HP9300# 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 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 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:

HP9300> 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 6.17: CLI Display of IP Traffic Statistics – routing switch**

<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>
</tbody>
</table>

**ICMP statistics**

The ICMP statistics are derived from RFC 792, “Internet Control Message Protocol”, RFC 950, “Internet Standard Subnetting Procedure”, and RFC 1256, “ICMP Router Discovery Messages”. Statistics are organized into Sent and Received. The field descriptions below apply to each.

<table>
<thead>
<tr>
<th>Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>
</tbody>
</table>
Table 6.17: CLI Display of IP Traffic Statistics – routing switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>
<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 SYN) sent 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>
</tbody>
</table>
### Table 6.17: CLI Display of IP Traffic Statistics – routing switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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 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 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 6.18: Web Display of IP Traffic Statistics – routing switch**

<table>
<thead>
<tr>
<th><strong>This Field...</strong></th>
<th><strong>Displays...</strong></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>
<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>
<tr>
<td><strong>ICMP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Total Received</td>
<td>The number of ICMP packets received by the device.</td>
</tr>
<tr>
<td>Total Sent</td>
<td>The number of ICMP packets sent by the device.</td>
</tr>
<tr>
<td>Received Errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Sent Errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Received Unreachable</td>
<td>The number of Destination Unreachable messages received by the device.</td>
</tr>
<tr>
<td>Sent Unreachable</td>
<td>The number of Destination Unreachable messages sent by the device.</td>
</tr>
<tr>
<td>Received Time Exceed</td>
<td>The number of Time Exceeded messages received by the device.</td>
</tr>
<tr>
<td>Sent Time Exceed</td>
<td>The number of Time Exceeded messages sent by the device.</td>
</tr>
<tr>
<td>Received Parameter</td>
<td>The number of Parameter Problem messages received by the device.</td>
</tr>
<tr>
<td>Sent Parameter</td>
<td>The number of Parameter Problem messages sent by the device.</td>
</tr>
<tr>
<td>Received Source Quench</td>
<td>The number of Source Quench messages received by the device.</td>
</tr>
<tr>
<td>Sent Source Quench</td>
<td>The number of Source Quench messages sent by the device.</td>
</tr>
</tbody>
</table>
### Table 6.18: Web Display of IP Traffic Statistics – routing switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>Received Redirect</td>
<td>The number of Redirect messages received by the device.</td>
</tr>
<tr>
<td>Sent Redirect</td>
<td>The number of Redirect messages sent by the device.</td>
</tr>
<tr>
<td>Received Echo</td>
<td>The number of Echo messages received by the device.</td>
</tr>
<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 SYNs) received from other devices.
- **Failed Attempts**
  - This information is used by HP customer support.
### Table 6.18: Web Display of IP Traffic Statistics – routing switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>

### 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>
Displaying IP Information – HP 6208M-SX
You can display the following IP configuration information statistics on the HP 6208M-SX:
- Global IP settings – see “Displaying Global IP Configuration Information” on page 6-100.

Displaying Global IP Configuration Information
To display the switch’s IP address and default gateway, use either of the following methods.

USING THE CLI
To display the IP configuration, enter the following command from any level of the CLI:

HP6208(config)# show ip

Switch IP address: 192.168.1.2
Subnet mask: 255.255.255.0
Default router address: 192.168.1.1
TFTP server address: None
Configuration filename: None
Image filename: None

Syntax: show ip

This display shows the following information.

<table>
<thead>
<tr>
<th>This Field</th>
<th>Displays</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>IP configuration</strong></td>
<td></td>
</tr>
<tr>
<td>Switch IP address</td>
<td>The management IP address you configured on the switch. Specify this address for Telnet or Web management access.</td>
</tr>
<tr>
<td>Subnet mask</td>
<td>The sub-net mask for the management IP address.</td>
</tr>
<tr>
<td>Default router address</td>
<td>The address of the default gateway, if you specified one.</td>
</tr>
<tr>
<td><strong>Most recent TFTP access</strong></td>
<td></td>
</tr>
<tr>
<td>TFTP server address</td>
<td>The IP address of the most-recently contacted TFTP server, if the switch has contacted a TFTP server since the last time the software was reloaded or the switch was rebooted.</td>
</tr>
<tr>
<td>Configuration filename</td>
<td>The name under which the switch’s startup-config file was uploaded or downloaded during the most recent TFTP access.</td>
</tr>
<tr>
<td>Image filename</td>
<td>The name of the switch flash image (system software file) that was uploaded or downloaded during the most recent TFTP access.</td>
</tr>
</tbody>
</table>
Configuring IP

**USING THE WEB MANAGEMENT INTERFACE**

To display the management IP address and default gateway:

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 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 IP Address link to display the IP address configuration panel.

**NOTE:** You cannot display the TFTP access information using the Web management interface.

**Displaying ARP Entries**

To display the entries the switch has placed in its ARP cache, use either of the following methods:

**USING THE CLI**

To display the ARP cache, enter the following command from any level of the CLI:

```
HP6208(config)# show arp
```

```
IP       Mac     Port   Age  VlanId
192.168.1.170 0010.5a11.d042 7 0 1
Total Arp Entries : 1
```

**Syntax:** show arp

This display shows the following information.

<table>
<thead>
<tr>
<th>Table 6.20: CLI Display of ARP Cache</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>This Field...</strong></td>
</tr>
<tr>
<td>IP</td>
</tr>
<tr>
<td>Mac</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Port</td>
</tr>
<tr>
<td>Age</td>
</tr>
<tr>
<td>VlanId</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td>Total ARP Entries</td>
</tr>
</tbody>
</table>
**USING THE WEB MANAGEMENT INTERFACE**

To display the ARP cache:

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 Monitor in the tree view to display the list of configuration options.

3. Select the **ARP Cache** link to display the ARP cache.

This display shows the following information.

<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>
<tr>
<td>Type</td>
<td>The type, which is always Dynamic on HP switches. The device learns dynamic entries from incoming packet.</td>
</tr>
<tr>
<td>Age</td>
<td>The number of minutes the entry has remained unused. If this value reaches the ARP aging period, the entry is removed from the cache.</td>
</tr>
<tr>
<td>Port</td>
<td>The port on which the entry was learned.</td>
</tr>
</tbody>
</table>

**Displaying IP Traffic Statistics**

To display IP traffic statistics on a switch, use one of the following methods.

**USING THE CLI**

To display IP traffic statistics, enter the following command at any CLI level:

```
HP6208# show ip traffic
```

**IP Statistics**

- 27 received, 24 sent
- 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**

- 0 received, 0 sent, 0 no port, 0 input errors

**TCP Statistics**
1 current active tcbs, 4 tcbs allocated, 0 tcbs freed 0 tcbs protected
0 active opens, 0 passive opens, 0 failed attempts
0 active resets, 0 passive resets, 0 input errors
27 in segments, 24 out segments, 0 retransmission

Syntax: show ip traffic

The show ip traffic command displays the following information.

Table 6.22: CLI Display of IP Traffic Statistics – switch

<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>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>
</tbody>
</table>
### Table 6.22: CLI Display of IP Traffic Statistics – switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>echo</td>
<td>The number of Echo messages sent or received by the device.</td>
</tr>
<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>Field</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>received</td>
<td>The number of UDP packets received by the device.</td>
</tr>
<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>Field</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td>current active tcbs</td>
<td>The number of TCP Control Blocks (TCBs) that are currently active.</td>
</tr>
<tr>
<td>tcbs allocated</td>
<td>The number of TCBs that have been allocated.</td>
</tr>
<tr>
<td>tcbs freed</td>
<td>The number of TCBs that have been freed.</td>
</tr>
<tr>
<td>tcbs protected</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>active opens</td>
<td>The number of TCP connections opened by this device by sending a TCP SYN to another device.</td>
</tr>
<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>
</tbody>
</table>
### Table 6.22: CLI Display of IP Traffic Statistics – switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<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>

### Using the Web Management Interface

To display IP traffic statistics:

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 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 6.23: Web Display of IP Traffic Statistics – switch

<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>
<tr>
<td>Packets Sent</td>
<td>The number of IP packets originated and sent by the 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>
<tr>
<td><strong>ICMP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Total Received</td>
<td>The number of ICMP packets received by the device.</td>
</tr>
<tr>
<td>Total Sent</td>
<td>The number of ICMP packets sent by the device.</td>
</tr>
<tr>
<td>Received Errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>This Field...</td>
<td>Displays...</td>
</tr>
<tr>
<td>-------------------------------</td>
<td>-----------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Sent Errors</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Received Unreachable</td>
<td>The number of Destination Unreachable messages received by the device.</td>
</tr>
<tr>
<td>Sent Unreachable</td>
<td>The number of Destination Unreachable messages sent by the device.</td>
</tr>
<tr>
<td>Received Time Exceed</td>
<td>The number of Time Exceeded messages received by the device.</td>
</tr>
<tr>
<td>Sent Time Exceed</td>
<td>The number of Time Exceeded messages sent by the device.</td>
</tr>
<tr>
<td>Received Parameter</td>
<td>The number of Parameter Problem messages received by the device.</td>
</tr>
<tr>
<td>Sent Parameter</td>
<td>The number of Parameter Problem messages sent by the device.</td>
</tr>
<tr>
<td>Received Source Quench</td>
<td>The number of Source Quench messages received by the device.</td>
</tr>
<tr>
<td>Sent Source Quench</td>
<td>The number of Source Quench messages sent by the device.</td>
</tr>
<tr>
<td>Received Redirect</td>
<td>The number of Redirect messages received by the device.</td>
</tr>
<tr>
<td>Sent Redirect</td>
<td>The number of Redirect messages sent by the device.</td>
</tr>
<tr>
<td>Received Echo</td>
<td>The number of Echo messages received by the device.</td>
</tr>
<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 Solication</td>
<td>The number of IRDP Solicitation messages received by the device.</td>
</tr>
<tr>
<td>Sent IRDP Solication</td>
<td>The number of IRDP Solicitation messages sent by the device.</td>
</tr>
</tbody>
</table>
### Table 6.23: Web Display of IP Traffic Statistics – switch (Continued)

<table>
<thead>
<tr>
<th>This Field...</th>
<th>Displays...</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>UDP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Received</td>
<td>The number of UDP packets received by the device.</td>
</tr>
<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>
<tr>
<td><strong>TCP statistics</strong></td>
<td></td>
</tr>
<tr>
<td>Active Opens</td>
<td>The number of TCP connections opened by this device by sending a TCP SYN to another device.</td>
</tr>
<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>
<tr>
<td>Current Active TCBs</td>
<td>The number of TCP Control Blocks (TCBs) that are currently active.</td>
</tr>
<tr>
<td>TCBs Allocated</td>
<td>The number of TCBs that have been allocated.</td>
</tr>
<tr>
<td>TCBs Freed</td>
<td>The number of TCBs that have been freed.</td>
</tr>
<tr>
<td>Keepalive Close Connection</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>Keepalive Failure Callback</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>TCP Connect Connection Exist</td>
<td>This information is used by HP customer support.</td>
</tr>
<tr>
<td>TCP Connect Out of TCB</td>
<td>This information is used by HP customer support.</td>
</tr>
</tbody>
</table>