16

IP Routing Features

Contents

Overview of IP Routing 16-2
- IP Interfaces 16-2
- IP Tables and Caches 16-3
- IP Global Parameters for Routing Switches 16-5
- IP Interface Parameters for Routing Switches 16-6

Configuring IP Parameters for Routing Switches 16-7
- Configuring IP Addresses 16-7
- Configuring ARP Parameters 16-7
- Configuring Forwarding Parameters 16-10
- Configuring ICMP 16-12

Configuring Static IP Routes 16-14
- Static Route Types 16-14
- Static IP Route Parameters 16-15
- Static Route States Follow VLAN (Interface) States 16-15
- Configuring a Static IP Route 16-16
- Configuring the Default Route 16-16
- Configuring a “Null” Route 16-17

Configuring IRDP 16-18
- Enabling IRDP Globally 16-19
- Enabling IRDP on an Individual VLAN Interface 16-19
- Displaying IRDP Information 16-21

Configuring DHCP Relay 16-22
- Overview 16-22
- DHCP Packet Forwarding 16-22
- Minimum Requirements for DHCP Relay Operation 16-23

Overview of IP Routing

The switches covered in this guide offer IP static routing, supporting up to 16 static routes.

IP static routing is configurable through the switch's console CLI.

This chapter refers the switch as a "routing switch". When IP routing is enabled on your switch, it behaves just like any other IP router.

Basic IP routing configuration consists of adding IP addresses and enabling IP routing.

For configuring the IP addresses, see chapter 7, "Configuring IP Addresses". The rest of this chapter describes IP routing 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.

IP Interfaces

On the HP ProCurve routing switches, IP addresses are associated with individual VLANs. By default, there is a single VLAN (Default_VLAN) on the routing switch. In that configuration, a single IP address serves as the management access address for the entire routing switch. If routing is enabled on the routing switch, the IP address on the single VLAN also acts as the routing interface.

Each IP address range, specified by an IP address and a subnet mask or mask bits, must be in a single subnet and must be configured on a single VLAN. For example, if you configure the IP address range 192.200.200.0/24 on a VLAN on the routing switch, you cannot add the address 192.200.200.1 to a different VLAN on the same routing switch. The address 192.200.200.1 is in the address range 192.200.200.0/24 and so is known to exist on that interface and cannot be duplicated on a second VLAN interface.

You can configure multiple IP subnets on the same VLAN. This is commonly known as multi-netting. The number of IP subnets you can configure on an individual VLAN interface is 8.

You can use any of the IP addresses you configure on the routing switch for Telnet, Web management, or SNMP access, as well as for routing.

Note

Your HP ProCurve switch supports IP addresses in classical sub-net format, which includes the IP address and the subnet mask (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 only, with or without the subnet mask.

IP Tables and Caches

The following sections describe the IP tables and caches:

- ARP cache table
- IP route table
- IP forwarding cache

The software enables you to display these tables.

ARP Cache 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.

ARP Cache. The ARP cache contains dynamic (learned) 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:

```
    IP Address        MAC Address       Type      Port
1   207.95.6.102      0800.5afc.ea21    Dynamic   6
```

Figure 16-1. Example of a Dynamic Entry

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

To configure other ARP parameters, see "Configuring ARP Parameters" on page 16-7.

IP Route Table

The IP route table contains routing paths to IP destinations.

Note

The default gateway, which is configured as part of the IP address configuration described in chapter 7, "IP Addressing", is used only when routing is not enabled on the switch.

The IP route table can receive the routing 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

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.

The IP route table is displayed by entering the CLI command **show ip route** from any context level in the console CLI. Here is an example of an entry in the IP route table:

```
Destination     Network Mask    | Gateway         Type      Sub-Type   Metric
--------------- --------------- + --------------- --------- ---------- ------
1.1.0.0         255.255.0.0     | 99.1.1.2        connected            1
```

Figure 16-2. Example of IP Route Table Entry

Each IP route table entry contains the destination's IP address and subnet mask and the IP address of the next-hop router interface to the destination. Each entry also indicates route type. The type indicates how the IP route table received the route.

To configure a static IP route, see "Configuring a Static IP Route" on page 16-16.

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, 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 five minutes, the software removes the entry. The age timer is not configurable.

Note You cannot add static entries to the IP forwarding cache.

IP Global Parameters for Routing Switches

The following table lists the IP global parameters and the page where you can find more information about each parameter.

Table 16-1. IP Global Parameters for Routing Switches

Parameter	Description	Default	See page
Address Resolution Protocol (ARP)	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.	Enabled	16-7
ARP age	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.	20 minutes	16-9
Proxy ARP	An IP mechanism a router can use to answer an ARP request on behalf of a host. It replies with the router's own MAC address instead of the host's.	Disabled	16-10
Time to Live (TTL)	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.	64 hops	7-11
Directed broadcast forwarding	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. **Note**: You also can enable or disable this parameter on an individual interface basis. See table 16-2 on page 16-6.	Disabled	16-11

Parameter	Description	Default	See page
ICMP Router Discovery Protocol (IRDP)	An IP protocol that a router can use to advertise the IP addresses of its router interfaces to directly attached hosts. You can enable or disable the protocol at the Global CLI Config level. You also can enable or disable IRDP and configure the following protocol parameters on an individual VLAN interface basis at the VLAN Interface CLI Config level. • Forwarding method (broadcast or multicast) • Hold time • Maximum advertisement interval • Minimum advertisement interval • Router preference level	Disabled	16-18 16-19
Static route	An IP route you place in the IP route table.	No entries	16-14
Default network route	The router uses the default network route if the IP route table does not contain a route to the destination. For the Switch 5300XL Series devices, enter an explicit default route (0.0.0.0 0.0.0.0 or 0.0.0.0/0) as a static route in the IP route table.	None configured	16-16

IP Interface Parameters for Routing Switches

Table 16-2 lists the interface-level IP parameters for routing switches.

Table 16-2. IP Interface Parameters – Routing Switches

Parameter	Description	Default	See page
IP address	A Layer 3 network interface address; separate IP addresses on individual VLAN interfaces.	None configured	chapter 7
ICMP Router Discovery Protocol (IRDP)	Locally overrides the global IRDP settings. See table 16-1 on page 16-5 for global IRDP information.	Disabled	16-19
IP helper address	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 routing switch to forward requests for certain UDP applications from a client on one sub-net to a server on another sub-net.	None configured	16-23

Configuring IP Parameters for Routing Switches

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

Note

This section describes how to configure IP parameters for routing switches. For IP configuration information when routing is not enabled, refer to chapter 8, ‘Configuring IP Addressing” .

Configuring IP Addresses

You can configure an IP address on the routing switch’s VLAN interfaces. Configuring IP addresses is described in detail in chapter 8, ‘Configuring IP Addressing” .

Configuring ARP Parameters

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

How ARP Works

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

The routing switch encapsulates IP packets in Layer 2 packets regardless of whether the ultimate destination is locally attached or is multiple router hops away. Since the routing switch’s IP route table and IP forwarding cache contain IP address information but not MAC address information, the routing switch cannot forward IP packets based solely on the information in the route

table or forwarding cache. The routing switch needs to know the MAC address that corresponds with the IP address of either the packet's locally attached destination or the next-hop router that leads to the destination.

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

To obtain the MAC address required for forwarding a datagram, the routing switch does the following:

- First, the routing switch looks in the ARP cache (not the static ARP table) for an entry that lists the MAC address for the IP address. The ARP cache maps IP addresses to MAC addresses. The cache also lists the port attached to the device and, if the entry is dynamic, the age of the entry. A dynamic ARP entry enters the cache when the routing switch receives an ARP reply or receives an ARP request (which contains the sender's IP address and MAC address). A static entry enters the ARP cache from the static ARP table (which is a separate table) when the interface for the entry comes up.

  To ensure the accuracy of the ARP cache, each dynamic entry has its own age timer. The timer is reset to zero each time the routing switch receives an ARP reply or ARP request containing the IP address and MAC address of the entry. If a dynamic entry reaches its maximum allowable age, the entry times out and the software removes the entry from the table. Static entries do not age out and can be removed only by you.
- If the ARP cache does not contain an entry for the destination IP address, the routing switch broadcasts an ARP request out all its IP interfaces. The ARP request contains the IP address of the destination. If the device with the IP address is directly attached to the routing switch, the device sends an ARP response containing its MAC address. The response is a unicast packet addressed directly to the routing switch. The routing switch places the information from the ARP response into the ARP cache.

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

  Note: The ARP request broadcast is a MAC broadcast, which means the broadcast goes only to devices that are directly attached to the routing switch. A MAC broadcast is not routed to other networks. However, some

routers, including 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" below.

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, it 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 default ARP age is twenty minutes. You can change the ARP age to a value of 1 - 240 minutes.

To change the ARP age value to 30 minutes, you would use the following CLI command from the global configuration level:

```
HPswitch(config)# ip arp-age 30
```

syntax: ip arp-age < 1-240 >

To display the configured ARP age value, use the command **show config** from any CLI context level. The ARP age value is displayed unless you have not configured a value for ARP age and the default configuration is still being used.

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.

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. To enable Proxy ARP, enter the following commands from the VLAN context level in the CLI:

```
HPswitch(config)# vlan 1
HPswitch(vlan-1)# ip proxy-arp
```

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

```
HPswitch(vlan-1)# no ip proxy-arp
```

Syntax: [no] ip proxy-arp

Configuring Forwarding Parameters

The following configurable parameters control the forwarding behavior of your routing switch:

- Time-To-Live (TTL) threshold — configuring this parameter is covered in chapter 8, ‘Configuring IP Addressing” .
- Forwarding of directed broadcasts — see below.

Note

These parameters are global and thus affect all IP interfaces configured on the routing switch.

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, enter the following CLI command:

```
HPswitch(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 CLI command:

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

Configuring ICMP

You can configure the following ICMP limits:

- **Burst-Normal** – The maximum number of ICMP replies to send per second.
- **Reply Limit** – You can enable or disable ICMP reply rate limiting.

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.
- **Address Mask replies** – You can enable or disable ICMP address mask replies.

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.

To disable response to broadcast ICMP echo packets (ping requests), enter the following command:

```
HPswitch(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:

```
HPswitch(config)# ip icmp echo broadcast-request
```

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. The following types of ICMP Unreachable messages are generated:

- **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.

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.

To disable all ICMP Unreachable messages, enter the following command:

```
HPswitch(config)# no ip icmp unreachable
```

Syntax: [no] ip icmp unreachable

Disabling ICMP Redirects

You can disable ICMP redirects on the HP routing switch. only on a global basis, for all the routing switch interfaces. To disable ICMP redirects globally, enter the following command at the global CONFIG level of the CLI:

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

Syntax: [no] ip icmp redirects

Configuring Static IP Routes

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

- **Directly-connected networks** – When you add an IP VLAN interface, the routing switch automatically creates a route for the network the interface is in.
- **Statically configured route** – You can add up to 16 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.
- **Default network route** – This is a specific static route that the routing switch uses if other routes to the destination are not available. See “Configuring the Default Route” on page 16-16.

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.
- **Null (reject)** – the static route consists of the destination network address and network mask, and the **reject** 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
  - A "null" interface. The routing switch drops traffic forwarded to the null interface.

The HP ProCurve routing switch applies fixed default values for the following routing 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.

Static Route States Follow VLAN (Interface) States

IP static routes remain in the IP route table only so long as the VLAN interface used by the route is available. If the VLAN becomes unavailable, the software removes the static route from the IP route table. If the VLAN 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.

Configuring a Static IP Route

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, you would enter the following commands:

```
HPswitch(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1
HPswitch(config)# write memory
```

Syntax: ip route < *dest-ip-addr* > < *dest-mask* > < *next-hop-ip-addr* >

— *or* —

ip route < *dest-ip-addr* >/< *mask-bits* > < *next-hop-ip-addr* >

The < *dest-ip-addr* > is the route's destination.

The < *dest-mask* > parameter specifies the subnet mask for the routes destination IP address. 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 subnet address specified by the < *dest-ip-addr* >. Alternatively, you can use the CIDR notation and 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 < *next-hop-ip-addr* > is the IP address of the next router in the path to the destination.

Configuring the Default Route

You can also assign a default route and enter it in the routing table. The default route is the route assigned to all traffic that has destinations that are not in the local routing table. For example, if 208.45.228.35 is the IP address of your ISP router, all non-local traffic could be directed to that route by entering the commands:

```
HPswitch(config)# ip route 0.0.0.0  0.0.0.0  208.45.228.35
HPswitch(config)# write 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 to drop packets destined for network 209.157.22.x, enter the following commands:

```
HPswitch(config)# ip route 209.157.22.0  255.255.255.0  reject
HPswitch(config)# write memory
```

Syntax: ip route < *ip-addr* > < *ip-mask* > reject

— *or* —

ip route < *ip-addr* >/< *mask-bits* > reject

Using this command, the routing switch will drop packets that contain the specified IP address in the destination field instead of forwarding them.

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

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 enabled by default. You can enable the feature on a global basis or on an individual VLAN interface 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 VLAN interfaces, you can configure these parameters on an individual VLAN interface 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 default packet type is IP broadcast.
- **Hold time** - Each Router Advertisement message contains a hold time value. This value specifies the maximum about 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.
- **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.

- **Preference** - If a host receives multiple Router Advertisement messages from different routers, the host selects the router that send 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, enter the following command:

```
HPswitch(config)# ip irdp
```

This command enables IRDP on the IP interfaces on all ports. Each port uses the default values for the IRDP parameters.

Enabling IRDP on an Individual VLAN Interface

To enable IRDP on an individual VLAN interface and configure IRDP parameters, enter commands such as the following:

```
HPswitch(config)# vlan 1
HPswitch(vlan-1)# ip irdp maxadvertinterval 400
```

This example shows how to enable IRDP on a specific interface (VLAN 1) and change the maximum advertisement interval for Router Advertisement messages to 400 seconds.

Syntax: [no] ip irdp

Enables or disables (the default) ip irdp on the specified VLAN.

[broadcast | multicast]

This parameter specifies the packet type the routing switch uses to send the Router Advertisement:
broadcast - *The routing switch sends Router Advertisements as IP broadcasts.*
multicast - *The routing switch sends Router Advertisements as multicast packets addressed to IP multicast group 224.0.0.1. This is the default.*

[holdtime < *seconds* >]

This 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.*

[maxadvertinterval < *seconds* >]

This 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. ***Default:*** **600** *(seconds).*

[minadvertinterval < *seconds* >]

This parameter specifies the minimum amount of time the routing switch can wait between sending Router Advertisements. ***Default:*** *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.*

[preference < *number* >]

This 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 preference as the host's default gateway. The valid range is -4294967296 to 4294967295. ***Default:*** **0**.

Displaying IRDP Information

To display IRDP information, enter the following command from any CLI level:

```
HPswitch# show ip irdp

Status and Counters - ICMP Router Discovery Protocol

  Global Status : Disabled
  VLAN Name      Status   Advertising  Min int Max int Holdtime Preference
                            Address     (sec)   (sec)   (sec)
  -------------- -------- ------------ ------- ------- -------- -----------
  DEFAULT_VLAN   Enabled  multicast    450     600     1800     0
  VLAN20         Enabled  multicast    450     600     1800     0
  VLAN30         Enabled  multicast    450     600     1800     0
```

Figure 16-3. Example of Displaying IRDP Information

Configuring DHCP Relay

Overview

The Dynamic Host Configuration Protocol (DHCP) is used for configuring hosts with IP address and other configuration parameters without human intervention. The protocol is composed of three components: the DHCP client, the DHCP server, and the DHCP relay agent. The DHCP client sends broadcast request packets to the network, the DHCP servers respond with broadcast packets that offer IP parameters, such as an IP address for the client. After the client chooses the IP parameters, communication between the client and server is by unicast packets.

The function of the DHCP relay agent is to forward the DHCP messages to other subnets so that the DHCP server doesn't have to be on the same subnet as the DHCP clients. The DHCP relay agent transfers the DHCP messages from DHCP clients located on a subnet without DHCP server, to other subnets. It also relays answers from DHCP servers to DHCP clients.

DHCP Packet Forwarding

The DHCP relay agent on the routing switch forwards DHCP client packets to all DHCP servers that are configured in the table administrated for each VLAN.

Unicast Forwarding

The packets are forwarded using unicast forwarding if the IP address of the DHCP server is a specific host address. The DHCP relay agent sets the destination IP address of the packet to the IP address of the DHCP server and forwards the message.

Broadcast Forwarding

The packets are forwarded using broadcast forwarding if the IP address of the DHCP server is a subnet address or IP broadcast address (255.255.255.255). The DHCP relay agent sets the DHCP server IP address will be set to broadcast IP address and forwarded to all VLANs with configured IP interfaces (except the source VLAN).

Minimum Requirements for DHCP Relay Operation

In order for the DHCP Relay agent to work, the following steps must be completed:

1. DHCP Relay is enabled on the routing switch
2. A DHCP server is servicing the routing switch
3. IP Routing is enabled on the routing switch
4. There is a route from the DHCP server to the routing switch and back
5. An IP Helper address is configured on the routing switch, set to the IP address of the DHCP server on the VLAN that is connected to the DHCP Client.

Enabling DHCP Relay

To enable the DHCP Relay function for the routing switch, at the Config CLI context level, enter the command:

```
HPswitch(config)# dhcp-relay
```

To disable the DHCP Relay function, enter the command:

```
HPswitch(config)# no dhcp-relay
```

Configuring a Helper Address

At the VLAN configuration CLI context level, enter the commands to add the DHCP server's IP address to the VLANs list. For example, to configure a helper address of 18.38.127.53 for VLAN 1, you would enter these commands:

```
HPswitch(conf)# vlan 1
HPswitch(vlan-1)# ip helper-address 18.38.127.53
```

To remove the DHCP server helper address 18.38.127.53 , you would enter this command:

```
HPswitch(vlan-1)# no ip helper-address 18.38.127.53
```

— This page is intentionally unused. —