IP Routing Features

Contents

Overview of IP Routing ........................................... 7-3
IP Interfaces ......................................................... 7-3
IP Tables and Caches ............................................ 7-4
  ARP Cache Table ............................................. 7-4
  IP Route Table .............................................. 7-5
  IP Forwarding Cache ....................................... 7-5
IP Global Parameters for Routing Switches .................... 7-6
IP Interface Parameters for Routing Switches ................. 7-7
Configuring IP Parameters for Routing Switches .............. 7-8
  Configuring IP Addresses .................................... 7-8
  Configuring ARP Parameters ................................. 7-8
    How ARP Works ........................................... 7-8
    Changing the ARP Aging Period ......................... 7-10
    Enabling Proxy ARP ..................................... 7-11
  Configuring Forwarding Parameters ......................... 7-11
    Enabling Forwarding of Directed Broadcasts .......... 7-12
  Configuring ICMP ........................................... 7-13
    Disabling ICMP Messages ................................ 7-13
    Disabling Replies to Broadcast Ping Requests ........ 7-13
    Disabling ICMP Destination Unreachable Messages .... 7-14
    Disabling ICMP Redirects ................................ 7-15
Configuring Static IP Routes .................................. 7-15
  Static Route Types .......................................... 7-15
  Static IP Route Parameters ................................ 7-16
  Static Route States Follow VLAN (Interface) States .... 7-16
  Configuring a Static IP Route ............................... 7-16
  Configuring the Default Route .............................. 7-17
  Configuring a “Null” Route .................................. 7-17
  Displaying Static Route Information ....................... 7-18
Configuring IRDP .................................................. 7-20
Enabling IRDP Globally ........................................... 7-21
Enabling IRDP on an Individual VLAN Interface .......... 7-21
Displaying IRDP Information .................................. 7-23

Configuring DHCP Relay ........................................ 7-24
Overview ......................................................... 7-24
DHCP Packet Forwarding ...................................... 7-24
Unicast Forwarding ............................................. 7-24
Broadcast Forwarding ......................................... 7-24
Minimum Requirements for DHCP Relay Operation ....... 7-25
Enabling DHCP Relay .......................................... 7-25
Configuring a Helper Address ................................. 7-25
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 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.
Your 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.

**AR 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:

<table>
<thead>
<tr>
<th>IP Address</th>
<th>MAC Address</th>
<th>Type</th>
<th>Port</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 207.95.6.102</td>
<td>0800.5afc.ea21</td>
<td>Dynamic</td>
<td>6</td>
</tr>
</tbody>
</table>

**Figure 7-1. 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 7-8.
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:

<table>
<thead>
<tr>
<th>Destination</th>
<th>Network Mask</th>
<th>Gateway</th>
<th>Type</th>
<th>Sub-Type</th>
<th>Metric</th>
</tr>
</thead>
<tbody>
<tr>
<td>1.1.0.0</td>
<td>255.255.0.0</td>
<td>99.1.1.2</td>
<td>connected</td>
<td></td>
<td>1</td>
</tr>
</tbody>
</table>

**Figure 7-2. 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 7-16.

IP Forwarding Cache

The IP forwarding cache provides a fast-path mechanism for forwarding IP packets. The cache contains entries for IP destinations. When a 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 7-1. IP Global 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>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>7-8</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>20 minutes</td>
<td>7-10</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. It replies with the router’s own MAC address instead of the host’s.</td>
<td>Disabled</td>
<td>7-11</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>7-11</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.</td>
<td>Disabled</td>
<td>7-12</td>
</tr>
</tbody>
</table>

**Note:** You also can enable or disable this parameter on an individual interface basis. See table 7-2 on page 7-7.
### Table 7-2. IP Interface Parameters – Routing Switches

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Description</th>
<th>Default</th>
<th>See page</th>
</tr>
</thead>
<tbody>
<tr>
<td>ICMP Router Discovery Protocol (IRDP)</td>
<td>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</td>
<td>Disabled</td>
<td>7-20</td>
</tr>
<tr>
<td>Static route</td>
<td>An IP route you place in the IP route table.</td>
<td>No entries</td>
<td>7-15</td>
</tr>
<tr>
<td>Default network route</td>
<td>The router uses the default network route if the IP route table does not contain a route to the destination. 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.</td>
<td>None configured</td>
<td>7-17</td>
</tr>
</tbody>
</table>

**IP Interface Parameters for Routing Switches**

Table 7-2 lists the interface-level IP parameters for routing switches.
IP Routing Features
Configuring IP Parameters for Routing Switches

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 the chapter on IP addressing in the Management and Configuration Guide.

Configuring IP Addresses

You can configure an IP address on the routing switch's VLAN interfaces. Configuring IP addresses is described in detail in the chapter on IP addressing in the Management and Configuration Guide.

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

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

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

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

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

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

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

**Note:** The ARP request broadcast is a MAC broadcast, which means the broadcast goes only to devices that are directly attached to the routing switch. A MAC broadcast is not routed to other networks. However, some
routers, including ProCurve routing switches, can be configured to reply to ARP requests from one network on behalf of devices on another network. See “Enabling Proxy ARP” 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:

```
ProCurve(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 ProCurve routing switches. To enable Proxy ARP, enter the following commands from the VLAN context level in the CLI:

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

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

```
ProCurve(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 the chapter on IP addressing in the *Management and Configuration Guide*.
- Forwarding of directed broadcasts — see below.

**Note**

These parameters are global and thus affect all IP interfaces configured on the routing switch.
IP Routing Features
Configuring IP Parameters for Routing Switches

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:

ProCurve(config)# ip directed-broadcast

Syntax: [no] ip directed-broadcast

ProCurve 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:

ProCurve(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

ProCurve 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, ProCurve 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:

```
ProCurve(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:

```
ProCurve(config)# ip icmp echo broadcast-request
```
Disabling ICMP Destination Unreachable Messages

By default, when a ProCurve 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 ProCurve 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 ProCurve device cannot forward the packet without fragmenting it.
- **Host** – The destination network or sub-net of the packet is directly connected to the ProCurve device, but the host specified in the destination IP address of the packet is not on the network.
- **Network** – The ProCurve 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 ProCurve 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 ProCurve 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:

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

**Syntax:** [no] ip icmp unreachable
Disabling ICMP Redirects

You can disable ICMP redirects on the ProCurve 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:

```
ProCurve(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. Refer to “Configuring the Default Route” in the chapter titled “IP Routing Features” in the Management and Configuration Guide for your switch.

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.
- **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. By default, when IP routing is enabled, a route for the 127.0.0.0/8 network is created to the null interface. Traffic to this interface is rejected (dropped). This route is for all traffic to the “loopback” network, with the single exception of traffic to the host address of
the switch’s loopback interface (127.0.0.1/32). Figure Figure 7-4. on page 19 illustrates the default Null route entry in the switch’s routing table.

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. In this case the routing switch invokes a “reject” parameter on a static route entry, which results in the switch dropping traffic forwarded to the null interface.

The switch automatically assigns a metric of “1” to an IP static route.

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 (that is, if all ports in the VLAN are offline), 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 static IP route with a destination network 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:

```
ProCurve(config)# ip route 192.0.0.0 255.0.0.0 195.1.1.1
ProCurve(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.
**IP Routing Features**

**Configuring Static IP Routes**

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 all hosts within the Class C sub-net address specified by the `<dest-ip-addr>`. Alternatively, you can use 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.

**Note**

The switch allows one static route configured for a particular network destination. If you configure a static route to a given network and then later configure a different static route to the same network, the switch replaces the first static route with the second.

**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 network 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:

```
ProCurve(config)# ip route 0.0.0.0 0.0.0.0 208.45.228.35
ProCurve(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” 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 209.157.22.0, enter the following commands:

```
ProCurve(config)# ip route 209.157.22.0 255.255.255.0 reject
ProCurve(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.

**Displaying Static Route Information**

The **show ip route** command provides several options for displaying route data.

**Syntax:**
```
show ip route
debug
static
connected
< dest-ip-addr >
```

Lists the route data for the network destination specified by `< dest-ip-addr >`.

For example, Figure 7-3 illustrates a routing topology with two possible gateways to support a static route from switch “A” to the 10.31.224.0 network in switch “C”.

**Figure 7-3. Example of a Routed Network**

Figure 7-4 illustrates the **show ip route** output describing the routes available in the above topology.
### IP Routing Features

**Configuring Static IP Routes**

#### Figure 7-4. Examples of the Show IP Route Command

<table>
<thead>
<tr>
<th>Default Loopback Network</th>
<th>Default Loopback Interface</th>
<th>Configured Static Route</th>
<th>Default Null Route</th>
<th>Destinations Directly Connected to the Switch</th>
<th>Lists the Data for the Specified Route</th>
</tr>
</thead>
<tbody>
<tr>
<td>ProCurve Switch 4104GL(config)# show ip route default</td>
<td>ProCurve Switch 4104GL(config)# show ip route default</td>
<td>ProCurve Switch 4104GL(config)# show ip route default</td>
<td>ProCurve Switch 4104GL(config)# show ip route default</td>
<td>ProCurve Switch 4104GL(config)# show ip route default</td>
<td></td>
</tr>
<tr>
<td><strong>ProCurve Switch 4104GL(config)# show ip route</strong></td>
<td><strong>ProCurve Switch 4104GL(config)# show ip route</strong></td>
<td><strong>ProCurve Switch 4104GL(config)# show ip route</strong></td>
<td><strong>ProCurve Switch 4104GL(config)# show ip route</strong></td>
<td><strong>ProCurve Switch 4104GL(config)# show ip route</strong></td>
<td></td>
</tr>
<tr>
<td><strong>IP Route Entries</strong></td>
<td><strong>IP Route Entries</strong></td>
<td><strong>IP Route Entries</strong></td>
<td><strong>IP Route Entries</strong></td>
<td><strong>IP Route Entries</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Destination</strong></td>
<td><strong>Network Mask</strong></td>
<td><strong>Gateway</strong></td>
<td><strong>Type</strong></td>
<td><strong>Sub-Type</strong></td>
<td></td>
</tr>
<tr>
<td>13.29.224.0</td>
<td>255.255.249.0</td>
<td>VLAN29</td>
<td>connected</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13.30.224.0</td>
<td>255.255.248.0</td>
<td>VLAN30</td>
<td>connected</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>13.31.224.0</td>
<td>255.255.248.0</td>
<td>13.30.224.1</td>
<td>static</td>
<td>1</td>
<td></td>
</tr>
<tr>
<td>127.0.0.0</td>
<td>255.0.0.0</td>
<td>reject</td>
<td>static</td>
<td>0</td>
<td></td>
</tr>
<tr>
<td>127.0.0.1</td>
<td>255.255.255.255</td>
<td>100</td>
<td>connected</td>
<td>0</td>
<td></td>
</tr>
</tbody>
</table>

**ProCurve Switch 4104GL(config)# show ip route default static**

<table>
<thead>
<tr>
<th><strong>IP Route Entries</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>13.31.224.0</td>
</tr>
<tr>
<td>127.0.0.0</td>
</tr>
<tr>
<td>127.0.0.1</td>
</tr>
</tbody>
</table>

**ProCurve Switch 4104GL(config)# show ip route default connected**

<table>
<thead>
<tr>
<th><strong>IP Route Entries</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>13.29.224.0</td>
</tr>
<tr>
<td>13.30.224.0</td>
</tr>
<tr>
<td>127.0.0.0</td>
</tr>
</tbody>
</table>

**ProCurve Switch 4104GL(config)# show ip route 13.31.224.0**

<table>
<thead>
<tr>
<th><strong>IP Route Entries</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>13.31.224.0</td>
</tr>
</tbody>
</table>

**List the Data for the Specified Route**

<table>
<thead>
<tr>
<th><strong>IP Route Entries</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Destination</strong></td>
</tr>
<tr>
<td>13.31.224.0</td>
</tr>
</tbody>
</table>

---

7-19
Configuring IRDP

The ICMP Router Discovery Protocol (IRDP) is used by ProCurve routing switches to advertise the IP addresses of its router interfaces to directly attached hosts. IRDP is 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 ProCurve routing switch, the routing switch responds to the Router Solicitation messages. Some clients interpret this response to mean that the routing switch is the default gateway. If another router is actually the default gateway for these clients, leave IRDP disabled on the ProCurve routing switch.

IRDP uses the following parameters. If you enable IRDP on individual 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:

```
ProCurve(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:

```
ProCurve(config)# vlan 1
ProCurve(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.
IP Routing Features
Configuring IRDP

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:

```
ProCurve# show ip irdp
```

Status and Counters - ICMP Router Discovery Protocol

<table>
<thead>
<tr>
<th>VLAN Name</th>
<th>Status</th>
<th>Address</th>
<th>Min int</th>
<th>Max int</th>
<th>Holdtime</th>
<th>Preference</th>
</tr>
</thead>
<tbody>
<tr>
<td>DEFAULT_VLAN</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>VLAN20</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
<tr>
<td>VLAN30</td>
<td>Enabled</td>
<td>multicast</td>
<td>450</td>
<td>600</td>
<td>1800</td>
<td>0</td>
</tr>
</tbody>
</table>

Figure 7-5. 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:

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

To disable the DHCP Relay function, enter the command:

```
ProCurve(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:

```
ProCurve(conf)# vlan 1
ProCurve(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:

```
ProCurve(vlan-1)# no ip helper-address 18.38.127.53
```
DHCP Option 82

DHCP operation modifies client IP address request packets to the extent needed to forward the packets to a DHCP server. Option 82, supported on the Series 2600 and 2800 switches, enhances this operation by enabling the routing switch to append an Option 82 field to such client requests. This field includes two suboptions for identifying both the routing switch (by MAC address or IP address) and the routing switch port the client is using to access the network. A DHCP server with Option 82 capability can read the appended field and use this data as criteria for selecting the IP addressing it will return to the client through the usual DHCP server response packet.

DHCP Option 82 provides several advantages over DHCP without Option 82:

- An Option 82 DHCP server can use a relay agent’s identity and client source port information to administer IP addressing policies based on client and relay agent location within the network, regardless of whether the relay agent is the client’s primary relay agent or a secondary agent.

- A routing switch operating as a primary Option 82 relay agent for DHCP clients requesting an IP address can enhance network access protection by blocking attempts to use an invalid Option 82 field to imitate an authorized client, or by blocking attempts to use response packets with missing or invalid Option 82 suboptions to imitate valid response packets from an authorized DHCP server.

- An Option 82 relay agent can also eliminate unnecessary broadcast traffic by forwarding an Option 82 DHCP server response only to the port on which the requesting client is connected, instead of broadcasting the DHCP response to all ports on the VLAN.

**Note**

The routing switch’s DHCP Relay Information (Option 82) feature can be used in networks where the DHCP server(s) are compliant with RFC 3046 Option 82 operation. DHCP Servers that are not compliant with Option 82 operation ignore Option 82 fields. For information on configuring an Option 82 DHCP server, refer to the documentation provided with the server application.

Some client applications can append an Option 82 field to their DHCP requests. Refer to the documentation provided for your client application.

It is not necessary for all relay agents on the path between a DHCP client and the server to support Option 82, and a relay agent without Option 82 should forward DHCP packets regardless of whether they include Option 82 fields.
However, Option 82 relay agents should be positioned at the DHCP policy boundaries in a network to provide maximum support and security for the IP addressing policies configured in the server.

Option 82 Server Support

To apply DHCP Option 82, the routing switch must operate in conjunction with a server that supports Option 82. (DHCP servers that do not support Option 82 typically ignore Option 82 fields.) Also, the routing switch applies Option 82 functionality only to client request packets being routed to a DHCP server. DHCP relay with Option 82 does not apply to switched (non-routed) client requests.

For information on configuring policies on a server running DHCP Option 82, refer to the documentation provided for that application.

**Figure 6. Example of a DHCP Option 82 Application**

**Terminology**

*Circuit ID:* In Option 82 applications, the number of the port through which the routing switch receives a DHCP client request. On ProCurve fixed-port switches, the Circuit ID of a given port corresponds to the port number appearing on the front of the switch for that port. On ProCurve chassis switches, the port number for a given port corresponds to the internal ifIndex number for that port. This value is included as a suboption in an Option 82 field that the relay agent appends to a Client DHCP request before forwarding the request toward a DHCP server. (For more on Circuit ID, refer to “Circuit ID” in the bulleted list on page 31.)
**DHCP Policy Boundary:** For Option 82 applications, an area of a network as defined by connection to a given routing switch or subnet and/or a specific port belonging to the routing switch or subnet.

**DHCP relay agent:** See Relay Agent.

**Forwarding Policy:** The Option 82 method the routing switch uses to process incoming client DHCP requests. For a given inbound DHCP client request, the forwarding policy determines whether the routing switch will add Option 82 information, replace existing Option 82 information, or leave any existing information unchanged. The policy also determines whether the routing switch will forward the client request toward a DHCP server or drop the request. For a DHCP server response to an Option 82 client request, the routing switch can optionally perform a validation check to determine whether to forward or drop the response. Each Option 82 relay agent in the path between a DHCP client and an Option 82 DHCP server can be configured with a unique forwarding policy, which enhances DHCP policy control over discrete areas of a network.

**Primary Relay Agent:** In the path between a DHCP client and a DHCP server, the first routing switch (configured to support DHCP operation) that a client DHCP request encounters in the path from the client to a DHCP server.

**Relay Agent:** A routing switch that is configured to support DHCP operation.

**Remote ID:** In Option 82 applications on ProCurve switches, either the MAC address of a relay agent, or the IP address of a VLAN or subnet configured on a relay agent. This value is included as a suboption in an Option 82 field that the relay agent appends to a Client DHCP request before forwarding the request toward a DHCP server. (For more on Remote ID, refer to “Remote ID” in the bulleted list on page <zBlue>30.)

**Secondary Relay Agent:** In the path between a DHCP client and a DHCP server, any routing switch (configured to support DHCP operation) other than the primary relay agent.

**General DHCP Option 82 Requirements and Operation**

**Requirements.** DHCP Option 82 operation can be configured on the Series 2600 and 2800 switches at the global config level and requires the following:

- IP routing enabled on the switch
- DHCP-Relay Option 82 enabled (global command level)
IP Routing Features
Configuring DHCP Relay

- routing switch access to an Option 82 DHCP server on a different subnet than the clients requesting DHCP Option 82 support
- one IP Helper address configured on each VLAN supporting DHCP clients

General DHCP-Relay Operation with Option 82. Typically, the first (primary) Option 82 relay agent to receive a client's DHCP request packet appends an Option 82 field to the packet and forwards it toward the DHCP server identified by the IP Helper address configured on the VLAN in which the client packet was received. Other, upstream relay agents used to forward the packet may append their own Option 82 fields, replace the Option 82 field(s) they find in the packet, forward the packet without adding another field, or drop the packet. (Intermediate next-hop routing switches without Option 82 capability can be used to forward—route—client request packets with Option 82 fields.) Response packets from an Option 82 server are routed back to the primary relay agent (routing switch), and include an IP addressing assignment for the requesting client and an exact copy of the Option 82 data the server received with the client request. The relay agent strips off the Option 82 data and forwards the response packet out the port indicated in the response as the Circuit ID (client access port). Under certain validation conditions described later in this section, a relay agent detecting invalid Option 82 data in a response packet may drop the packet.

![Diagram of DHCP Option 82 Operation in a Network with a Non-Compliant Relay Agent](image)

**Figure 7. Example of DHCP Option 82 Operation in a Network with a Non-Compliant Relay Agent**

**Relay Agent 1** adds an Option 82 field to a client request, and then forwards the request toward the server. This includes any client requests received from Relay Agent 2 without an Option 82 field.

**Note:** DHCP Option 82 does not operate with clients on VLAN 4 because DHCP requests from these clients are not routed.

**Relay Agent 2** does not add an Option 82 field to client requests before forwarding the requests. However, any client requests received from Relay Agent 3 will be forwarded with the Option 82 fields that were added by Relay Agent 3.

**Relay Agent 3** adds an Option 82 field to a client request and then forwards the request.
IP Routing Features
Configuring DHCP Relay

Option 82 Field Content

The Remote ID and Circuit ID subfields comprise the Option 82 field a relay agent appends to client requests. A DHCP server configured to apply a different IP addressing policy to different areas of a network uses the values in these subfields to determine which DHCP policy to apply to a given client request.

- **Remote ID**: This configurable subfield identifies a policy area that comprises either the routing switch as a whole (by using the routing switch MAC address) or an individual VLAN configured on the routing switch (by using the IP address of the VLAN receiving the client request).
  - Use the IP address option if the server will apply different IP addressing policies to DHCP client requests from ports in different VLANs on the same routing switch.
  - Use the MAC address option if, on a given routing switch, it does not matter to the DHCP server which VLAN is the source of a client request (that is, use the MAC address option if the IP addressing policies supported by the target DHCP server do not distinguish between client requests from ports in different VLANs in the same routing switch).

To view the MAC address for a given routing switch, execute the `show system-information` command in the CLI.

<table>
<thead>
<tr>
<th>Status and Counters</th>
<th>General System Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>System Name</td>
<td>ProCurve switch</td>
</tr>
<tr>
<td>System Contact</td>
<td></td>
</tr>
<tr>
<td>System Location</td>
<td></td>
</tr>
<tr>
<td>MAC Age Time (sec)</td>
<td>300</td>
</tr>
<tr>
<td>Time Zone</td>
<td>0</td>
</tr>
<tr>
<td>Daylight Time Zone</td>
<td>None</td>
</tr>
<tr>
<td>Firmware revision</td>
<td>1.08.60</td>
</tr>
<tr>
<td>ROM Version</td>
<td>1.08.05</td>
</tr>
<tr>
<td>Base MAC Addr</td>
<td>00113a-85ce20</td>
</tr>
<tr>
<td>Serial Number</td>
<td>SG426HBO18</td>
</tr>
<tr>
<td>Up Time</td>
<td>32 mins</td>
</tr>
<tr>
<td>CPU Util (%)</td>
<td>4</td>
</tr>
<tr>
<td>Memory - Total</td>
<td>33,043,456</td>
</tr>
<tr>
<td>Free</td>
<td>26,335,136</td>
</tr>
<tr>
<td>IP Mgmt - Pkts Rx</td>
<td>0</td>
</tr>
<tr>
<td>Packet - Total</td>
<td>1998</td>
</tr>
<tr>
<td>Errors</td>
<td>1268</td>
</tr>
</tbody>
</table>

Figure 8. Using the CLI To View the Switch MAC Address
- **Circuit ID**: This nonconfigurable subfield identifies the port number of the physical port through which the routing switch received a given DHCP client request, and is necessary to identify if you want to configure an Option 82 DHCP server to use the Circuit ID to select a DHCP policy to assign to clients connected to the port. This number is the identity of the inbound port. On ProCurve fixed-port switches, the port number used for the Circuit ID is always the same as the physical port number shown on the front of the switch. On ProCurve chassis switches, where a dedicated, sequential block of internal port numbers are reserved for each slot, regardless of whether a slot is occupied, the circuit ID for a given port is the sequential index number for that port position in the slot. (To view the Index number assignments for ports in the routing switch, use the `walkmib ifname` command.)

For example, the circuit ID for a client connected to port 11 on a ProCurve 2650-PWR (J8165A) switch is “11”. However, the Circuit ID for port B11 on a ProCurve 5304xl (J4850A) is “37”. (See figure 7-9, below.)

![Figure 7-9. Using Walkmib To Determine the Circuit ID for a Port on a ProCurve Chassis](image)
IP Routing Features
Configuring DHCP Relay

For example, suppose you wanted port 10 on a given relay agent to support no more than five DHCP clients simultaneously, you could configure the server to allow only five IP addressing assignments at any one time for the circuit ID (port) and remote ID (MAC address) corresponding to port 10 on the selected relay agent.

Similarly, if you wanted to define specific ranges of addresses for clients on different ports in the same VLAN, you could configure the server with the range of IP addresses allowed for each circuit ID (port) associated with the remote ID (IP address) for the selected VLAN.

Forwarding Policies

DHCP Option 82 on ProCurve switches offers four forwarding policies, with an optional validation of server responses for three of the policy types (append, replace, or drop).

Table 8. Configuration Options for Managing DHCP Client Request Packets

<table>
<thead>
<tr>
<th>Option 82 Configuration</th>
<th>DHCP Client Request Packet Inbound to the Routing Switch</th>
<th>Packet Has No Option 82 Field</th>
<th>Packet Includes an Option 82 Field</th>
</tr>
</thead>
<tbody>
<tr>
<td>Append</td>
<td>Append an Option 82 Field</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Keep</td>
<td>Append an Option 82 Field</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

**Append** allows the most detail in defining DHCP policy boundaries. For example, where the path from a client to the DHCP Option 82 server includes multiple relay agents with Option 82 capability, each relay agent can define a DHCP policy boundary and append its own Option 82 field to the client request packet. The server can then determine in detail the agent hops the packet took, and can be configured with a policy appropriate for any policy boundary on the path.

**Note:** In networks with multiple relay agents between a client and an Option 82 server, append can be used only if the server supports multiple Option 82 fields in a client request. If the server supports only one Option 82 field in a request, consider using the keep option.

This policy does not include the validate option (described in the next section) and allows forwarding of all server response packets arriving inbound on the routing switch (except those without a primary relay agent identifier.)
Multiple Option 82 Relay Agents in a Client Request Path

Where the client is one router hop away from the DHCP server, only the Option 82 field from the first (and only) relay agent is used to determine the policy boundary for the server response. Where there are multiple Option 82 router hops between the client and the server, you can use different configuration options on different relay agents to achieve the results you want. This includes configuring the relay agents so that the client request arrives at the server with either one Option 82 field or multiple fields. (Using multiple Option 82 fields assumes that the server supports multiple fields and is configured to assign IP addressing policies based on the content of multiple fields.)

<table>
<thead>
<tr>
<th>Option 82 Configuration</th>
<th>DHCP Client Request Packet Inbound to the Routing Switch</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Packet Has No Option 82 Field</td>
</tr>
</tbody>
</table>
| Replace                | Append an Option 82 Field | Replace replaces any existing Option 82 fields from downstream relay agents (and/or the originating client) with an Option 82 field for the current relay agent. Some applications for replace include:  
  - The relay agent is located at a point in the network that is a DHCP policy boundary and you want to replace any Option 82 fields appended by downstream devices with an Option 82 field from the relay agent at the boundary. (This eliminates downstream Option 82 fields you do not want the server to use when determining which IP addressing policy to apply to a client request.)  
  - In applications where the routing switch is the primary relay agent for clients that may append their own Option 82 field, you can use replace to delete these fields if you do not want them included in client requests reaching the server. |
| Drop                   | Append an Option 82 Field | Drop causes the routing switch to drop an inbound client request with an Option 82 field already appended. If no Option 82 fields are present, drop causes the routing switch to add an Option 82 field and forward the request. As a general guideline, configure drop on relay agents at the edge of a network, where an inbound client request with an appended Option 82 field may be unauthorized, a security risk, or for some other reason, should not be allowed. |

The above combination allows for detection and dropping of client requests with spurious Option 82 fields. If none are found, then the drop policy on the first relay agent adds an Option 82 field, which is then kept unchanged over
the next two relay agent hops (“B” and “C”). The server can then enforce an IP addressing policy based on the Option 82 field generated by the edge relay agent (“A”). In this example, the DHCP policy boundary is at relay agent 1.

![Diagram showing DHCP Option 82 field contributions](image)

**Figure 11. Example Configured To Allow Multiple Relay Agents To Contribute an Option 82 Field**

This is an enhancement of the previous example. In this case, each hop for an accepted client request adds a new Option 82 field to the request. A DHCP server capable of using multiple Option 82 fields can be configured to use this approach to keep a more detailed control over leased IP addresses. In this example, the primary DHCP policy boundary is at relay agent “A”, but more global policy boundaries can exist at relay agents “B” and “C”.

![Diagram showing DHCP Option 82 field replacements](image)

**Figure 12. Example Allowing Only an Upstream Relay Agent To Contribute an Option 82 Field**

Like the first example, above, this configuration drops client requests with spurious Option 82 fields from clients on the edge relay agent. However, in this case, only the Option 82 field from the last relay agent is retained for use by the DHCP server. In this case the DHCP policy boundary is at relay agent “C”. In the previous two examples the boundary was with relay “A”.

**Validation of Server Response Packets**

A valid Option 82 server response to a client request packet includes a copy of the Option 82 field(s) the server received with the request. With validation disabled, most variations of Option 82 information are allowed, and the corresponding server response packets are forwarded.
Server response validation is an option you can specify when configuring Option 82 DHCP for \texttt{append}, \texttt{replace}, or \texttt{drop} operation. (Refer to “Forwarding Policies” on page 7-32.) Enabling validation on the routing switch can enhance protection against DHCP server responses that are either from untrusted sources or are carrying invalid Option 82 information.

With validation enabled, the relay agent applies stricter rules to variations in the Option 82 field(s) of incoming server responses to determine whether to forward the response to a downstream device or to drop the response due to invalid (or missing) Option 82 information. Table 7-13, below, illustrates relay agent management of DHCP server responses with optional validation enabled and disabled.

<table>
<thead>
<tr>
<th>Response Packet Content</th>
<th>Option 82 Configuration</th>
<th>Validation Enabled on the Relay Agent</th>
<th>Validation Disabled (The Default)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Valid DHCP server response packet without an Option 82 field.</td>
<td>\texttt{append, replace, or drop\textsuperscript{1}}</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td></td>
<td>\texttt{keep\textsuperscript{2}}</td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a \textit{Remote ID} and \textit{Circuit ID} combination that did not originate with the given relay agent.</td>
<td>\texttt{append}</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td></td>
<td>\texttt{replace or drop\textsuperscript{1}}</td>
<td>Drop the server response packet.</td>
<td>Drop the server response packet.</td>
</tr>
<tr>
<td></td>
<td>\texttt{keep\textsuperscript{2}}</td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>The server response packet carries data indicating a given routing switch is the primary relay agent for the original client request, but the associated Option 82 field in the response contains a \textit{Remote ID} that did not originate with the relay agent.</td>
<td>\texttt{append}</td>
<td>Drop the server response packet.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td></td>
<td>\texttt{replace or drop\textsuperscript{1}}</td>
<td>Drop the server response packet.</td>
<td>Drop the server response packet.</td>
</tr>
<tr>
<td></td>
<td>\texttt{keep\textsuperscript{2}}</td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
<tr>
<td>All other server response packets\textsuperscript{3}</td>
<td>\texttt{append, keep\textsuperscript{2}, replace, or drop\textsuperscript{1}}</td>
<td>Forward server response packet to a downstream device.</td>
<td>Forward server response packet to a downstream device.</td>
</tr>
</tbody>
</table>

\textsuperscript{1}Drop is the recommended choice because it protects against an unauthorized client inserting its own Option 82 field for an incoming request.

\textsuperscript{2}A routing switch with DHCP Option 82 enabled with the \texttt{keep} option forwards all DHCP server response packets except those that are not valid for either Option 82 DHCP operation (compliant with RFC 3046) or DHCP operation without Option 82 support (compliant with RFC 2131).

\textsuperscript{3}A routing switch with DHCP Option 82 enabled drops an inbound server response packet if the packet does not have any device identified as the primary relay agent (\texttt{giaddr} = \texttt{null}; refer to RFC 2131).
Multinetted VLANs

On a multinetted VLAN, each interface can form an Option 82 policy boundary within that VLAN if the routing switch is configured to use IP for the remote ID suboption. That is, if the routing switch is configured with IP as the remote ID option and a DHCP client request packet is received on a multinetted VLAN, the IP address used in the Option 82 field will identify the subnet on which the packet was received instead of the primary IP address for the VLAN. This enables an Option 82 DHCP server to support more narrowly defined DHCP policy boundaries instead of defining the boundaries at the VLAN or whole routing switch levels. If the MAC address option (the default) is configured instead, then the routing switch MAC address will be used regardless of which subnet was the source of the client request. (The MAC address is the same for all VLANs configured on the routing switch.)

Note that all request packets from DHCP clients in the different subnets in the VLAN must be able to reach any DHCP server identified by the IP Helper Address(es) configured on that VLAN.

Configuring Option 82 Operation on the Routing Switch

**Syntax:**
```
```

**append:** Configures the routing switch to append an Option 82 field to the client DHCP packet. If the client packet has any existing Option 82 field(s) assigned by another device, then the new field is appended to the existing field(s).

The appended Option 82 field includes the switch Circuit ID (inbound port number*) associated with the client DHCP packet, and the switch Remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN's IP address instead of the switch MAC address for the remote ID, use the `ip` option (below).

**replace:** Configures the routing switch to replace any existing Option 82 field(s) in an inbound client DHCP packet with one Option 82 field for the current routing switch.

The replacement Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet, and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN's IP address instead of the switch MAC address for the remote ID, use the `ip` option (below).
**drop:** Configures the routing switch to unconditionally drop any client DHCP packet received with existing Option 82 field(s). This means that such packets will not be forwarded. Use this option where access to the routing switch by untrusted clients is possible.

*If the routing switch receives a client DHCP packet without an Option 82 field, it adds an Option 82 field to the client and forwards the packet. The added Option 82 field includes the switch circuit ID (inbound port number*) associated with the client DHCP packet, and the switch remote ID. The default switch remote ID is the MAC address of the switch on which the packet was received from the client. To use the incoming VLAN’s IP address instead of the switch MAC address for the remote ID, use the IP option (below).*

**keep:** For any client DHCP packet received with existing Option 82 field(s), configures the routing switch to forward the packet as-is, without replacing or adding to the existing Option 82 field(s).

*[For more on identifying the inbound port number, refer to “Circuit ID” in the bulleted list on page <zBlue>31.]*

[ validate ]: This option operates when the routing switch is configured with append, replace, or drop as a forwarding policy. With validate enabled, the routing switch applies stricter rules to an incoming Option 82 server response to determine whether to forward or drop the response. For more information, refer to “Validation of Server Response Packets” on page 7-34.

[ip | mac]

This option specifies the remote ID suboption the routing switch will use in Option 82 fields added or appended to DHCP client packets. The choice of type depends on how you want to define DHCP policy areas in the client requests sent to the DHCP server. (Refer to “Option 82 Field Content” on page 7-30.)

**ip:** Specifies the IP address of the VLAN on which the client DHCP packet enters the switch.

**mac:** Specifies the routing switch’s MAC address. (The MAC address used is the same MAC address that is assigned to all VLANs configured on the routing switch.) This is the default setting.

**Notes on Default Remote ID Selection:** Executing the Option 82 command without specifying either ip or mac configures the remote ID as the MAC address of the switch on which the packet was received from the client. The command options for viewing the routing switch MAC address are listed at the end of the “Remote ID” description that begins on page <zBlue>30.
IP Routing Features
Configuring DHCP Relay

Operating Notes

- This implementation of DHCP relay with Option 82 complies with the following RFCs:
  - RFC 2131
  - RFC 3046

- Moving a client to a different port allows the client to continue operating as long as the port is a member of the same VLAN as the port through which the client received its IP address. However, rebooting the client after it moves to a different port can alter the IP addressing policy the client receives if the DHCP server is configured to provide different policies to clients accessing the network through different ports.

- The IP address of the primary DHCP relay agent receiving a client request packet is automatically added to the packet, and is identified as the `giaddr` (gateway interface address). (That is, the giaddr is the IP address of the VLAN on which the request packet was received from the client.) For more information, refer to RFC 2131 and RFC 3046.

- DHCP request packets from multiple DHCP clients on the same relay agent port will be routed to the same DHCP server(s). Note that when using 802.1X on a 5300xl switch running software release E.09.xx or greater, a port’s VLAN membership may be changed by a RADIUS server responding to a client authentication request. In this case the DHCP server(s) accessible from the port may change if the VLAN assigned by the RADIUS server has different DHCP helper addresses than the VLAN used by unauthenticated clients.

- Where multiple DHCP servers are assigned to a VLAN, a DHCP client request cannot be directed to a specific server. Thus, where a given VLAN is configured for multiple DHCP servers, all of these servers should be configured with the same IP addressing policy.

- Where routing switch “A” is configured to insert its MAC address as the Remote ID in the Option 82 fields appended to DHCP client requests, and upstream DHCP servers use that MAC address as a policy boundary for assigning an IP addressing policy, then replacing switch “A” makes it necessary to reconfigure the upstream DHCP server(s) to recognize the MAC address of the replacement switch. This does not apply in the case where an upstream relay agent “B” is configured with option 82 replace, which removes the Option 82 field originally inserted by switch “A”.

---

7-38
• Relay agents without Option 82 can exist in the path between Option 82 relay agents and an Option 82 server. The agents without Option 82 will forward client requests and server responses without any effect on Option 82 fields in the packets.

• If the routing switch is not able to add an Option 82 field to a client’s DHCP request due to the message size exceeding the MTU (Maximum Transmission Unit) size, then the request is forwarded to the DHCP server without Option 82 information and an error message is logged in the switch’s Event Log.