Chapter 20

Configuring DHCP Relay

The Dynamic Host Configuration Protocol (DHCP) provides a mechanism through which computers using Transmission Control Protocol/IP (TCP/IP) can obtain protocol configuration parameters automatically from a DHCP server on the network.

The following sections describe how to configure your E-series router to provide DHCP support:

Configuring DHCP Relay and BOOTP Relay

The DHCP relay feature relays a request from a remote client to a DHCP server for an IP address. When the router receives a DHCP request from an IP client, it forwards the request to the DHCP server and passes the response back to the IP client.

Configuring DHCP relay also enables bootstrap protocol (BOOTP) relay. The router relays any BOOTP requests it receives to the same set of servers that you configured for DHCP relay. A DHCP server can respond to the BOOTP request only if it is also a BOOTP server. The router relays any BOOTP responses it receives to the originator of the BOOTP request. If you do not configure DHCP relay, then BOOTP relay is disabled.

The router must wait for an acknowledgment from the DHCP server that the assigned address has been accepted. The IP client must accept an IP address from one of the servers. When the DHCP server sends an acknowledgment message back to the DHCP client via the router, the router updates its routing table with the IP address of the client.

If a DHCP relay request is received on an unnumbered interface, the router determines the loopback address for that interface and passes that IP address to the server.

DHCP carries other important configuration parameters, such as the subnet mask, default router, and DNS server. You can also use the DHCP relay agent information option (option 82) to add information to the DHCP packets sent to DHCP servers—the additional information, in the form of suboptions to the option 82 value, helps you to manage the IP address and service level assignments granted to your subscribers. For example, you can add the E-series hostname or the virtual router name to the front of the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82). See *Configuring Relay Agent Option 82 Information* on page 432.

Enabling DHCP Relay

You use the **set dhcp relay** command to create and enable DHCP relay in the current virtual router.

- Include the IP address variable to enable DHCP relay and BOOTP relay and to specify an IP address for the DHCP server. When you include the IP address of a DHCP server, the router adds the IP address to the list of DHCP servers (up to five) and forwards all request packets to all configured servers.

  Issuing this command also enables relay of BOOTP requests to the configured DHCP servers. If one of the DHCP servers is also a BOOTP server and responds, the router relays the response to the request originator.

  host1(config)#**set dhcp relay 192.168.29.10**

- Use the **no** version with an IP address to remove the specified DHCP server:

  host1(config)#**no set dhcp relay 192.168.29.25**

- Use this command without an IP address to create the DHCP relay independent of any DHCP servers. Use this version of the command when configuring support for DHCP vendor-option strings (option 60). For information about configuring option 60 support, see *Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers* on page 429.

  host1(config)#**set dhcp relay**

- Use the **no** version without specifying an IP address to explicitly delete the DHCP relay from the current virtual router.

  host1(config)#**no set dhcp relay**

Removing Access Routes from Routing Tables and NVS

You can remove existing access routes for an interface from routing tables and nonvolatile storage (NVS).

- To remove access routes:

  host1(config)#**set dhcp relay discard-access-routers**

NOTE: When this feature is configured, the client bypasses the DHCP relay component and communicates directly with the DHCP server to request address renewal or to release the address. The DHCP relay component has no role in determining when or whether to remove the installed host route.

Treating All Packets as Originating at Trusted Sources

By default, the DHCP relay treats all packets destined for DHCP servers as if the packets originated at an untrusted source; if the packets have a gateway IP address (giaddr) of 0 and if option 82 information is present, these packets are dropped.

- To enable the trust-all method on the DHCP relay:

  host1(config)#**set dhcp relay trust-all**

In the trust-all method, the DHCP relay treats the packets as if they are from trusted sources and forwards the packets to the DHCP server. When you enable this command:

- If the DHCP packets contain option 82 and a giaddr field of 0, the DHCP relay inserts its giaddr into the packets and then forwards the packets.
- If the DHCP relay is configured to add option 82, it does not add an additional option 82 if one is already present in the DHCP packets.

Assigning the Giaddr to Source IP Address

As a security measure, DHCP servers typically use the giaddr included in DHCP packets to ensure that the packets come from a recognized DHCP gateway. The servers verify that the giaddr in the DHCP packet matches the source IP address in the IP packet header. You can use the **set dhcp relay assign-giaddr-source-ip** command to specify that the DHCP relay and DHCP relay proxy assign the giaddr to the source IP packet header of packets they send to DHCP servers—the DHCP servers can then compare the giaddr in the IP packet header to the giaddr in the DHCP packets.

- To assign the giaddr to the source IP packet header:

  host1(config)#**set dhcp relay assign-giaddr-source-ip**

Protecting Against Spoofed Giaddr and Relay Agent Option Values

DHCP relay includes an override feature that provides enhanced security to protect against spoofed giaddr and relay agent option (option 82) values in packets destined for DHCP servers.

DHCP relay can detect spoofed giaddrs when the giaddr value is equal to a local IP address on which the DHCP relay can be accessed; otherwise, DHCP relay does not detect spoofed giaddrs. Also, DHCP relay does not detect spoofed relay agent option values.

Spoofed giaddrs are a concern when the DHCP relay is used if the giaddr value in received DHCP packets is different from the local IP address on which the DHCP relay is accessed. In this situation, DHCP relay always honors the giaddr. To configure DHCP relay to override all giaddrs (including valid giaddrs) that are received from downstream network elements, use the **set dhcp relay override** command with the **giaddr** keyword. DHCP relay then takes control of the client, adding its own giaddr to the packets before forwarding the packets to the DHCP server.

Spoofed relay agent options are a concern if the giaddr is not null, or if it is null and the DHCP relay is operating in the trust-all method. In these two situations, DHCP relay always honors the relay agent option value in received DHCP packets.

- To protect against spoofed giaddrs and relay agent option values:

  host1(config)#**set dhcp relay override agent-option**

  DHCP relay then overrides all relay agent option values that are received from downstream network elements, performing one of the following actions:

  - If the DHCP relay is configured to add relay agent option 82 to the packets, it clears the existing option 82 values and inserts the new values.
  - If the DHCP relay is not configured to add relay agent option 82, it clears the existing option values but does not add any new values.

Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets

Each DHCP request packet includes a broadcast flag that, if set, specifies how to transmit DHCP Offer reply packets and DHCP ACK and NAK reply packets to DHCP clients during the discovery process. To configure DHCP relay and DHCP relay proxy to use the setting of the broadcast flag to control the transmission of DHCP Offer, DHCP ACK, and DHCP NAK reply packets, use the **set dhcp relay broadcast-flag-replies** command from Global Configuration mode.

When you issue the **set dhcp relay broadcast-flag-replies** command, the method that DHCP relay and DHCP relay proxy use to transmit DHCP Offer reply packets and ACK and NAK reply packets depends on whether the broadcast flag in the DHCP request packet is set or not set, as follows:

- If the broadcast flag is set in the DHCP request packet, using the **set dhcp relay broadcast-flag-replies** command causes DHCP relay and DHCP relay proxy to broadcast DHCP reply packets to clients.
- If the broadcast flag is not set in the DHCP request packet, using the **set dhcp relay broadcast-flag-replies** command causes DHCP relay and DHCP relay proxy to use the layer 2 unicast transmission method to send DHCP reply packets using the client's layer 2 (MAC) address and layer 3 (IP) unicast address.

There are exceptions to this behavior for DHCP relay proxy when the DHCP client is already bound to an IP address or is renewing the lease on its IP address. For information, see *Behavior for Bound Clients and Address Renewals* on page 447.

To display whether support for broadcast flag replies is currently on or off on the router, use the **show dhcp relay** command. For information, see *Chapter 22, Monitoring and Troubleshooting DHCP*.

To troubleshoot applications that use this feature, you can use the dhcpCapture system event log category. For information about how to log system events, see *JUNOSe System Event Logging Reference Guide, Chapter 1, System Logging Overview*.

Interaction with Layer 2 Unicast Transmission Method

As described in *Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients* on page 428, you can use the **set dhcp relay layer2-unicast-replies** command to configure DHCP relay and DHCP relay proxy to use the layer 2 unicast and layer3 broadcast transmission method to send DHCP Offer reply packets and DHCP ACK and NAK reply packets to clients.

The **set dhcp relay broadcast-flag-replies** command and the **set dhcp relay layer2-unicast-replies** command are mutually exclusive. If you attempt to issue the **set dhcp relay broadcast-flag-replies** command when the **set dhcp relay layer2-unicast-replies** command is already in effect, the operation fails and the router displays the following message:

```
% layer2-unicast-replies and broadcast-flag-replies are mutually exclusive
```

If this message appears, you must first issue the **no set dhcp relay layer2-unicast-replies** command to disable layer 2 unicast replies, and then issue the **set dhcp relay broadcast-flag-replies** command again to enable broadcast flag replies.

Table 96 summarizes how the configuration of the **set dhcp relay broadcast-flag-replies** command and the **set dhcp relay layer2-unicast-replies** command interacts with the setting of the broadcast flag in DHCP request packets to control how the router transmits DHCP reply packets to clients during the discovery process. Because these commands are mutually exclusive, broadcast flag replies and layer 2 unicast replies cannot both be enabled on the router at the same time.

Table 96: Router Configuration and Transmission of DHCP Reply Packets

Broadcast Flag Replies	Layer 2 Unicast Replies	Router Behavior if Broadcast Flag Set	Router Behavior if Broadcast Flag Not Set
Enabled (on)	Disabled (off)	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients.	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 unicast transmission to send DHCP reply packets to clients.
Disabled (off)	Enabled (on)	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 broadcast transmission to send DHCP reply packets to clients.	DHCP relay and DHCP relay proxy use layer 2 unicast and layer 3 broadcast transmission to send DHCP reply packets to clients.

Table 96: Router Configuration and Transmission of DHCP Reply Packets (continued)

Broadcast Flag Replies	Layer 2 Unicast Replies	Router Behavior if Broadcast Flag Set	Router Behavior if Broadcast Flag Not Set
Disabled (off)	Disabled (off)	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. For information about exceptions to this behavior for DHCP relay proxy, see *Behavior for Bound Clients and Address Renewals* on page 447.	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. For information about exceptions to this behavior for DHCP relay proxy, see *Behavior for Bound Clients and Address Renewals* on page 447.

Preventing DHCP Relay from Installing Host Routes by Default

The Address Resolution Protocol (ARP) performs spoof checking on all incoming ARP requests by default. For each incoming packet, ARP does a route lookup on the source IP address to determine the interface on which that IP address was routed. ARP then verifies that the interface on which the packet was received matches the routed interface. If the interface on which the packet was received does not match the routed interface, the router drops the packet.

When you configure applications such as DHCP relay that automatically install routes, you must ensure that the routes are correctly installed for your configuration. DHCP relay installs host routes by default, which is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of host routes might cause a conflict when you configure DHCP relay with static subscriber interfaces. To avoid these configuration conflicts, use the **set dhcp relay inhibit-access-route-creation** command to prevent DHCP relay from installing host routes by default.

Configuration Example—Preventing Installation of Host Routes

This example describes a sample procedure for configuring multiple subscribers over a particular static subscriber interface (ip53001 in this example)—you might use commands similar to the following to create demultiplexer table entries and a subnet route that points to the static subscriber interface.

In the example, the host routes are associated with the primary IP interface on Gigabit Ethernet 1/0. Because the host routes are statically configured with the subscriber interface, there is no need for the router to install DHCP host routes. Therefore, in step 7, the **set dhcp relay inhibit-access-route-creation** command is used to prevent DHCP relay from installing host routes.

1. Create a shared IP interface.

   host1(config)#**interface ip ip53001**

2. Associate the shared IP interface with a static layer 2 interface.

   host1(config-if)#**ip share-interface gigabitEthernet 1/0**

3. Make the shared interface an unnumbered interface.

   host1(config-if)#**ip unnumbered loopback 53**

4. Specify the source addresses that the subscriber interface uses to demultiplex traffic.

   host1(config-if)#**ip source-prefix 10.10.10.0 255.255.255.252**

5. Exit Interface Configuration mode.

   host1(config-if)#**exit**

6. Create a static route that sends traffic for destination address 10.10.10.0 to subscriber interface ip53001.

   host1(config)#**ip route 10.10.10.0 255.255.255.252 ip ip53001**

7. Prevent DHCP relay from installing host routes—this avoids a conflict that can cause undesirable ARP behavior.

   host1(config)#**set dhcp relay inhibit-access-route-creation**

In the example, if you do not prevent DHCP relay from installing host routes, the ARP spoof-checking mechanism associates the ARP traffic with the primary IP interface (Gigabit Ethernet 1/0), although packets actually arrive on the subscriber interface (ip53001), causing the router to detect a spoof and drop the packet.

Including Relay Agent Option Values in the PPPoE Remote Circuit ID

You can enable the router to capture and format a vendor-specific tag containing a PPPoE remote circuit ID value transmitted from a digital subscriber line access multiplexer (DSLAM) device. The router can then send this value to a Remote Authentication Dial-In User Service (RADIUS) server or to a Layer 2 Tunneling Protocol (L2TP) network server (LNS) to uniquely identify subscriber locations.

By default, the router formats the captured PPPoE remote circuit ID to include only the agent-circuit-id suboption (suboption 1) of the DHCP relay agent information option (option 82). You can use the **radius remote-circuit-id-format** command to configure the following nondefault formats for the PPPoE remote circuit ID value:

- Include either or both of the agent-circuit-id (suboption 1) and agent-remote-id (suboption 2) suboptions of the DHCP relay agent information option, with or without the NAS-Identifier [32] RADIUS attribute.

- Append the agent-circuit-id suboption value to an interface specifier that is consistent with the recommended format in the DSL Forum Technical Report (TR)-101—Migration to Ethernet-Based DSL Aggregation (April 2006).

For information about configuring the PPPoE remote circuit ID, see *Using the PPPoE Remote Circuit ID to Identify Subscribers* and *Configuring PPPoE Remote Circuit ID Capture* in *JUNOSe Link Layer Configuration Guide, Chapter 10, Configuring Point-to-Point Protocol over Ethernet*.

Using the Giaddr to Identify the Primary Interface for Dynamic Subscriber Interfaces

When creating dynamic subscriber interfaces, the router builds the dynamic interfaces on the associated primary interface. By default, the router identifies the primary interface based on the interface on which DHCP client discover packets are received. The router then builds all dynamic interfaces on that primary interface.

In some cases you might want more control over the determination of the primary interface and you might not want to use the primary interface that is determined by the default behavior. The JUNOSe software enables you to configure DHCP relay to use information in the giaddr in DHCP ACK messages to specify which interface is to be used as the primary interface. This capability allows you to build dynamic interfaces on the primary interface of your choice.

- To use information in the giaddr to identify the primary interface for dynamic subscriber interfaces:

  host1(config)#**set dhcp relay giaddr-selects-interface**

Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients

By default, DHCP relay and relay proxy broadcast DHCP Offer reply packets and DHCP ACK and NAK reply packets to DHCP clients during the discovery process. In some environments, this default broadcast method might be a security concern because all clients can receive packets intended for all other clients.

You use the **set dhcp relay layer2-unicast-replies** command in Global Configuration mode to configure the optional layer 2 unicast and layer 3 broadcast transmission method for DHCP relay and DHCP relay proxy. This method uses the client's layer 2 (MAC) address and layer 3 (IP) broadcast address to provide secure transmission of DHCP Offer reply packets and ACK and NAK reply packets. The optional layer 2 unicast method enables reply packets to be broadcast through the layer 3 network but received only by the specified client.

There are exceptions to this behavior for DHCP relay proxy when the DHCP client is already bound to an IP address or is renewing the lease on its IP address. For information, see *Behavior for Bound Clients and Address Renewals* on page 447.

To display whether the layer 2 unicast method is currently on or off on the router, use the **show dhcp relay** command. For information, see *Chapter 22, Monitoring and Troubleshooting DHCP*.

The dhcpRelayGeneral logging event category uses the debug severity level to log DHCP reply packets that are transmitted to clients using a layer 2 unicast address and a layer 3 broadcast address.

The **set dhcp relay broadcast-flag-replies** command configures the router to use the setting of the broadcast flag in DHCP request packets to control the transmission of DHCP reply packets. The **set dhcp relay layer2-unicast-replies** command and the **set dhcp relay broadcast-flag-replies** command are mutually exclusive. For more information, see *Interaction with Layer 2 Unicast Transmission Method* on page 425.

NOTE: When you enable the layer 2 unicast transmission feature, the DHCP relay and DHCP relay proxy instance must be the next hop from the DHCP clients. Otherwise, the DHCP reply packets might be discarded.

The layer 2 unicast transmission method is not supported on non-ASIC line modules.

- To configure the optional broadcast transmission method:

  host1(config)#**set dhcp relay layer2-unicast-replies**

Using Option 60 Strings to Forward Client Traffic to Specific DHCP Servers

The DHCP functionality supports the DHCP vendor class identifier option (option 60). This support allows DHCP relay to compare option 60 strings in received DHCP client packets against strings that you configure on the router. You can use the DHCP relay option 60 feature when providing converged services in your network environment—option 60 support enables DHCP relay to direct client traffic to the specific DHCP server (the vendor-option server) that provides the service that the client requires. Or, as another option, you can configure option 60 strings to direct traffic to the DHCP local server in the current virtual router.

For example, you might have an environment in which some DHCP clients require only Internet access, while other clients require IPTV service. The clients that need Internet access get their addresses assigned by the DHCP local server on the E-series router (in equal-access mode). Clients requiring IPTV must be relayed to a specific DHCP server that provides the service. To support both types of clients, you configure two option 60 strings on the DHCP relay. Now, when any DHCP client packets are received with option 60 strings configured, the strings are matched against all strings configured on the DHCP relay. If the client string matches the first string you configured, that client is directed to the DHCP local server and gains Internet access. Client traffic with an option 60 string that matches your second string is relayed to the DHCP server that provides the IPTV service. In addition, you can configure a default action, which DHCP relay performs when a client option 60 string does not match any strings you have configured—for example, you might specify that all clients with non-matching strings be dropped.

You use the **set dhcp vendor-option** command to configure vendor-option (option 60) strings to control DHCP client traffic Create DHCP vendor-option servers by configuring DHCP relay to match DHCP option 60 strings and to specify what action to use for the traffic.Use the following guidelines when configuring the **set dhcp vendor-option** command:

- Use the **equals** or **starts-with** keywords to specify a unique string to match, and to configure the action to take for traffic with a matching string:
  - **equals**—The DHCP client string is an exact match of the specified string
  - **starts-width**—The DHCP client string is a partial match, from left-to-right, of the specified string. For example, a client string of **day** matches a **starts-width** configured string of **daytime**.
- Use the following keywords to configure actions for matching strings:
  - **local-server**—Forward packets to the DHCP local server
  - **relay**—Forward packets to the DHCP server with the specified IP address
- Use the **default** keyword to set the default action to take when the option 60 string does not match a configured vendor-option string. Use the following keywords to configure actions for nonmatching strings:
  - **drop**—Discard traffic
  - **local-server**—Forward packets to the DHCP local server
  - **proxy-client**—Forward traffic to the DHCP proxy client server
  - **relay**—Forward packets to the DHCP server with the specified IP address
  - **relay-server-list**—Forward traffic to all non-vendor option DHCP servers. The relay-server-list consists of all non-vendor option servers. Non-vendor option servers are those servers that are configured with the **set dhcp relay** command but not with the **set dhcp vendor-option** command.
  - When you configure the first DHCP vendor-option and no default action is specified for a configured DHCP application, the router chooses the default action according to the preference of the DCHP applications. The order of preference from first to last is DHCP local server, DHCP relay, and DHCP proxy client.

You can map multiple strings to the same DHCP server, and you can map a single string to multiple servers. However, mapping one string to more than five DHCP vendor-option servers might impact performance.

You can configure a maximum of 100 option 60 strings per DHCP relay. Strings can contain a maximum of 254 characters.

Client packets that have option 60 configured but have no string specified (a string of 0 length) are treated as nonmatching strings and handled accordingly.

- To configure an exact match:

  host1(config)#**set dhcp vendor-option equals myword relay 192.168.7.7**

- To configure a partial match:

  host1(config)#**set dhcp vendor-option starts-with abcd local-server**

- To configure the default action:

  host1(config)#**set dhcp vendor-option default drop**

- To remove a configuration:

  host1(config)#**no set dhcp vendor-option starts-with abcd local-server**

Configuration Example—Using DHCP Relay Option 60 to Specify Traffic Forwarding

You use the DHCP relay option 60 feature to specify the action performed on DHCP client traffic. The DHCP relay uses the option 60 string in the client traffic to determine what action to take with the incoming traffic.

The following example describes a sample procedure that creates three actions for incoming DHCP client traffic, depending on the traffic's option 60 string.

1. Enable the DHCP relay. Do not specify an IP address when you configure DHCP relay to support vendor-option strings.

   host1(config)#**set dhcp relay**

2. Configure the action DHCP relay takes when the incoming traffic has an exact option 60 string of myword. DHCP relay forwards this traffic to the DHCP server with an IP address of 192.168.7.7.

   host1(config)#**set dhcp vendor-option equals myword relay 192.168.7.7**

3. Configure the action DHCP relay takes when the incoming traffic has a partial match, from left-to-right, with an option 60 string you have configured. For this command, matching strings include a, ab, abc, and abcd. DHCP relay forwards matching traffic to the DHCP server with IP address 192.168.15.2.

   host1(config)#**set dhcp vendor-option starts-with abcd relay 192.168.15.2**

4. Configure the default option 60 action. DHCP relay takes this action when the incoming traffic has an option 60 string that does not match any of the option 60 strings that you have configured. In this example, the traffic is sent to the DHCP local server.

   host1(config)#**set dhcp vendor-option default local-server**

5. (Optional) View your DHCP relay vendor-option configuration.

```
host1(config)#run show dhcp vendor-option
Codes:
 *       - the configured vendor-string is an exact-match
 default - all DHCP client packets not matching a configured vendor-string
 implied - the DHCP application is configured but has not been enabled
           with the vendor-option command
 drop    - the DHCP application responsible for the action has not been
           configured yet therefore all packets for this application
           will be dropped
 Total 3 entries.
         Vendor-option                          Action
------------------------------- ----------------------------------------
abcd                            relay to 192.168.15.2 (rx: 0)
default(*)                      local-server (rx: 0, no-match: 0)
myword(*)                       relay to 192.168.7.7 (rx: 0)
```

Relaying DHCP Packets that Originate from a Cable Modem

You can use the DHCP vendor class identifier option (option 60) to configure DHCP relay to relay DHCP packets that originate from a cable modem to an external DHCP server that provides the cable modem with the configuration it requests.

Configure the vendor class identifier option to match the string used by cable modems—DHCP relay then forwards the packets to each DHCP server that you configured with the **set dhcp vendor-option** command (these servers are also considered to be cable-modem DHCP servers).

- To relay DHCP packets from a cable modem:

  host1(config)#**set dhcp relay**
  host1(config)#**service dhcp-local equal-access**
  host1(config)#**set dhcp vendor-option equals docsis relay 192.168.1.1**
  host1(config)#**set dhcp vendor-option equals cablemodem relay 192.168.1.1**

  Use the **show dhcp summary** and **show dhcp vendor-option** commands to display information about the cable modem DHCP relay configuration. See *Chapter 22, Monitoring and Troubleshooting DHCP*.

Configuring Relay Agent Option 82 Information

You can specify the type the relay agent option 82 information that the router adds to DHCP packets before it relays the packets to the DHCP server. You can use one of the following keywords to add either the hostname or virtual router name to the front of the Circuit-Id field or to strip the subinterface ID from the Interface-Id field:

- **hostname**—Adds the router's hostname to the front of the Circuit-Id field; a colon separates the hostname from the circuit information

- **vrname**—Adds the router's virtual router name to the front of the Circuit-Id field; a colon separates the virtual router name from the circuit information

- Use the **exclude-subinterface-id** to strip the subinterface ID from the Interface-Id field. When the interface ID is constructed, it contains the slot/port numbers, the subinterface ID, and the VPI/VCI for ATM interfaces or the VLAN ID for Ethernet interfaces. Use this keyword to remove the subinterface ID from the Interface-Id field.

The **hostname** and **vrname** keywords are a toggle; that is, specifying either hostname or virtual router name turns off the other selection.

- To configure the relay agent option 82 information:

  host1(config)#**set dhcp relay options hostname**

Preventing Option 82 Information from Being Stripped from Trusted Client Packets

You can configure DHCP relay or DHCP relay proxy to preserve option 82 information for trusted clients. This ensures that DHCP relay and DHCP relay proxy prevent option 82 information from being stripped off packets destined for a trusted client. A trusted client has a giaddr value of 0. If DHCP relay is configured not to remove option 82 and the giaddr field is 0, option 82 information remains in the packets.

- To prevent the option 82 information from being removed from packets destined for a trusted client:

  host1(config)#**set dhcp relay preserve-trusted-client-option**

Configuring Relay Agent Information Option (Option 82) Suboption Values

The DHCP relay agent information option (option 82) enables you to include additional useful information in the client-originated DHCP packets that the DHCP relay forwards to a DHCP server.

When the DHCP relay agent information option is enabled, the DHCP relay adds the option 82 information to packets it receives from clients, then forwards the packets to the DHCP server. The DHCP server uses the option 82 information to decide which IP address to assign to the client—the DHCP server might also use information in the option 82 field for additional purposes, such as determining which services to grant to the client. The DHCP server sends its reply back to the DHCP relay, which removes the option 82 information field from the message, and then forwards the packet to the client.

The option 82 information is made up of a sequence of suboptions. JUNOSe software supports the following DHCP relay agent information suboptions.

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which a client DHCP packet is received.

- Agent Remote ID (suboption 2)—An ASCII string assigned by the relay agent that securely identifies the client.

- Vendor-Specific (suboption 9)—The JUNOSe software data field, which contains the Internet Assigned Numbers Authority (IANA) enterprise number (4874) used by JUNOSe software and either or both the layer 2 circuit ID and the user packet class.

  - Layer 2 Circuit ID (type 1)—The hexadecimal representation of the layer 2 identifier in the Agent Circuit ID (suboption 1) value (for example, the ATM VPI/VCI or Ethernet SVLAN/VLAN ID.) You can configure this suboption type without the Agent Circuit ID.

  - User Packet Class (type 2)—The hexadecimal representation of the user packet class field, whose value is assigned by the layer 2 policy application. The layer 2 policy application can be used to map the DHCP packet or message IEEE 802.1p value to the user packet class field. See the *JUNOSe Policy Management Configuration Guide* for information about layer 2 policies.

The Agent Circuit ID suboption (suboption 1) and the Agent Remote ID suboption (suboption 2) are typically determined by the client network access device and depend on the network configuration. The Vendor-Specific suboption (suboption 9) is more flexible and can be used by administrators to associate specific data with the DHCP messages relayed between the DHCP relay and the DHCP server. For example the Vendor-Specific suboption can include the client's IEEE 802.1p value, which identifies the client's user priority.

NOTE: The DHCP relay agent replaces any existing Vendor-Specific value in the client packet with the relay agent's value.

The JUNOSe software provides two commands that you can use to configure DHCP relay agent information suboptions.

- The **set dhcp relay agent sub-option** command—Enables you to configure option 82 to include any combination of the supported suboptions, including the Vendor-Specific suboption.

- The **set dhcp relay agent** command—Enables you to configure option 82 to include either or both the Agent Circuit ID suboption (suboption 1) and Agent Remote ID suboption (suboption 2). The command does not support the Vendor-Specific suboption (suboption 9).

NOTE: The **set dhcp relay agent** command is a legacy command, which JUNOSe software continues to support to provide backward-compatibility for existing scripts. We recommend that all new configurations use the **dhcp relay agent sub-option** command.

The **set dhcp relay agent sub-option** command enables you to manage specific option 82 suboptions without impacting the configuration of other suboptions. The legacy **set dhcp relay agent** command, however, changes the configuration of suboptions in some cases.

Table 97 indicates the effect each command has on enabling or disabling relay agent information suboptions.

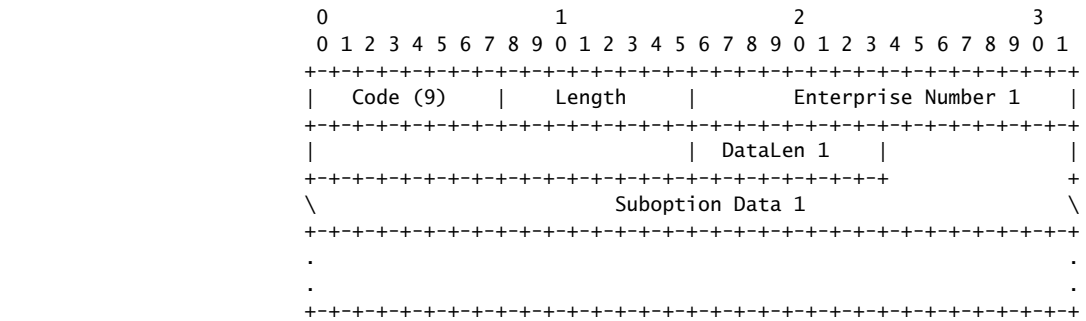
Table 97: Effect of Commands on Option 82 Suboption Settings

Command	Suboption and Status		
	Agent Circuit ID	**Agent Remote ID**	**Vendor-Specific**
set dhcp relay agent sub-option circuit-id	Enable	No change	No change
set dhcp relay agent sub-option remote-id	No change	Enable	No change
set dhcp relay agent sub-option vendor-specific *suboption-type*	No change	No change	Enable specified suboption type
no set dhcp relay agent sub-option circuit-id	Disable	No change	No change
no set dhcp relay agent sub-option remote-id	No change	Disable	No change
no set dhcp relay agent sub-option vendor-specific *suboption-type*	No change	No change	Disable specified suboption type
set dhcp relay agent	Enable	Enable	Not supported
set dhcp relay agent circuit-id-only	Enable	Disable	Not supported
set dhcp relay agent remote-id-only	Disable	Enable	Not supported
no set dhcp relay agent	Disable	Disable	Disable

Format of the JUNOSe Data Field in the Vendor-Specific Suboption for Option 82

RFC 4243 describes support for data fields from multiple vendors in the Vendor-Specific suboption for option 82. The JUNOSe software DHCP relay agent, however, supports only the JUNOSe software data field.

RFC 4243 supports the following format of the Vendor-Specific suboption:



The JUNOSe software data field appears after the JUNOSe software enterprise number and data length fields in the Vendor-Specific suboption. The format of the JUNOSe data field is a sequence of type/length/value (TLV) tuples. The type field and length field (the length of the following value field) are each 1 byte in size. The JUNOSe data length field specifies the total length of all TLV tuples. The JUNOSe software enterprise number is 4874 (0x130a.)

The format of the Layer 2 Circuit ID type field (type 1) is hexadecimal. The data field length of a normal non-stacked VLAN is 2 bytes, with the VLAN ID occupying the 12 low-order bits of the value; the 4 high-order bits are 0. The data field length of a stacked VLAN is 4 bytes, with the SVLAN ID occupying the 12 low-order bits of the 2 high-order bytes, and the VLAN ID occupying the 12 low-order bits of the 2 low-order bytes; the unused bits are 0. The data field length of a VPI/VCI is 4 bytes, with the VPI occupying the 8 to 10 low-order bits of the 2 high-order bytes, and the VCI occupying the 16 bits of the 2 low-order bytes; the unused bits are 0.

The format of the UPC data field (type 2) is hexadecimal; its data field length is 1 byte, with the UPC occupying the 4 low-order bits of the value; the 4 high-order bits are 0.

Example 1—The Vendor-Specific suboption for a VLAN ID of 2468 (0x09a4) and a UPC of 5 is formatted as follows:

```
09 0c 00 00 13 0a 07 01 02 09 a4 02 01 05
|  |  |           |  |  |  |     |  |  |
|  |  |           |  |  |  |     |  |  UPC val: 5
|  |  |           |  |  |  |     |  UPC len: 1 byte
|  |  |           |  |  |  |     UPC type: 2
|  |  |           |  |  |  L2 Circuit ID val: 09 a4
|  |  |           |  |  L2 Circuit ID len: 2 bytes
|  |  |           |  L2 Circuit ID type: 1
|  |  |           JUNOSe data len: 7 bytes
|  |  JUNOSe IANA: 13 0a
|  subopt 9 len: 12 bytes
subopt code: 9
```

Example 2—The Vendor-Specific suboption for a VLAN ID of 135-2468 (0x87-0x09a4, format <SVLAN ID>-<VLAN ID>) and a UPC of 5 is formatted as follows:

```
09 0e 00 00 13 0a 09 01 04 00 87 09 a4 02 01 05
|  |  |           |  |  |  |           |  |  |
|  |  |           |  |  |  |           |  |  UPC val: 5
|  |  |           |  |  |  |           |  UPC len: 1 byte
|  |  |           |  |  |  |           UPC type: 2
|  |  |           |  |  |  L2 Circuit ID val: 00 87 09 a4
|  |  |           |  |  L2 Circuit ID len: 4 bytes
|  |  |           |  L2 Circuit ID type: 1
|  |  |           JUNOSe data len: 9 bytes
|  |  JUNOSe IANA: 13 0a
|  subopt 9 len: 14 bytes
subopt code: 9
```

Example 3—The Vendor-Specific suboption for a VPI/VCI of 123.45678 (0x7b.0xb26e, format <VPI>.<VCI>) and a UPC of 5 is formatted as follows:

```
09 0e 00 00 13 0a 09 01 04 00 7b b2 6e 02 01 05
|  |  |           |  |  |  |           |  |  |
|  |  |           |  |  |  |           |  |  UPC val: 5
|  |  |           |  |  |  |           |  UPC len: 1 byte
|  |  |           |  |  |  |           UPC type: 2
|  |  |           |  |  |  L2 Circuit ID val: 00 7b b2 6e
|  |  |           |  |  L2 Circuit ID len: 4 bytes
|  |  |           |  L2 Circuit ID type: 1
|  |  |           JUNOSe data len: 9 bytes
|  |  JUNOSe IANA: 13 0a
|  subopt 9 len: 14 bytes
subopt code: 9
```

Using the set dhcp relay agent sub-option Command to Enable Option 82 Suboption Support

NOTE: We recommend that you use the **set dhcp relay agent sub-option** command for new option 82 suboption configurations. However, JUNOSe software continues to support the **set dhcp relay agent** command, with option 82 suboptions, to provide backward-compatibility for existing scripts.

You use the **set dhcp relay agent sub-option** command to enable support for a specific DHCP relay agent option 82 suboption—Agent Circuit ID (suboption 1), Agent Remote ID (suboption 2), and Vendor-Specific (suboption 9). When you issue this command, the router adds DHCP relay agent information suboption 1 to every packet it relays from a DHCP client to a DHCP server. The Agent Circuit ID suboption identifies the interface on which DHCP packets are received. When the packets are received on a LAG interface, the router clearly identifies the interface.

The suboptions include information from the DHCP relay agent that the DHCP server can use to implement parameter assignment policies. The DHCP server echoes the suboptions when it replies to the DHCP client, but the DHCP relay strips the suboptions before relaying the packets to the client.

The Agent Circuit ID suboption identifies the interface on which the DHCP packets are received. This suboption contains the following information, based on interface type:

- ATM interface

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:<vpi>.<vci>

  Examples:

  atm 4/1.2:0.101
  relayVr:atm 4/1:0.101
  bostonHost:atm 4/1.2:0.101

- Ethernet interface

  [<hostname>|<vrname>:]<interface type> <slot>/<port>

  Examples:

  fastEthernet 1/2
  relayVr:fastEthernet 1/2
  bostonHost:fastEthernet 1/2

- Ethernet interface with VLAN

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:<vlan id>

  Examples:

  fastEthernet 1/2.3:4
  relayVr:fastEthernet 1/2:4
  bostonHost:fastEthernet 1/2.3:4

- Ethernet interface with Stacked VLAN

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:
  <svlan id>-<vlan id>

  Examples:

  fastEthernet 1/2.3:4-5
  relayVr:fastEthernet 1/2:4-5
  bostonHost:fastEthernet 1/2.3:4-5

- LAG interface

  [<hostname>|<vrname>:]<interface type> <bundle name>

  Examples:

  lag bundleA
  relayVr:lag bundleA
  bostonHost:lag bundleA

- LAG interface with VLAN

  [<hostname>|<vrname>:]<interface type> <bundle name>[.<sub-if>]:<vlan id>

  Examples:

  lag bundleA.1:2
  relayVr:lag bundleA:2
  bostonHost:lag bundleA.1:2

- LAG interface with Stacked VLAN

  [<hostname>|<vrname>:]<interface type> <bundle name>[.<sub-if>]:
  <svlan id>-<vlan id>

  Examples:

  lag bundleA.1:2-3
  relayVr:lag bundleA:2-3
  bostonHost:lag bundleA.1:2-3

The Agent Remote ID suboption contains a value only when (1) the interface is a dynamic ATM interface and (2) the **subscriber** command is used to configure a username and domain name for the interface. If both conditions are met, the suboption contains a string with the username and domain name in the format: *username@domainname*.

The Vendor-Specific suboption contains a value that includes a JUNOSe data field. You can configure the data field to support one or both of the following values:

- **layer2-circuit-id** (type 1)—The hexadecimal representation of the layer 2 identifier in the Agent Circuit ID (suboption 1) value (for example, the ATM VPI/VCI or Ethernet SVLAN/VLAN ID). You can configure this suboption type without the Agent Circuit ID.

- **user-packet-class** (type 2)—The hexadecimal representation of the user packet class field, whose value is assigned by the layer 2 policy application. The layer 2 policy application can be used to map the DHCP packet or message IEEE 802.1p value to the user packet class field. See the *JUNOSe Policy Management Configuration Guide* for information about layer 2 policies.

Configuration Example—Using DHCP Relay Option 82 to Pass IEEE 802.1p Values to DHCP Servers

Using the DHCP relay agent option 82 feature, you can configure an environment in which a customized DHCP server assigns an IP address that provides the desired service to the DHCP client.

The DHCP server uses information based on the IEEE 802.1p values, which are extracted from the DHCP packets using JUNOSe software layer 2 policies, to determine the appropriate IP address to assign to the client.

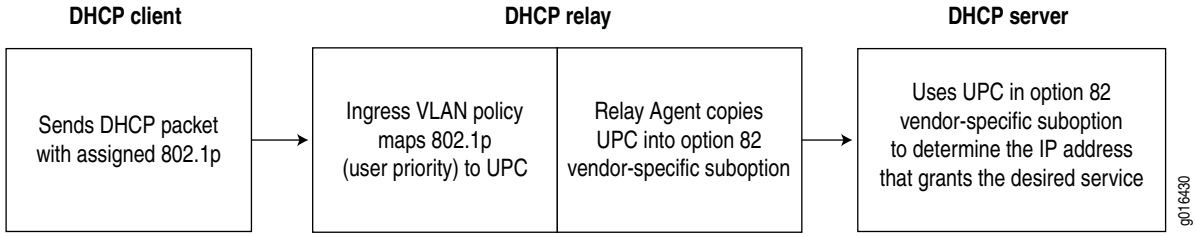
This type of environment, which is illustrated in Figure 13, includes the following components:

- Layer 2 policy on the ingress interface (that is, the interface that receives the client's DHCP packet) that maps the 802.1p value from the packet to a user packet class (UPC.)

NOTE: To ensure optimal performance when mapping 802.1p values to UPCs, order the classifier groups in the VLAN policy list with the most often used UPC values listed first.

- DHCP relay agent option 82 configuration that enables Vendor-Specific suboption type 2 (User Packet Class) support and maps the Layer 2 policy user packet class to the option 82 user packet class suboption.
- Customized DHCP server configuration that assigns IP addresses based on the option 82 user packet class suboption. The IP address is associated with the appropriate quality, type, or class of service for the user packet class specified in the option 82 suboption.

Figure 13: Passing 802.1p Values to the DHCP Server



The following example describes a sample procedure that creates an environment that passes 802.1p values to the DHCP server, which then assigns an IP address that enables the desired service to the DHCP client.

1. Configure a layer 2 policy that maps 802.1p values to user packet class values for a VLAN interface.

```
host1(config)# vlan classifier-list dot1p0 user-priority 0
host1(config)# vlan classifier-list dot1p1 user-priority 1
host1(config)# vlan classifier-list dot1p2 user-priority 2
host1(config)# vlan classifier-list dot1p3 user-priority 3
host1(config)# vlan classifier-list dot1p4 user-priority 4
host1(config)# vlan classifier-list dot1p5 user-priority 5
host1(config)# vlan classifier-list dot1p6 user-priority 6
host1(config)# vlan classifier-list dot1p7 user-priority 7
host1(config)# vlan policy-list dot1pToUpc
host1(config-policy-list)# classifier-group dot1p0
host1(config-policy-list-classifier-group)# user-packet-class 0
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p1
host1(config-policy-list-classifier-group)# user-packet-class 1
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p2
host1(config-policy-list-classifier-group)# user-packet-class 2
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p3
host1(config-policy-list-classifier-group)# user-packet-class 3
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p4
host1(config-policy-list-classifier-group)# user-packet-class 4
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p5
host1(config-policy-list-classifier-group)# user-packet-class 5
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p6
host1(config-policy-list-classifier-group)# user-packet-class 6
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)# classifier-group dot1p7
```

```
host1(config-policy-list-classifier-group)# user-packet-class 7
host1(config-policy-list-classifier-group)#exit
host1(config-policy-list)#exit
host1(config)# profile atm1483BaseProfile
host1(config-profile)# vlan policy input dot1pToUpc statistics enabled
host1(config-profile)#exit
host1(config)#
```

2. (Optional) Verify the policy list configuration.

```
host1(config)# run show policy-list dot1pToUpc

                                Policy Table
                                ------ -----
VLAN Policy dot1pToUpc
   Administrative state: enable
   Reference count:      1
   Classifier control list: dot1p0, precedence 100
      user-packet-class 0
   Classifier control list: dot1p1, precedence 100
      user-packet-class 1
   Classifier control list: dot1p2, precedence 100
      user-packet-class 2
   Classifier control list: dot1p3, precedence 100
      user-packet-class 3
   Classifier control list: dot1p4, precedence 100
      user-packet-class 4
   Classifier control list: dot1p5, precedence 100
      user-packet-class 5
   Classifier control list: dot1p6, precedence 100
      user-packet-class 6
   Classifier control list: dot1p7, precedence 100
      user-packet-class 7

   Referenced by interface(s):
      None

   Referenced by profile(s):
      atm1483BaseProfile  input policy, statistics enabled

   Referenced by merged policies:
      None
```

3. Configure the DHCP relay to use the option 82 suboptions. This configuration includes the command that specifies the mapping of the user packet class values from the layer 2 policy to the user-packet-class type in the option 82 Vendor-Specific suboption.

```
host1(config)# set dhcp relay 192.168.32.1 proxy
host1(config)# set dhcp relay 192.168.32.2
host1(config)# set dhcp relay agent sub-option circuit-id
host1(config)# set dhcp relay agent sub-option remote-id
host1(config)# set dhcp relay agent sub-option vendor-specific
user-packet-class
host1(config)# set dhcp relay agent sub-option vendor-specific
layer2-circuit-id
host1(config)# set dhcp relay options hostname
host1(config)# set dhcp relay options exclude-subinterface-id
host1(config)# set dhcp relay inhibit-access-route-creation
host1(config)# set dhcp relay trust-all
host1(config)# set dhcp relay override agent-option
```

4. (Optional) Verify the DHCP Relay configuration.

```
host1(config)# run show dhcp relay

DHCP Relay Configuration
------------------------
Mode: Proxy
  Restore Client Timeout: 72
Inhibit Access Route Creation: off
Assign Giaddr to Source IP: off
Layer 2 Unicast Replies: off
Giaddr Selects Interface: off
Relay Agent Information Option (82):
  Override Giaddr: off
  Override Option: on
  Trust All Clients: on
  Preserve Option From Trusted Clients: off
  Circuit-ID Sub-option (1): on
    select - hostname
    select - exclude-subinterface-id
  Remote-ID Sub-option (2): on
  Vendor-Specific Sub-option (9): on
    select - layer2-circuit-id
    select - user-packet-class

DHCP Server Addresses
---------------------
192.168.32.1
192.168.32.2
```

Using the set dhcp relay agent Command to Enable Option 82 Suboption Support

NOTE: The **set dhcp relay agent** command, when used to configure option 82 suboptions is a legacy command, which JUNOSe software continues to support to provide backward-compatibility for existing scripts. We recommend that you use the **dhcp relay agent sub-option** command for new option 82 suboption configurations.

You can use the **set dhcp relay agent** command to enable support for DHCP relay agent option, which includes the option 82 suboptions—Agent Circuit ID (suboption 1) and Agent Remote ID (suboption 2). This command does not support the Vendor-Specific option (suboption 9).

The suboptions include information from the DHCP relay agent that the DHCP server can use to implement parameter assignment policies. The DHCP server echoes the suboptions when it replies to the client—the DHCP relay agent can optionally strip the option 82 information before relaying the packets to the client. (Use the CLI command **set dhcp relay preserve-trusted-client-option** to configure this behavior for trusted clients.)

When you issue the **set dhcp relay agent** command, the router adds the configured DHCP relay agent information suboptions to every packet it relays from a DHCP client to a DHCP server.

The **circuit-id-only** keyword specifies the Agent Circuit ID suboption, which contains the following information, based on interface type. This keyword disables support for the Agent Remote ID suboption.

- ATM interface

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:<vpi>.<vci>

  Examples:

  atm 4/1.2:0.101
  relayVr:atm 4/1:0.101
  bostonHost:atm 4/1.2:0.101

- Ethernet interface

  [<hostname>|<vrname>:]<interface type> <slot>/<port>

  Examples:

  fastEthernet 1/2
  relayVr:fastEthernet 1/2
  bostonHost:fastEthernet 1/2

- Ethernet interface with VLAN

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:<vlan id>

  Examples:

  fastEthernet 1/2.3:4
  relayVr:fastEthernet 1/2:4
  bostonHost:fastEthernet 1/2.3:4

- Ethernet interface with Stacked VLAN

  [<hostname>|<vrname>:]<interface type> <slot>/<port>[.<sub-if>]:
  <svlan id>-<vlan id>

  Examples:

  fastEthernet 1/2.3:4-5
  relayVr:fastEthernet 1/2:4-5
  bostonHost:fastEthernet 1/2.3:4-5

- LAG interface

  [<hostname>|<vrname>:]<interface type> <bundle name>

  Examples:

  lag bundleA
  relayVr:lag bundleA
  bostonHost:lag bundleA

- LAG interface with VLAN

  [<hostname>|<vrname>:]<interface type> <bundle name>[.<sub-if>]:<vlan id>

  Examples:

  lag bundleA.1:2
  relayVr:lag bundleA:2
  bostonHost:lag bundleA.1:2

- LAG interface with Stacked VLAN

  [<hostname>|<vrname>:]<interface type> <bundle name>[.<sub-if>]:
  <svlan id>-<vlan id>

  Examples:

  lag bundleA.1:2-3
  relayVr:lag bundleA:2-3
  bostonHost:lag bundleA.1:2-3

The **remote-id-only** keyword specifies the Agent Remote ID suboption, which contains a value only when (1) the interface is a dynamic ATM interface and (2) the **subscriber** command is used to configure a username and domain name for the interface. If both conditions are met, the suboption contains a string with the username and domain name in the format: *username@domainname*. The **remote-id-onl**y keyword disables support for the Agent Circuit ID suboption.

If you do not explicitly specify the **circuit-id-only** or **remote-id-only** keyword, both suboptions are used.

Related Topics

- **radius remote-circuit-id-format** command
- **set dhcp relay** command
- **set dhcp relay agent** command
- **set dhcp relay agent sub-option** command
- **set dhcp relay assign-giaddr-source-ip** command
- **set dhcp relay broadcast-flag-replies** command
- **set dhcp relay giaddr-selects-interface** command
- **set dhcp relay layer2-unicast-replies** command
- **set dhcp relay options** command

- **set dhcp relay override** command
- **set dhcp relay preserve-trusted-client-option** command
- **set dhcp relay trust-all** command
- **set dhcp vendor-option** command

Configuring DHCP Relay Proxy

The DHCP relay proxy is an enhancement to the E-series router's DHCP relay component. The DHCP relay proxy manages host routes for DHCP clients, and determines which offer to use when there are multiple DHCP servers configured.

NOTE: The E-series router configured as a DHCP relay proxy must be the first hop from the DHCP client. If it is not the first hop, the router defaults to the DHCP relay configuration.

Enabling DHCP Relay Proxy

Enable DHCP relay proxy and specify an IP address for the DHCP server. After you are in DHCP relay proxy mode, all **set dhcp relay** commands are supported.

```
host1(config)#set dhcp relay 192.168.29.10 proxy
```

When you issue this command, the router adds the IP address to the list of DHCP servers (up to five) and forwards all request packets to all configured servers.

After you are in DHCP relay proxy mode, all **set dhcp relay** commands are supported.

Use the First Offer from a DHCP Server

You can configure the DHCP relay proxy to use the first offer it receives from any configured DHCP server and send that offer to the DHCP client. By default, DHCP relay proxy sends the most appropriate offer it receives from the configured DHCP servers to the DHCP client.

```
host1(config)#set dhcp relay proxy send-first-offer
```

Set a Timeout for DHCP Client Renewal Messages

You can set the amount of time, in the range 1–168 hours, that the DHCP relay proxy waits for a renewal message from DHCP clients after a router reboot or switchover occurs. A renewal message is required from DHCP clients when a router reboot or switchover occurs. If no renewal message is received before the timeout expires, the relay proxy declares the client no longer active and removes the client's host route By default, DHCP relay proxy uses timeout of 72 hours.

```
host1(config)#set dhcp relay proxy timeout 8
```

NOTE: DHCP relay proxy does not remove a DHCP client's host route when the lease for the client's IP address expires. DHCP relay proxy will instead remove the host route when the relay proxy timeout expires. To prevent a host route from remaining long after lease expiration, modify the relay proxy timeout from its default setting of 72 hours to a setting close to, but not less than the lease time.

Managing Host Routes

The DHCP relay proxy feature enables the E-series router to efficiently manage host routes for DHCP clients, including:

- Installing routes when DHCP clients are configured
- Removing routes when DHCP clients release their DHCP-assigned addresses or when the addresses expire

When a DHCP client sends a request to an external DHCP server, the relay proxy receives the request and forwards it to the external DHCP server. The relay proxy then sends the DHCP server's response back to the client. This process is similar to that used by the DHCP relay component. The DHCP client views the relay proxy as a DHCP server, and the DHCP server sees the relay proxy as a DHCP relay agent.

To DHCP clients, there is no difference when they use a DHCP relay or a DHCP relay proxy. However, the DHCP relay proxy differs from the DHCP relay in how client address renewals and releases are handled:

- With the DHCP relay proxy, DHCP clients communicate with the relay proxy to renew and release addresses.
- With the DHCP relay, DHCP clients communicate directly with the DHCP server to renew and release addresses.

A major benefit of the relay proxy configuration is that the E-series router is kept informed of the status of a DHCP client's address. When addresses are released by clients, the router removes the installed host route for that client. In the DHCP relay configuration, the router does not know when addresses have been renewed or released; the host routes that are no longer needed are still unavailable.

For additional information on managing client bindings, see *Viewing and Deleting DHCP Client Bindings*, in *Chapter 17, DHCP Overview*.

Selecting the DHCP Server Response

Similar to the DHCP relay, the DHCP relay proxy enables you to specify up to five DHCP servers to provide address and configuration information for a DHCP client. As an added benefit over the relay, when using multiple DHCP external servers, you can configure how the DHCP relay proxy determines which offer to send to the DHCP client. You can configure the DHCP relay proxy to use either the single best offer or the first offer it receives from the DHCP servers.

If there are multiple offers, the DHCP relay proxy selects the final offer based on the following priorities:

1. The offer that contains the IP address requested by the DHCP client.
2. The offer that contains an IP address on the same subnetwork as the requested IP address.
3. The offer that has the longest lease time.

If you have enabled the optional select-first-offer feature, the DHCP relay proxy immediately uses the first offer that it receives from any DHCP server.

Behavior for Bound Clients and Address Renewals

When a DHCP client is already bound to an IP address or is renewing the lease on its IP address, DHCP relay proxy unicasts DHCP ACK and DHCP NAK replies to the client regardless of the current configuration of the **set dhcp relay layer2-unicast-replies** command or the **set dhcp relay broadcast-flag-replies** command. These commands control the transmission method used for DHCP reply packets.

This behavior applies only to DHCP relay proxy; it does not apply to DHCP relay because DHCP relay does not maintain a list of active clients or receive address renewal requests from clients.

For information about using the **set dhcp relay layer2-unicast-replies** command, see *Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients* on page 428. For information about using the **set dhcp relay broadcast-flag-replies** command, see *Configuring Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients* on page 428.

Related Topics

- Managing Host Routes on page 446
- **set dhcp relay proxy** command
- **set dhcp relay proxy send-first-offer** command
- **set dhcp relay proxy timeout** command