JUNIPER NETWORKS

JunosE™ Software for E Series™ Broadband Services Routers

DHCP Relay and Relay Proxy

Release
14.3.x

Published: 2013-07-15

Juniper Networks, Inc.
1194 North Mathilda Avenue
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

JunosE™ Software for E Series™ Broadband Services Routers DHCP Relay and Relay Proxy
Release 14.3.x

Revision History
July 2013—FRS JunosE 14.3.x

The information in this document is current as of the date on the title page.

YEAR 2000 NOTICE

Juniper Networks hardware and software products are Year 2000 compliant. Junos OS has no known time-related limitations through the year 2038. However, the NTP application is known to have some difficulty in the year 2036.

END USER LICENSE AGREEMENT

The Juniper Networks product that is the subject of this technical documentation consists of (or is intended for use with) Juniper Networks software. Use of such software is subject to the terms and conditions of the End User License Agreement ("EULA") posted at http://www.juniper.net/support/eula.html. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

List of Figures

List of Tables

About the Documentation

E Series and JunosE Documentation and Release Notes

For a list of related JunosE documentation, see http://www.juniper.net/techpubs/software/index.html.

If the information in the latest release notes differs from the information in the documentation, follow the *JunosE Release Notes.*

To obtain the most current version of all Juniper Networks® technical documentation, see the product documentation page on the Juniper Networks website at http://www.juniper.net/techpubs/.

Audience

This guide is intended for experienced system and network specialists working with Juniper Networks E Series Broadband Services Routers in an Internet access environment.

E Series and JunosE Text and Syntax Conventions

Table 1 on page xii defines notice icons used in this documentation.

Table 1: Notice Icons

Icon	Meaning	Description
	Informational note	Indicates important features or instructions.
	Caution	Indicates a situation that might result in loss of data or hardware damage.
	Warning	Alerts you to the risk of personal injury or death.
	Laser warning	Alerts you to the risk of personal injury from a laser.

Table 2 on page xii defines text and syntax conventions that we use throughout the E Series and JunosE documentation.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents commands and keywords in text.	• Issue the **clock source** command. • Specify the keyword **exp-msg**.
Bold text like this	Represents text that the user must type.	**host1(config)#traffic class low-loss1**

`Fixed-width text like this`	Represents information as displayed on your terminal's screen.	**host1#show ip ospf 2**
		`Routing Process OSPF 2 with Router ID 5.5.0.250`
		`Router is an Area Border Router (ABR)`

Italic text like this	• Emphasizes words. • Identifies variables. • Identifies chapter, appendix, and book names.	• There are two levels of access: *user* and *privileged*. • *clusterId, ipAddress.* • *Appendix A, System Specifications*
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
Syntax Conventions in the Command Reference Guide		
Plain text like this	Represents keywords.	terminal length
Italic text like this	Represents variables.	*mask*, *accessListName*

Table 2: Text and Syntax Conventions *(continued)*

Convention	Description	Examples
| (pipe symbol)	Represents a choice to select one keyword or variable to the left or to the right of this symbol. (The keyword or variable can be either optional or required.)	diagnostic | line
[ ] (brackets)	Represent optional keywords or variables.	[internal | external]
[ ]* (brackets and asterisk)	Represent optional keywords or variables that can be entered more than once.	[level1 | level2 | l1]*
{ } (braces)	Represent required keywords or variables.	{ permit | deny } { in | out } { *clusterId* | *ipAddress* }

Obtaining Documentation

To obtain the most current version of all Juniper Networks technical documentation, see the Technical Documentation page on the Juniper Networks Web site at http://www.juniper.net/.

To download complete sets of technical documentation to create your own documentation CD-ROMs or DVD-ROMs, see the Portable Libraries page at

http://www.juniper.net/techpubs/resources/index.html

Copies of the Management Information Bases (MIBs) for a particular software release are available for download in the software image bundle from the Juniper Networks Web site athttp://www.juniper.net/.

Documentation Feedback

We encourage you to provide feedback, comments, and suggestions so that we can improve the documentation to better meet your needs. Send your comments to techpubs-comments@juniper.net, or fill out the documentation feedback form at https://www.juniper.net/cgi-bin/docbugreport/. If you are using e-mail, be sure to include the following information with your comments:

- Document or topic name
- URL or page number
- Software release version

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract,

or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

- JTAC policies—For a complete understanding of our JTAC procedures and policies, review the *JTAC User Guide* located at http://www.juniper.net/us/en/local/pdf/resource-guides/7100059-en.pdf .
- Product warranties—For product warranty information, visit http://www.juniper.net/support/warranty/ .
- JTAC hours of operation—The JTAC centers have resources available 24 hours a day, 7 days a week, 365 days a year.

Self-Help Online Tools and Resources

For quick and easy problem resolution, Juniper Networks has designed an online self-service portal called the Customer Support Center (CSC) that provides you with the following features:

- Find CSC offerings: http://www.juniper.net/customers/support/
- Search for known bugs: http://www2.juniper.net/kb/
- Find product documentation: http://www.juniper.net/techpubs/
- Find solutions and answer questions using our Knowledge Base: http://kb.juniper.net/
- Download the latest versions of software and review release notes: http://www.juniper.net/customers/csc/software/
- Search technical bulletins for relevant hardware and software notifications: https://www.juniper.net/alerts/
- Join and participate in the Juniper Networks Community Forum: http://www.juniper.net/company/communities/
- Open a case online in the CSC Case Management tool: http://www.juniper.net/cm/

To verify service entitlement by product serial number, use our Serial Number Entitlement (SNE) Tool: https://tools.juniper.net/SerialNumberEntitlementSearch/

Opening a Case with JTAC

You can open a case with JTAC on the Web or by telephone.

- Use the Case Management tool in the CSC at http://www.juniper.net/cm/.
- Call 1-888-314-JTAC (1-888-314-5822 toll-free in the USA, Canada, and Mexico).

For international or direct-dial options in countries without toll-free numbers, see http://www.juniper.net/support/requesting-support.html.

PART 1

Overview

CHAPTER 1

How DHCP Relay Works

DHCP Relay and BOOTP Relay Overview

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 Information Option (Option 82) Suboption Values" on page 34.

Related Documentation

- Configuring DHCP Relay Settings on page 17
- Enabling DHCP Relay on page 17
- Configuring DHCP Relay Proxy on page 20

- Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets on page 25

Rate of DHCP Client Packets Processed by DHCP Relay Overview

In instances when multiple IP clients send a large number of packets, DHCP relay is kept busy processing client packets. While DHCP relay processes client packets, it does not process the packets returned from DHCP server at the same rate. This causes a drop in the number of successful transactions between the remote clients and DHCP server.

You can avoid this situation by limiting the number of client packets that DHCP relay processes and assigning a higher priority to packets that DHCP server sends. While DHCP relay monitors the load on the uplink line module, it calculates the number of client packets it can process for the next second. This calculation enables DHCP relay to handle only that number of client packets and process all the packets as calculated. DHCP relay continues to monitor the uplink line module and sets a new rate for packets processed every second. DHCP assigns higher priority to server packets so, when processing an excessive number of packets, DHCP relay discards the client packets first.

Manually Configuring the Maximum Rate of Client Packets Processed Per Second by DHCP Relay

DHCP relay monitors the load on the interface controller (IC). In some cases, when packets are discarded before they reach the IC, the DHCP relay cannot set the maximum client packet rate automatically. You can then manually reconfigure the rate at which DHCP relay processes client packets per second. Manual reconfiguration of the maximum client packet rate is necessary in cases such as the following:

- When DHCP relay forwards a large number of client packets, DHCP server might not be able to process all of them. DHCP server discards the excess packets. You can set the maximum rate of client packets based on the server capability.
- When the uplink line module cannot handle heavy loads, packets are discarded before they reach the IC. You can set the maximum rate of client packets based on the uplink load capacity.
- When DoS parameters are configured on the uplink line module, packets are discarded at the forwarding controller (FC). You can set the maximum rate of client packets based on these DoS parameters.

Related Documentation

- *Configuring the Rate of Client Packets Processed by DHCP Relay*

CHAPTER 2

DHCP Option 60 Attribute for Traffic Forwarding

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.

NOTE: You must enter the **set dhcp relay** command to create and enable DHCP relay before you enter the **set dhcp vendor-option** command to compare option 60 strings in received DHCP client packets against strings that you configure on the router and forward them to specific DHCP servers. Otherwise, the client traffic that matches the configured option 60 strings are 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-with**—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-with** 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. However, you cannot map the same vendor option string to multiple servers. An error message is displayed in the CLI interface when you attempt to associate the same option 60 string to more than one server.

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.

Related Documentation

- set dhcp relay on page 57
- set dhcp vendor-option on page 71

CHAPTER 3

DHCP Option 82 Attribute and Suboptions for Traffic Forwarding

DHCP Relay Agent Information Option (Option 82) Suboption Values Overview

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 3 on page 10 indicates the effect each command has on enabling or disabling relay agent information suboptions.

Table 3: 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

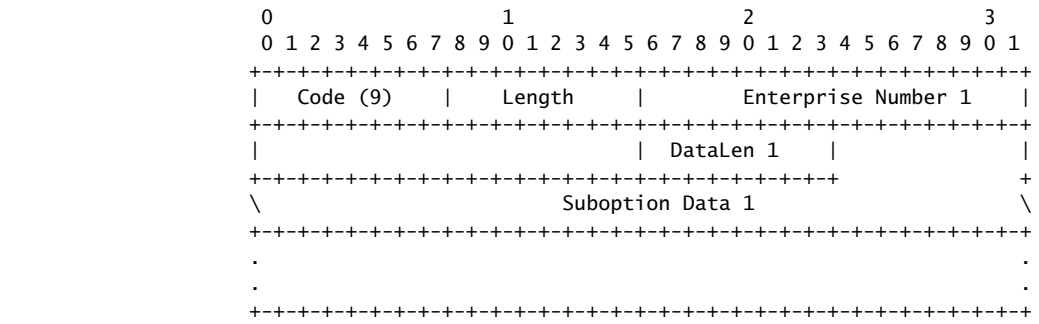
Table 3: Effect of Commands on Option 82 Suboption Settings *(continued)*

Command	Suboption and Status		
	Agent Circuit ID	Agent Remote ID	Vendor-Specific
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
```

Related Documentation

- Configuring the DHCP Relay Agent Option 82 Settings on page 33

PART 2

Configuration

CHAPTER 4

Configuration Tasks for DHCP Relay Functions

Configuring DHCP Relay Settings

You can configure DHCP relay using the following set of tasks:

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 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 5.

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

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

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

Removing Access Routes from Routing Tables and NVS

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

This command removes all installed host routes from IP and deletes host routes from mirrored storage and NVS for specified interfaces. In relay proxy mode, this command enforces consistent state of the route and client database and discards all client information for specified interfaces.

Because DHCP relay cannot distinguish between temporary dynamic interface deletions—where the interface is subsequently re-created—and permanent deletions, sometimes it retains routing information for dynamic interfaces that have already been deleted. You can use the **unknown** keyword with the **dhcp relay discard access-routes** command to remove the routing information for these interfaces.

- To remove access routes:

```
host1(config)#set dhcp relay discard-access-routes
```

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 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**

Related Documentation

- Configuring DHCP Relay Proxy on page 20
- Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets on page 25
- **set dhcp relay on page 57**
- **set dhcp relay assign-giaddr-source-ip on page 60**
- **set dhcp relay giaddr-selects-interface on page 62**
- **set dhcp relay override on page 66**
- **set dhcp relay trust-all on page 70**

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.**

You can configure a DHCP relay proxy using the following set of tasks:

- Enabling DHCP Relay Proxy on page 20
- Use the First Offer from a DHCP Server on page 21
- Set a Timeout for DHCP Client Renewal Messages on page 21

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.

Related Documentation

- set dhcp relay on page 57
- set dhcp relay proxy send-first-offer on page 68
- set dhcp relay proxy timeout on page 69

Managing Host Routes Using DHCP Relay Proxy

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*.

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 the Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients" on page 41. For information about using the **set dhcp relay broadcast-flag-replies** command, see "Configuring the Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients" on page 41.

Related Documentation

- Interaction of DHCP Relay Broadcast Flag with the Layer 2 Unicast Transmission Method on page 26
- Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets on page 25
- **set dhcp relay on page 57**
- **set dhcp relay broadcast-flag-replies on page 61**
- **set dhcp relay layer2-unicast-replies on page 63**

CHAPTER 5

Broadcast Flag Settings for DHCP Relay

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.

```
host1(config)#set dhcp relay broadcast-flag-replies
```

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 the *Behavior for Bound Clients and Address Renewals* section in "Managing Host Routes Using DHCP Relay Proxy" on page 21.

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 *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*.

Related Documentation

- Interaction of DHCP Relay Broadcast Flag with the Layer 2 Unicast Transmission Method on page 26
- Configuring the Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients on page 41
- **set dhcp relay broadcast-flag-replies on page 61**

Interaction of DHCP Relay Broadcast Flag with the Layer 2 Unicast Transmission Method

As described in "Configuring the Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients" on page 41, 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 4 on page 26 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 4: 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.

Table 4: 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)	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.
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 the *Behavior for Bound Clients and Address Renewals* section in "Managing Host Routes Using DHCP Relay Proxy" on page 21.	DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. For information about exceptions to this behavior for DHCP relay proxy, see see the *Behavior for Bound Clients and Address Renewals* section in "Managing Host Routes Using DHCP Relay Proxy" on page 21.

Related Documentation

- Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets on page 25
- Configuring the Layer 2 Unicast Transmission Method for Reply Packets to DHCP Clients on page 41
- **set dhcp relay broadcast-flag-replies on page 61**
- **set dhcp relay layer2-unicast-replies on page 63**

CHAPTER 6

Preventing Host Routes Installation

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. The command enforces consistent state of the route and client database.

In relay mode, this command removes all installed host routes from IP, deletes all host routes from mirrored storage and NVS, and stops accumulating host route information.

In relay proxy mode, this command removes all installed host routes from IP, deletes all NVS client data, and stops installing host routes for newly bound clients in IP. However, it does preserve the client data in mirrored storage and continues preservation of newly bound clients in mirrored storage.

The **no set dhcp relay inhibit-access-route-creation** command enforces consistent state of the route and client database. In relay proxy mode, after the unified ISSU is completed and normal operations resume, this command installs a host route for all existing bound clients in IP and saves it in NVS.

Related Documentation

- Example: Preventing Installation of Host Routes on page 43
- set dhcp relay on page 57

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 the *Using the PPPoE Remote Circuit ID to Identify Subscribers* and *Configuring PPPoE Remote Circuit ID Capture* sections in *JunosE Link Layer Configuration Guide* .

Related Documentation

- *radius remote-circuit-id-format*

CHAPTER 7

Configuring DHCP Option 60 for Relaying Packets

Configuring the DHCP Relay Option 60 Attribute for 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 procedure 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)
```

Related Documentation

- set dhcp relay on page 57
- set dhcp vendor-option on page 71
- show dhcp vendor-option on page 91

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 the *Monitoring and Troubleshooting DHCP* chapter in this guide.

Related Documentation

- set dhcp relay on page 57
- set dhcp vendor-option on page 71

CHAPTER 8

Configuring DHCP Option 82 and Suboptions for Relaying Packets

Configuring the DHCP Relay Agent Option 82 Settings

You can configure the option 82 attribute for DHCP relay using the following set of tasks

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 JunosE Software provides two commands that you can use to configure DHCP relay agent information suboptions.

- To configure option 82 to include any combination of the supported suboptions, including the Vendor-Specific suboption:

  host1(config)#set dhcp relay agent sub-option remote-id
  host1(config)#set dhcp relay agent sub-option circuit-id
  host1(config)#set dhcp relay agent sub-option vendor-specific layer2-circuit-id
  host1(config)#set dhcp relay agent sub-option vendor-specific user-packet-class

- 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).

  host1(config)#set dhcp relay agent

Related Documentation

- DHCP Relay Agent Information Option (Option 82) Suboption Values Overview on page 9
- set dhcp relay on page 57
- set dhcp relay agent sub-option on page 59
- set dhcp relay options on page 65
- set dhcp relay preserve-trusted-client-option on page 67

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 Documentation

- DHCP Relay Agent Information Option (Option 82) Suboption Values Overview on page 9
- Configuring the DHCP Relay Agent Option 82 Settings on page 33

- set dhcp relay on page 57

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.

Related Documentation

- DHCP Relay Agent Information Option (Option 82) Suboption Values Overview on page 9
- Configuring the DHCP Relay Agent Option 82 Settings on page 33
- **set dhcp relay agent sub-option on page 59**

CHAPTER 9

Unicast Tranmission of DHCP Replies

Configuring the 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 in .

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 the *Behavior for Bound Clients and Address Renewals* section in "Managing Host Routes Using DHCP Relay Proxy" on page 21.

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 of DHCP Relay Broadcast Flag with the Layer 2 Unicast Transmission Method" on page 26.

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**

Related Documentation

- Using the Broadcast Flag Setting to Control Transmission of DHCP Reply Packets on page 25
- Interaction of DHCP Relay Broadcast Flag with the Layer 2 Unicast Transmission Method on page 26
- **set dhcp relay layer2-unicast-replies on page 63**

CHAPTER 10

Examples

Example: Preventing Installation of Host Routes

This example describes the configuration of a DHCP relay to prevent installation of host routes.

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Overview

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.

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.

Configuring DHCP Relay to Prevent Installation of Host Routes

Step-by-Step Procedure

This example describes how you can configure the DHCP relay to not install 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

Related Documentation

- Preventing DHCP Relay from Installing Host Routes by Default on page 29
- interface ip on page 50
- ip route on page 51
- ip share-interface on page 53
- ip source-prefix on page 54
- ip unnumbered on page 55
- set dhcp relay on page 57

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

This example shows how you can use the DHCP relay agent option 82 feature to enable the DHCP server to assign an IP address to provide the desired service to the DHCP client.

Requirements

This example uses the following software and hardware components:

- JunosE Release 7.1.0 or higher-numbered releases
- E Series router (ERX7xx models, ERX14xx models, the ERX310 router, the E120 router, or the E320 router)
- ASIC-based line modules that support Fast Ethernet or Gigabit Ethernet

Overview

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.

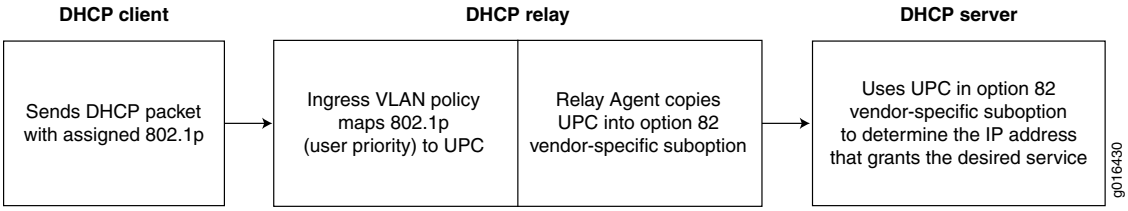
This type of environment, which is illustrated in Figure 1 on page 46, includes the following components:

- 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 1: Passing 802.1p Values to the DHCP Server



Configuring DHCP Relay Option 82 to Pass IEEE 802.1p Values to DHCP Servers

Step-by-Step Procedure

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
```

Related Documentation

- Configuring the DHCP Relay Agent Option 82 Settings on page 33
- Configuring Relay Agent Option 82 Information on page 33
- *classifier-group*
- set dhcp relay on page 57
- set dhcp relay agent sub-option on page 59
- set dhcp relay assign-giaddr-source-ip on page 60
- set dhcp relay broadcast-flag-replies on page 61
- set dhcp relay giaddr-selects-interface on page 62
- set dhcp relay layer2-unicast-replies on page 63
- set dhcp relay options on page 65
- set dhcp relay override on page 66
- set dhcp relay preserve-trusted-client-option on page 67
- set dhcp relay trust-all on page 70
- set dhcp vendor-option on page 71
- *vlan classifier-list*

CHAPTER 11

Configuration Commands

interface ip

Syntax [no] interface ip *interfaceName*

Release Information Command introduced before JunosE Release 7.1.0.

Description Defines a shared IP interface. You can use the specified name to refer to the shared IP interface; you cannot use the layer 2 interface to refer to the shared IP interface, because the shared interface can be moved. The **no** version removes the IP interface.

Options
- *interfaceName*—String of up to 15 characters

Mode Global Configuration

ip route

Syntax

ip route [vrf *vrfName*] { *ipAddress ipMask* { *ipNextHop*
[*interfaceType interfaceSpecifier*] | *interfaceType interfaceSpecifier* } }
[*distance*] [tag *tagVal*] [permanent] [[verify rtr *rtrIndex*]
[verify bfd-liveness-detection [minimum-interval *minInterval* |
[minimum-receive-interval *minRecInterval*]
[minimum-transmit-interval *minTransInterval*]]] [multiplier *multValue*]]
[last-resort]] [reject | discard]

no ip route [vrf *vrfName*] *ipAddress ipMask* [*ipNextHop* | *interfaceType interfaceSpecifier*
] [*distance*]

Release Information

Command introduced before JunosE Release 7.1.0.
reject and **discard** keywords added in JunosE Release 12.0.0.

Description

Establishes static routes and can also enable Bidirectional Forwarding Detection (BFD) for the static route. The **no** version removes static routes or removes BFD from the static route.

NOTE: BFD sessions might not be maintained when the multiplier value is 1 and configured intervals are very short. We recommend that you do not use a multiplier value of 1 with very short intervals.

Options

- *vrfName*—Name of the VRF if the static route is being established within a VRF context; available only in Global Configuration mode
- *ipAddress*—Destination IP address
- *ipMask*—IP mask for the destination
- *ipNextHop*—IP address of the next hop that can be used to reach the destination network
- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- *distance*—Administrative distance for this route in the range 0–254
- *tagVal*—Number in the range 0–4294967295 that identifies the tag for this route
- permanent—Specifies that the route will not be removed, even if the interface shuts down
- verify rtr—Installs the static route in the routing table only if the next hop to the specified destination address is resolved and if the specified RTR operation is currently reachable
- *rtrIndex*—Number of the RTR operation to be verified; there is no default value

- verify bfd-liveness-detection—Installs the static route in the routing table only if the next hop to the specified destination address is verifiable by means of BFD liveness detection
- *minInterval*—Minimum proposed transmit interval and required receive interval for BFD control packets. It has the same effect as configuring the minimum receive interval and the minimum transmit interval to the same value. The range for the value is 10–65535 milliseconds except for ES2 4G LM, for which it is 100–65535 milliseconds. The default value is 300 milliseconds.
- *minRecInterval*—Minimum interval at which the local peer must receive BFD control packets sent by the remote peer. The range for the value is 10–65535 milliseconds except for ES2 4G LM, for which it is 100–65535 milliseconds. The default value is 300 milliseconds.
- *minTransInterval*—Minimum proposed interval between BFD control packets sent by the local peer. The range for the value is 10–65535 milliseconds except for ES2 4G LM, for which it is 100–65535 milliseconds. The default value is 300 milliseconds.
- *multValue*—Detection multiplier value that the remote peer router multiplies by the local peer's negotiated transmit interval to determine the remote peer's BFD liveness detection interval. This value is equal to the number of BFD packets that can be missed before the BFD session is declared down. The range for the value is 1–255. The default value is 3.
- last-resort—Installs the static route in the routing table even if the specified RTR operation is currently unreachable, provided that no other static route to the same network prefix is available
- reject—Discards packets received on the static route for the specified interface that are not processed by the router and sends ICMP unreachable messages to the originator. This option is available only for null interfaces
- discard—Discards packets received on the static route for the specified interface that are not processed by the router and does not send ICMP unreachable messages to the originator. This option is available only for null interfaces

Mode Global Configuration

ip share-interface

Syntax ip share-interface *interfaceType interfaceSpecifier*

no ip share-interface

Release Information Command introduced before JunosE Release 7.1.0.

Description Specifies the layer 2 interface that an IP interface will share in the current virtual router. The command fails if the layer 2 interface does not yet exist.

If you issue this command on a shared IP interface, you cannot issue the **ip share-nexthop** command for the interface. After creating the shared IP interface, you can configure it as you do any other IP interface. The shared interface is operationally up when the layer 2 interface is operationally up and IP is properly configured. You can create operational shared IP interfaces in the absence of a primary IP interface.

The **no** version removes the association between the layer 2 interface and the shared IP interface. You can delete shared and primary IP interfaces independently

Options

- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*

Mode Interface Configuration

ip source-prefix

Syntax [no] ip source-prefix *ipAddress ipAddressMask* deny

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures a subscriber interface or a primary IP interface that is enabled for dynamic creation of subscriber interfaces to demultiplex traffic with the specified IP address and mask. On the ERX1440 router or the E320 router, you can configure up to 1024 subnets for static subscriber interfaces per primary IP interface when each subnet has a variable network mask that is less than /32. The number of subnets identifying a single route (/32) is still limited by the global maximum of 16,000 hosts per line module. The **no** version removes the association between the interface and the specified IP address and mask.

Options

- *ipAddress*—IP address of the physical interface that receives messages for this subscriber
- *ipAddressMask*—Network mask for associated IP subnet
- deny—Filters packets matching this command

Mode Interface Configuration, Subinterface Configuration

ip unnumbered

Syntax [no] ip unnumbered *interfaceType interfaceSpecifier*

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables IP processing on an interface without assigning an explicit IP address to the interface. You must specify an interface location, which is the identifier of another interface on which the router has an assigned IP address. This interface cannot be another unnumbered interface. The **no** version disables IP processing on the interface.

NOTE: You can specify an unnumbered interface using RADIUS instead of using this command in a profile. For more information about how to specify an unnumbered interface using RADIUS, see *Configuring RADIUS Attributes* in the *JunosE Broadband Access Configuration Guide*.

Options

- *interfaceType*—Interface type; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*

Mode Interface Configuration, Profile Configuration, Subinterface Configuration

Related Documentation

- *Setting Up an Unnumbered Interface*
- *Configuring Profile Attributes for IP*
- *Configuring IPv4 Characteristics for a Profile*

service dhcp-local

Syntax [no] service dhcp-local [equal-access | standalone [authenticate]]

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the DHCP local server. In standalone mode, the **authenticate** keyword enables AAA-based authentication for incoming DHCP clients. The **no** version disables the DHCP local server and does not save the previous settings.

Options

- equal-access—Enables the DHCP local server to work with the SRC (formerly SDX or SSC) or HTTP local server for non-PPP equal access, the default option
- standalone—Configures the router as a DHCP local server
- authenticate—Enables AAA-based authentication of incoming DHCP clients

Mode Global Configuration

set dhcp relay

Syntax

To create the DHCP relay independent of any DHCP servers and to explicitly delete the DHCP server

[no] set dhcp relay

To create and disable the DHCP relay for a specific DHCP server

set dhcp relay { *dhcpServerAddress* [proxy] | agent [circuit-ID-only | remote-ID-only] |inhibit-access-route-creation | discard-access-routes { all | *interfaceType interfaceSpecifier* | | unknown } }

no set dhcp relay { *dhcpServerAddress* | agent | inhibit-access-route-creation }

Release Information

Command introduced before JunosE Release 7.1.0.
Command used without any keywords introduced in JunosE Release 8.2.0.
unknown keyword added in JunosE Release 9.2.0.

Description

When used without any optional keywords, creates and enables DHCP relay in the current virtual router independent of any DHCP servers.

When used with optional keywords, adds a new DHCP/BOOTP server and specifies that the E Series router is either a DHCP relay or DHCP relay proxy between the DHCP client and DHCP server. Optionally, configures the DHCP relay agent, including specifying the DHCP relay agent information (option 82) that is included in all packets forwarded to the DHCP server.

If you issue the **set dhcp relay** command when a local server has been configured, the local server is deactivated.

The **no** version used without other keywords deletes the DHCP relay agent and its configuration from the virtual route. The **no** version used with optional keywords removes the specified server or disables the specified relay agent configuration.

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.

Options

- *dhcpServerAddress*—IP address of the DHCP server
- proxy—Specifies that the router is a DHCP relay proxy between the DHCP client and DHCP server; if omitted, the router functions as a DHCP server
- agent—Adds the agent information suboptions (circuit-ID and remote-ID) to every packet the router relays from a DHCP client to a DHCP server

- circuit-ID-only—Specifies circuit ID suboption (suboption 1) only
- remote-ID-only—Specifies remote-ID suboption (suboption 2) only
- inhibit-access-route-creation—Specifies that host routes are not installed; enforces consistent state of route/client database
  - In relay mode, removes all installed host routes from IP; deletes all host routes data in the routing table and NVS; stops accumulating host route information
  - In relay proxy mode, removes all installed host routes from IP; deletes all NVS client data and stops installing host routes for newly bound clients in IP; preserves the routing table client data and continues preservation of newly bound clients in the routing table
- discard-access-routes—Removes existing access routes from the routing table and from NVS
- all—Removes all existing access routes
- *interfaceType*—Interface type whose access routes should be discarded; see *Interface Types and Specifiers*
- *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
- unknown—Removes existing host routes from unknown (nonexistent) interfaces—dynamic interfaces for which DHCP relay retains route information after these interfaces have been deleted

Mode Global Configuration

set dhcp relay agent sub-option

Syntax set dhcp relay agent sub-option { circuit-id | remote-id | vendor-specific { layer2-circuit-id | user-packet-class } }

no set dhcp relay agent sub-option { circuit-id | remote-id | vendor-specific [layer2-circuit-id | user-packet-class] }

Release Information Command introduced in JunosE Release 8.0.0.

Description Configures DHCP relay and DHCP relay proxy to add values into the DHCP relay agent information option (option 82) of the packets sent to a DHCP server. The **no** version restores the default configuration, in which the specified values are not relayed to the DHCP server.

NOTE: We recommend that you use this 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.

Options

- circuit-id—Specifies the Agent Circuit ID suboption (suboption 1)
- remote-id—Specifies the Agent Remote ID suboption (suboption 2)
- vendor-specific—Specifies the Vendor-Specific suboption (suboption 9)
- layer2-circuit-id—Specifies the SVLAN ID or VLAN ID or both for Ethernet interfaces or the VPI/VCI for ATM 1483 interfaces
- user-packet-class—Specifies the user packet class, whose value is configured by the JunosE Software layer 2 policy application

Mode Global Configuration

set dhcp relay assign-giaddr-source-ip

Syntax [no] set dhcp relay assign-giaddr-source-ip

Release Information Command introduced in JunosE Release 7.1.0.

Description Configures DHCP relay and DHCP relay proxy to assign the gateway IP address (giaddr) to the source IP address of traffic they send to DHCP servers. The **no** version restores the default, in which the DHCP relay and DHCP relay proxy do not assign the giaddr to the source IP address.

Mode Global Configuration

set dhcp relay broadcast-flag-replies

Syntax [no] set dhcp relay broadcast-flag-replies

Release Information Command introduced in JunosE Release 8.1.0.

Description Configures DHCP relay and DHCP relay proxy to use the setting of the broadcast flag in the DHCP request packet to control how DHCP Offer reply packets and ACK and NAK reply packets are transmitted to DHCP clients during the discovery process. If the broadcast flag is set in the request packet, DHCP relay and DHCP relay proxy broadcast DHCP reply packets to clients. If the broadcast flag is not set in the request packet, DHCP relay and DHCP relay proxy 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. The **no** version causes the router not to use the broadcast flag setting and restores the default behavior, which broadcasts DHCP Offer reply packets and ACK and NAK reply packets to all clients during the discovery process.

NOTE: 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 an error.

Mode Global Configuration

set dhcp relay giaddr-selects-interface

Syntax [no] set dhcp relay giaddr-selects-interface

Release Information Command introduced in JunosE Release 8.0.0.

Description Configures DHCP relay to use information in the giaddr in the DHCP ACK packets that are generated by the server and destined for the DHCP client. The DHCP server uses this information to determine the primary interface that is used to optionally build dynamic subscriber interfaces.

The **no** version restores the default that builds dynamic subscriber interfaces on the IP interface on which DHCP client discover packets are received.

Mode Global Configuration

set dhcp relay layer2-unicast-replies

Syntax [no] set dhcp relay layer2-unicast-replies

Release Information Command introduced in JunosE Release 7.2.0.

Description Configures DHCP relay and DHCP relay proxy to use the optional layer 2 unicast and layer 3 broadcast transmission method to transmit DHCP Offer reply packets and ACK reply packets to DHCP clients during the discovery process. The **no** version restores the default method that broadcasts DHCP Offer reply packets and ACK reply packets to all DHCP clients during the discovery process.

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

Mode Global Configuration

set dhcp relay max-client-packet-rate

Syntax [no] set dhcp relay max-client-packet-rate [*packetsPerSecond*]

Release Information Command introduced in JunosE Release 11.2.0.

Description Configures DHCP relay to limit the maximum number of client packets that DHCP relay processes per second. The **no** version returns to the default, in which DHCP relay processes 4096 packets per second.

Options
- *packetsPerSecond*—Number of client packets that are processed per second in the range 0–4096.

Mode Global Configuration

set dhcp relay options

Syntax set dhcp relay options { hostname | vrname | exclude-subinterface-id }

no set dhcp relay options [hostname | vrname | exclude-subinterface-id]

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures the relay agent option 82 information that the router adds to DHCP packets before it relays the packets to the DHCP server. You can add either the E Series hostname or the virtual router name to the front of the Circuit-Id field. You cannot add both hostname and virtual router name. The last option specified is the one in use. You can also strip the subinterface ID from the Interface-Id field. The **no** version returns to the default, in which no information is added to the Circuit-Id field and/or the subinterface ID is not stripped from the interface string.

Options

- hostname—Adds the router's hostname to the front of the Circuit-Id field; the hostname is separated from the circuit information by a colon
- vrname—Adds the router's virtual router name to the front of the Circuit-Id field; the virtual router name is separated from the circuit information by a colon
- exclude-subinterface-id—Strips the subinterface ID from the Interface-Id field

Mode Global Configuration

set dhcp relay override

Syntax [no] set dhcp relay override { agent-option | giaddr }

Release Information Command introduced before JunosE Release 7.1.0.

Description Configures DHCP relay to override the relay agent option 82 or giaddr values in packets destined for a DHCP server. The **no** version returns to the default, in which the option 82 or giaddr value is not overridden.

Options
- agent-option—Overrides the option 82 information
- giaddr—Overrides giaddr

Mode Global Configuration

set dhcp relay preserve-trusted-client-option

Syntax [no] set dhcp relay preserve-trusted-client-option

Release Information Command introduced in JunosE Release 7.1.0.

Description Configures DHCP relay and DHCP relay proxy to prevent option 82 information from being stripped from packets destined for a trusted client. The **no** version restores the default, in which the option 82 information is stripped from the packets.

Mode Global Configuration

set dhcp relay proxy send-first-offer

Syntax [no] set dhcp relay proxy send-first-offer

Release Information Command introduced in JunosE Release 8.0.0.

Description Configures the DHCP relay proxy to immediately send the first DHCP offer it receives from any DHCP server to the DHCP client. The **no** version restores the default value, in which DHCP relay proxy sends the single most appropriate address offer it receives from multiple DHCP servers.

Mode Global Configuration

set dhcp relay proxy timeout

Syntax set dhcp relay proxy timeout *hours*

no set dhcp relay proxy timeout

Release Information Command introduced before JunosE Release 7.1.0.

Description Sets the time that the DHCP relay proxy waits for a renewal message from the DHCP client after a reboot or switchover occurs. The **no** version restores the default value.

Options
- *hours*—Number of hours for the timeout, in the range 1–168 (1 hour to 7 days); default value is 72 hours

Mode Global Configuration

set dhcp relay trust-all

Syntax [no] set dhcp relay trust-all

Release Information Command introduced before JunosE Release 7.1.0.

Description Enables the DHCP relay trust-all method. When the trust-all method is enabled, the DHCP relay processes packets that are destined for a DHCP server as if they are from trusted sources. The **no** version restores the default, which disables the trust-all method.

Mode Global Configuration

set dhcp vendor-option

Syntax To set the default action to take when the option 60 string does not match a configured vendor-option string:

[no] set dhcp vendor-option default [drop | local-server | proxy-client | relay *address* | relay-server-list]

To set the action to take when the option 60 string matches a configured vendor-option string:

[no] set dhcp vendor-option { equals | starts-with } *string* [local-server | relay *address*]

Release Information Command introduced in JunosE Release 8.2.0.

Description Configures vendor-option strings that control DHCP client traffic. Creates DHCP vendor-option servers by configuring DHCP relay to match DHCP option 60 strings and to specify the action the router takes when it receives DHCP option 60 strings. The **no** version disables the setting.

Options

- drop—Discards packets
- local-server—Forwards packets to the DHCP local server
- proxy-client—Forwards packets to the DHCP proxy client server
- *address*—IP address of the vendor-option server to which packets are forwarded
- relay-server-list—Forwards packets 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.
- equals—Configures a string that must be matched exactly for option 60 processing
- starts-with—Configures the string that is matched from left-to-right for option 60 processing
- *string*—Option 60 string to match; up to 254 hexadecimal characters

Mode Global Configuration

PART 3

Administration

CHAPTER 12

Configuring Baselines for DHCP Relay and Relay Proxy Statistics

Setting Baselines for DHCP Statistics

You can use the **baseline dhcp** commands to set statistics baselines for DHCP operations. The router implements the baseline by reading and storing the statistics at the time the baseline is set and then subtracting this baseline when you retrieve baseline-relative statistics.

Use the **delta** keyword with the **show dhcp** commands to display baselined statistics.

Tasks to set a baseline for DHCP statistics are:

Setting a Baseline for DHCP Relay and Relay Proxy

To set a statistics baseline for DHCP relay and DHCP relay proxy: :

- Issue the **baseline dhcp relay** command:

  host1#baseline dhcp relay

There is no **no** version.

Setting a Baseline for DHCP Proxy Server Statistics

To set a baseline for DHCP proxy server statistics.

- Issue the **baseline dhcp server** command:

  host1#baseline dhcp server

There is no **no** version.

Setting a Baseline for DHCP External Server Statistics

To set a baseline for DHCP external server statistics.

- Issue the **baseline ip dhcp-external** command:

  host1#baseline ip dhcp-external

There is no **no** version.

Setting a Baseline for DHCP Local Server Statistics

To set a baseline for DHCP local server statistics:

- Issue the **baseline ip dhcp-local** command:

  host1#baseline ip dhcp-local

There is no **no** version.

To set a baseline for DHCP local server statistics for a specific ATM, Fast Ethernet, or Gigabit Ethernet interface:

- Issue the **baseline ip dhcp-local** command with the optional **interface** keyword to specify the type of interface and interface specifier:

  host1#baseline ip dhcp-local interface atm 3/1

To set a baseline for DHCPv6 local server statistics:

- Issue the **baseline ipv6 dhcpv6-local** command:

  host1#baseline ipv6 dhcpv6-local

CHAPTER 13

Monitoring DHCP Relay and Relay Proxy Settings

Monitoring DHCP Relay Configuration Information

Purpose Display DHCP relay configuration information and the IP addresses of the configured DHCP servers.

Action To display information about the DHCP relay configuration and the IP address of the DHCP servers.

```
host1#show dhcp relay

DHCP Relay Configuration
------------------------
Mode: Proxy
  Restore Client Timeout: 72
  Send First Offer: off
Inhibit Access Route Creation: off
Assign Giaddr to Source IP: off
Layer 2 Unicast Replies: off
Giaddr Selects Interface: off
Broadcast Flag Replies: on
Maximum client pps : 4096
Relay Agent Information Option (82):
  Override Giaddr: off
  Override Option: off
  Trust All Clients: off
  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
---------------------
30.3.7.1
```

Meaning Table 5 on page 78 lists the **show dhcp relay** command output fields.

Table 5: show dhcp relay Output Fields

Field Name	Field Description
Mode	DHCP relay mode; either Standard (DHCP relay mode) or Proxy (DHCP relay proxy mode)
Restore Client Timeout	(DHCP relay proxy mode only) number of hours
Send First Offer	On or off
Inhibit Access Route Creation	On or off
Assign Giaddr to Source IP	On or off
Layer 2 Unicast Replies	On or off
Giaddr Selects Interface	On or off
Broadcast Flag Replies	On or off
Maximum client pps	Maximum number of client packets processed per second
Override Giaddr	On or off
Override Option	On or off
Trust All Clients	On or off
Preserve Option From Trusted Clients	On or off
Circuit-ID Sub-option (1)	On or off; when on includes a list of selected suboptions
Remote-ID Sub-option (2)	On or off
Vendor-Specific Sub-option (9)	On or off; when on includes a list of selected suboptions
DHCP Server Addresses	IP addresses of configured DHCP servers

Related Documentation

- show dhcp relay on page 88

Monitoring DHCP Option 60 Information

Purpose Display configuration and action information for the DHCP vendor-option (option 60) feature.

- Use the command without additional keywords to display information for all vendor option configurations.
- Use the **vendor-option-relay-server** keyword and server address to display information for option 60 strings that match a configured string that results in the packets being sent to the specified vendor-option server.
- Use the **default** keyword to display information for option 60 strings that do not match a configured vendor-option string.

Action To display information for all vendor option configurations:

```
host1#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 4 entries.
         Vendor-option                          Action
------------------------------ ----------------------------------------
Juniper                        relay to 10.10.1.1 (rx: 0)
default(*)                     relay to 192.168.5.5 (rx: 0, no-match: 0)
someString(*)                  relay to 192.168.7.7 (rx: 0)
someString2(*)                 local-server (rx: 0)
```

To display information for option 60 strings that match a configured string:

```
host1#show dhcp vendor-option vendor-option-relay-server 10.10.1.1
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 4 entries.
         Vendor-option                          Action
------------------------------ ----------------------------------------
Juniper                        relay to 10.10.1.1 (rx: 0)
```

Meaning Table 6 on page 79 lists the **show dhcp vendor-option** command output fields.

Table 6: show dhcp vendor-option Output Fields

Field Name	Field Description
Vendor-option	Option 60 string; an asterisk (*) indicates that the string exactly matches a configured option 60 string, default indicates the action to take when the string does not match a configured option 60 string
Action	Action to take for the indicated string match; drop, forward to local-server, proxy client server, or all configured DHCP vendor option servers; or relay to the specified DHCP server

Table 6: show dhcp vendor-option Output Fields *(continued)*

Field Name	Field Description
rx	Received packets that match a vendor-option string
no-match	Received packets that do not match a vendor-option string; no-match statistics appear only for default entries

Related Documentation

- show dhcp vendor-option on page 91

Monitoring DHCP Packet Capture Settings

Purpose Display the configuration for per-interface DHCP packet logging.

Action To display configuration information about the DHCP packet capture feature:

```
host1#show ip dhcp-capture

      Dhcp Capture Configuration
      --------------------------
Router    Interface   Type    Priority
-------   ---------   -----   --------
default   ip3/1       Rx/Tx   low/low
default   ip5/1       Rx      high
```

Meaning Table 7 on page 80 lists the **show ip dhcp-capture** command output fields.

Table 7: show ip dhcp-capture Output Fields

Field Name	Field Description
Router	Router name
Interface	Interface whose DHCP packets are logged
Type	Packet type to be logged, Rx (received), Tx (transmitted), or Rx/Tx (all)
Priority	Priority assigned to logged packets, low or high

Related Documentation

- *show ip dhcp-capture*

CHAPTER 14

Monitoring DHCP Relay and Relay Proxy Statistics

Monitoring DHCP Relay Statistics

Purpose Display DHCP packet error and relay agent option statistics that are reported for both DHCP relay and DHCP relay proxy, and also to display DHCP server statistics related only to DHCP relay.

NOTE: The **show dhcp relay proxy statistics** command displays additional DHCP statistics that the router reports only for DHCP relay proxy.

Action To display DHCP relay statistics:

```
host1# show dhcp relay statistics
                        DHCP Relay Statistics
                        ---------------------
                          Statistic                                 Values
------------------------------------------------------------------  ------
Packet error statistics (standard & proxy modes):
  dropped discover packets, no resources                            0
  dropped dhcp packets, no resources                                0
  dropped bad message operation packets                             0
  dropped unknown message type request packets                      0
  dropped unknown message type reply packets                        0
Packet Pacing Algorithm (standard & proxy modes):
  Speed up pacer                                                    0
  Slow down pacer                                                   0
  Current client pps                                                1024
Relay Agent Option statistics (standard & proxy modes):
  add Relay Agent Option circuit ID suboption                       On
  add Relay Agent Option remote ID suboption                        On
  packets with giaddr override                                      0
  packets with Relay Agent Option override                          2
  packets forwarded with Relay Agent Option already present         4
  dropped packets with Relay Agent Option already present           3
  dropped giaddr spoof packets                                      0
DHCP server statistics (standard mode only):
```

```
  dropped duplicate request packets                          12
  packets transmitted to servers                             38
  packets received from servers                              26
  dropped unknown xid reply packets                          0
  dropped stale request packets                              12
```

To display detailed statistics for DHCP relay only, use the optional **detail** keyword—this command displays DHCP server statistics and dropped unknown message type reply packets statistics:

```
host1# show dhcp relay statistics detail
                    DHCP Relay Detail Statistics
                    ----------------------------
            Statistics                 10.10.1.1  192.168.32.12   192.168.32.1
-----------------------------------   ---------  -------------   ------------
Dropped unknown message type replies   0          0               0
Dropped duplicate requests             6          6               0
Packets transmitted to server          6          6               26
Packets received from server           0          0               26
Dropped unknown xids replies           0          0               0
Dropped stale requests                 6          6               0
```

Meaning Table 8 on page 82 lists the **show dhcp relay statistics** command output fields.

Table 8: show dhcp relay statistics Output Fields

Field Name	Field Description
Packet error statistics (standard & proxy modes)	
dropped discover packets, no resources	Number of received DHCP relay discover messages that were discarded because of lack of resources
dropped dhcp packets, no resources	Number of received DHCP relay messages, other then discover messages, that were discarded because of lack of resources
dropped bad message operation packets	Number of received DHCP relay messages that were discarded because their message operation (for example, bootrequest, bootreply) was unknown, possibly due to corruption
dropped unknown message type request packets	Number of received DHCP relay request messages that were discarded because their message type (for example, discover, offer-request) was unknown, possibly due to corruption
dropped unknown message type reply packets	Number of received DHCP relay reply messages that were discarded because their message type (for example, offer, ack) was unknown, possibly due to corruption
Packet Pacing Algorithm (standard & proxy modes)	

Table 8: show dhcp relay statistics Output Fields *(continued)*

Field Name	Field Description
Speed up pacer	Number of times the DHCP relay increased the rate of client packets processed
Slow down pacer	Number of times the DHCP relay decreased the rate of client packets processed
Current client pps	Rate of client packets processed per second
Relay Agent Option statistics (standard & proxy modes)	
add Relay Agent Option circuit ID suboption	Status of circuit ID suboption, on or off
add Relay Agent Option remote ID suboption	Status of remote ID suboption, on or off
packets with giaddr override	Number of received DHCP relay requests whose giaddr field is overridden with IP address 0.0.0.0
packets with Relay Agent Option override	Number of received DHCP relay requests whose relay agent information option is overridden with an option string created by this relay agent
packets forwarded with Relay Agent Option already present	Number of received DHCP relay requests already containing the relay agent information option that were forwarded to DHCP servers
dropped packets with Relay Agent Option already present	Number of received DHCP relay requests that were discarded because they already contained the relay agent information option when this relay agent was configured to insert the option
dropped giaddr spoof packets	Number of received DHCP relay requests that were discarded because the gateway IP address field already contained this relay agent's IP address
DHCP server statistics (standard mode only)	
dropped duplicate request packets	Number of received DHCP relay requests that were discarded because they have a matching server address and XID of an outstanding DHCP server request
packets transmitted to servers	Number of DHCP relay requests successfully transmitted to DHCP servers
packets received from servers	Number of DHCP relay replies successfully received from DHCP servers

Table 8: show dhcp relay statistics Output Fields *(continued)*

Field Name	Field Description
dropped unknown xid reply packets	Number of DHCP relay replies received from DHCP servers that were discarded because their server address and XID do not match an outstanding DHCP server request
dropped stale request packets	Number of DHCP relay requests sent to DHCP servers that were discarded because their replies timed out

Related Documentation

- show dhcp relay statistics on page 90

Monitoring DHCP Relay Proxy Statistics

Purpose Display statistics for the DHCP relay proxy.

NOTE: The **show dhcp relay statistics** command displays additional DHCP statistics that the router reports for both DHCP relay and DHCP relay proxy.

Action To display DHCP relay proxy statistics:

```
host1# show dhcp relay proxy statistics
                        DHCP Relay/Proxy Statistics
                        ---------------------------
    Address     Disc.  Offer    Req.     Ack     Nak   Decline Release Inform
--------------- ------ ------ -------- -------- ------ -------- ------- ------
    192.168.1.1      9      0        0        0      0        0       0      0
    192.168.1.2      9      0        0        0      0        0       0      0
   192.168.32.1      9      5        5        5      0        0       0      0
Active Clients: 5
Clients to Restore: 0
Client Packets: 14
Server Packets: 10
Timed Out: 0
No Offers: 4
Modify Fail: 0
```

Meaning Table 9 on page 84 lists the **show dhcp relay proxy statistics** command output fields.

Table 9: show dhcp relay proxy statistics Output Fields

Field Name	Field Description
Address	IP address of the DHCP server
Disc.	Number of discover messages sent to server
Offer	Number of offers received from a server

Table 9: show dhcp relay proxy statistics Output Fields *(continued)*

Field Name	Field Description
Req.	Number of requests sent to a server
Ack	Number of ACK messages received from a server
Nak	Number of NAK messages received from a server
Decline	Number of decline messages sent to a server
Release	Number of releases sent to a server
Inform	Number of information messages sent to a server
Active Clients	Number of clients being maintained by the relay proxy
Clients to Restore	Number of host routes installed without an active client (waiting for renewal)
Client Packets	Total number of packets received from clients
Server Packets	Total number of packets received from servers
Timed Out	Number of clients removed because of lease expiration
No Offers	Number of clients removed because no server sent an offer
Modify Fail	Number of clients deleted because the relay proxy failed to modify the DHCP packet

Related Documentation

- show dhcp relay proxy statistics on page 89

CHAPTER 15

Monitoring Commands

show dhcp relay

Syntax show dhcp relay [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays DHCP relay configuration information and IP addresses of configured DHCP servers.

Options
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

Related Documentation
- Monitoring DHCP Relay Configuration Information on page 77

show dhcp relay proxy statistics

Syntax show dhcp relay proxy statistics [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.

Description Displays the statistics of the configured DHCP relay proxy.

Options
- delta—Displays baselined statistics
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

Related Documentation
- *Monitoring DHCP Server and DHCP Relay Agent Statistics*

show dhcp relay statistics

Syntax show dhcp relay statistics [detail] [delta] [*filter*]

Release Information Command introduced before JunosE Release 7.1.0.
detail keyword added in JunosE Release 7.2.0.

Description Displays statistics that are common to both DHCP relay and DHCP relay proxy, and also to display DHCP server statistics for DHCP relay only.

Options
- statistics—Displays statistics for the DHCP relay
- detail—Displays a subset of statistics on a per-DHCP server basis
- delta—Displays baselined statistics
- *filter*—See *Filtering show Commands*

Mode Privileged Exec

Related Documentation
- Monitoring DHCP Relay Statistics on page 81

show dhcp vendor-option

Syntax show dhcp vendor-option [default | vendor-option-relay-server *ServerAddress*]

Release Information Command introduced in JunosE Release 8.2.0.

Description Displays configuration and action information for the DHCP vendor-option feature.

Options
- default—Displays where DHCP client packets that do not match a configured vendor-string are sent by default
- vendor-option-relay-server—Displays DHCP string matches that are sent to the specified vendor-option server
- *ServerAddress*—IP address of the DHCP vendor-option server

Mode Privileged Exec

Related Documentation
- Monitoring DHCP Option 60 Information on page 78

PART 4

Index

Index