JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

DHCP User Guide

Published
2024-06-12

JUNOS

Juniper Networks, Inc.
1133 Innovation Way
Sunnyvale, California 94089
USA
408-745-2000
www.juniper.net

Juniper Networks, the Juniper Networks logo, Juniper, and Junos are registered trademarks of Juniper Networks, Inc. in the United States and other countries. All other trademarks, service marks, registered marks, or registered service marks are the property of their respective owners.

Juniper Networks assumes no responsibility for any inaccuracies in this document. Juniper Networks reserves the right to change, modify, transfer, or otherwise revise this publication without notice.

Junos® OS DHCP User Guide
Copyright © 2024 Juniper Networks, Inc. All rights reserved.

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 https://support.juniper.net/support/eula/. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

About This Guide | xiii

1 Overview

DHCP Overview | 2

- Benefits of DHCP | 2
- Introduction to DHCP | 3
- Understand DHCP | 3

DHCP Access Service Overview | 9

- IP Address Assignments | 9
- DHCP Address Allocation Methods | 12
- DHCP Lease Time Management | 13
- DHCP Options | 13

Legacy DHCP and Extended DHCP | 16

- Understanding Differences Between Legacy DHCP and Extended DHCP | 16
- DHCP Statement Hierarchy and Inheritance | 20
- Difference in Legacy DHCP Relay and Extended DHCP Relay | 24
- Restrictions in Using Legacy DHCP and Extended DHCP | 24

2 Address Assignment Pool

IP Address Assignment Pool | 27

- Address-Assignment Pools Overview | 27
- Extended DHCP Local Server and Address-Assignment Pools | 30
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 31
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 32
- Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option | 34

Configuring Address-Assignment Pools | 34

Configuring an Address-Assignment Pool Name and Addresses | 35

Configuring a Named Address Range for Dynamic Address Assignment | 35

Configuring Static Address Assignments | 36

Configuring Address-Assignment Pool Linking | 37

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools | 37

DHCPv6 Address-Assignment Pools | 39

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 39

Requirements | 40

Overview | 40

Configuration | 40

Verification | 42

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 43

Configuring an Address-Assignment Pool for Router Advertisement | 44

Configuring Nontemporary Address Assignment | 44

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 45

Configuring Auto-Prefix Delegation | 46

Multiple Address Assignment for DHCPv6 Clients | 47

3 **DHCP Server**

DHCP Server | 49

Understanding DHCP Server Operation | 49

Graceful Routing Engine Switchover for DHCP | 50

DHCP Server Configuration | 52

DHCP Server Configuration Overview | 52

Minimum DHCP Local Server Configuration | 54

Example: Complete DHCP Server Configuration | 56

Requirements | 56

Overview | 56

Configuration | 57

Configure a Router as an Extended DHCP Local Server | 60

Configuring a Switch as a DHCP Server | 63

Configuring the Switch as a Local DHCP Server | 63

Configuring a DHCP Server on Switches | 67

Configuring an Extended DHCP Server on a Switch | 67

Example: Configuring a Security Device as a DHCP Server | 69

Requirements | 69

Overview | 69

Configuration | 70

Verification | 74

DHCP Server Options | 77

Configure DHCP Server Identifier | 78

Configure Address Pools for DHCP Dynamic Bindings | 78

Configure Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address | 79

Enabling TCP/IP Propagation on a DHCP Local Server | 80

Specify DHCP Lease Times for IP Address Assignments | 81

Configure a DHCP Boot File and DHCP Boot Server | 82

Configure Domain Name and Domain Search List | 83

Configure Routers Available to the DHCP Client | 83

Configure User-Defined DHCP Options | 84

Configure DHCP SIP Server | 85

Overriding the Default DHCP Local Server Configuration Settings | 85

Legacy DHCP Server Configuration Options | 88

Verifying DHCP Server Configuration | 96

Verifying DHCP Server Binding and Server Statistics | 96

Viewing DHCP Bindings (Legacy DHCP) | **98**

Viewing DHCP Address Pools (Legacy DHCP) | **99**

Viewing and Clearing DHCP Conflicts (Legacy DHCP) | **99**

Monitoring the DHCP Server Configuration | 100

Tracing DHCP Local Server Operations | **101**

Configuring the Filename of the DHCP Local Server Processes Log | **102**

Configuring the Number and Size of DHCP Local Server Processes Log Files | **102**

Configuring Access to the Log File | **102**

Configuring a Regular Expression for Lines to Be Logged | **103**

Configuring Trace Option Flags | **103**

DHCPv6 Server | 104

DHCPv6 Local Server Overview | **105**

DHCPv6 Server Overview | **106**

Example: Configuring DHCPv6 Server Options | **108**

Requirements | **108**

Overview | **108**

Configuration | **109**

Verification | **112**

Specifying the Address Pool for IPv6 Prefix Assignment | **113**

Specifying the Delegated Address Pool for IPv6 Prefix Assignment | **114**

Preventing Binding of Clients That Do Not Support Reconfigure Messages | **115**

Configuring DHCPv6 Rapid Commit (MX Series, EX Series) | **116**

Allow Host Inbound Traffic for DHCPv6 Traffic | **117**

Verifying and Managing DHCPv6 Local Server Configuration | **118**

Understanding Cascaded DHCPv6 Prefix Delegating | **119**

Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) | **120**

Requirements | **121**

Overview | **121**

Configuration | **122**

Verification | **143**

SLAAC (Stateless Address Auto-Configuration) | **150**

4 **DHCP Relay Agent**

DHCP Relay Agent | 153

Understanding DHCP Relay Agent Operation | **153**

Minimum DHCP Relay Agent Configuration | **156**

Configuring DHCP Relay Agent | **159**

Requirements | **160**

Overview | **160**

Configuration | **161**

Verification | **170**

Configuring a DHCP Relay Agent on EX Series Switches | **172**

Configuring DHCP Smart Relay (Legacy DHCP Relay) | **172**

Disabling Automatic Binding of Stray DHCP Requests | **173**

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets | **175**

Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent | **176**

Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address | **176**

Overriding the Default DHCP Relay Configuration Settings | **177**

Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally | **179**

Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings | **180**

Requirements | **180**

Overview | **181**

Configuration | **181**

Verification | **184**

Verifying and Managing DHCP Relay Configuration | **185**

Extended DHCP Relay Agent Overview | **187**

DHCP and BOOTP Relay Agent | 190

DHCP and BOOTP Relay Overview for Switches | **190**

Configuring DHCP and BOOTP Relay | **194**

Configuring DHCP and BOOTP Relay on QFX Series | **194**

- Configuring a DHCP and BOOTP Relay Agent on QFX Series | **195**
- Configuring DHCP Smart Relay on QFX Series | **197**

DHCP Relay Agent Information Option (Option 82) | 198

Using DHCP Relay Agent Option 82 Information | **199**

- Configuring Option 82 Information | **200**
- Overriding Option 82 Information | **202**
- Including a Prefix in DHCP Options | **203**
- Including a Textual Description in DHCP Options | **206**

How DHCP Relay Agent Uses Option 82 for Auto Logout | **209**

Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | **210**

Check if Your Device Support DHCP Option-82 | **211**

Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82 | **212**

Example: Configure DHCP Relay in Forward Only Mode | **213**

- Requirements | **214**
- Overview | **214**
- Configuration | **215**
- Verification | **218**

DHCPv6 Relay Agent | 222

DHCPv6 Relay Agent Overview | **222**

Configuring DHCPv6 Relay Agent | **223**

- Requirements | **224**
- Overview | **224**
- Configuration | **226**

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets | **235**

Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets | **236**

Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets | **238**

Verifying and Managing DHCPv6 Relay Configuration | **239**

DHCP Relay Proxy | 240

DHCP Relay Proxy Overview | **241**

Enabling DHCP Relay Proxy Mode | **243**

5 **DHCP Client**

DHCP Client | 245

Understanding DHCP Client Operation | **245**

Minimum DHCP Client Configuration | **246**

Configuring a DHCP Client | **246**

Example: Configuring the Device as a DHCP Client | **249**

Requirements | **249**

Overview | **250**

Configuration | **251**

Verification | **254**

Verifying and Managing DHCP Client Configuration | **256**

Example: Configuring as a DHCP Client in Chassis Cluster Mode | **257**

Requirements | **257**

Overview | **258**

Configuration | **258**

Verification | **264**

DHCPv6 Client | 266

DHCPv6 Client Overview | **267**

Understanding DHCPv6 Client and Server Identification | **268**

Minimum DHCPv6 Client Configuration on SRX Series Devices | **269**

Configuring DHCP Client-Specific Attributes | **271**

DHCPv6 Client Configuration Options | **271**

Configuring the DHCPv6 Client Rapid Commit Option | **273**

Configuring a DHCPv6 Client in Autoconfig Mode | **274**

Configuring TCP/IP Propagation on a DHCPv6 Client | **275**

6 DHCP with External Authentication Server

DHCP with External Authentication Server | 277

Using External AAA Authentication Services to Authenticate DHCP Clients | 277

Steps to Configure DHCP with External Authentication Server | 278

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | 279

Example-Configuring DHCP with External Authentication Server | 280

Specifying Authentication Support | 281

Creating Unique Usernames for DHCP Clients | 282

Grouping Interfaces with Common DHCP Configurations | 285

Centrally Configure DHCP Options on a RADIUS Server | 288

7 Managing DHCP Services

Group-Specific DHCP Configurations | 294

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces | 294

Configuring Group-Specific DHCP Local Server Options | 296

Configuring Group-Specific DHCP Relay Options | 296

Configuring DHCP Server Configuration with Optional Pool Matching Using Groups | 298

DHCP Snooping | 299

DHCP Snooping Support | 299

Example: Configuring DHCP Snooping Support for DHCP Relay Agent | 302

Requirements | 302

Overview | 302

Configuration | 303

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | 305

DHCP Auto Logout | 308

DHCP Auto Logout Overview | 308

Automatically Logging Out DHCP Clients | 310

Additional Configurations for DHCP Clients | 312

Specifying the Maximum Number of DHCP Clients Per Interface | **312**

DHCP Local Server Handling of Client Information Request Messages | **313**

Enabling Processing of Client Information Requests | **314**

Sending Release Messages When Clients Are Deleted | **315**

Dynamic Reconfiguration of DHCP Servers and Clients | 317

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients | **317**

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview | **321**

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings | **322**

Configuring Dynamic Reconfiguration Attempts for DHCP Clients | **323**

Configuring Deletion of the Client When Dynamic Reconfiguration Fails | **324**

Configuring a Token for DHCP Local Server Authentication | **325**

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | **326**

DHCP Liveness Detection | 327

DHCP Liveness Detection Overview | **328**

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD | **330**

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | **332**

Requirements | **332**

Overview | **333**

Configuration | **333**

Configuring Detection of DHCP Local Server Client Connectivity with BFD | **336**

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | **338**

Requirements | **339**

Overview | **339**

Configuration | **339**

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | **343**

How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works | **343**

Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets | **348**

Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets | **351**

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets | **354**

Secure DHCP Message Exchange | 355

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs | **355**

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances | **356**

Client-Side Support | **358**

Server-Side Support | **358**

DHCP Local Server Support | **359**

DHCP Active Server Groups | 360

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups | **361**

Suppressing DHCP Routes | 365

Suppressing DHCP Access, Access-Internal, and Destination Routes | **365**

Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | **366**

8 **Configuration Statements and Operational Commands**

Junos CLI Reference Overview | 369

About This Guide

Dynamic Host Configuration Protocol (DHCP) is a standardized client/server network protocol that dynamically assigns IP addresses and other related configuration information to network devices. On Junos OS devices, DHCP provides a framework for passing configuration information to clients and provides reusable network addresses and configuration options to the hosts. Use the topics on this guide to configure essential DHCP features for your system.

1
CHAPTER

Overview

DHCP Overview | 2

DHCP Access Service Overview | 9

Legacy DHCP and Extended DHCP | 16

DHCP Overview

SUMMARY

Learn about Dynamic Host Configuration Protocol (DHCP), a network management protocol where a DHCP server dynamically assigns an IP address and other network configuration parameters to end hosts in the network to facilitate communication among the endpoints.

IN THIS SECTION

- Benefits of DHCP | 2
- Introduction to DHCP | 3
- Understand DHCP | 3

Benefits of DHCP

Benefits of DHCP include:

- DHCP enables network administrators centrally manage a pool of IP addresses among hosts and automate the assignment of IP addresses in a network.
- DHCP help you reduce the number of IP addresses needed on the network when you use it to manage a pool of IP addresses among hosts. DHCP does this by leasing an IP address to a host for a limited period of time, allowing the DHCP server to share a limited number of IP addresses.
- DHCP minimizes the overhead required to add clients to the network by providing a centralized, server-based setup, which means that you do not have to manually create and maintain IP address assignments for clients.
- DHCP provides a central database of devices that are connected to the network and eliminates duplicate resource assignments.
- DHCP automates network-parameter assignment to network devices. Even in small networks, DHCP is useful because it makes it easy to add new machines to the network.
- DHCP provides other configuration information, particularly the IP addresses of local caching Domain Name System (DNS) resolvers, network boot servers, or other service hosts in addition to IP addresses for clients.
- DHCP on the Junos OS device can automatically upgrade software on client systems.

Introduction to DHCP

Dynamic Host Configuration Protocol (DHCP) is a network management protocol used in TCP/IP networks to dynamically assign IP addresses and other related configuration information to network devices.

On Junos OS devices, DHCP provides:

- A framework for passing configuration information to clients in the subnet.
- Reusable network addresses and configuration options to Internet hosts.

DHCP is based on BOOTP, a bootstrap protocol that allows a client to discover its own IP address, the IP address of a server host, and the name of a bootstrap file. DHCP servers can handle requests from BOOTP clients, but provide additional capabilities beyond BOOTP, such as the automatic allocation of reusable IP addresses and additional configuration options.

The Juniper Networks device acts as the DHCP server, providing IP addresses and settings to hosts that are connected to the device interfaces. The DHCP server is compatible with the DHCP servers of other vendors on the network. The device can also operate as a DHCP client and DHCP relay agent.

Understand DHCP

IN THIS SECTION

- DHCP Use Cases | 3
- DHCP Components | 4
- DHCP Client and Server Model | 5
- DHCP Client, Server, and Relay Agent Model | 7
- DHCP Conflict Detection and Resolution | 8
- Enable a DHCP Local Server, DHCP Relay Agent, and DHCP Client in a Routing Instance | 8

DHCP Use Cases

- In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.

- In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.
- In a typical branch network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the device between the DHCP client and one or more DHCP local servers.

DHCP Components

The DHCP architecture consists DHCP servers, DHCP clients, and DHCP relay agents. The client interacts with servers using DHCP messages in a DHCP conversation to obtain and renew IP address leases and network configuration parameters. Here is a brief description of the DHCP components:

DHCP Server

A DHCP server is a device or server in the network that automatically assigns IP addresses and other network parameters to client devices. A Junos OS device acting as a DHCP server is compatible with DHCP servers from other vendors on the network.

DHCP server assigns the following configuration parameters to client device:

- Provides temporary IP addresses from an IP address pool to all clients on a specified subnet (dynamic binding)
- Assigns permanent IP addresses to specific clients based on their media access control (MAC) addresses (static binding).
- Assigns following configuration parameters:
    - IP address
    - Subnet mask
    - Default gateway for the network
    - DNS server
- A DHCP server provides persistent storage of network parameters for clients. Because DHCP is an extension of BOOTP, DHCP servers can handle BOOTP requests.

The server does not support IPv6 address assignment, user class-specific configuration, DHCP failover protocol, dynamic DNS updates, or VPN connections. The Junos-FIPS software does not support the DHCP server.

NOTE: You cannot configure a router as a DHCP server and a BOOTP relay agent at the same time.

DHCP Client

A DHCP client is any IP device connected in the network that is configured to act as a host requesting configuration parameters such as an IP address from a DHCP server.

A Juniper Networks device acting as a DHCP client receives its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP Relay

DHCP relay agent is any TCP/IP host that forwards DHCP messages between servers and clients when DHCP client and a DHCP server reside in different subnets. For example, in large network that has multiple subnets, a single DHCP server can serve all the clients in the entire network with help of DHCP relay agents located on the interconnecting routers.

You can configure a Junos OS device either as a DHCP server or as a DHCP relay server, but not both. Whereas a DHCP server replies to a client with an IP address, a DHCP relay server relays DHCP messages to and from the configured DHCP server, even if the client and server are on different IP networks. Configure a device to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

DHCP Client and Server Model

DHCP IP address allocation works on a client/server model in which the server, in this case a Junos OS, assigns the client reusable IP information from an address pool. A DHCP client might receive offer messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 1 on page 6.

Figure 1: DHCP Client/Server Model

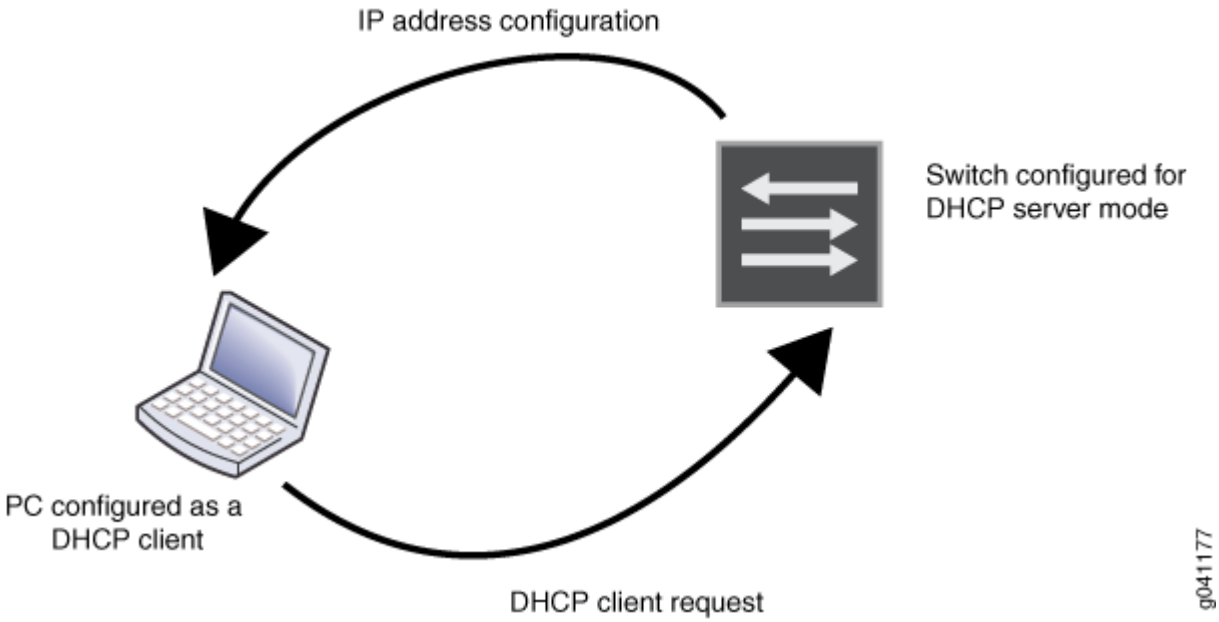
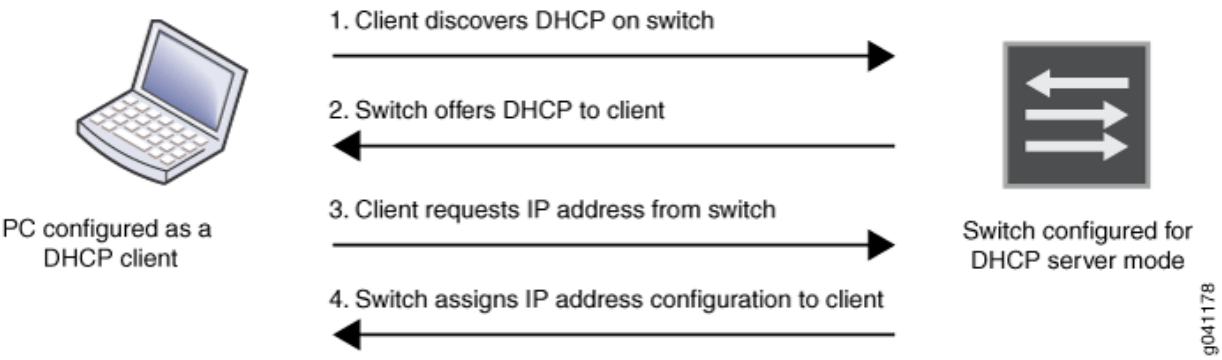


Figure 2: DHCP Four-Step Transfer



DHCP consists of a four-step transfer process beginning with a broadcast DHCP discovery message from the client. As the second step, the client receives a DHCP offer message from the server. This message includes the IP address and mask, and some other specific parameters. The client then sends a DHCP request message to accept the IP address and other parameters that it received from the server in the previous step. The DHCP server sends a DHCP response message and removes the now-allocated address from the DHCP address pool. See Figure 2 on page 6.

NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you

might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

The device supports DHCP client requests received on any Ethernet interface. DHCP requests received from a relay agent are supported on all interface types. DHCP is not supported on interfaces that are part of a virtual private network (VPN).

DHCP Client, Server, and Relay Agent Model

The DHCP relay agent is located between a DHCP client and DHCP server and forwards DHCP messages between servers and clients as following:

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to

determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

DHCP Conflict Detection and Resolution

A client that receives an IP address from the device operating as a DHCP server performs a series of Address Resolution Protocol (ARP) tests to verify that the address is available and no conflicts exist. If the client detects an address conflict, it informs the DHCP server about the conflict and can request another IP address from the DHCP server.

The device maintains a log of all client-detected conflicts and removes addresses with conflicts from the DHCP address pool. To display the conflicts list, you use the `show system services dhcp conflict` command. The addresses in the conflicts list remain excluded until you use the `clear system services dhcp conflict` command to manually clear the list.

Enable a DHCP Local Server, DHCP Relay Agent, and DHCP Client in a Routing Instance

The following considerations apply when you enable a DHCP local server, DHCP relay agent, or DHCP client in a routing instance:

- The DHCP local server, DHCP relay agent, and DHCP client can be configured in one routing instance, but the functionality is mutually exclusive on one interface. If the DHCP client is enabled on one interface, the DHCP local server or the DHCP relay agent cannot be enabled on that interface.
- The DHCP client, DHCP relay agent and DHCP local server services act independently in their respective routing instance. The following features can function simultaneously on a device:
  - DHCP client and DHCP local server
  - DHCP client and DHCP relay agent
  - Multiple routing instances. Each instance can have a DHCP local server, DHCP relay agent, or DHCP client, or each routing instance can have a DHCP client and DHCP local server or a DHCP client and DHCP relay agent.
- Before you enable DHCP services in a routing instance, you must remove all the configuration related to DHCP services that does not include routing instance support. If you do not do this, the old default routing instance configuration will override the new routing instance configuration.
- On all SRX Series Firewalls, logical systems and routing instances are not supported for a DHCP client in chassis cluster mode.

RELATED DOCUMENTATION

DHCP Server | 49
DHCP Relay Agent | 153
DHCP Client | 245

DHCP Access Service Overview

IN THIS SECTION

IP Address Assignments | 9
DHCP Address Allocation Methods | 12
DHCP Lease Time Management | 13
DHCP Options | 13

DHCP access service consists of two components:

- A method for allocating network addresses to a client host
- A protocol for delivering host-specific configuration information from a server to a client host

For more information, read this topic.

IP Address Assignments

IN THIS SECTION

Network Address Assignments (Allocating a New Address) | 10
Network Address Assignments (Reusing a Previously Assigned Address) | 12

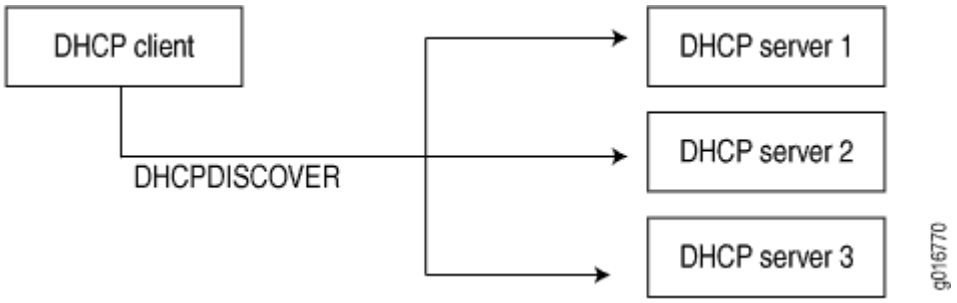
The following topics describe IP address assignment in detail:

Network Address Assignments (Allocating a New Address)

To receive configuration information and a network address assignment, a DHCP client negotiates with DHCP servers in a series of messages. The following steps show the messages exchanged between a DHCP client and servers to allocate a new network address. When allocating a new network address, the DHCP process can involve more than one server, but only one server is selected by the client.

1. When a client computer is started, it broadcasts a `DHCPDISCOVER` message on the local subnet, requesting a DHCP server. This request includes the hardware address of the requesting client.

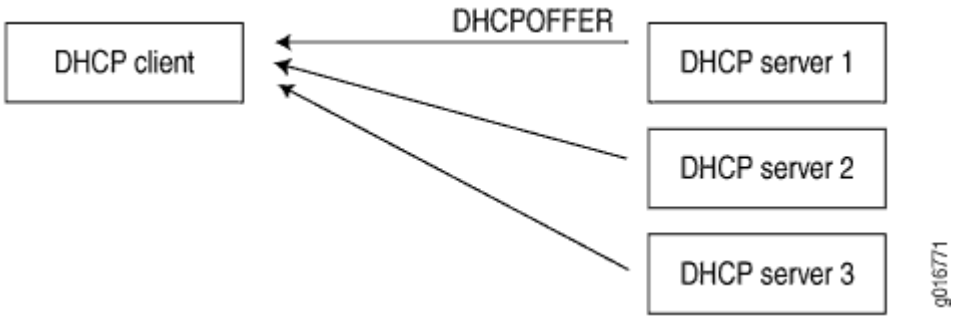
Figure 3: DHCP Discover



> **NOTE**: For improved operation with DHCP clients that do not strictly conform to RFC 2131, the DHCP server accepts and processes `DHCPDISCOVER` messages even if the overload options in the messages are not properly terminated with an `end` statement.

2. Each DHCP server receiving the broadcast sends a `DHCPOFFER` message to the client, offering an IP address for a set period of time, known as the lease period.

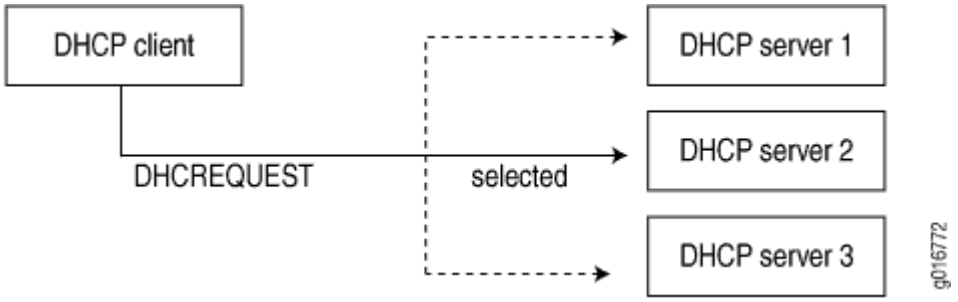
Figure 4: DHCP Offer



3. The client receives one or more DHCPOFFER messages from one or more servers and selects one of the offers received. Normally, a client looks for the longest lease period.

4. The client broadcasts a DHCPREQUEST message indicating the client has selected an offered leased IP address and identifies the selected server.

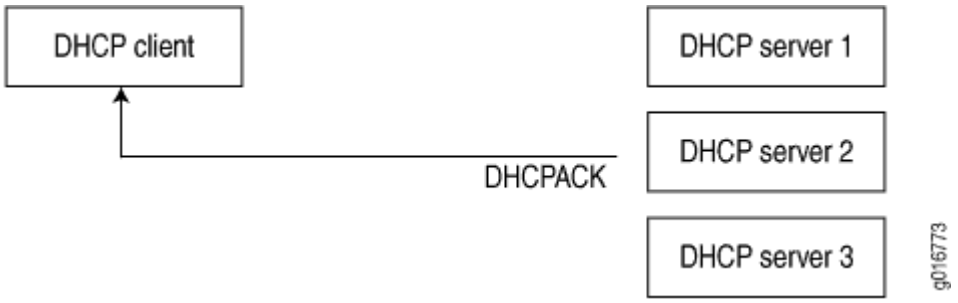
Figure 5: DHCP Request



5. Those servers not selected by the DHCPREQUEST message return the unselected IP addresses to the pool of available addresses.

6. The selected DHCP server sends a DHCPACK acknowledgment that includes configuration information such as the IP address, subnet mask, default gateway, and the lease period.

Figure 6: DHCP ACK



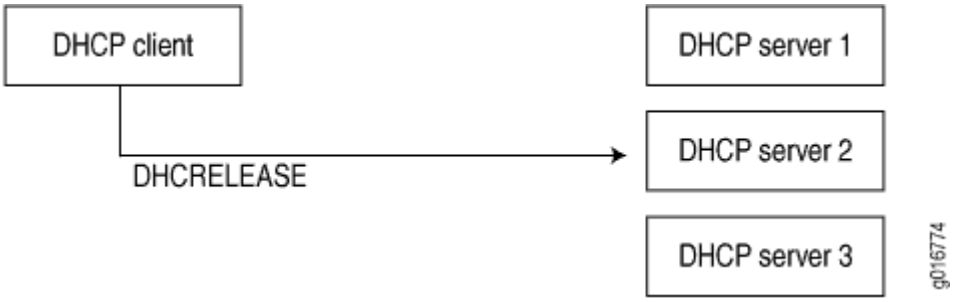
The information offered by the server is configurable.

7. The client receives the DHCPACK message with configuration information. The process is complete. The client is configured and has access to the network.

   - If the client receives a DHCPNAK message (for example, if the client has moved to a new subnet), the client restarts the negotiation process.

- The client can relinquish its lease on a network address by sending a `DHCPRELEASE` message to the server (for example, when the client is restarted). When the server receives the `DHCPRELEASE` message, it marks the lease as free and the IP address becomes available again.

Figure 7: DHCP Release



Network Address Assignments (Reusing a Previously Assigned Address)

To enable reuse of a previously allocated network address, the following events occur:

1. A client that previously had a lease broadcasts a `DHCPREQUEST` message on the local subnet.
2. The server with knowledge of the client's configuration responds with a `DHCPACK` message.
3. The client verifies the DHCP configuration information sent by the server and uses this information to reestablish the lease.

DHCP Address Allocation Methods

A DHCP server either assigns or sends an IP address to a client in following two ways:

- **Dynamic bindings**—The DHCP server assigns a reusable IP address from a pool of IP addresses to a client for a specific period of time. This method of address allocation is useful when the clients need only temporary access to the network.

- **Static bindings**—The DHCP server assigns IP addresses to the client which are permanent. You can reserve an address which is used by DHCP server to assign to a particular client based on it's media access control (MAC) addresses.

  Static allocation is useful if you have a printer on a LAN and you do not want its IP address to keep changing

You can configure a DHCP server to include both address pools and static bindings. Static bindings take precedence over dynamic bindings. See "IP Address Assignment Pool" on page 27 for more information.

DHCP Lease Time Management

DHCP lease is a temporary assignment of IP address to a device on the network. The IP address information assigned is only valid for a limited period of time, and is known as a DHCP lease.

When using DHCP server to manage a pool of IP addresses, it “rents” IP address to various clients for specific period of time. Thus, IP addresses managed by a DHCP server are only assigned for a limited period of time. When the lease expires, the client can no longer use the IP address and has to stop all communication with the IP network unless he requests to extend the lease “rent” via the DHCP lease renewal cycle.

If a client does not use its assigned address for some period of time, the DHCP server can assign that IP address to another client.

When assignments are made or changed, the DHCP server updates information in the DNS server. The DHCP server provides clients with their previous lease assignments whenever possible.

DHCP Options

IN THIS SECTION

- Setting DHCP Options | **14**
- How DHCP Provides Minimum Network Configuration | **15**

DHCP options are tagged data items identified by Option Numbers that can be included in the request or in the acknowledgment to pass information between a client and server. The options are sent in a variable-length field at the end of a DHCP message. A DHCP client can use DHCP options to negotiate with the DHCP server and limit the server to send only those options that client requests.

DHCP allows the client to receive options from the DHCP server describing the network configuration and various services that are available on the network. DHCP options are used by a client to configure itself dynamically during its booting procedure.

In a typical DHCP client-server settings, the DHCP client sends a DHCP Request to a DHCP server and receives back a DHCP Acknowledgment. The DHCP request can contain information about the client and requests for additional information from the server. The DHCP Acknowledgment contains the IP address assigned to the client by the server along with any additional information as requested by the client.

Table 1 on page 14 lists commonly used DHCP options.

Table 1: Commonly Used DHCP Options

Parameter	Equivalent DHCP Option
List of Domain Name servers (DNS) and NetBIOS servers	DHCP option 6
List of gateway routers	DHCP option 3
The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.	DHCP option 15
Subnet mask for client IP address	DHCP option 1
DHCP server identification	DHCP option 54
Parameter Request List	DHCP option 55
IP address of the boot server and the filename of the boot file to use	DHCP option 67

DHCP options are defined in RFC 2132, DHCP Options and BOOTP Vendor Extensions.

Setting DHCP Options

DHCP option statements always start with the option keyword, followed by an option name, followed by option data.

```
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

Extended DHCP

```
[edit access address-assignment pool pool-name family inet]
dhcp-attributes {
    option 19 flag false;
    option 40 string domain.tld;
    option 16 ip-address 10.3.3.33;
}
```

Legacy DHCP

```
[edit system services dhcp]
option 19 flag off; # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

How DHCP Provides Minimum Network Configuration

The DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

- Router—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
- Domain name—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
- Domain name server—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

Legacy DHCP and Extended DHCP

IN THIS SECTION

- Understanding Differences Between Legacy DHCP and Extended DHCP | 16
- DHCP Statement Hierarchy and Inheritance | 20
- Difference in Legacy DHCP Relay and Extended DHCP Relay | 24
- Restrictions in Using Legacy DHCP and Extended DHCP | 24

JDHCP or extended DHCP is the enhanced versions of the DHCP daemon available in the recent versions of Junos OS (non-EoL Junos releases). To find out the extended DHCP support for specific Junos OS release, see Feature Explorer.

Legacy DHCP functionality is deprecated—rather than immediately removed—to provide backward compatibility and an opportunity to bring your configuration into compliance with the new configuration.

Read this topic to understand the new enhancements and the changes done in CLI configuration statement syntax.

Understanding Differences Between Legacy DHCP and Extended DHCP

IN THIS SECTION

- New Features and Enhancements in Extended DHCP | 17
- Benefits of Extended DHCP | 19
- Change in Configuring DHCP Local Server in Extended DHCP Environment | 19
- Legacy DHCP and Extended DHCP Server Hierarchy Levels Changes | 19

This topic covers the following sections:

New Features and Enhancements in Extended DHCP

Extended DHCP or JDHCP extends and enhances traditional DHCP operation. With the extended DHCP local server, the client configuration information resides in a centralized address-assignment pool, which supports advanced pool matching and address range selection. aAny new features are only added to the Extended DHCP. Extended DHCP supports following features and enhancements:

- In extended DHCP, the address-assignment pools are external to the DHCP local server. The external address-assignment pools are managed by the **authd** process, independently of the DHCP local server, and can be shared by different client applications such as DHCP or PPPoE access. In legacy DHCP, client address pool and client configuration information reside on the DHCP server.
- Extended DHCP server interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication.
- You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.
- Extended DHCP local server supports IPv6 clients.
- Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.
- The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:
    - **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
    - **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
    - **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.
- You can configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

- The extended DHCP server supports following features:
  - *Graceful Routing Engine switchover* (GRES), which provides mirroring support for clients.
  - Virtual routing and forwarding (VRF). The extended DHCP is also referred to as virtual router (VR) aware DHCP. See EX Series Switch Software Features Overview for a list of switches that support extended DHCP (VR-aware DHCP).

Table 2 on page 18 provides a comparison of the extended DHCP and a legacy DHCP configuration options.

Table 2: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

Feature	Legacy DHCP Local Server	Extended DHCP Local Server
Local address pools	X	X
External, centrally-managed address pools	–	X
Local configuration	X	X
External configuration using information from address-assignment pools or RADIUS servers	–	X
Dynamic-profile attachment	–	X
RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs	–	X
IPv6 client support	–	X
Default minimum client configuration	X	X

Benefits of Extended DHCP

- Extended DHCP local server enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment.
- Extended DHCP local server enables service providers to take advantage of external address-assignment pools and integrated RADIUS-based configuration capabilities in addition to the continued support of traditional local address pools.

Change in Configuring DHCP Local Server in Extended DHCP Environment

In extended DHCP, use the following steps to configure DHCP server and address assignment pool:

- Configure the extended DHCP local server on the device and specify how the DHCP local server determines which address-assignment pool to use.
- Configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients.

The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Legacy DHCP and Extended DHCP Server Hierarchy Levels Changes

Legacy DHCP and extended DHCP servers can be configured at the hierarchy levels shown in Table 3 on page 19:

Table 3: Legacy DHCP and Extended DHCP Server Hierarchy Levels

DHCP Service	Hierarchy
Legacy DHCP server	`edit system services dhcp`
Extended DHCP server	`edit system services dhcp-local-server`
Legacy DHCP relay	`edit forwarding-options helpers bootp`
Extended DHCP relay	`edit forwarding-options dhcp-relay`

Table 3: Legacy DHCP and Extended DHCP Server Hierarchy Levels *(Continued)*

DHCP Service	Hierarchy
Legacy DHCP address pool	`edit system services dhcp pool`
Extended DHCP address pool	`edit access address-assignment pool`

Since legacy DHCP is deprecated, that is, the commands are 'hidden' . These commands do not show in the help nor automatic completion. When you use the option `show configuration` to display your configuration, the system displays the following warning:

```
##     ## Warning: configuration block ignored: unsupported platform (...)     ##
```

DHCP packets on non-configured interfaces are dropped

Once you enable DHCP-Relay on the MX routers, or QFX or EX switches, the DHCP Snooping feature gets enabled and all DHCP packets incoming through any interface (both configured and unconfigured interface) of the device are analyzed. The interfaces that are not listed under the DHCP configuration are considered ‘unconfigured’.

Depending on the configuration, DHCP packets received on unconfigured interfaces are dropped.

If the DHCP packets are dropped on ‘unconfigured’ interface, the DHCP traceoptions report it as:

```
May 25 18:26:31.796241 [MSTR][NOTE] [default:default][RLY][INET][irb.82] jdhcpd_packet_handle:
BOOTPREQUEST irb.82 arrived on unconfigured interface DISCOVER, flags 23, config 0x0
```

Some behaviors specific for some platforms have changed along the releases. See, Release Notes.

DHCP Statement Hierarchy and Inheritance

Junos OS devices support two syntax styles for configuring DHCP Client, Server, and Relay—for legacy DHCP and extended DHCP. Table 4 on page 21, Table 5 on page 21, and Table 6 on page 23 provide differences in hierarchies for configuring some common features.

Table 4: DHCP Client Configuration - Difference in Legacy DHCP and Extended DHCP Server Hierarchy Levels

Legacy DHCP	Extended DHCP
Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet dhcp]	Hierarchy Level: [edit interfaces interface-name unit logical-unit-number family inet dhcp-client]
client-identifier • ascii • hexadecimal	client-identifier • userid ascii • userid hexadecimal

Table 5: DHCP Server Configuration - Difference in Legacy DHCP and Extended DHCP Server Hierarchy Levels

Legacy DHCP	Extended DHCP
Hierarchy Level: • [edit system services dhcp] • [edit system services dhcp pool]	Hierarchy Level: [edit access address-assignment pool *pool-name* family inet]
subnet-ip-address/mask	network
address-range	range
static-binding • mac-address • fixed-address	host *host-name* • hardware-address • ip-address
[edit system services dhcp pool subnet-ip-address/mask]	[edit access address-assignment pool *pool-name* family inet dhcp-attributes]

Table 5: DHCP Server Configuration - Difference in Legacy DHCP and Extended DHCP Server Hierarchy Levels *(Continued)*

Legacy DHCP	Extended DHCP
boot-file	boot-file
boot-server	boot-server
default-lease-time	maximum-lease-time
domain-name	domain-name
domain-search	option 119 string
exclude-address	excluded-address
maximum-lease-time	maximum-lease-time seconds
name-server	*name-server*
next-server	next-server
router	router
option	option
propagate-ppp-settings	propagate-ppp-settings
server-identifier	server-identifier
sip-server • address • name	sip-server • address • name

Table 5: DHCP Server Configuration - Difference in Legacy DHCP and Extended DHCP Server Hierarchy Levels *(Continued)*

Legacy DHCP	Extended DHCP
wins-server	wins-server
Hierarchy Level: `[edit system services dhcp]`	Hierarchy Level: `[edit access address-assignment pool pool-name family inet]`
option	option
byte-stream	hex-string

Table 6: DHCP Relay Configuration - Difference in Legacy DHCP and Extended DHCP Server Hierarchy Levels

Legacy DHCP	Extended DHCP
Hierarchy Level: `[edit forwarding-options helpers bootp]`	Hierarchy Level: `[edit forwarding-options dhcp-relay]`
dhcp-option-82	*relay-option-82*
interface interface-name	group group-name
relay-agent-option	relay-option-82
server	*server-group*

Note if you are using legacy DHCP—In legacy DHCP, DHCP configuration statements are organized hierarchically. Statements at the top of the hierarchy apply to the DHCP server and network, branches contain statements that apply to address pools in a subnetwork, and leaves contain statements that apply to static bindings for individual clients.

To minimize configuration changes, include common configuration statements shown in tables above. For example, include the `domain-name` statement at the highest applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited

from a higher level. For example, if a statement appears at both the `[edit system services dhcp]` and `[edit system services dhcp pool]` hierarchy levels, the value assigned to the statement at the `[edit system services dhcp pool]` level takes priority.

Difference in Legacy DHCP Relay and Extended DHCP Relay

Legacy DHCP Relay can work as a DHCP IP helper, forwarding DHCP packets from DHCP servers to all interfaces. Extended DHCP Relay cannot work as an DHCP IP helper; it can leverage Option-82 to forward DHCP packets from DHCP server. See "DHCP Relay Agent Information Option (Option 82)" on page 198.

Restrictions in Using Legacy DHCP and Extended DHCP

IN THIS SECTION

- Features Not Supported by Extended DHCP | **25**

Remember the following items while configuring extended DHCP:

- You can configure extended DHCP server and DHCP relay agent and legacy DHCP server and DHCP relay agent in the same network.
- You cannot configure extended DHCP server and DHCP relay agent and legacy DHCP server and DHCP relay agent on the same device. Because the newer extended DHCP server version has more features, we recommend that you configure the extended DHCP server if it is supported by the switch. A commit error is displayed if both legacy DHCPD and extended DHCP is configured simultaneously.
- DHCP clients on a switch are always configured at the hierarchy level `[edit interfaces` *`interface-name`* `family dhcp]`.
- If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Features Not Supported by Extended DHCP

- Legacy DHCP supports the circuit ID and the remote ID fields for the relay agent option (option 82). Extended DHCP for the relay agent option supports only circuit ID. For more information on option 82, see "Using DHCP Relay Agent Option 82 Information" on page 199.
- In Junos Release 12.1X46, autoinstallation is not compatible with JDHCPd:

```
version 12.1X46-D40.2;
system {
    /* not compatible with jDHCPd */   <<<<<<
    autoinstallation {
        usb {
            disable;
        }
    }
```

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information | 199

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

DHCP Client | 245

2

CHAPTER

Address Assignment Pool

IP Address Assignment Pool | 27

DHCPv6 Address-Assignment Pools | 39

IP Address Assignment Pool

IN THIS SECTION

- Address-Assignment Pools Overview | 27
- Extended DHCP Local Server and Address-Assignment Pools | 30
- Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools | 31
- Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use | 32
- Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option | 34
- Configuring Address-Assignment Pools | 34
- Configuring an Address-Assignment Pool Name and Addresses | 35
- Configuring a Named Address Range for Dynamic Address Assignment | 35
- Configuring Static Address Assignments | 36
- Configuring Address-Assignment Pool Linking | 37
- Configuring DHCP Client-Specific Attributes for Address-Assignment Pools | 37

Address pool is a set of Internet Protocol (IP) addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You can create centralized IPv4 and IPv6 address pools independently of the client applications that use the pools. For more information, read this topic.

Address-Assignment Pools Overview

IN THIS SECTION

- Address Assignment Types | 28
- Named Address Ranges in Address Assignment Pool | 28
- Address Allocation from Linked Address Pools | 28
- Address Pool Hold-Down State | 29

- Address-Assignment Pool for Neighbor Discovery Router Advertisement | 29
- Excluding Specified Address or Address Range | 29
- Licensing Requirement | 30
- Benefits of Address Assignment Pools | 30

The address-assignment pool enables you to create centralized IPv4 and IPv6 address pools independent of the client applications that use the pools. The authd process manages the pools and the address allocation, whether the addresses come from local pools or from a RADIUS server.

For example, multiple client applications, such as DHCP, can use the same address-assignment pool to provide addresses for their particular clients. Client applications can acquire addresses for either authenticated or unauthenticated clients. The pool selected for a subscriber, based on the RADIUS server or network matching or other rule, is called the matching pool for the subscriber.

Address Assignment Types

Address-assignment pools support both dynamic and static address assignment. In dynamic address assignment, a client is automatically assigned an address from the address-assignment pool. In static address assignment, which is supported for IPv4 pools only, you reserve an address that is then always used by a particular client. Addresses that are reserved for static assignment are removed from the dynamic address pool and cannot be assigned to other clients.

Named Address Ranges in Address Assignment Pool

You can configure named address ranges within an address-assignment pool. A named range is a subset of the overall address range. A client application can use named ranges to manage address assignment based on client-specific criteria. For example, for IPv4 address-assignment pools, you might create a named range that is based on a specific DHCP option 82 value. Then, when a DHCP client request matches the specified option 82 value, an address from the specified range is assigned to the client.

Address Allocation from Linked Address Pools

You can link address-assignment pools together to provide backup pools for address assignment. When no addresses are available in the primary or in the matching address pool, the device automatically proceeds to the linked (secondary) address pool to search for an available address to allocate.

Although the first pool in a chain of linked pools is generally considered the primary pool, a matching pool is not necessarily the first pool in the chain.

Starting in Junos OS Release 18.1R1, search mechanism for an available address proceeds through a chain of linked pools. This behavior enables the DHCP to search addresses contiguously..

Lets use an example on how the search mechanism works. Consider a chain of three pools— A, B, and C. Pool A is the primary pool, Pool B is the matching pool for certain subscribers based on information returned by the RADIUS server. The search for an available address for those subscribers uses the following sequence:

- By default, the matching pool (Pool B) is searched first.
- The search moves to the first pool (Pool A) in the chain if address not found.
- The search proceeds through the chain (Pool C) until an available address is found and allocated, or until the search determines no addresses are free.
- In each pool, all address ranges are fully searched for an address.

You can configure the `linked-pool-aggregation` statement to start searching within a block of addresses in each range in the matching pool and then successively through the linked pools. The search then moves back to the first pool in the chain and searches all addresses in all ranges in each pool through the last pool in the chain.

Address Pool Hold-Down State

You can configure an address-assignment pool in hold-down state. When the address pool is in hold-down state, the pool is no longer available to allocate IP addresses for the subscribers. This configuration gracefully transforms the active pool to an inactive state as the previously allocated addresses are returned to the pool. When the pool is inactive, you can safely perform maintenance on the pool without affecting any active subscribers.

Address-Assignment Pool for Neighbor Discovery Router Advertisement

You can explicitly allocate an address-assignment pool for Neighbor Discovery Router Advertisement (NDRA).

Excluding Specified Address or Address Range

Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool.

For example, you might want to reserve certain addresses or ranges to be used only for static subscribers. When you configure an address or range to be excluded, and the address or an address within the range, has already been allocated, that subscriber is logged out, the address is deallocated, and the address is marked for exclusion.

Licensing Requirement

This feature requires a license. To understand more about Subscriber Access Licensing , see Subscriber Access Licensing Overview. Please refer to the Juniper Licensing Guide for general information about License Management. Please refer to the product Data Sheets for details, or contact your Juniper Account Team or Juniper Partner.

Benefits of Address Assignment Pools

- The address-assignment pool feature supports both subscriber management and DHCP management.
- You can create centralized pools of addresses independent of client applications.
- You can specify blocks of addresses, named ranges, so that a given address pool can be used to supply different addresses for different client applications or for subscribers that match different sets of criteria.
- You can link pools together to ensure that pools are searched for free addresses in a specific manner, contiguously or noncontiguously.
- You can gracefully transition an address pool from active to inactive by specifying that no further addresses are allocated from the pool.

Extended DHCP Local Server and Address-Assignment Pools

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order.

In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use.

In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See *Address-Assignment Pool Configuration Overview* for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools

The pattern of interaction between the DHCP local server, the DHCP client, and address-assignment pools is the same regardless of whether you are using a router or a switch. However, there are some differences in the details of usage.

- On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer or customer premises equipment (CPE), and the DHCP local server is configured on the router.
- On switches—In a typical network configuration, the DHCP client is on an access device, such as a personal computer, and the DHCP local server is configured on the switch.

The following steps provide a high-level description of the interaction among the DHCP local server, DHCP client, and address-assignment pools:

1. The DHCP client sends a discover packet to one or more DHCP local servers in the network to obtain configuration parameters and an IP address for the subscriber (or DHCP client).
2. Each DHCP local server that receives the discover packet then searches its address-assignment pool for the client address and configuration options. Each local server creates an entry in its internal client table to keep track of the client state, then sends a DHCP offer packet to the client.
3. On receipt of the offer packet, the DHCP client selects the DHCP local server from which to obtain configuration information and sends a request packet indicating the DHCP local server selected to grant the address and configuration information.
4. The selected DHCP local server sends an acknowledgement packet to the client that contains the client address lease and configuration parameters. The server also installs the host route and ARP entry, and then monitors the lease state.

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

You can specify the match order in which the extended DHCP local server uses the client data to determine the address-assignment pool that provides the IP address and configuration for a DHCP client. If you do not specify any pool match order, the device uses the default IP address configured in IP address first matching option to select the address pool.

Example:

```
[edit system services dhcp-local-server]
user@host# set pool-match-order
```

You can specify the order for pool matching methods. You can specify the methods in any order. All methods are optional. IP address first method is default method.

- IP address first—Default option. The server selects the address-assignment pool to use by matching the IP address in the client DHCP request with the network address of the address-assignment pool.
  - If the client request contains the gateway IP address (giaddr), the local server matches the giaddr to the address-assignment pool's address.
  - If the client request does not contain the giaddr, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

  Example:

  ```
  [edit system services dhcp-local-server pool-match-order]
  user@host# set ip-address-first
  ```

- External authority—The DHCP local server receives the address assignment from an external authority, such as RADIUS or Diameter.
  - If RADIUS is the external authority, the DHCP local server uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool.
  - If Diameter is the external authority, the server uses the Diameter counterpart of the Framed-IPv6-Pool attribute to determine the pool.

Example:

```
[edit system services dhcp-local-server pool-match-order]
user@host# set external-authority
```

- Option 82—For IPv4 address-Extended DHCP local server matches the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.

  Example:

  ```
  [edit system services dhcp-local-server pool-match-order]
  user@host# set option-82
  ```

  To use the DHCP local server option 82 matching feature with an IPv4 address-assignment pool, you must ensure that the `option-82` statement is included in the `dhcp-attributes` statement for the address-assignment pool.

This example shows an extended DHCP local server configuration that includes optional IPv4 address-assignment pool matching and interface groups. For pool matching, this configuration specifies that the DHCP local server first check the response from an external authentication authority (for example, RADIUS) and use the Framed-IPv6-Pool attribute to determine the address-assignment pool to use for the client address. If no external authority match is found, the DHCP local server then uses ip-address-first matching together with the option 82 information to match the named address range for client IPv4 address assignment. The option 82 matching must also be included in the address-assignment pool configuration.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        external-authority
        ip-address-first;
```

```
        option-82;
    }
}
```

Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option

Subscriber management or DHCP management enables you to specify that DHCP local server assign a particular address to a client. For example, if a client is disconnected, you might use this capability to assign the same address that the client was using prior to being disconnected. If the requested address is available, DHCP assigns it to the client. If the address is unavailable, the DHCP local server offers another address, based on the address allocation process.

Both DHCP local server and DHCPv6 local server support the specific address request feature. DHCP local server uses DHCP option 50 in DHCP discover messages to request a particular address, while DHCPv6 local server uses the IA_NA option (Identity Association for Non-Temporary Addresses) in DHCPv6 solicit messages.

NOTE: Subscriber management (DHCP management) supports only one address for each of the DHCPv6 IA_NA or IA_PD address types. If the DHCPv6 client requests more than one address for a given type, the DHCPv6 local server uses only the first address and ignores the other addresses.

Configuring Address-Assignment Pools

The address-assignment pool feature enables you to create address pools that can be shared by different client applications such as DHCPv4 or DHCPv6.

To configure an address-assignment pool, use the following order. The following procedures are tested on for SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

1. Configure the address-assignment pool name and specify the addresses for the pool.
2. (Optional) Configure named ranges (subsets) of addresses.
3. (Optional; IPv4 only) Create static address bindings.
4. (Optional) Configure attributes for DHCP clients.

Configuring an Address-Assignment Pool Name and Addresses

When configuring an address-assignment pool on devices, you must specify the name of the pool and its addresses.

To configure an IPv4 address-assignment pool:

1. Configure the name of the pool and specify the IPv4 family.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the network address and the prefix length of the addresses in the pool.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set network 192.168.0.0/16
```

NOTE: You can configure an IPv4 address-assignment pool in a routing instance by configuring the address-assignment statements at the`[edit routing-instance routing-instance-name]` hierarchy level. For example `[edit routing-instances routing-instances name access address-assignment pool blr-pool family inet]`. The above steps shows only the `[edit access]` configuration.

Configuring a Named Address Range for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets, of addresses within an address-assignment pool. During a dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range.

This example is tested on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices.

To create a named range within an IPv4 address-assignment pool:

1. Specify the name of the address-assignment pool.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit access address-assignment pool isp_1 family inet]
user@host# set range southeast low 192.168.102.2 high 192.168.102.254
```

To configure named address ranges in a routing instance, configure the `address-assignment` statements in the `[edit routing-instances]` hierarchy level.

Configuring Static Address Assignments

You can optionally create a static IPv4 address binding by reserving a specific address for a particular client. The address is removed from the address-assignment pool so that it is not assigned to another client. When you reserve an address, you identify the client host and create a binding between the client MAC address and the assigned IP address.

This example is tested on SRX300, SRX320, SRX340, SRX345, SRX1500, and SRX550M devices.

To configure a static IPv4 address binding:

1. Specify the name of the IPv4 address-assignment pool containing the IP address you want to reserve for the client.

```
[edit access]
user@host# edit address-assignment pool blr-pool family inet
```

2. Specify the name of the client for the static binding, the client MAC address, and the IP address to reserve for the client. This configuration specifies that the client with MAC address 01:03:05:07:09:0b is always assigned IP address 192.168.10.2.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set host svale6_boston_net  hardware-address 01:03:05:07:09:0b ip-address 192.168.10.2
```

NOTE: To configure static binding for an IPv4 address in a routing instance, configure the `address-assignment` statements in the `[edit routing-instances]` hierarchy.

Configuring Address-Assignment Pool Linking

Address-assignment pool linking enables you to specify a secondary address pool for the device to use when the primary address-assignment pool is fully allocated. When the primary pool has no available addresses remaining, the device automatically switches over to the linked secondary pool and begins allocating addresses from that pool. The device uses a secondary pool only when the primary address-assignment pool is fully allocated.

To link a primary address-assignment pool named pool-1 to a secondary pool named pool-2, use the following option:

```
[edit access address-assignment]
user@host# set pool pool1 link pool2
```

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. The client application, such as DHCP, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCP application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCP specifies additional DHCP attributes such as the boot file that the client uses, the DNS server, and the maximum lease time.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

You use the `dhcp-attributes` statement to configure DHCP client-specific attributes for address-assignment pools.

To configure address-assignment pool attributes for DHCP clients:

1. Specify the name of the address-assignment pool.

```
[edit access]
 user@host# edit address-assignment pool blr-pool family inet
```

2. Configure optional DHCP client attributes.

```
[edit access address-assignment pool blr-pool family inet]
user@host# set dhcp-attributes maximum-lease-time 2419200
user@host# set dhcp-attributes name-server 192.168.10.2
user@host# set dhcp-attributes boot-file boot-file.txt
user@host# set dhcp-attributes boot-file boot-server example.com
```

NOTE: To configure DHCP client-specific attributes in a routing instance, configure the `dhcp-attributes` statements in the `[edit routing-instances]` hierarchy.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.1R1	Starting in Junos OS Release 18.1R1, search mechanism for an available address proceeds through a chain of linked pools. This behavior enables the DHCP to search addresses contiguously.
18.1R1	Starting in Junos OS Release 18.1R1, you can exclude a specified address or range of consecutive addresses to prevent them from being allocated from an address pool.

RELATED DOCUMENTATION

DHCPv6 Address-Assignment Pools | 39

DHCP Overview | 2

Legacy DHCP and Extended DHCP | 16

DHCPv6 Address-Assignment Pools

IN THIS SECTION

- Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 39
- Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 43
- Configuring an Address-Assignment Pool for Router Advertisement | 44
- Configuring Nontemporary Address Assignment | 44
- Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 45
- Configuring Auto-Prefix Delegation | 46
- Multiple Address Assignment for DHCPv6 Clients | 47

Address pool is a set of Internet Protocol addresses available for allocation to users, such as in host configurations with the DHCP. An address-assignment pool can support either IPv4 address or IPv6 addresses. You cannot use the same pool for both types of address. For more information, read this topic.

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

IN THIS SECTION

- Requirements | 40
- Overview | 40
- Configuration | 40
- Verification | 42

This example shows how to configure an address-assignment pool on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Requirements

Before you begin:

- Specify the name of the address-assignment pool and configure addresses for the pool.
- Set DHCPv6 attributes for the address-assignment pool.

Overview

In this example, you configure an address-pool called my-pool and specify the IPv6 family as inet6. You configure the IPv6 prefix as 2001:db8:3000:1::/64, the range name as range1, and the IPv6 range for DHCPv6 clients from a low of 2001:db8:3000:1::1/64 to a high of 2001:db8:3000:1::100/64. You can define the range based on the lower and upper boundaries of the prefixes in the range or based on the length of the prefixes in the range. Finally, you specify the DHCPv6 attribute for the DNS server as 2001:db8:3001::1, the grace period as 3600, and the maximum lease time as 120.

NOTE: Note: Configure DHCPv6 Identity association for non-temporary addresses (IA_NA) option to request a specific DHCPv6 IP address instead of prefix.

Configuration

IN THIS SECTION

- Procedure | 40

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low 2001:db8:3000:1::1/64
high 2001:db8:3000:1::100/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
2001:db8:3000:1::1
```

```
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period 3600
set access address-assignment pool my-pool family inet6 dhcp-attributes maximum-lease-time 120
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure an IPv6 address-assignment pool:

1. Configure an address-pool and specify the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool family inet6
```

2. Configure the IPv6 prefix, the range name, and IPv6 range for DHCPv6 clients.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set prefix 2001:db8:3000:1::/64
user@host# set range range1 low 2001:db8:3000:1::1/64  high 2001:db8:3000:1::100/64
```

3. Configure the DHCPv6 attribute for the DNS server for the address pool.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:3001::1
```

4. Configure the DHCPv6 attribute for the grace period.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes grace-period 3600
```

5. Configure the DHCPv6 attribute for the maximum lease time.

```
[edit access address-assignment pool my-pool family inet6]
user@host# set dhcp-attributes maximum-lease-time 120
```

Results

From configuration mode, confirm your configuration by entering the `show access address-assignment` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
    user@host# show access address-assignment
    pool my-pool {
        family inet6 {
                prefix 2001:db8:3000:1::/64;
                range range1 {
                    low 2001:db8:3000:1::1/64 ;
                    high 2001:db8:3000:1::100/64;
                }
            dhcp-attributes {
                maximum-lease-time 120;
                grace-period 3600;
                dns-server {
                    2001:db8:3001::1;
                    }
                }
            }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying Configuration | 42

Verifying Configuration

Purpose

Verify that the address-assignment pool has been configured.

Action

From operational mode, enter the `show access address-assignment` command.

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment

You can optionally configure multiple named ranges, or subsets of addresses, within an address-assignment pool. During dynamic address assignment, a client can be assigned an address from a specific named range. To create a named range, you specify a name for the range and define the address range and DHCPv6 attributes.

To configure a named address range for dynamic address assignment:

1. Specify the name of the address-assignment pool and the IPv6 family.

```
[edit access]
user@host# edit address-assignment pool my-pool2 family inet6
```

2. Configure the IPv6 prefix and then define the range name and IPv6 range for DHCPv6 clients. You can define the range based on the lower and upper boundaries of the prefixes in the range, or based on the length of the prefixes in the range.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set prefix 2001:db8:3000:5::/64
user@host# set range range2 low 2001:db8:3000:2::/64  high 2001:db8:3000:300::/64
```

3. Configure DHCPv6 attributes for the address pool.

```
[edit access address-assignment pool my-pool2 family inet6]
user@host# set dhcp-attributes dns-server 2001:db8:18:: grace-period 3600 maximum-lease-time
120
```

4. If you are done configuring the device, enter `commit` from configuration mode.

Configuring an Address-Assignment Pool for Router Advertisement

For SRX1500, SRX5400, SRX5600, and SRX5800 devices, you can create an address-assignment pool that is explicitly used for router advertisement address assignment. You populate the address-assignment pool using the standard procedure, but you additionally specify that the pool is used for router advertisement.

To configure an address-assignment pool that is used for router advertisement:

1. Create the IPv6 address-assignment pool.
2. Specify that the address-assignment pool is used for router advertisement.

```
[edit access address-assignment]
user@host# set neighbor-discovery-router-advertisement router1
```

3. If you are done configuring the device, enter `commit` from configuration mode.

Configuring Nontemporary Address Assignment

Nontemporary address assignment is also known as stateful address assignment. In the stateful address assignment mode, the DHCPv6 client requests global addresses from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the global addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

This example is tested on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as **statefull**.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation

The DHCPv6 client requests IPv6 addresses and prefixes from the DHCPv6 server. Based on the DHCPv6 server's response, the DHCPv6 client assigns the IPv6 addresses to interfaces and sets a lease time for all valid responses. When the lease time expires, the DHCPv6 client renews the lease from the DHCPv6 server.

To configure identity association for nontemporary addresses (IA_NA) and identity association for prefix delegation (IA_PD) on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the client type as `statefull`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the IA_NA.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

4. Specify the IA_PD.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

Configuring Auto-Prefix Delegation

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating router delegates IPv6 prefixes to a requesting router. The requesting router then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting router can also assign subnet addresses to subnets on the LAN.

To configure auto-prefix delegation for SRX300, SRX320. SRX340, SRX345, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as `statefull`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

2. Specify the identity association type as `ia-na` for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the identity association type as `ia-pd` for prefix delegation.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DUID type.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

5. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

Multiple Address Assignment for DHCPv6 Clients

For a DHCPv6 local server, you can assign multiple addresses to a single DHCPv6 client. Multiple address support is enabled by default, and is activated when the DHCPv6 local server receives a DHCPv6 Solicit message from a DHCP client that contains multiple addresses.

For example, if you are implementing this feature on the routers, you might use the multiple address assignment feature when a customer premises equipment (CPE) device requires a host address and a delegated prefix.

You can use either local address pools or RADIUS when assigning multiple addresses to a DHCP client. When at least one address is successfully allocated, the switch creates a DHCP client entry and binds the entry to the assigned address. If both addresses are successfully allocated, the switch creates a single DHCP client entry and binds both addresses to that entry.

You can also configure a delegated address pool, which explicitly specifies the address pool that DHCP management uses to assign IPv6 prefixes for DHCP clients.

SEE ALSO

> *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*

RELATED DOCUMENTATION

> IP Address Assignment Pool | **27**
>
> DHCPv6 Server | **104**
>
> DHCPv6 Relay Agent | **222**
>
> DHCPv6 Client | **266**

3

CHAPTER

DHCP Server

DHCP Server | 49

DHCP Server Configuration | 52

DHCP Server Options | 77

Verifying DHCP Server Configuration | 96

Monitoring the DHCP Server Configuration | 100

DHCPv6 Server | 104

DHCP Server

IN THIS SECTION

- Understanding DHCP Server Operation | 49
- Graceful Routing Engine Switchover for DHCP | 50

A DHCP Server is a network server that automatically provides and assigns IP addresses, default gateways, and other network parameters to client devices. It relies on the standard protocol known as Dynamic Host Configuration Protocol or DHCP to respond to broadcast queries by clients. Read this topic for more information on DHCP server operations, configuring DHCP server and extended DHCP server.

Understanding DHCP Server Operation

IN THIS SECTION

- DHCP Options | 50
- Compatibility with Autoinstallation | 50
- Chassis Cluster Support | 50

As a DHCP server, a Juniper Networks device can provide temporary IP addresses from an IP address pool to all clients on a specified subnet, a process known as dynamic binding. Juniper Networks devices can also perform static binding, assigning permanent IP addresses to specific clients based on their media access control (MAC) addresses. Static bindings take precedence over dynamic bindings.

NOTE: All DHCP packets passing through a DHCP unconfigured interface might be dropped.

Enabling the DHCP relay or DHCP server feature also enables the DHCP snooping feature, which analyzes all DHCP packets received through any interface of the device (both DHCP configured and unconfigured interfaces) .

Interfaces not listed under DHCP settings are considered as `unconfigured` interfaces. Depending on the configuration, DHCP packets received on DHCP unconfigured interfaces are dropped.

This section contains the following topics:

DHCP Options

In addition to its primary DHCP server functions, you can also configure the device to send configuration settings like the following to clients through DHCP:

- IP address of the DHCP server (Juniper Networks device)
- List of Domain Name System (DNS) and NetBIOS servers
- List of gateway routers
- IP address of the boot server and the filename of the boot file to use
- DHCP options defined in RFC 2132, *DHCP Options and BOOTP Vendor Extensions*

Compatibility with Autoinstallation

The functions of a Juniper Networks device acting as a DHCP server are compatible with the autoinstallation feature. The DHCP server automatically checks any autoinstallation settings for conflicts and gives the autoinstallation settings priority over corresponding DHCP settings. For example, an IP address set by autoinstallation takes precedence over an IP address set by the DHCP server.

Chassis Cluster Support

DHCP server operations are supported on all SRX Series Firewalls in chassis cluster mode.

Graceful Routing Engine Switchover for DHCP

For EX Series switches, only extended DHCP local server maintains the state of active DHCP client leases. The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide

subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces. The extended DHCP local server also supports the use of Junos address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.

For MX Series routers, the extended DHCP local server and the DHCP relay agent applications both maintain the state of active DHCP client leases in the session database. The extended DHCP application can recover this state if the DHCP process fails or is manually restarted, thus preventing the loss of active DHCP clients in either of these circumstances. However, the state of active DHCP client leases is lost if a power failure occurs or if the kernel stops operating (for example, when the router is reloaded) on a single Routing Engine.

You can enable graceful switchover support on both EX Series switches and MX Series routers. To enable graceful switchover support for the extended DHCP local server or extended DHCP relay agent on a switch, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. To enable *graceful Routing Engine switchover* support on MX Series routers, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. You cannot disable graceful Routing Engine switchover support for the extended DHCP application when the router is configured to support graceful Routing Engine switchover.

For more information about using graceful Routing Engine switchover, see Understanding Graceful Routing Engine Switchover.

SEE ALSO

- Legacy DHCP and Extended DHCP | **16**
- *Extended DHCP Relay Agent Overview*
- *Unified ISSU for High Availability in Subscriber Access Networks*

RELATED DOCUMENTATION

- DHCP Overview | **2**
- DHCPv6 Server | **104**
- DHCP Client | **245**
- DHCPv6 Client | **266**
- DHCP with External Authentication Server | **277**
- Dynamic Reconfiguration of DHCP Servers and Clients | **317**

DHCP Server Configuration

IN THIS SECTION

- DHCP Server Configuration Overview | 52
- Minimum DHCP Local Server Configuration | 54
- Example: Complete DHCP Server Configuration | 56
- Configure a Router as an Extended DHCP Local Server | 60
- Configuring a Switch as a DHCP Server | 63
- Configuring a DHCP Server on Switches | 67
- Example: Configuring a Security Device as a DHCP Server | 69

This topic discusses on minimum DHCP server configuration, complete DHCP server configuration, extended DHCP server configuration. You can also use this topic for information on how to configure a router as a DHCP server, switch as a DHCP server, DHCP server on switches, and a device as a DHCP server.

NOTE: For MX Series Routers, the DHCP server functionality for Junos OS is part of the subscriber management feature. You must have the S-SA-FP, S-MX80-SA-FP or S-MX104-SA-FP license in order to enable the DHCP server. For service accounting, you must also have S-SSM-FP.

For details, See Licenses for PTX, MX, M and T Series or Juniper Licensing User Guide.

DHCP Server Configuration Overview

A typical DHCP server configuration provides the following configuration settings for a particular subnet on a device ingress interface:

- An IP address pool, with one address excluded from the pool.
- Default and maximum lease times.

- Domain search suffixes. These suffixes specify the domain search list used by a client when resolving hostnames with DNS.
- A DNS name server.
- Device solicitation address option (option 32). The IP address excluded from the IP address pool is reserved for this option.

In addition, the DHCP server might assign a static address to at least one client on the subnet. Table 7 on page 53 provides the settings and values for the sample DHCP server configuration.

Table 7: Sample DHCP Server Configuration Settings

Setting	Sample Value
DHCP Subnet Configuration	
Address pool subnet address	`192.168.2.0/24`
High address in the pool range	`192.168.2.254`
Low address in the pool range	`192.168.2.2`
Address pool default lease time, in seconds	`1,209,600` (14 days)
Address pool maximum lease time, in seconds	`2,419,200` (28 days)
Domain search suffixes	`mycompany.net` `mylab.net`
Address to exclude from the pool	`192.168.2.33`
DNS server address	`192.168.10.2`
Identifier code for router solicitation address option	`32`
Type choice for router solicitation address option	`Ip address`

Table 7: Sample DHCP Server Configuration Settings *(Continued)*

Setting	Sample Value
IP address for router solicitation address option	192.168.2.33
DHCP MAC Address Configuration	
Static binding MAC address	01:03:05:07:09:0B
Fixed address	192.168.2.50

Minimum DHCP Local Server Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP server. In this output, the server group is named mobileusers, and the DHCP local server is enabled on ingress interface ge-1/0/1.0 within the group. The address pool is named acmenetwork from low range of 192.168.1.10/24 to a high range of 192.168.1.20/24.

```
[edit access]
address-assignment {
    pool acmenetwork {
        family inet {
            network 192.168.1.0/24;
            range r1 {
                low 192.168.1.10;
                high 192.168.1.20;
            }
        }
    }
}
```

```
[edit system services]
dhcp-local-server {
    group mobileusers {
```

```
        interface ge-1/0/1.0
    }
}
```

```
[edit interfaces ge-1/0/1 unit 0]
family {
    inet {
        address 192.168.1.1/24
    }
}
```

NOTE: You can configure the DHCP local server in a routing instance by using the `dhcp-local server`, `interface`, and `address-assignment` statements in the `[edit routing-instances]` hierarchy level.

This example shows the minimum configuration you need to use for the extended DHCP local server at group-level:

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface ge-0/0/2.0;
    }
}
```

This example creates the server group named `group_one`, and specifies that the DHCP local server is enabled on interface `ge-0/0/2.0` within the group. The DHCP local server uses the default pool match configuration of `ip-address-first`.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

This example shows the minimum configuration you need to use for the extended DHCP local server at group-level. If there is a dynamic profile configuration for interface ge-0/0/2, you should add an interface in the *ifd*.0 format. For example ge-0/0/2.0:

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface ge-0/0/2.0;
    }
}
```

This example creates the server group named group_one, and specifies that the DHCP local server is enabled on interface ge-0/0/2.0 within the group.

Example: Complete DHCP Server Configuration

IN THIS SECTION

- Requirements | 56
- Overview | 56
- Configuration | 57

This topic shows a complete DHCP server configuration.

Watch the following video to learn how to configure DHCP server using J-Web:

Video:

Requirements

- This example uses is tested on Junos OS Release 20.1R1.

Overview

You can configure a DHCP server only on an interface's primary IP address. The primary address on an interface is the address that is used by default as the local address for broadcast and multicast packets sourced locally and sent out the interface.

The following example shows statements at the `[edit interfaces]` hierarchy level. The interface's primary address (**10.3.3.1/24**) has a corresponding address pool range (**10.3.3.33 to 10.3.3.254**) defined at the `[edit system services]` hierarchy level.

Configuration

IN THIS SECTION

- Configuring [item] | **57**
- Configure Legacy DHCP Server | **59**

To configure the DHCP server, perform these tasks:

Configuring [item]

Step-by-Step Procedure

1. Configure DHCP server.

```
[edit access address-assignment pool P1 family inet dhcp-attributes]
range R1 {
    low 10.3.3.33;
    high 10.3.3.254;
}
dhcp-attributes {
    maximum-lease-time 7200;
    server-identifier 10.3.3.1;
    domain-name domain.tld;
    name-server {
        10.6.6.6;
        10.6.6.7;
    }
    wins-server {
        10.7.7.7;
        10.7.7.9;
    }
    router {
        198.51.100.0;
```

```
        198.51.100.1;
        10.6.6.1;
        10.7.7.1;
    }
    boot-file boot-client;
    boot-server 10.4.4.1;
    option 19 flag false;
    option 40 string domain.tld;
    option 16 ip-address 10.3.3.3;
}
host H1 {
    hardware-address 00:0d:56:f4:20:01;
    ip-address 10.4.4.4;
}
host H2 {
    hardware-address 00:0d:56:f4:01:ab;
    ip-address 10.5.5.6;
}
excluded-address 10.3.3.33;
excluded-address 192.0.2.5;
}
```

2. Configure client options.

```
[edit interfaces]
ge-0/0/1 {
    unit 0 {
        family inet {

            dhcp {
                client-identifier {
                    user-id ascii 01aa.001a.bc65.3e;
                }
                lease-time 4100;
                update-server;
            }
            address 10.3.3.1/24;
        }
}
```

Configure Legacy DHCP Server

Step-by-Step Procedure

1. Specify DHCP server configuration option.

```
dhcp {
    domain-name "domain.tld";
    maximum-lease-time 7200;
    default-lease-time 3600;
    name-server {
        10.6.6.6;
         10.6.6.7;
    }
    domain-search [ subnet1.domain.tld subnet2.domain.tld ];
    wins-server {
         10.7.7.7;
        10.7.7.9;
    }
    router {
        10.6.6.1;
        10.7.7.1;
    }
    option 19 flag off;       # 19: "IP Forwarding" option
    option 40 string "domain.tld"; # 40: "NIS Domain" option
    option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
    pool 10.3.3.0/24 {
        address-range low 10.3.3.2 high 10.3.3.254;
        exclude-address {
            10.3.3.33;
        }
        router {
            10.3.3.1;
        }
        server-identifier 10.3.3.1;
    }
    pool 10.4.4.0/24 {
        boot-file "boot.client";
        boot-server 10.4.4.1;
    }
    static-binding 00:0d:56:f4:20:01 {
```

```
        fixed-address 10.4.4.4;
        host-name "host.domain.tld";
    }
    static-binding 00:0d:56:f4:01:ab {
        fixed-address {
            10.5.5.5;
            10.6.6.6;
        }
        host-name "another-host.domain.tld";
        client-identifier "01aa.001a.bc65.3e";
    }
}
```

2. Configure client options.

```
[edit interfaces]
ge-0/0/1 {
    unit 0 {
        family inet {

            address 10.3.3.1/24;
        }
}
```

Configure a Router as an Extended DHCP Local Server

You can enable the router to function as an extended DHCP local server and configure the extended DHCP local server options on the router. The extended DHCP local server provides an IP address and other configuration information in response to a client request.

The extended DHCP local server enhances traditional DHCP server operation in which the client address pool and client configuration information reside on the DHCP server. With the extended DHCP local server, the client address and configuration information reside in centralized address-assignment pools, which are managed independently of the DHCP local server and which can be shared by different client applications.

The extended DHCP local server also supports advanced pool matching and the use of named address ranges. You can also configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information,

which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.

Configuring the DHCP environment that includes the extended DHCP local server requires two independent configuration operations, which you can complete in any order. In one operation, you configure the extended DHCP local server on the router and specify how the DHCP local server determines which address-assignment pool to use. In the other operation, you configure the address-assignment pools used by the DHCP local server. The address-assignment pools contain the IP addresses, named address ranges, and configuration information for DHCP clients. See "IP Address Assignment Pool" on page 27 for details about creating and using address-assignment pools.

NOTE: The extended DHCP local server and the address-assignment pools used by the server must be configured in the same logical system and routing instance.

You cannot configure the extended DHCP local server and extended DHCP relay on the same interface.

To configure the extended DHCP local server on the router, include the `dhcp-local-server` statement at the `[edit system services]` hierarchy level:

```
[edit system services]
dhcp-local-server {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
```

```
                domain-name domain-name-string;
                logical-system-name;
                mac-address;
                option-60;
                option-82 <circuit-id> <remote-id>;
                routing-instance-name;
                user-prefix user-prefix-string;
            }
        }
        interface interface-name <upto upto-interface-name> <exclude>;
    }
    pool-match-order {
        ip-address-first;
        option-82;
    }
}
```

You can also include these statements at the following hierarchy levels:

- [edit logical-systems *logical-system-name* system services]
- [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services]
- [edit routing-instances *routing-instance-name* system services]

In addition, you can configure tracing for DHCP local server operations by including the traceoptions statement at the [edit system processes dhcp-service] hierarchy level:

```
[edit system processes]
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-
readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Configuring a Switch as a DHCP Server

IN THIS SECTION

- Configuring the Switch as a Local DHCP Server | 63

NOTE: This topic applies to Junos OS for EX Series switches and QFX Series switches with support for the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that does not support ELS, see "Configuring a DHCP Server on Switches" on page 67. For ELS details, see Using the Enhanced Layer 2 Software CLI.

A Dynamic Host Configuration Protocol (DHCP) server provides a framework to pass configuration information to client hosts on a TCP/IP network. A switch acting as a DHCP server can dynamically allocate IP addresses and other configuration parameters, minimizing the overhead that is required to add clients to the network.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the switch as a local DHCP server using DHCP for IPv4 (DHCPv4). For information about DHCPv6 local server, see *DHCPv6 Local Server Overview*.

This topic describes the following task:

Configuring the Switch as a Local DHCP Server

To configure a switch as a local DHCP server, you must configure a DHCP address pool and indicate IP addresses for the pool. The switch, operating as the DHCP server, dynamically distributes the IP addresses from this pool. The switch can dynamically assign additional configuration parameters, such as default gateway, to provide the client with information about the network.

Multiple address pools can be configured for a DHCP server. DHCP maintains the state information about all configured pools. Clients are assigned addresses from pools with subnets that match the interface on which the DHCPDISCOVER packet sent by the client is received on the server. When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

You must ensure that you do not assign addresses that are already in use in the network to the address pools. The DHCP server does not check whether the addresses are already in use in the network before it assigns them to clients.

1. Configure a Layer 3 interface with an IP address on which the DHCP server will be reachable:

```
[edit]
user@switch# set interfaces interface-name unit unit-number family inet address address/
prefix-length
user@switch# set vlans vlan-name vlan-id vlan-id
user@switch# set vlans vlan-name l3-interface irb-name
user@switch# set interfaces irb-name family inet address address/prefix-length
```

   For example:

```
[edit]
user@switch# set interfaces ge-0/0/1 unit 0 family inet address 192.0.2.1/24
user@switch# set vlans server vlan-id 301
user@switch# set vlans server l3-interface irb.301
user@switch# set interfaces irb.301 family inet address 192.0.2.2/24
```

2. Configure the DHCP server for the Layer 3 interface:

```
[edit]
user@switch# set system services dhcp-local-server group-name interface interface-name
```

   For example:

```
[edit]
user@switch# set system services dhcp-local-server group server1 interface ge-0/0/1
user@switch# set system services dhcp-local-server group server1 interface irb.301
```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]
user@switch# set access address-assignment pool pool-name family inet network  address/prefix-
length
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet network 198.51.100.0/24
```

4. (Optional) Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range:

```
[edit]
user@switch# set access address-assignment pool pool-name family inet range range-name low
low-IP-address
user@switch# set access address-assignment pool pool-name family inet range range-name high
high-IP-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet range range1 low
198.51.100.1
user@switch# set access address-assignment pool pool1 family inet range range1 high
198.51.100.2
```

5. (Optional) Configure one or more routers as the default gateway on the client's subnet:

```
[edit]
user@switch# set access address-assignment pool pool-name family inet dhcp-attributes router
gateway-ip-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes router
198.1.1.254
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@switch# set access address-assignment pool pool-name family inet dhcp-attributes server-identifier ip-address
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes server-identifier 198.51.100.254
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease:

```
[edit]
user@switch# set access address-assignment pool pool-name family inet dhcp-attributes maximum-lease-time seconds
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes maximum-lease-time 43,200
```

8. (Optional) Specify user-defined options to be included in DHCP packets:

```
[edit]
user@switch# set access address-assignment pool pool-name family inet dhcp-attributes option option-id-number option-type option-value
```

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes option 98 string test98
```

Configuring a DHCP Server on Switches

IN THIS SECTION

- Configuring an Extended DHCP Server on a Switch | 67

NOTE: This task uses Junos OS for EX Series switches that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Configuring a Switch as a DHCP Server" on page 63. For ELS details, see Using the Enhanced Layer 2 Software CLI.

A Dynamic Host Configuration Protocol (DHCP) server can provide two valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients and it can also deliver software upgrades to clients.

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers configuration of the DHCP server. For information about reconfiguring a DHCP client, see "Configuring a DHCP Client" on page 246.

You can configure either of two versions of a DHCP server on a switch— the extended server version or the legacy server version. We recommend that you configure the extended server unless you need to keep your DHCP server configuration backward-compatible with the legacy server version.

This topic includes the following tasks:

Configuring an Extended DHCP Server on a Switch

To configure an extended DHCP server, you must configure a DHCP pool, indicate IP addresses for the pool, and create a server group. Additional configurations are optional.

Do not assign addresses that are already in use in the network to address pools. The extended DHCP server does not check whether addresses are already in use before it assigns them to clients.

1. Create an address pool for DHCP IP addresses:

```
[edit]
user@switch# set access address-pool  address-pool
```

2. Configure an address-assignment pool that can be used by different client applications for DHCP dynamic assignment:

```
[edit access address-assignment]
user@switch# set pool  address-pool-name
```

3. Create a server group on the switch, providing a group name and an interface name for DHCP:

```
[edit system services dhcp-local-server]
user@switch# set group group-name interface interface-name
```

4. (Optional) Process the information protocol data units (PDUs):

```
[edit system services dhcp-local-server]
user@switch# set overrides process-inform
```

5. (Optional) Redefine the order of attribute matching for pool selection:

```
[edit system services dhcp-local-server]
user@switch# set pool-match-order ip-address-first
```

6. (Optional) Enable dynamic reconfiguration triggered by the DHCP extended server for all DHCP clients or only for the DHCP clients serviced by the specified group of interfaces:

```
[edit system services dhcp-local-server]
user@switch# set reconfigure
```

```
[edit system services dhcp-local-server group group-name]
user@switch# set reconfigure
```

Example: Configuring a Security Device as a DHCP Server

IN THIS SECTION

- Requirements | 69
- Overview | 69
- Configuration | 70
- Verification | 74

This example shows how to configure the device as a DHCP server.

For information on how to configure JDHCP in a routing instance, see How to configure JDHCP in a routing instance.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP server. You specify the IP address pool as 192.168.2.0/24 and from a low range of 192.168.2.2 to a high range of 192.168.2.254. You set the maximum-lease-time to 2,419,200. Then you specify the DNS server IP address as 192.168.10.2.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series Firewalls is being deprecated. and only the new JDHCP CLI is supported. When you upgrade to

Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

Configuration

IN THIS SECTION

- Procedure | 70

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `set access` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
set system services dhcp-local-server group g1 interface ge-0/0/2.0
set access address-assignment pool p1 family inet network 192.168.2.0/24
set access address-assignment pool p1 family inet range r1 low 192.168.2.2
set access address-assignment pool p1 family inet range r1 high 192.168.2.254
set access address-assignment pool p1 family inet dhcp-attributes maximum-lease-time 2419200
set access address-assignment pool p1 family inet dhcp-attributes name-server 192.168.10.2
```

GUI Quick Configuration

Step-by-Step Procedure

To configure the device as a DHCP server, specify the DHCP pool information, server information, lease time, and option information:

1. In the J-Web interface, select **Configure** > **DHCP** > **DHCP Services**.

2. Select DHCP Pools. Click **Add**.
3. Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
4. Specify the subnet information for the IPv4 address-assignment pool. Type **192.168.2.0/24**.
5. In the Address Range Low, type **192.168.2.2**.
6. In the Address Range High, type **192.168.2.254**.
7. In the Exclude Addresses box, type the addresses you want excluded from a DHCP address pool. Type **192.168.2.0/24**
8. Specify the server identifier to assign to any DHCP clients in this address pool. The identifier can be used to identify a DHCP server in a DHCP message.
9. Specify the domain name to assign to any DHCP clients in this address pool.
10. Specify the next server that DHCP clients need to contact. Type **192.168.10.2**
11. Define the maximum amount of time (in seconds) that DHCP should lease an address. Type **2419200**.
12. Define DHCP option 32, the device solicitation address option. You must enter a numeric value for option code. Select the option type from the list that corresponds to the option code.
13. Click **OK**.
14. If you are done configuring the device, click **Commit** > **Commit**.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the device as a DHCP server:

1. Configure an interface with an IP address on which the DHCP server will be reachable.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 192.168.2.1/24
```

2. Configure the DHCP server.

```
[edit]
user@host#  set system services dhcp-local-server group g1 interface ge-0/0/2.0
```

3. Create an address pool for IPv4 addresses that can be assigned to clients. The addresses in the pool must be on the subnet in which the DHCP clients reside. Do not include addresses that are already in use on the network.

```
[edit]]
user@host# set access address-assignment pool p1 family inet network 192.168.2.0/24
```

4. (Optional) Specify the IP address pool range. Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

```
[edit]]
user@host# set access address-assignment pool p1 192.168.2.0/24 address-range low 192.168.2.2
high 192.168.2.254
```

5. (Optional) Configure one or more routers as the default gateway on the client's subnet.

```
[edit]
user@host# set access address-assignment pool p1 family inet dhcp-attributes router
192.168.10.3
```

6. (Optional) Configure the IP address that is used as the source address for the DHCP server in messages exchanged with the client. Clients use this information to distinguish between lease offers.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes server-
identifier 192.168.10.1
```

7. (Optional) Specify the maximum time period, in seconds, that a client holds the lease for an assigned IP address if the client does not renew the lease.

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes maximum-lease-
time 2419200
```

8. (Optional) Specify user-defined options to be included in DHCP packets

```
[edit]
user@host# set access address-assignment pool pool1 family inet dhcp-attributes option 98
string test98
```

9. Assign a fixed IP address with the MAC address of the client.

```
[edit]
user@host# set access address-assignment pool pool1 family inet host host1 ip-address
192.168.2.100 hardware-address 2c:56:dc:72:99:f3
```

Results

- From configuration mode, confirm your configuration by entering the `show access address-assignment` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
    network 192.168.2.0/24;
    range r1 {
    low 192.168.2.2;
        high 192.168.2.254;
    }
    dhcp-attributes {
        maximum-lease-time 2419200;
        name-server {
         192.168.10.2;
                }
```

```
            }
        }
    }
}
```

- From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
group g1 {
interface ge-0/0/2.0;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Binding Database | 74
- Verifying DHCP Server Operation | 75

Confirm that the configuration is working properly.

Verifying the DHCP Binding Database

Purpose

Verify that the DHCP binding database reflects the DHCP server configuration.

Action

From operational mode, enter these commands:

- `show dhcp server binding` command to display all active bindings in the database.

- `show dhcp server binding` *address* `detail` command (where *address* is the IP address of the client) to display more information about a client.

These commands produce following sample output:

```
user@host> show dhcp server binding
IP Address   Hardware Address   Type          Lease expires at
30.1.1.20  00:12:1e:a9:7b:81  dynamic       2007-05-11 11:14:43 PDT
```

```
user@host> show dhcp server binding address detail
    IP address           192.0.2.2
    Hardware address     00:a0:12:00:13:02
    Pool                 192.0.2.0/24
    Interface  fe-0/0/0, relayed by 192.0.2.200

Lease information:
    Type                 DHCP
    Obtained at          2004-05-02 13:01:42 PDT
    Expires at           2004-05-03 13:01:42 PDT
    State                active

DHCP options:
     Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
     Name: domain-name, Value: mydomain.tld
    Code: 32, Type: ip-address, Value: 192.0.2.33
```

Verifying DHCP Server Operation

Purpose

Verify that the DHCP server operation has been configured.

Action

From operational mode, enter the following command:

- `show dhcp server statistics` command to verify the DHCP server statistics.

```
user@host> show dhcp server statistics
Packets dropped:
```

```
    Total                     0

Messages received:
    BOOTREQUEST               45
    DHCPDECLINE               0
    DHCPDISCOVER              1
    DHCPINFORM                39
    DHCPRELEASE               0
    DHCPREQUEST               5
    DHCPLEASEQUERY            0
    DHCPBULKLEASEQUERY        0

Messages sent:
    BOOTREPLY                 6
    DHCPOFFER                 1
    DHCPACK                   3
    DHCPNAK                   2
    DHCPFORCERENEW            0
    DHCPLEASEUNASSIGNED       0
    DHCPLEASEUNKNOWN          0
    DHCPLEASEACTIVE           0
    DHCPLEASEQUERYDONE        0
```

SEE ALSO

Understanding DHCP Relay Agent Operation | 153

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series Firewalls is being deprecated. and only the new JDHCP CLI is supported.

RELATED DOCUMENTATION

DHCP Overview | 2

DHCP Server | 49
DHCP Server Options | 77
Verifying DHCP Server Configuration | 96
Monitoring the DHCP Server Configuration | 100
Legacy DHCP and Extended DHCP | 16

DHCP Server Options

IN THIS SECTION

- Configure DHCP Server Identifier | 78
- Configure Address Pools for DHCP Dynamic Bindings | 78
- Configure Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address | 79
- Enabling TCP/IP Propagation on a DHCP Local Server | 80
- Specify DHCP Lease Times for IP Address Assignments | 81
- Configure a DHCP Boot File and DHCP Boot Server | 82
- Configure Domain Name and Domain Search List | 83
- Configure Routers Available to the DHCP Client | 83
- Configure User-Defined DHCP Options | 84
- Configure DHCP SIP Server | 85
- Overriding the Default DHCP Local Server Configuration Settings | 85
- Legacy DHCP Server Configuration Options | 88

DHCP options are tagged data items that provide information to a DHCP client. The options are sent in a variable-length field at the end of a DHCP message. For more information about various DHCP options, read this topic.

Configure DHCP Server Identifier

The server identifier identifies a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

To configure a DHCP server identifier, include the `server-identifier` statement at [`edit access address-assignment pool` *`pool-name`* `family inet dhcp-attributes`] hierarchy level.

Example:

```
[edit access address-assignment pool P1 family inet]
dhcp-attributes {
    server-identifier 192.0.2.0;
}
```

You can also include the `server-identifier` statement at the following hierarchy levels:

- [`edit logical-systems` *`logical-system-name`* `access address-assignment pool` *`pool-name`* `family inet dhcp-attributes`]
- [`edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `access address-assignment pool` *`pool-name`* `family inet dhcp-attributes`]
- [`edit routing-instances` *`routing-instance-name`* `access address-assignment pool` *`pool-name`* `family inet dhcp-attributes`]

Configure Address Pools for DHCP Dynamic Bindings

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet. Configure the following options:

- Network - Include the client subnet number and prefix length (in bits). The addresses in the pool must be on the subnet in which the DHCP clients reside.
- Address Range -Specify the range of IP addresses in the pool that are available for dynamic address assignment. This statement is optional. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)
- Excluded Addresses –Specify the addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range. This statement is optional.

The following is an example of a pool configuration.

```
[edit access address-assignment pool P1 family inet]
network 192.0.2.0/24;
range R1 {
    low 192.0.2.0;
    high 192.0.2.10;
}
excluded-address 10.3.3.33;
}
```

Note the following when configuring address pools:

- You can configure multiple address pools for a DHCP server, but only one address range per pool is supported.
- DHCP maintains the state information for all pools configured. Clients are assigned addresses from pools with subnets that match the interface on which the `DHCPDISCOVER` packet is received.
- When more than one pool exists on the same interface, addresses are assigned on a rotating basis from all available pools.

Configure Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

A static binding defines a mapping between a fixed IP address and the client's MAC address.

The *hardware-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.

The `ip-address` statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

The following is an example of a static binding configuration:

```
[edit access address-assignment pool P1 family inet]
host H1 {
    hardware-address 2c:56:dc:72:99:f3;
```

```
    ip-address 192.0.2.0;
}
```

You can also include the `server-identifier` statement at the following hierarchy levels:

- `[edit logical-systems` *`logical-system-name`* `access address-assignment pool` *`pool-name`* `family inet]`
- `[edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `access address-assignment pool` *`pool-name`* `family inet]`
- `[edit routing-instances` *`routing-instance-name`* `access address-assignment pool` *`pool-name`* `family inet]`

Enabling TCP/IP Propagation on a DHCP Local Server

Propagation of TCP/IP Settings for DHCP

The Juniper Networks device can operate simultaneously as a client of the DHCP server in the untrust zone and a DHCP server to the clients in the trust zone. The device takes the TCP/IP settings that it receives as a DHCP client and forwards them as a DHCP server to the clients in the trust zone. The device interface in the untrust zone operates as the DHCP client, receiving IP addresses dynamically from an Internet service provider (ISP) on the external network.

During the DHCP protocol exchange, the device receives TCP/IP settings from the external network on its DHCP client interface. Settings include the address of the ISP's DHCP name server and other server addresses. These settings are propagated to the DHCP server pools configured on the device to fulfill host requests for IP addresses on the device's internal network.

This topic describes how to configure TCP/IP settings on a DHCP local server, which includes a DHCP client and a DHCP local server.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX345, SRX550M, and SRX1500 devices.

To enable TCP/IP setting propagation on a DHCP local server:

1. Configure the `update-server` option on the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp {
```

```
    update-server;
}
```

2. Configure the address pool to specify the interface (where `update-server` is configured) from which TCP/IP settings can be propagated.

```
[edit access]
address-assignment {
    pool P1 family inet {
        network 192.168.2.0/24;
            dhcp-attributes {
                propagate-settings ge-0/0/1.0;
        }
    }
}
```

3. Configure the DHCP local server.

```
edit system services
dhcp-local-server {
    group G1 {
        interface ge-1/0/1.0
    }
}
```

Specify DHCP Lease Times for IP Address Assignments

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure maximum lease time, include the `maximum-lease-time` statement:

```
user@host# set access address-assignment pool P1 family inet dhcp-attributes maximum-lease-time
7200
```

To configure default lease time, include the `lease-time` statement:

```
user@host# set interfaces ge-0/0/1 unit 0 family inet dhcp  lease-time 4100
```

Configure a DHCP Boot File and DHCP Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the `boot-file` and `boot-server` statements:

After a client receives a **DHCPOFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

The `boot-file` statement configures the name and location of the initial boot file that the DHCP client loads and executes. This file stores the boot image for the client. In most cases, the boot image is the operating system the client uses to load.

The `boot-server` statement configures the IP address of the TFTP server that contains the client's initial boot file. You must configure an IP address or a hostname for the server.

You must configure at least one boot file and boot server. Optionally, you can configure multiple boot files and boot servers. For example, you might configure two separate boot servers and files: one for static binding and one for address pools. Boot file configurations for pools or static bindings take precedence over boot file configurations at the `[edit system services dhcp]` hierarchy level.

The following example specifies a boot file and server for an address pool:

```
[edit access address-assignment pool P1 family inet]
dhcp-attributes {
    boot-file "boot.client";
    boot-server 10.4.4.1;
}
```

Configure Domain Name and Domain Search List

To configure the name of the domain in which clients search for a DHCP server host, include the `domain-name` statement:

The `domain-name` statement sets the domain name that is appended to hostnames that are not fully qualified. This statement is optional. If you do not configure a domain name, the default is the client's current domain.

```
[edit access address-assignment pool P1 family inet]
dhcp-attributes {
    domain-name example.com;
}
```

To configure a domain search list, include the `option 119` statement in hexadecimal-string using hexadecimal values. Following is an example for 'jnpr.net' domain name:

```
[edit access]
set address-assignment pool hawk family inet dhcp-attributes option 119 array hex-string
046a6e7072036e657400
```

See How to configure DHCP server (JDHCPD) to support domain search (option 119).

Configure Routers Available to the DHCP Client

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the `router` statement:

The `router` statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

Example:

```
[edit access address-assignment pool P1 family inet]
dhcp-attributes {
    router {
        198.51.100.0;
        198.51.100.1;
```

```
    }
}
```

Configure User-Defined DHCP Options

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

To configure a user-defined DHCP option, include the `option` statement:

```
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

The `option` statement specifies the following values:

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: `byte`, `byte-stream`, `flag`, `integer`, `ip-address`, `short`, `string`, `unsigned-integer`, `unsigned-short`.
- *array*—An option can include an array of values.
- *option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an `On` or `Off` value for a `flag` type).

The following example shows user-defined DHCP options:

```
[edit access address-assignment pool P1 family inet]
    dhcp-attributes {
        option 19 flag false;
        option 40 string domain.tld;
        option 16 ip-address 10.3.3.33;
    }
```

Configure DHCP SIP Server

You can use the `sip-server` statement on the EX Series switch to configure option 120 on a DHCP server. The DHCP server sends configured option values—Session Initiation Protocol (SIP) server addresses or names—to DHCP clients when they request them. You specify either an IPv4 address or a fully qualified domain name to be used by SIP clients to locate a SIP server. You cannot specify both an address and name in the same statement.

To configure a SIP server using the `dhcp-attributes` option:

```
[edit access address-assignment pool P1 family inet]
    dhcp-attributes {
        sip-server 198.51.100.0;
    }
```

Overriding the Default DHCP Local Server Configuration Settings

Subscriber management enables you to override certain default DHCP local server configuration settings. You can override the configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP local server configuration options, include the `overrides` statement and its subordinate statements at the `[edit system services dhcp-local-server]` hierarchy level.
- To override DHCP local server configuration options for a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group` *`group-name`*`]` hierarchy level.
- To override DHCP local server configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit system services dhcp-local-server group` *`group-name`* `interface` *`interface-name`*`]` hierarchy level.
- To configure overrides for DHCPv6 local server at the global level, group level, or per-interface, use the corresponding statements at the `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

To override default DHCP local server configuration settings:

- (DHCPv4 and DHCPv6) Specify that you want to configure override options.
  - DHCPv4 overrides.

Global override:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

Group-level override:

```
[edit system services dhcp-local-server]
user@host# edit group group-name overrides
```

Per-interface override:

```
[edit system services dhcp-local-server]
user@host# edit group group-name overrides interface interface-name
```

DHCPv6 overrides.

Global override:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

Group level override:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name overrides
```

Per-interface override:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name overrides interface interface-name
```

- (Optional) Override the maximum number of DHCP clients allowed per interface.
  See *Specifying the Maximum Number of DHCP Clients Per Interface*.
- (Optional) Configure DHCP client auto logout.
  See *Automatically Logging Out DHCP Clients*.
- (Optional) Enable processing of information requests from clients.

See *Enabling Processing of Client Information Requests*.

- (Optional) Specify that DHCP NAK and FORCERENEW messages support option 82 information.

  See *Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances*.

- (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.

  See *Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation*.

- (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.

  See *Configuring DHCPv6 Rapid Commit (MX Series, EX Series)*.

- (Optional, DHCPv6 only) Specify that DHCPv6 local server return DNS server addresses as IA_NA or IA_PD suboptions rather than as a global DHCPv6 option.

  See *Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment*.

- (Optional, DHCPv6 only) Automatically log out existing client when new client solicits on same interface.

  See *Automatically Logging Out DHCPv6 Clients*.

- (Optional) Specify that when the DHCP or DHCPv6 local server receives a Discover or Solicit message that has a client ID that matches the existing client entry, the local server deletes the existing client entry.

  See *DHCP Behavior When Renegotiating While in Bound State*.

- (Optional, DHCPv4 and DHCPv6) Specify that a short lease be sent to the client.

  See *Configuring DHCP Asymmetric Leasing*.

- (Optional, DHCPv4 and DHCPv6) Specify DHCP attributes globally or for groups.

  See *Configuring DHCP Attributes for All Clients or a Group of Clients*.

- Load balance traffic by allowing some local servers to respond to specific clients while preventing other local servers from responding immediately to these clients.

  See *Delaying DHCP Offer and Advertise Responses to Load Balance DHCP Servers*.

Legacy DHCP Server Configuration Options

IN THIS SECTION

- DHCP Server Identifier | 88
- Static-Binding | 89
- Configuring Address Pools | 90
- Maximum Lease Time | 90
- Boot File and Boot Server | 91
- Domain Name and Domain Search | 92
- Router Name | 93
- DHCP Options | 94
- DHCP SIP Server | 95

If you are using the legacy DHCP on your device, use the following configuration options:

DHCP Server Identifier

The server identifier identifies a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).

You can configure DHCP server identifier in following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Example:

The following example shows a DHCP server identifier configured for an address pool:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
```

```
    server-identifier 10.3.3.1;
}
```

Static-Binding

A static binding defines a mapping between a fixed IP address and the client's MAC address.

Static bindings provide configuration information for specific clients. This information can include one or more fixed Internet addresses, the client hostname, and a client identifier.

```
[edit system services dhcp]
static-binding mac-address {
    fixed-address {
        address;
    }
    host client-hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
}
```

In the static-binding configuration, you must configure following parameters:

- The *mac-address* variable specifies the MAC address of the client. This is a hardware address that uniquely identifies each client on the network.
- The `fixed-address` statement specifies the fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.
- The `host` statement specifies the hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the `domain-name` statement.
- The `client-identifier` statement is used by the DHCP server to index the database of address bindings. The client identifier is either an ASCII string or hexadecimal digits. It can include a type-value pair as specified in RFC 1700, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

  For each unique `client-identifier` *client-id* value, the DHCP server issues a unique lease and IP address from the pool. Previously, when the client provided an incorrect `client-identifier` *client-id* value, the DHCP server did not issue a lease.

Example:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
```

```
    fixed-address {
        10.5.5.5;
        10.6.6.6;
    }
    host-name "another-host.domain.tld";
    client-identifier hexadecimal 01001122aabbcc;
}
```

Configuring Address Pools

For dynamic bindings, set aside a pool of IP addresses that can be assigned to clients. Addresses in a pool must be available to clients on the same subnet. Configure the following options:

```
[edit system services dhcp]
pool address</prefix-length> {
    address-range {
        low address;
        high address;
    }
    exclude-address {
        address;
    }
}
```

Example:

```
[edit system services dhcp]
pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
    exclude-address {
        10.3.3.33;
    }
}
```

Maximum Lease Time

For clients that do not request a specific lease time, the default lease time is one day. You can configure a maximum lease time for IP address assignments or change the default lease time.

To configure maximum lease time, include the `maximum-lease-time` statement:

```
maximum-lease-time;
default-lease-time;
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Lease times defined for static bindings and address pools take priority over lease times defined at the `[edit system services dhcp]` hierarchy level.

The `maximum-lease-time` statement configures the maximum length of time in seconds for which a client can request and hold a lease. If a client requests a lease longer than the maximum specified, the lease is granted only for the maximum time configured on the server. After a lease expires, the client must request a new lease.

NOTE: Maximum lease times do not apply to dynamic BOOTP leases. These leases are not specified by the client and can exceed the maximum lease time configured.

The following example shows a configuration for maximum and default lease times:

```
[edit system services dhcp]
maximum-lease-time 7200;
default-lease-time 3600;
```

Boot File and Boot Server

When a DHCP client starts, it contacts a boot server to download the boot file.

To configure a boot file and boot server, include the `boot-file` and `boot-server` statements:

After a client receives a **DHCPOFFER** response from a DHCP server, the client can communicate directly with the boot server (instead of the DHCP server) to download the boot file. This minimizes

network traffic and enables you to specify separate boot server/file pairs for each client pool or subnetwork.

```
boot-file filename;
boot-server (address | hostname);
```

You can include these statements at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

Example:

```
[edit system services dhcp]
pool 10.4.4.0/24 {
    boot-file "boot.client";
    boot-server 10.4.4.1;
}
```

Domain Name and Domain Search

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

To configure a domain search list, include the `domain-search` statement:

```
domain-search [ domain-list ];
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

The `domain-search` statement sets the order in which clients append domain names when searching for the IP address of a host. You can include one or more domain names in the list. For more information, see RFC 3397, *Dynamic Host Configuration Protocol (DHCP) Domain Search Option*.

The `domain-search` statement is optional, if you do not configure a domain search list, the default is the client's current domain.

Router Name

After a DHCP client loads the boot image and has booted, the client sends packets to a router.

To configure routers available to the DHCP client, include the `router` statement:

The `router` statement specifies a list of IP addresses for routers on the client's subnet. List routers in order of preference. You must configure at least one router for each client subnet.

The following example shows routers configured at the `[edit system services dhcp]` hierarchy level:

```
router {
    address;
}
```

Example:

```
[edit system services dhcp]
router {
    10.6.6.1;
    10.7.7.1;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

DHCP Options

You can configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

Example

```
[edit system services dhcp]
option 19 flag off;       # 19: "IP Forwarding" option
option 40 string "domain.tld"; # 40: "NIS Domain" option
option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
```

User-defined options that conflict with DHCP configuration statements are ignored by the server. For example, in the following configuration, the DHCP server ignores the user-defined `option 3 router` statement and uses the `router` statement instead:

```
[edit system services dhcp]
option 3 router 10.7.7.2;      # 3: "Default Router" option
router {
    10.7.7.1;
}
```

You can include this statement at the following hierarchy levels:

```
[edit system services dhcp]
[edit system services dhcp pool]
[edit system services dhcp static-binding]
```

DHCP SIP Server

You can use the `sip-server` statement on the EX Series switch to configure option 120 on a DHCP server. The DHCP server sends configured option values—Session Initiation Protocol (SIP) server addresses or names—to DHCP clients when they request them. Previously, you were only allowed to specify a SIP server by address using `[edit system services dhcp option 120]`. You specify either an IPv4 address or a fully qualified domain name to be used by SIP clients to locate a SIP server. You cannot specify both an address and name in the same statement.

```
[edit system services dhcp]
user@switch# set sip-server address
```

For example, to configure one address:

```
[edit system services dhcp]
user@switch set sip-server 192.168.0.11
```

To configure a SIP server using the *name* option:

```
[edit system services dhcp]
user@switch# set sip-server name
```

For example, to configure a name:

```
[edit system services dhcp]
user@switch set sip-server abc.example.com
```

RELATED DOCUMENTATION

- IP Address Assignment Pool | 27
- DHCPv6 Address-Assignment Pools | 39
- Legacy DHCP and Extended DHCP | 16

Verifying DHCP Server Configuration

IN THIS SECTION

- Verifying DHCP Server Binding and Server Statistics | 96
- Viewing DHCP Bindings (Legacy DHCP) | 98
- Viewing DHCP Address Pools (Legacy DHCP) | 99
- Viewing and Clearing DHCP Conflicts (Legacy DHCP) | 99

This topic discusses on various steps involved in verifying the DHCP server configuration.

Verifying DHCP Server Binding and Server Statistics

IN THIS SECTION

- Purpose | 96
- Action | 97

Purpose

View or clear information about client address bindings and statistics for the extended DHCP local server.

NOTE: If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Action

- To display the address bindings in the client table on the extended DHCP local server:

```
user@host> show dhcp server binding
```

- To display extended DHCP local server statistics:

```
user@host> show dhcp server statistics routing-instance customer routing instance
```

- To display the address bindings in the client table on the extended DHCP local server at routing-instance level:

```
user@host> show dhcp server binding routing-instance customer routing instance
```

- To display extended DHCP local server statistics at routing-instance level:

```
user@host> show dhcp server statistics routing-instance customer routing instance
```

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server at routing-instance level:

```
user@host> clear dhcp server binding routing-instance customer routing instance
```

- To clear all extended DHCP local server statistics:

```
user@host> clear dhcp server statistics
```

- To clear the binding state of a DHCP client from the client table on the extended DHCP local server:

```
user@host> clear dhcp server binding
```

- To clear all extended DHCP local server statistics at routing-instance level:

```
user@host> clear dhcp server statistics routing-instance customer routing instance
```

Viewing DHCP Bindings (Legacy DHCP)

Use the CLI command `show system services dhcp binding` to view information about DHCP address bindings, lease times, and address conflicts.

The following example shows the binding type and lease expiration times for IP addresses configured on a router that supports a DHCP server:

```
user@host> show system services dhcp binding
IP Address       Hardware Address     Type    Lease expires at
192.168.1.2      00:a0:12:00:12:ab       static      never
192.168.1.3      00:a0:12:00:13:02       dynamic     2004-05-03 13:01:42 PDT
```

Enter an IP address to show binding for a specific IP address:

```
user@host> show system services dhcp binding 192.168.1.3
DHCP binding information:
IP address      192.168.1.3
Hardware address      00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30 aced-00:a0:12:00
3a 31 33 3a 30 32
Lease information:
Type       dynamic
Obtained at       2004-05-02 13:01:42 PDT
Expires at       2004-05-03 13:01:42 PDT
```

Use the `detail` option to show detailed binding information:

```
user@host> show system services dhcp binding detail
DHCP binding information:
```

```
IP address                 192.168.1.3
Hardware address           00:a0:12:00:12:ab
Pool                       192.168.1.0/24
Interface                  fe-0/0/0, relayed by 192.168.4.254
Lease information:
Type                       dynamic
Obtained at                2004-05-02 13:01:42 PDT
Expires at                 2004-05-03 13:01:42 PDT
DHCP options:
name-server foo.mydomain.tld
domain-name mydomain.tld
option 19 flag off
```

Viewing DHCP Address Pools (Legacy DHCP)

Use the CLI `show system services dhcp pool` command to view information about DHCP address pools.

The following example show address pools configured on a DHCP server:

```
user@ host> show system services dhcp pool
Pool name        Low address     High address     Excluded addresses
10.40.1.0/24     10.40.1.1       10.40.1.254      10.40.1.254
```

Viewing and Clearing DHCP Conflicts (Legacy DHCP)

When a client receives an IP address from the DHCP server, the client performs a series of ARP tests to verify that the IP address is available and no conflicts exist. If the client detects an address conflict, the client notifies the DHCP server about the conflict and may request another IP address from the DHCP server.

The DHCP server keeps a log of all conflicts and removes addresses with conflicts from the pool. These addresses remain excluded until you manually clear the conflicts list with the `clear system services dhcp conflict` command. Use the CLI command `show system services dhcp conflict` to show conflicts.

```
user@host> show system services dhcp conflict
Detection time                 Detection method       Address
```

```
2004-08-03 19:04:00 PDT         client      192.168.1.5
2004-08-04 04:23:12 PDT         ping      192.168.1.8
```

Use the `clear system services dhcp conflicts` command to clear the conflicts list and return IP addresses to the pool. The following command shows how to clear an address on the server that has a conflict:

```
user@host> clear system services dhcp conflict 192.168.1.5
```

For more information about CLI commands you can use with the DHCP server, see the CLI Explorer.

RELATED DOCUMENTATION

- DHCP Server | 49
- DHCP Server Options | 77
- IP Address Assignment Pool | 27
- DHCP Access Service Overview | 9

Monitoring the DHCP Server Configuration

IN THIS SECTION

- Tracing DHCP Local Server Operations | 101

This topic discusses about how to trace various DHCP operations in a DHCP server. You can use various trace options discussed in this topic to troubleshoot any issues that arise in the DHCP server. For more information, read this topic.

Tracing DHCP Local Server Operations

IN THIS SECTION

- Configuring the Filename of the DHCP Local Server Processes Log | 102
- Configuring the Number and Size of DHCP Local Server Processes Log Files | 102
- Configuring Access to the Log File | 102
- Configuring a Regular Expression for Lines to Be Logged | 103
- Configuring Trace Option Flags | 103

The extended DHCP tracing operations track the extended DHCP local server operations and record them in a log file. By default, no extended DHCP local server processes are traced. If you include the `traceoptions` statement at the `[edit system processes dhcp-service]` hierarchy level, the default tracing behavior is the following:

- Important extended DHCP local server events are logged in a file called **jdhcpd** located in the **/var/log** directory.
- When the file **jdhcpd** reaches 128 kilobytes (KB), it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten. For more information about how log files are created, see the *Junos System Log Messages Reference*.
- Log files can be accessed only by the user who configures the tracing operation.

To trace DHCP local server operations, include the `traceoptions` statement at the `[edit system processes dhcp-service]` hierarchy level:

```
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-
readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

The following topics describe the tracing operation configuration statements:

Configuring the Filename of the DHCP Local Server Processes Log

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the `file` statement at the `[edit system processes dhcp-service traceoptions]` hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename;
```

Configuring the Number and Size of DHCP Local Server Processes Log Files

By default, when the trace file reaches 128 kilobytes (KB) in size, it is renamed **jdhcpd.0**, then **jdhcpd.1**, and so on, until there are three trace files. Then the oldest trace file (**jdhcpd.2**) is overwritten.

You can configure the limits on the number and size of trace files by including the following statements at the `[edit system processes dhcp-service traceoptions]` hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename files number size size;
```

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**jdhcpd**) reaches 2 MB, **jdhcpd** is renamed **jdhcpd.0**, and a new file called **jdhcpd** is created. When the new **jdhcpd** reaches 2 MB, **jdhcpd.0** is renamed **jdhcpd.1** and ***filename*** is renamed **jdhcpd.0**. This process repeats until there are 20 trace files. Then the oldest file (**jdhcpd.19**) is overwritten by the newest file (**jdhcpd.0**).

The number of files can be from 2 through 1000 files. The file size of each file can be from 10KB through 1 gigabyte (GB).

Configuring Access to the Log File

By default, log files can be accessed only by the user who configures the tracing operation.

To specify that any user can read all log files, include the `file world-readable` statement at the `[edit system processes dhcp-service traceoptions]` hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename world-readable;
```

To set the default behavior explicitly, include the `file no-world-readable` statement at the `[edit system processes dhcp-service traceoptions]` hierarchy level:

```
[edit system processes dhcp-service traceoptions]
file filename no-world readable;
```

Configuring a Regular Expression for Lines to Be Logged

By default, the trace operations output includes all lines relevant to the logged events.

You can refine the output by including the `match` statement at the `[edit system processes dhcp-service traceoptions]` hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system processes dhcp-service traceoptions]
file filename match regex;
```

Configuring Trace Option Flags

By default, only important events are logged. You can configure the trace operations to be logged by including extended DHCP local server tracing flags at the `[edit system processes dhcp-service traceoptions]` hierarchy level:

```
[edit system processes dhcp-service traceoptions]
flag flag;
```

You can configure the following tracing flags:

- `all`—Trace all operations.
- `auth`—Trace authentication operations.
- `database`—Trace database events.
- `fwd`—Trace firewall process events.
- `general`—Trace miscellaneous events.
- `ha`—Trace high availability-related events.
- `interface`—Trace interface operations.
- `io`—Trace I/O operations.

- `packet`—Trace packet decoding operations.
- `performance`—Trace performance measurement operations.
- `profile`—Trace profile operations.
- `rpd`—Trace routing protocol process events.
- `rtsock`—Trace routing socket operations.
- `session-db`—Trace session database operations.
- `state`—Trace changes in state.
- `statistics`—Trace baseline statistics.
- `ui`—Trace user interface operations.

RELATED DOCUMENTATION

DHCP Server | **49**

DHCP Server Options | **77**

DHCP Server Configuration | **52**

Legacy DHCP and Extended DHCP | **16**

DHCPv6 Server

IN THIS SECTION

- DHCPv6 Local Server Overview | **105**
- DHCPv6 Server Overview | **106**
- Example: Configuring DHCPv6 Server Options | **108**
- Specifying the Address Pool for IPv6 Prefix Assignment | **113**
- Specifying the Delegated Address Pool for IPv6 Prefix Assignment | **114**
- Preventing Binding of Clients That Do Not Support Reconfigure Messages | **115**
- Configuring DHCPv6 Rapid Commit (MX Series, EX Series) | **116**

- Allow Host Inbound Traffic for DHCPv6 Traffic | **117**
- Verifying and Managing DHCPv6 Local Server Configuration | **118**
- Understanding Cascaded DHCPv6 Prefix Delegating | **119**
- Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) | **120**
- SLAAC (Stateless Address Auto-Configuration) | **150**

Junos OS device can act as a DHCPv6 server and allocates IP addresses to IPv6 clients. DHCPv6 server also delivers configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. For more information, read this topic.

DHCPv6 Local Server Overview

The DHCPv6 local server is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the extended DHCP local server or DHCP relay agent.

The DHCPv6 local server provides many of the same features as the DHCP local server, including:

- Configuration for a specific interface or for a group of interfaces
- Site-specific usernames and passwords
- Numbered Ethernet interfaces
- Statically configured CoS and filters
- AAA directed login
- Use of the IA_NA option to assign a specific address to a client

When a DHCPv6 client logs in, the DHCPv6 local server can optionally use the AAA service framework to interact with the RADIUS server. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters.

The client username, which uniquely identifies a subscriber or a DHCP client, must be present in the configuration in order for DHCPv6 local server to use RADIUS authentication.

You can configure DHCPv6 local server to communicate the following attributes to the AAA service framework and RADIUS at login time:

- Client username
- Client password

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 8 on page 106 to configure the client:

Table 8: RADIUS Attributes and VSAs for DHCPv6 Local Server

Attribute Number	Attribute Name	Description
27	Session-Timeout	Lease time, in seconds. If not supplied, the lease does not expire
123	Delegated-IPv6-Prefix	Prefix that is delegated to the client
26-143	Max-Clients-Per-Interface	Maximum number of clients allowed per interface

To configure the extended DHCPv6 local server on the router (or switch), you include the `dhcpv6` statement at the `[edit system services dhcp-local-server]` hierarchy level.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems` *`logical-system-name`* `system services dhcp-local-server]`
- `[edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `system services dhcp-local-server]`
- `[edit routing-instances` *`routing-instance-name`* `system services dhcp-local-server]`

DHCPv6 Server Overview

A Dynamic Host Configuration Protocol version 6 (DHCPv6) server can automatically allocate IP addresses to IPv6 clients and deliver configuration settings to client hosts on a subnet or to the requesting devices that need an IPv6 prefix. A DHCPv6 server allows network administrators to manage pool of IP addresses centrally among hosts and to automate the assignment of IP addresses in a network.

NOTE: SRX Series Firewalls do not support DHCP client authentication. In a DHCPv6 deployment, security policies control access through the device for any DHCP client that has received an address and other attributes from the DHCPv6 server.

Some features include:

- Configuration for a specific interface or a group of interfaces
- Stateless address autoconfiguration (SLAAC)
- Prefix delegation, including access-internal route installation
- DHCPv6 server groups

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the `[edit system services dhcp-local-server]` hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the `[edit access address-assignment pool]` hierarchy level using the `family inet6` statement.

You can also include the `dhcpv6` statement at the `[edit routing-instances` *`routing-instance-name`* `system services dhcp-local-server]` hierarchy.

NOTE: Existing DHCPv4 configurations in the `[edit system services dhcp]` hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 39

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 43

Example: Configuring DHCPv6 Server Options

IN THIS SECTION

- Requirements | 108
- Overview | 108
- Configuration | 109
- Verification | 112

This example shows how to configure DHCPv6 server options on SRX1500, SRX5400, SRX5600, and SRX5800 devices.

Requirements

Before you begin:

- Determine the IPv6 address pool range.
- Determine the IPv6 prefix. See the *Understanding Address Books*.
- Determine the grace period, maximum lease time, or any custom options that should be applied to clients.
- List the IP addresses that are available for the devices on your network; for example, DNS and SIP servers.

Overview

In this example, you set a default client limit as 100 for all DHCPv6 groups. You then create a group called my-group that contains at least one interface. In this case, the interface is ge-0/0/3.0. You set a range of interfaces using the upto command and set a custom client limit as 200 for group my-group that overrides the default limit. Finally, you configure interface ge-0/0/3.0 with IPv6 address 2001:db8:3001::1/64 and set router advertisement for interface ge-0/0/3.0. Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option **dynamic-server** to dynamically support prefix and attributes that are updated by the WAN server.

NOTE: A DHCPv6 group must contain at least one interface.

Configuration

IN THIS SECTION

- Procedure | 109

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0
set system services dhcp-local-server dhcpv6 group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
set system services dhcp-local-server dhcpv6 group my-group overrides interface-client-limit 200
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
set protocols router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure DHCPv6 server options:

1. Configure a DHCP local server.

```
[edit]
user@host# edit system services dhcp-local-server dhcpv6
```

2. Set a default limit for all DHCPv6 groups.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set overrides interface-client-limit 100
```

3. Specify a group name and interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0
```

4. Set a range of interfaces.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface ge-0/0/3.0 upto ge-0/0/6.0
```

5. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

6. Configure an interface with an IPv6 address.

```
[edit interfaces]
user@host# set ge-0/0/3 unit 0 family inet6 address 2001:db8:3000::1/64
```

7. Set router advertisement for the interface.

```
[edit protocols]
user@host# set router-advertisement interface ge-0/0/3.0 prefix 2001:db8:3000::/64
```

Results

From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server`, `show interfaces ge-0/0/3`, and `show protocols` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
    overrides {
    interface-client-limit 100;
    ]
        group my-group {
        overrides {
        interface-client-limit 200;
        }
        interface ge-0/0/3.0 {
            upto ge-0/0/6.0;
        }
    }
}
        [edit]
            user@host# show interfaces ge-0/0/3
        unit 0 {
        family inet6 {
            address 2001:db8:3000::1/64;
        }
    }
        [edit]
            user@host# show protocols
            router-advertisement {
            interface ge-0/0/3.0 {
            prefix 2001:db8:3000::1/64;
        }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying DHCPv6 Local Server Configuration | **112**

Verifying DHCPv6 Local Server Configuration

Purpose

Verify that the client address bindings and statistics for the DHCPv6 local server have been configured

Action

From operational mode, enter the `show dhcpv6 server binding` command to display the address bindings in the client table on the DHCPv6 local server.

```
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:bd8:1111:2222::/64 6           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:01
2001:bd8:1111:2222::/64 7           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
2001:bd8:1111:2222::/64 8           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
2001:bd8:1111:2222::/64 9           86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:04
2001:bd8:1111:2222::/64 10          86321    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:05
```

From operational mode, enter the `show dhcpv6 server statistics` command to display the DHCPv6 local server statistics.

```
Dhcpv6 Packets dropped:
    Total               0
```

```
Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
```

- `clear dhcpv6 server bindings all` command to clear all DHCPv6 local server bindings. You can clear all bindings or clear a specific interface, or routing instance.
- `clear dhcpv6 server statistics` command to clear all DHCPv6 local server statistics.

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 39

Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment | 43

Specifying the Address Pool for IPv6 Prefix Assignment

The DHCPv6 server configuration usually consists of DHCPv6 options for clients, an IPv6 prefix, an address pool that contains IPv6 address ranges and options, and a security policy to allow DHCPv6 traffic. In a typical setup, the provider Juniper Networks device is configured as an IPv6 prefix delegation server that assigns addresses to the customer edge device. The customer's edge router then provides addresses to internal devices.

To configure DHCPv6 local server on a device, you include the DHCPv6 statement at the `[edit system services dhcp-local-server]` hierarchy level. You then create an address assignment pool for DHCPv6 that is configured in the `[edit access address-assignment pool]` hierarchy level using the `family inet6` statement.

You can also include the `dhcpv6` statement at the `[edit routing-instances` *`routing-instance-name`* `system services dhcp-local-server]` hierarchy.

NOTE: Existing DHCPv4 configurations in the `[edit system services dhcp]` hierarchy are not affected when you upgrade to Junos OS Release 10.4 from an earlier version or enable DHCPv6 server.

To configure the address pool for DHCPv6 local server:

1. Set an address-assignment pool name, family name, and prefix.

```
[edit access]
user@host# set address-assignment pool POOL family inet6 prefix 2001:db8::/64
```

2. Set the range.

```
[edit access]
user@host# set address-assignment pool POOL family inet6 range RANGE1 low 2001:db8::2/128
user@host# set address-assignment pool POOL family inet6 range RANGE1 high 2001:db8::aaaa/128
```

SEE ALSO

IP Address Assignment Pool | 27

DHCPv6 Address-Assignment Pools | 39

Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

- On routers—Subscriber management uses the pool to assign IPv6 prefixes for subscribers. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.
- On switches—DHCP management uses the pool to assign IPv6 prefixes for DHCP clients. You can specify the delegated address pool globally, for a specific group of interfaces, or for a particular interface.

NOTE: You can also use by Juniper Networks VSA 26-161 to specify the delegated address pool. The VSA-specified value always takes precedence over the `delegated-address` statement.

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

2. Configure the delegated address pool.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set delegated-pool paris-cable-12
```

SEE ALSO

Overriding the Default DHCP Local Server Configuration Settings

Understanding Differences Between Legacy DHCP and Extended DHCP

Extended DHCP Relay Agent Overview

Preventing Binding of Clients That Do Not Support Reconfigure Messages

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.

To configure the DHCPv6 local server to bind only clients that support client-initiated reconfiguration:

- Specify strict reconfiguration.

  For all DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set strict
  ```

  For only a particular group of DHCPv6 clients:

  ```
  [edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
  user@host# set strict
  ```

The `show dhcpv6 server statistics` command displays a count of solicit messages that the server has discarded.

SEE ALSO

> *Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview*
>
> *Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients*

Configuring DHCPv6 Rapid Commit (MX Series, EX Series)

You can configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the `overrides` options:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

2. Enable rapid commit support:

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set  rapid-commit
```

SEE ALSO

> *Overriding the Default DHCP Local Server Configuration Settings*

Allow Host Inbound Traffic for DHCPv6 Traffic

For the DHCPv6 server to allow DHCPv6 requests, you must configure host inbound traffic system services to allow DCHPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 2001:db8:3001::1.

To create a security zone policy to allow DHCPv6 on SRX1500, SRX5400, SRX5600, and SRX5800 devices:

1. Create the zone and add an interface to that zone.

```
[edit security zones]
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```

2. Configure host inbound traffic system services to allow DCHPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]
user@host# set host-inbound-traffic system-services dhcpv6
```

3. If you are done configuring the device, enter `commit` from configuration mode.

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses | 39

Verifying and Managing DHCPv6 Local Server Configuration

IN THIS SECTION

- Purpose | 118
- Action | 118

Purpose

View or clear information about client address bindings and statistics for the DHCPv6 local server.

Action

- To display the address bindings in the client table on the DHCPv6 local server:

```
user@host> show dhcpv6 server binding
```

- To display DHCPv6 local server statistics:

```
user@host> show dhcpv6 server statistics
```

- To clear all DHCPv6 local server statistics:

```
user@host> clear dhcpv6 server binding
```

- To clear all DHCPv6 local server statistics:

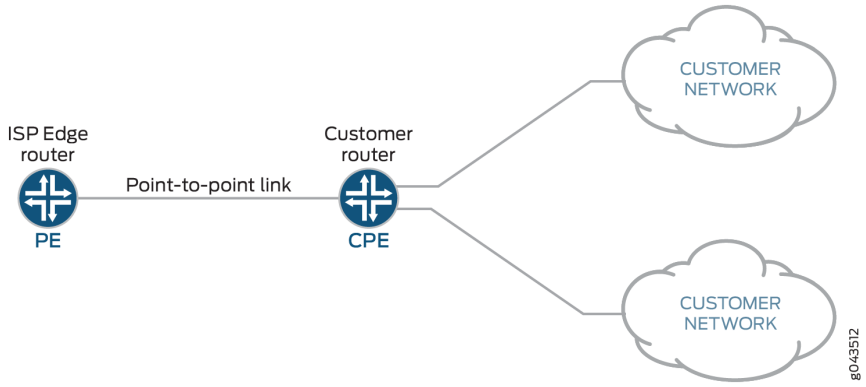
```
user@host> clear dhcpv6 server statistics
```

Understanding Cascaded DHCPv6 Prefix Delegating

You can use DHCPv6 client prefix delegation to automate the delegation of IPv6 prefixes to the customer premises equipment (CPE). With prefix delegation, a delegating device delegates IPv6 prefixes to a requesting device. The requesting device then uses the prefixes to assign global IPv6 addresses to the devices on the subscriber LAN. The requesting device can also assign subnet addresses to subnets on the LAN.

With cascaded prefix delegation, the IPv6 address block is delegated to a DHCPv6 client that is running on the WAN interface of a customer edge device. The identity association (IA) for the client is used for the identity association for prefix delegation (IA_PD). The CE device requests, through DHCPv6, an IPv6 address with the IA type of nontemporary addresses (IA_NA). Both IA_PD and IA_NA are requesting in the same DHCPv6 exchange.

Figure 8: IPv6 Prefix Delegation

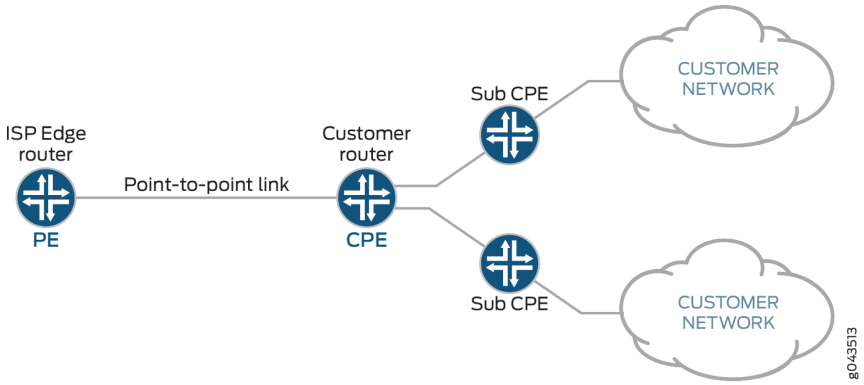


The topology in Figure 8 on page 119shows an SRX Series Firewall acting as the CPE. The WAN interface links to the provider edge (PE) device and the LAN interfaces link to the customer networks. The service provider delegates a prefix (delegated-prefix) and an IPv6 address (cpe-wan-ipv6-address) to a DHCPv6 client. When a requesting device receives that IPv6 address through the DHCPv6 client, the device must install the IPv6 address on its WAN interface. The DHCPv6 client then divides the delegated prefix into sub-prefixes and subsequently assigns them to the connected LAN interfaces of the CPE device, making some subset of the remaining space available for sub-prefix delegation.

A CPE assigns sub-prefixes to its LAN interfaces and broadcasts the sub-prefixes through device advertisement. In this scenario, the CPE acts as a sub-PE and delegates sub-prefixes and assigns them to sub-CPEs.

NOTE: The requirements of sub-prefix delegation are the same as for the prefix delegation defined in RFC 3769.

Figure 9: Sub-prefix Delegation



There can be multi-level sub prefix delegations, see Figure 9 on page 120. The top level CPE gets a delegated prefix from the PE and delegates the sub prefixes to second level sub-CPEs, then to the third level sub-CPEs, and finally to the end levels. The end level sub-CPEs assign the IPv6 address to end hosts through SLAAC, stateless DHCPv6 or stateful DHCPv6. This is called cascaded prefix delegating.

Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE)

IN THIS SECTION

- Requirements | 121
- Overview | 121
- Configuration | 122
- Verification | 143

This example shows how to configure DHCPv6 PD over PPPoE on SRX Series Firewalls.

Requirements

No special configuration beyond the device initialization is required before configuring this feature.

Overview

IN THIS SECTION

- Topology | 121

The example uses SRX550M devices for configuring DHCPv6 PD over PPPoE. Before you begin, configure DHCPv6 server to permit in host-inbound traffic and receive DHCPv6 packet. Provide a host-name to establish PPPoE session. To enable IPv6, chassis reboot is required.

Configuring DHCPv6 PD over PPPoE involves the following configurations:

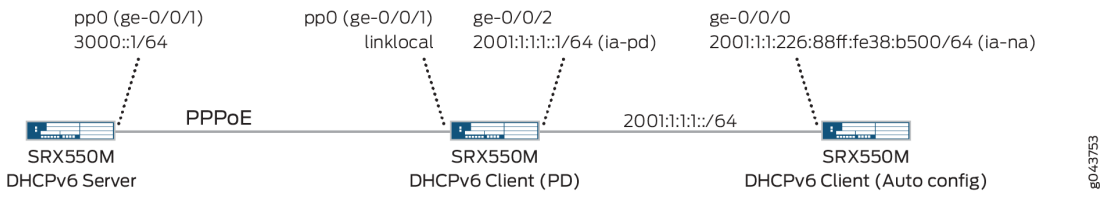
- Configuring DHCPv6 Server
- DHCPv6 Client (PD)
- DHCPv6 Client (Auto)

Topology

The following illustration describes DHCPv6 PD over PPPoE topology which provide a configuration suite using SRX Series Firewalls.

Figure 10 on page 121 shows the topology used in this example.

Figure 10: Configuring SRX Series Firewalls for DHCPv6 PD over PPPoE



Configuration

IN THIS SECTION

- CLI Quick Configuration | 122
- Procedure | 125
- Procedure | 129
- Procedure | 133
- Results | 134

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Quick configuration for DHCPv6 Server:

- DHCPv6 server configuration

```
set interfaces ge-0/0/1 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group overrides interface-client-limit
200
set system services dhcp-local-server dhcpv6 group my-group overrides delegated-pool v6-pd-
pool
set system services dhcp-local-server dhcpv6 group my-group interface pp0.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap access-profile prof-ge001
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options server
set interfaces pp0 unit 0 family inet6 address 3000::1/64
```

- Router advertisement configuration

```
set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
set protocols router-advertisement interface pp0.0 managed-configuration
set protocols router-advertisement interface pp0.0 other-stateful-configuration
set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- PPPoE profile configuration

```
set access profile prof-ge001 client test_user chap-secret test
```

- PD address pool configuration

```
set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-length 48
set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-server 3000::1
```

- Security zone configuration

```
set security zones security-zone trust interface pp0.0 host-inbound-traffic system-services
dhcpv6
```

Quick configuration for DHCPv6 Client (PD):

- DHCPv6 server configuration

```
set interfaces ge-0/0/1 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
set interfaces pp0 unit 0 ppp-options chap local-name test_user
set interfaces pp0 unit 0 ppp-options chap passive
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options client
```

- DHCPv6 client configuration

```
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 other-stateful-configuration
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 max-advertisement-interval 10
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 min-advertisement-interval 5
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
set protocols router-advertisement interface pp0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- DHCPv6 server propagate configuration

```
set access address-assignment pool p1 family inet6 prefix 2001::/16
set access address-assignment pool p1 family inet6 dhcp-attributes propagate-settings pp0.0
```

- Security zone configuration

```
set security zones security-zone untrust interface pp0.0 host-inbound-traffic system-services
dhcpv6
```

```
set security zones security-zone trust interface ge-0/0/2.0 host-inbound-traffic system-
services dhcpv6
```

Quick configuration for DHCPv6 Client (Auto):

- DHCPv6 client configuration

```
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

- Router advertisement configuration

```
set protocols router-advertisement interface ge-0/0/0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- Security zone configuration

```
set security zones security-zone trust interface ge-0/0/0.0 host-inbound-traffic system-
services dhcpv6
```

Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

1. To configure DHCPv6 server on SRX550M device:

   a. Set the interface.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet6
```

b. Configure a DHCP local server.

```
[edit ]
user@host# set system services dhcp-local-server dhcpv6
```

c. Set a default limit for all DHCPv6 groups.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set overrides interface-client-limit 100
```

d. Set a custom client limit for the group.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides interface-client-limit 200
```

e. Specify delegated pool name.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides delegated-pool v6-pd-pool
```

f. Create a group called my-group that contains pp0 interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface pp0.0
```

2. Configuring PPPoE:

a. Set interface to encapsulate PPPoE.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

b. Set chap access profile value.

```
[edit system interface]
user@host# set interface pp0 unit 0 ppp-options chap access-profile prof-ge001
```

c. Set underlying interface name.

```
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

d. Set PPPoE-options server.

```
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options server
```

e. Set family name and address.

```
[edit system interface]
user@host# set interface pp0 unit 0 family inet6 address 3000::1/64
```

3. Configuring Router advertisement:

a. Set max advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
```

b. Set minimum advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
```

c. Set the configuration state to managed configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 managed-configuration
```

d. Set the configuration state to other stateful configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 other-stateful-configuration
```

e. Set the prefix value.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

4. Enable IPv6:

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring PPPoE profile:

a. Set access profile name, client name and chap secret.

```
[edit]
user@host# set access profile prof-ge001 client test_user chap-secret test
```

6. Configuring PD address pool:

a. Set address-assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
```

b. Set range and prefix length.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-
length 48
```

c. Set dhcp attributes with dns server value.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-
server 3000::1
```

7. Configuring Security zone:

   a. Set the zone name, interface and host-inbound-traffic system-services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic
system-services dhcpv6
```

Procedure

Step-by-Step Procedure

1. To configure DHCPv6 client (PD) on SRX550M device:

   a. Set the interface.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet6
```

   b. Set DHCPv6 local server to override the interface client limit.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
```

   c. Set the process-inform pool name.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
```

   d. Set group name and interface.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
```

2. Configuring PPPoE:

a. Set the interface to encapsulate ppp over ethernet.

```
[edit system interface]
user@host# set interface ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

b. Set default chap secret.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
```

c. Set chap local name.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name test_user
```

d. Set PPP options chap state.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
```

e. Set underlying-interface.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

f. Set pppoe-options.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options client
```

3. Configuring DHCPv6 client:

a. Set the family name and dhcpv6 client type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
```

b. Set the dhcpv6 client identity association type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
```

c. Set update-router-advertisement interface and other stateful-configuration.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 other-stateful-configuration
```

d. Set maximum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 max-advertisement-interval 10
```

e. Set minimum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 min-advertisement-interval 5
```

f. Set client-identifier duid type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-
type duid-11
```

g. Set requested option for DHCPv6 client.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

h. Update the server.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
```

i. Set the protocols and the interface.

```
[edit]
user@host# set protocols router-advertisement interface pp0.0
```

4. Enable IPv6

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring DHCPv6 server to propagate DNS server information to end device:

a. Set address assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 prefix 2001::/16
```

b. Set the interface name for propagating TCP/IP settings to pool.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 dhcp-attributes propagate-
settings pp0.0
```

6. Configuring security zone:

a. Set the zone name, untrust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic
system-services dhcpv6
```

b. Set the trust interface.

```
[edit]
user@host# set security zones security-zone trust interface ge-0/0/2.0 host-inbound-
traffic system-services dhcpv6
```

Procedure

Step-by-Step Procedure

1. To configure DHCPv6 client (Auto) on SRX550M device:

   a. Set the interface, unit value, family name and DHCPv6 client type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
   ```

   b. Set Dhcpv6 client identity association type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
   ```

   c. Set client-identifier type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier
   duid-type duid-11
   ```

   d. Set DHCPV6 client requested option.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
   ```

2. Configuring router advertisement:

a. Set the protocol and interface.

```
[edit]
user@host# set protocols router-advertisement interface fe-0/0/0.0
```

3. Enable IPv6.

a. Set family name and mode.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

4. Configuring security zone:

5. Set the zone name, trust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic system-
services dhcpv6
```

Results

- Result for DHCPv6 Server:

From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server`, `show interfaces`, `show protocols`, `show security forwarding-options`, `show access profile prof-ge001`, `show access address-assignment pool`, and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
    overrides {
        interface-client-limit 100;
    }
    group my-group {
        overrides {
            interface-client-limit 200;
            delegated-pool v6-pd-pool;
        }
```

```
        interface pp0.0set;
        interface pp0.0;
    }
    }
...
[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
```

```
    }
}
...
[edit]
user@host# show protocols
interface pp0.0 {
    max-advertisement-interval 20;
    min-advertisement-interval 10;
    managed-configuration;
    other-stateful-configuration;
    prefix 3000::1/64;
}
...
[edit]
user@host# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
...
[edit]
user@host#  show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
        }
    }
}
...
[edit]
user@host# show security zones
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
```

```
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
```

- Result for DHCPv6 Client (PD):

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
    overrides {
        interface-client-limit 10;
        process-inform {
            pool p1;
        }
    }
    group my-group {
        overrides {
            interface-client-limit 200;
            delegated-pool v6-pd-pool;
        }
        interface pp0.0;
    }
    group ipv6 {
        interface ge-0/0/2.0;
    }
}
...
[edit]
user@host# show interfaces
ge-0/0/1 {
```

```
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
                local-name test_user;
                passive;
            }
        }
        pppoe-options {
            underlying-interface ge-0/0/1.0;
            client;
        }
    }
}
...
[edit]
user@host# show interfaces pp0
unit 0 {
    ppp-options {
        chap {
            default-chap-secret "$ABC123"; ## SECRET-DATA
            local-name test_user;
            passive;
        }
    }
    pppoe-options {
        underlying-interface ge-0/0/1.0;
        client;
    }
    family inet6 {
        dhcpv6-client {
            client-type statefull;
            client-ia-type ia-pd;
```

```
            update-router-advertisement {
                interface ge-0/0/2.0 {
                    other-stateful-configuration;
                    max-advertisement-interval 10;
                    min-advertisement-interval 5;
                }
            }
            client-identifier duid-type duid-ll;
            req-option dns-server;
        }
    }
}
...
[edit]
user@host# show security forwarding-options
    family {
        inet6 {
            mode flow-based;
        }
    }
...
[edit]
user@host# show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
        }
    }
}
pool p1 {
    family inet6 {
        prefix 2001::/16;
        dhcp-attributes {
            propagate-settings pp0.0;
        }
    }
}
...
```

```
[edit]
user@host# show access address-assignment
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
security-zone untrust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
```

- Result for DHCPv6 Client (Auto):

```
[edit]
user@host# show interfaces ge-0/0/0
unit 0 {
    family inet6 {
        dhcpv6-client {

            client-type autoconfig;
            client-ia-type ia-na;
            req-option dns-server;

        }
    }
}
...
[edit]
user@host# show protocols
router-advertisement {
    interface pp0.0 {
        max-advertisement-interval 20;
        min-advertisement-interval 10;
        managed-configuration;
        other-stateful-configuration;
        prefix 3000::1/64;
    }
    interface fe-0/0/0.0;
}
...
[edit]
user@host#  show security forwarding-options
    family {
        inet6 {
            mode flow-based;
        }
    }
...
[edit]
user@host# show security zones
security-zone Host {
    host-inbound-traffic {
        system-services {
```

```
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        fe-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
security-zone untrust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
```

```
    }
}
```

Verification

IN THIS SECTION

- Verifying DHCPv6 Server Configuration | **143**
- Verifying DHCPv6 Client (PD) Configuration | **144**
- Verifying DHCPv6 client (Auto) Configuration | **148**

Verifying DHCPv6 Server Configuration

Purpose

Verify that the DHCPv6 Server has been configured.

Action

- From operational mode, enter the `show dhcpv6 server binding` command.

  The following output shows the options for the `show dhcpv6 server binding` command.

```
[edit]
user@host>show dhcpv6 server binding detail
Session Id:  75
     Client IPv6 Prefix:                  2001:1:1::/48
     Client DUID:                         LL0x1-3c:94:d5:98:90:01
     State:                               BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Expires:                       2016-03-26 10:12:37 JST
     Lease Expires in:                    86213 seconds
     Lease Start:                         2016-03-25 10:12:37 JST
     Last Packet Received:                2016-03-25 10:12:50 JST
     Incoming Client Interface:           pp0.0
     Server Ip Address:                   0.0.0.0
     Client Prefix Pool Name:             v6-pd-pool
```

```
    Client Id Length:                    10
    Client Id:                           /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:1:1::/48      *[Access/13] 00:03:45     <<<<<< Route for end device will be
automatically generated
                    > to fe80::3e94:d50f:fc98:8600 via pp0.0
3000::/64          *[Direct/0] 00:04:04
                    > via pp0.0
3000::1/128        *[Local/0] 19:53:18
                      Local via pp0.0
fe80::b2c6:9a0f:fc7d:6900/128
                   *[Local/0] 19:53:18
                      Local via pp0.0
```

- From operational mode, enter the `show interfaces pp0.0 terse` command.

  The following output shows the options for the `show interfaces pp0.0 terse` command.

```
[edit]
user@host>show interfaces pp0.0 terse
Interface               Admin Link Proto    Local                 Remote
pp0.0                   up    up   inet6    3000::1/64
                                            fe80::b2c6:9a0f:fc7d:6900/64
```

Verifying DHCPv6 Client (PD) Configuration

Purpose

Verify that the DHCPv6 Client (PD) has been configured.

Action

- From operational mode, enter the `show dhcpv6 client binding detail` command.

  The following output shows the options for the `show dhcpv6 client binding detail` command.

```
[edit]
user@host>show dhcpv6 client binding detail
Client Interface: pp0.0
     Hardware Address:             3c:94:d5:98:86:01
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND) <<<<< SRX is bound to
prefix via pp0.0
     ClientType:                   STATEFUL
     Lease Expires:                2016-03-26 10:12:50 JST
     Lease Expires in:             86232 seconds
     Lease Start:                  2016-03-25 10:12:50 JST
     Bind Type:                    IA_PD
     Client DUID:                  LL0x29-3c:94:d5:98:86:01
     Rapid Commit:                 Off
     Server Ip Address:            fe80::b2c6:9a0f:fc7d:6900
     Update Server                 Yes
     Client IP Prefix:             2001:1:1::/48
DHCP options:
    Name: server-identifier, Value: VENDOR0x00000583-0x41453530
    Name: dns-recursive-server, Value: 3000::1
```

- From operational mode, enter the `show dhcpv6 server binding detail` command.

  The following output shows the options for the `show dhcpv6 server binding detail` command.

```
[edit]
user@host>show dhcpv6 server binding detail
Session Id:  75
     Client IPv6 Prefix:                   2001:1:1::/48
     Client DUID:                          LL0x1-3c:94:d5:98:90:01
     State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Expires:                        2016-03-26 10:12:37 JST
     Lease Expires in:                     86213 seconds
     Lease Start:                          2016-03-25 10:12:37 JST
     Last Packet Received:                 2016-03-25 10:12:50 JST
     Incoming Client Interface:            pp0.0
     Server Ip Address:                    0.0.0.0
```

```
    Client Prefix Pool Name:               v6-pd-pool
    Client Id Length:                      10
    Client Id:                             /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[Access-internal/12] 00:03:35
                    > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
2001:1:1:1::/64    *[Direct/0] 00:03:48
                    > via ge-0/0/2.0
2001:1:1:1::1/128  *[Local/0] 00:03:48      <<<<<< IPv6 address allocated by Prefix
delegation
                      Local via ge-0/0/2.0
3000::/64          *[Access-internal/12] 00:03:35
                    > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
fe80::/64          *[Direct/0] 00:03:48
                    > via ge-0/0/2.0
fe80::3e94:d50f:fc98:8600/128
                   *[Local/0] 19:05:19
                      Local via pp0.0
fe80::3e94:d5ff:fe98:8602/128
                   *[Local/0] 00:03:48
                      Local via ge-0/0/2.0
```

- From operational mode, enter the `show interfaces pp0.0 terse` command.

  The following output shows the options for the `show interfaces pp0.0 terse` command.

```
[edit]
user@host>show interfaces pp0.0 terse
Interface               Admin Link Proto    Local                 Remote
pp0.0                   up    up   inet6    fe80::3e94:d50f:fc98:8600/64
```

- From operational mode, enter the `show interfaces ge-0/0/2.0 terse` command.

  The following output shows the options for the `show interfaces ge-0/0/2.0 terse` command.

```
[edit]
user@host>show interfaces ge-0/0/2.0 terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/2.0              up    up   inet6    2000:1:1:1::1/64
                                            fe80::3e94:d5ff:fe98:8602/64
```

- From operational mode, enter the `show ipv6 router-advertisement` command.

  The following output shows the options for the `show ipv6 router-advertisement` command.

```
[edit]
user@host>show ipv6 router-advertisement
Interface: pp0.0
  Advertisements sent: 3, last sent 00:01:56 ago
  Solicits received: 0
  Advertisements received: 10
  Advertisement from fe80::b2c6:9a0f:fc7d:6900, heard 00:00:08 ago
    Managed: 1 [0]
    Other configuration: 1 [0]
    Reachable time: 0 ms
    Default lifetime: 60 sec [1800 sec]
    Retransmit timer: 0 ms
    Current hop limit: 64
    Prefix: 3000::/64
      Valid lifetime: 2592000 sec
      Preferred lifetime: 604800 sec
      On link: 1
      Autonomous: 1
Interface: ge-0/0/2.0
  Advertisements sent: 24, last sent 00:00:03 ago
  Solicits received: 0
  Advertisements received: 0
```

Verifying DHCPv6 client (Auto) Configuration

Purpose

Verify that the DHCPv6 client (Auto) has been configured.

Action

- From operational mode, enter the `show dhcpv6 client binding detail` command.

  The following output shows the options for the `show dhcpv6 client binding detail` command.

```
[edit]
user@host>show dhcpv6 client binding detail
Client Interface: fe-0/0/0.0
     Hardware Address:             00:26:88:38:b5:00
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
     ClientType:                   AUTO
     Lease Expires:                2016-03-26 10:15:35 JST
     Lease Expires in:             86395 seconds
     Lease Start:                  2016-03-25 10:15:35 JST
     Bind Type:                    IA_NA
     Client DUID:                  LL0x3-00:26:88:38:b5:00
     Rapid Commit:                 Off
     Server Ip Address:            fe80::3e94:d5ff:fe98:8602
     Client IP Address:            2001:1:1:1:226:88ff:fe38:b500/128
     Client IP Prefix:             2001:1:1:1::/64

DHCP options:
    Name: server-identifier, Value: VENDOR0x00000583-0x414c3131
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[Access-internal/12] 00:02:36
```

```
                     > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
2001:1:1:1::/64    *[Access-internal/12] 00:02:36
                     > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
2001:1:1:1:226:88ff:fe38:b500/128
                   *[Direct/0] 00:02:36
                     > via fe-0/0/0.0
                     [Local/0] 00:02:36
                       Local via fe-0/0/0.0
fe80::/64          *[Direct/0] 1w3d 15:51:19
                     > via fe-0/0/0.0
fe80::226:88ff:fe38:b500/128
                   *[Local/0] 1w3d 15:51:19
                       Local via fe-0/0/0.0
```

- From operational mode, enter the `show ipv6 router-advertisement` command.

  The following output shows the options for the `show ipv6 router-advertisement` command.

```
[edit]
user@host>show ipv6 router-advertisement
Interface: fe-0/0/0.0
  Advertisements sent: 1, last sent 00:02:45 ago
  Solicits received: 0
  Advertisements received: 8
  Advertisement from fe80::3e94:d5ff:fe98:8602, heard 00:00:02 ago
    Managed: 0
    Other configuration: 1 [0]
    Reachable time: 0 ms
    Default lifetime: 30 sec [1800 sec]
    Retransmit timer: 0 ms
    Current hop limit: 64
    Prefix: 2001:1:1:1::/64
      Valid lifetime: 86400 sec
      Preferred lifetime: 86400 sec
      On link: 1
      Autonomous: 1
```

SLAAC (Stateless Address Auto-Configuration)

IN THIS SECTION

- SLAAC Process | 150
- Configuring SLAAC | 151

SLAAC is an IPv6 protocol that provides some similar functionality to DHCP in IPv4. Using SLAAC, network hosts can autoconfigure a globally unique IPv6 address based on the prefix provided by a nearby router in a router advertisement.

SLAAC enables an IPv6 client to generate its own addresses using a combination of locally-available information and information advertised by routers through Neighbor Discovery Protocol (NDP).

SLAAC Process

Generating a Link-Local Address

The client begins auto-configuration by generating a link-local address for the IPv6-enabled interface. This is done by combining the advertised link-local prefix (first 64 bits) with the interface identifier (last 64 bits). The address is generated according to the following format: [fe80 (10 bits) + 0 (54 bits)] + interface ID (64 bits). The auto generated link-local address cannot be deleted. However, a new link-local address can also be manually entered, which overwrites the auto generated link-local address.

Generating a Global Address

The client sends a Router Solicitation message to prompt all routers on the link to send Router Advertisement (RA) messages. Routers that are enabled to support SLAAC send an RA that contains a subnet prefix for use by neighboring hosts. The client appends the interface identifier to the subnet prefix to form a global address, and again runs DAD to confirm its uniqueness.

Checking Duplicate Address

Before assigning the link-local address to its interface, the client verifies the address by running Duplicate Address Detection (DAD). DAD sends a Neighbor Solicitation message destined to the new address. If there is a reply, then the address is a duplicate and the process stops. If the address is unique, it is assigned to the interface

Configuring SLAAC

To enable SLAAC, use the following commands:

- Specify forwarding options for IPv6 traffic and set packet mode.

```
user@host# set security forwarding-options family inet6 mode packet-based
```

- Assign an IPv6 address to physical and loopback interfaces.

```
user@host# set interfaces ge-0/0/0 unit 0 family inet6 address 2001:db8:0:1::/64 eui-64
user@host# set interfaces lo0 unit 1 family inet6 address 2001:db8::1/128
```

- Configure the device to send router advertisements (RA) for the /64 prefix via ge-0/0/0.

```
user@host# set protocols router-advertisement interface ge-0/0/0 prefix 2001:db8:0:1::/64
```

The host uses the 64-bit prefix from the router and assigns the rest randomly or using EUI-64 to complete the 128-bit address.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
15.1X49-D70	Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option **dynamic-server** to dynamically support prefix and attributes that are updated by the WAN server.

RELATED DOCUMENTATION

DHCP Server Configuration | 52

DHCP Server Options | 77

dynamic-server

4

CHAPTER

DHCP Relay Agent

DHCP Relay Agent | 153

DHCP and BOOTP Relay Agent | 190

DHCP Relay Agent Information Option (Option 82) | 198

DHCPv6 Relay Agent | 222

DHCP Relay Proxy | 240

DHCP Relay Agent

IN THIS SECTION

- Understanding DHCP Relay Agent Operation | 153
- Minimum DHCP Relay Agent Configuration | 156
- Configuring DHCP Relay Agent | 159
- Configuring a DHCP Relay Agent on EX Series Switches | 172
- Configuring DHCP Smart Relay (Legacy DHCP Relay) | 172
- Disabling Automatic Binding of Stray DHCP Requests | 173
- Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets | 175
- Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent | 176
- Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address | 176
- Overriding the Default DHCP Relay Configuration Settings | 177
- Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally | 179
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings | 180
- Verifying and Managing DHCP Relay Configuration | 185
- Extended DHCP Relay Agent Overview | 187

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks. For more information, read this topic.

Understanding DHCP Relay Agent Operation

IN THIS SECTION

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers | 154

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

NOTE: All DHCP packets passing through a DHCP unconfigured interface might be dropped. Enabling the DHCP relay or DHCP server feature also enables the DHCP snooping feature, which analyzes all DHCP packets received through any interface of the device (both DHCP configured and unconfigured interfaces) .

Interfaces not listed under DHCP settings are considered as `unconfigured` interfaces. Depending on the configuration, DHCP packets received on DHCP unconfigured interfaces are dropped.

Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some differences in the details of usage.

On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.

2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.

3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.

4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.

5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.

6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.

7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.

8. The DHCP relay agent receives the ACK packet and forwards it to the client.

9. The DHCP client receives the ACK packet and stores the configuration information.

10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.

11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

On all Junos OS devices, when the DHCP relay is configured with `forward-only` option, and the DHCP client is terminated on logical tunnel interface if the logical tunnel interface

- Includes multiple logical interfaces
- Use same VLAN on multiple logical interfaces of the same `lt` interface

In such cases, the DHCP relay might fail to send the *OFFER* messages.

This issue applies in Junos OS Releases 19.3R3, 19.4R2, 18.4R3, 19.4R1, 19.3R2, 18.4R3-S1, 17.4R3 releases.

Minimum DHCP Relay Agent Configuration

IN THIS SECTION

- Configuring IPv4 and IPv6 Addresses on the Loopback Interface | 158

This example shows the minimum configuration you need to use the extended DHCP relay agent on your Junos OS device. Ensure that the device can connect to the DHCP server.

In this example, you direct certain DHCP client traffic to a DHCP server. You specify an active server group to which each client groups traffic is forwarded. Add server IP addresses to the active server group, You can configure an interface group and specifying the DHCP relay interface for the group. The interface used as the DHCP relay agent can forward messages to specific servers.

Configure DHCP Option 82 and forward-only feature.

This example creates active server group named `my-dhcp-servers-group` with IP address 203.0.113.21. The DHCP relay agent configuration is applied to a interfaces group named `my-dhcp-interfaces`. Within this group, the DHCP relay agent is enabled on interface ge-0/0/1.0.

1. Configure the option to forward the traffic, without creating a new subscriber session.

```
user@host# set forwarding-options dhcp-relay forward-only
```

2. Enable DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

```
user@host# set forwarding-options dhcp-relay relay-option-82 circuit-id use-interface-
description device
```

   Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID in DHCP packets that the DHCP relay agent sends to a DHCP server.

3. Configure DHCP server group and add the IP addresses of the DHCP server belonging to the group.

```
user@host# set forwarding-options dhcp-relay server-group my-dhcp-servers-group 203.0.113.2
```

4. Set the DHCP server group as active server group.

```
user@host# set forwarding-options dhcp-relay active-server-group my-dhcp-servers-group
```

   The DHCP relay agent relays DHCP client requests to the DHCP servers defined in the active server group.

5. Configure an interface group and specify the DHCP relay interface for the group.

```
user@host# set forwarding-options dhcp-relay group my-dhcp-interf-group interface ge-0/0/1.0
```

   DHCP relay runs on the interfaces defined in the group.

> **NOTE**: To configure a switch with DHCP relay in `forward-only` mode, check whether your DHCP server supports DHCP Option 82. See Verify support of Option-82 in DHCP Server for details.

The `forward-only` option in DHCP relay configurations do not require the S-SA-FP license to be installed.

From configuration mode, confirm your configuration by entering the `show forwarding-options` command and verify your configuration.

```
user@srx-01# show forwarding-options
dhcp-relay {
    relay-option-82 {
        circuit-id {
            use-interface-description device;
        }
    }
    forward-only;
    server-group {
        my-dhcp-servers-group {
            203.0.113.21;
        }
    }
    active-server-group my-dhcp-servers-group;
    group my-dhcp-interf-group {
        interface ge-0/0/1.0;
    }
}
```

Configuring IPv4 and IPv6 Addresses on the Loopback Interface

When you have configured a DHCP server in a different service VRFs, you must configure IPv4 and IPv6 addresses on the loopback interface in the server VRF configuration for DCHP-relay function to work in all other VRFs.

Configure the dhcp-relay forward-only-replies option to enable DHCP response packets forwarded to the DHCP clients in the other VRF.

```
[edit routing-instances]
Svr-1 {
        instance-type vrf;
        routing-options {
            auto-export;
        }
        protocols {
            evpn {
                ip-prefix-routes {
                    advertise direct-nexthop;
                    encapsulation vxlan;
                    vni 11000;
                    export type5-export;
                }
            }
        }
        forwarding-options {
            dhcp-relay {
                dhcpv6 {
                    forward-only-replies;
                }
                forward-only-replies;
            }
        }
        interface lo0.2;
        route-distinguisher 103.0.0.1:5000;
        vrf-import import-tenant;
        vrf-target target:5000:1;
        vrf-table-label;
}

    lo0 {
        unit 0 {
```

```
            family inet {
                address 103.0.0.1/32;
            }
            family inet6 {
                address 1003::1/128;
            }
        }
        unit 1 {
            family inet {
                address 103.0.0.1/32;
            }
            family inet6 {
                address 1003::1/128;
            }
        }
        unit 2 {
            family inet {
                address 103.0.0.2/32;
            }
            family inet6 {
                address 1003::2/128;
            }
        }
```

Configuring DHCP Relay Agent

IN THIS SECTION

- Requirements | **160**
- Overview | **160**
- Configuration | **161**
- Verification | **170**

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

This example describes how to configure the DHCP relay agent on the SRX Series Firewall. SRX Series Firewall acting as DHCP relay agent is responsible for forwarding the requests and responses between the DHCP clients and the server which are part of different routing instances.

Requirements

This example uses the following hardware and software components:

- SRX Series Firewalls with Junos OS 15.1X49-D10 or later.

Overview

IN THIS SECTION

- Topology | **160**

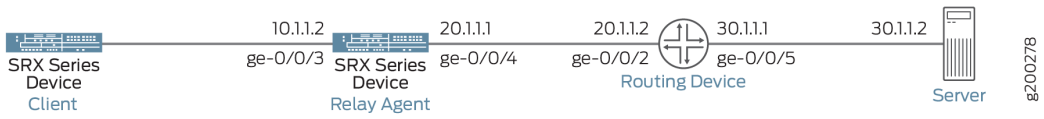
You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that is isolated from the client network.

Topology

To exchange DHCP messages between different routing instances, you must enable both the server-facing interface and the client-facing interface of the DHCP relay agent to recognize and forward DHCP packets.

The following Figure 11 on page 160 shows DHCP performance as DHCP local server, DHCP client, and DHCP relay agent

Figure 11: Understanding DHCP Services in a Routing Instance



The following list provides an overview of the tasks required to create the DHCP message exchange between the different routing instances:

- Configure the client-facing side of the DHCP relay agent.
- Configure the server-facing side of the DHCP relay agent.
- Configure the Security Zone to Allow the DHCP protocol.

Table1: DHCP Relay Parameters:

Parameters	Client-Side-Details	Server-Side-Details
interface	ge-0/0/3.0	ge-0/0/4.0
routing interface	trust-vr	untrust-vr
ip address	10.1.1.2/24	20.1.1.1/24

NOTE: In order to make this setup work, the DHCP server connecting route and relay agent interface route must be in both routing-instances. For example, in the above topology, the server route 30.1.1.0/24 needs to be shared with the dhcp-relay VR, and the dhcp-relay interface route 10.1.1.0/24 exact needs to be shared with the default routing instance.

Also, a dummy dhcp-relay config must be added in the routing instance with the DHCP server. If this is not configured, dhcp-relay will not be able to receive packets from the DHCP server.

Configuration

IN THIS SECTION

- CLI Quick Configuration | **162**
- Procedure | **163**
- Procedure | **164**
- Procedure | **164**
- Procedure | **166**

- Results | 166

CLI Quick Configuration

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different routing instances. To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Quick configuration for Client-Facing Support:

```
set routing-instances trust-vr instance-type virtual-router
set routing-instances trust-vr interface ge-0/0/3.0
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

Quick configuration for Server-Facing Support:

```
set routing-instances untrust-vr instance-type virtual-router
set routing-instances untrust-vr interface ge-0/0/4.0
set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Quick configuration for DHCP Relay Support:

```
set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-config
set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1 30.1.1.2
set routing-instances trust-vr forwarding-options dhcp-relay active-server-group server-1
set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr interface
ge-0/0/3.0
set routing-instances trust-vr routing-options instance-import export_dhcp_server_route
set policy-options policy-statement export_dhcp_server_route term 1 from instance untrust-vr
set policy-options policy-statement export_dhcp_server_route term 1 from route-filter
30.1.1.0/24 exact
set policy-options policy-statement export_dhcp_server_route term 1 then accept
set policy-options policy-statement export_dhcp_server_route term 2 then reject
```

```
set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance trust-vr
set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter
10.1.1.0/24 exact
set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
set policy-options policy-statement import_relay_route_to_server_vr term 2 then reject
set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
```

Quick configuration for Security Zone to Allow the DHCP Protocol:

```
set security policies default-policy permit-all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic system-
services all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic system-
services all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic protocols all
```

Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure support on the client-facing side of the DHCP relay agent:

1. Set a routing instance type as virtual router.

```
[edit]
user@host# set routing-instances trust-vr instance-type virtual-router
```

2. Set an interface to the virtual router

```
[edit]
user@host# set routing-instances trust-vr interface ge-0/0/3.0
```

3. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

Procedure

Step-by-Step Procedure

To configure support on the server-facing side of the DHCP relay agent:

1. Set a virtual router.

```
[edit]
user@host# set routing-instances untrust-vr instance-type virtual-router
```

2. Set an interface to the virtual router.

```
[edit]
user@host# set routing-instances untrust-vr interface ge-0/0/4.0
```

3. Set the forward-only-replies option.

```
[edit]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
```

4. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Procedure

Step-by-Step Procedure

To configure the DHCP local server to support:

1. Set the configuration in dhcp-relay for untrust-vr routing instance

```
[edit ]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-config
user@host# set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
user@host# set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
```

2. Set the configuration in dhcp-relay for trust-vr routing instance

```
[edit ]
user@host# set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1 30.1.1.2
user@host# set routing-instances trust-vr forwarding-options dhcp-relay active-server-group server-1
user@host# set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr interface ge-0/0/3.0
user@host# set routing-instances trust-vr routing-options instance-import export_dhcp_server_route
```

3. Set the configuration to share routes between routing instances.

```
[edit ]
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from instance untrust-vr
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from route-filter 30.1.1.0/24 exact
user@host# set policy-options policy-statement export_dhcp_server_route term 1 then accept
user@host# set policy-options policy-statement export_dhcp_server_route term 2 then reject
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance trust-vr
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter 10.1.1.0/24 exact
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 2 then
```

```
reject
user@host# set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
```

NOTE: You can enable an SRX Series Firewall to function as a DHCP local server. The DHCP local server provides an IP address and other configuration information in response to a client request.

Procedure

Step-by-Step Procedure

To configure the security zone to allow the DHCP Protocol:

1. Set the default security policy to permit all traffic.

```
[edit ]
user@host# set security policies default-policy permit-all
```

2. Set all system services and protocols on interface ge-0/0/4.0.

```
[edit ]
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic protocols all
```

3. Set all system services and protocols on interface ge-0/0/3.0.

```
[edit ]
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
protocols all
```

Results

- Result for Client-facing Support:

From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
    instance-type virtual-router;
    interface ge-0/0/3.0;
}
```

- Result for Server-Facing Support:

  From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
untrust-vr {
    instance-type virtual-router;
    interface ge-0/0/4.0;
    forwarding-options {
        dhcp-relay {
            forward-only-replies;
        }
    }
}
```

- Result for DHCP Local Server Support:

  From configuration mode, confirm your configuration by entering the `show routing-instances`, `show policy-options` and `show routing-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
    routing-options {
        instance-import export_dhcp_server_route;
    }
```

```
    forwarding-options {
        dhcp-relay {
            server-group {
                server-1 {
                    30.1.1.2;
                }
            }
            active-server-group server-1;
            group relay-in-vr {
                interface ge-0/0/3.0;
            }
        }
    }
}
untrust-vr {
    routing-options {
        static {
            route 30.1.1.0/24 next-hop 20.1.1.2;
        }
        instance-import import_relay_route_to_server_vr;
    }
    forwarding-options {
        dhcp-relay {
            server-group {
                dummy-config;
            }
        }
    }
}
[edit]
user@host# show policy-options
policy-statement export_dhcp_server_route {
    term 1 {
        from {
            instance untrust-vr;
            route-filter 30.1.1.0/24 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
```

```
policy-statement import_relay_route_to_server_vr {
    term 1 {
        from {
            instance trust-vr;
            route-filter 10.1.1.0/24 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
[edit]
user@host#  show routing-options
    static {
        route 30.1.1.2/32 next-table untrust-vr.inet.0;
    }
```

- Result for Security Zone to Allow the DHCP Protocol:

  From configuration mode, confirm your configuration by entering the `show security policies` and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security zones
    security-zone HOST {
        interfaces {
            all;
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/4.0 {
                host-inbound-traffic {
                    system-services {
                        all;
```

```
                }
                protocols {
                    all;
                }
            }
        }
    }
    security-zone trust {
        interfaces {
            ge-0/0/3.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Relay Statistics Configuration: | **170**
- Verifying DHCP client bindings in the routing instance. | **171**

Verifying the DHCP Relay Statistics Configuration:

Purpose

Verify that the DHCP Relay Statistics has been configured.

Action

- From operational mode, enter the `show dhcp relay statistics routing-instance dhcp-relay` command.

```
Packets dropped:
Total 0

Messages received:
BOOTREQUEST 1
DHCPDECLINE 0
DHCPDISCOVER 0
DHCPINFORM 0
DHCPRELEASE 0
DHCPREQUEST 1

Messages sent:
BOOTREPLY 1
DHCPOFFER 0
DHCPACK 1
DHCPNAK 0
DHCPFORCERENEW 0
```

Verifying DHCP client bindings in the routing instance.

Purpose

Verify that the DHCP client bindings in the routing instances has been configured.

Action

- From operational mode, enter the `show dhcp relay binding routing-instance dhcp-relay` command.

```
IP address   Session Id  Hardware address   Expires   State     Interface
10.10.10.2   14          00:0c:29:e9:6d:00  86381     BOUND     ge-0/0/1.0
```

Configuring a DHCP Relay Agent on EX Series Switches

You can configure an EX Series switch to act as an extended DHCP relay agent. This means that a locally attached host can issue a DHCP request as a broadcast message and the switch configured for DHCP relay relays the message to a specified DHCP server. Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Before you begin:

- Ensure that the switch can connect to the DHCP server.

To configure a switch to act as an extended DHCP relay agent server:

1. Create at least one DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

```
[edit forwarding-options dhcp-relay]
user@switch# set server-group server-group-name  ip-address
```

2. Set the global active DHCP server group. The DHCP relay agent relays DHCP client requests to the DHCP servers defined in the active server group:

```
[edit forwarding-options dhcp-relay]
user@switch# set active-server-group  server-group-name
```

3. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

```
[edit forwarding-options dhcp-relay]
user@switch# set group group-name interface  interface-name
```

Configuring DHCP Smart Relay (Legacy DHCP Relay)

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See Configuring IRB Interfaces on Switches and Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface for information about this approach.

- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See Understanding Layer 3 Logical Interfaces and Configuring a Layer 3 Logical Interface for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- `set forwarding-options helpers bootp smart-relay-global`: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.
- `set forwarding-options helpers bootp interface` *`interface-name`* `smart-relay-agent`: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

SEE ALSO

bootp

Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.

NOTE: Automatic binding of stray requests is enabled by default.

- To disable automatic binding behavior, include the `no-bind-on-request` statement when you configure DHCP overrides at the global, group, or interface level.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-bind-on-request
```

- To override the default behavior for DHCPv6 relay agent, configure the override at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
user@host# set no-bind-on-request
```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

1. Specify the named group.

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston
```

2. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit overrides
```

3. Disable automatic binding for the group.

```
[edit forwarding-options dhcp-relay group boston overrides]
user@host# set no-bind-on-request
```

To disable automatic binding of stray requests on a specific interface:

1. Specify the named group of which the interface is a member.

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston
```

2. Specify the interface on which you want to disable automatic binding.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2
```

3. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
user@host# edit overrides
```

4. Disable automatic binding on the interface.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request
```

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set layer2-unicast-replies
```

Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.

To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the giaddr of DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-giaddr
```

Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]
user@host# set replace-ip-source-with giaddr
```

Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP relay configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP relay agent configuration options, include the `overrides` statement and its subordinate statements at the `[edit forwarding-options dhcp-relay]` hierarchy level.
- To override DHCP relay configuration options for a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level.
- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name interface interface-name]` hierarchy level.
- To configure overrides for DHCPv6 relay at the global level, group level, or per-interface, use the corresponding statements at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

To override default DHCP relay agent configuration settings:

1. (DHCPv4 and DHCPv6) Specify that you want to configure override options.
   - DHCPv4 overrides.

     Global override:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

Group-level override:

```
[edit forwarding-options dhcp-relay]
user@host# edit group group-name overrides
```

Per-interface override:

```
[edit forwarding-options dhcp-relay]
user@host# edit group group-name interface interface-name overrides
```

- DHCPv6 overrides.

  Global override:

  ```
  [edit forwarding-options dhcp-relay dhcpv6]
  user@host# edit overrides
  ```

  Group-level override:

  ```
  [edit forwarding-options dhcp-relay dhcpv6]
  user@host# edit group group-name overrides
  ```

  Per-interface override:

  ```
  [edit forwarding-options dhcp-relay dhcpv6]
  user@host# edit group group-name interface interface-name overrides
  ```

2. (DHCPv4 only) Enable DHCP relay proxy mode.

   See *Enabling DHCP Relay Proxy Mode*.

3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.

   See *Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent*.

4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

   See *Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address*.

5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.

   See *Overriding Option 82 Information*.

6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.

   See *Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets*.

7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.

   See *Enable Processing of Untrusted Packets So Option 82 Information Can Be Used*.

8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.

   See *Specifying the Maximum Number of DHCP Clients Per Interface*.

9. (DHCPv4 only) Configure client auto logout.

   See *DHCP Auto Logout Overview*.

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.

    See *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*.

11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.

    See the *delay-authentication*.

12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.

    See *Sending Release Messages When Clients Are Deleted*.

13. (Optional) Specify that when the DHCP or DHCPv6 relay agent receives a Discover or Solicit message that has a client ID that matches the existing client entry, the relay agent deletes the existing client entry.

    See *DHCP Behavior When Renegotiating While in Bound State*.

14. (DHCPv6 only) Automatically log out existing client when new client solicits on same interface.

    See *Automatically Logging Out DHCPv6 Clients*.

15. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.

    See *Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally*.

16. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.

    See *Disabling Automatic Binding of Stray DHCP Requests*.

17. (DHCPv4 and DHCPv6) Assign a single-session DHCP dual-stack group to a specified group of subscribers. You must assign the group to both legs of the DHCP dual stack.

    See *Configuring Single-Session DHCP Dual-Stack Support*.

18. (Optional, DHCPv4 and DHCPv6l) Specify that a short lease be sent to the client.

    See *Configuring DHCP Asymmetric Leasing*.

Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Disable the DHCP relay agent.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set disable-relay
```

Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings

IN THIS SECTION

- Requirements | 180
- Overview | 181
- Configuration | 181
- Verification | 184

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

Requirements

This example uses the following hardware and software components:

- MX Series 5G Universal Routing Platforms or EX Series Switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.

  See *Extended DHCP Relay Agent Overview*.

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.

  See *Grouping Interfaces with Common DHCP Configurations*.

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

Configuration

IN THIS SECTION

- CLI Quick Configuration | **181**
- Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings | **182**
- Results | **183**

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
```

```
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group
servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal fffff local-server-group
servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

1. Specify that you want to configure DHCP relay agent support.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option option-number 60
```

3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group servergroup-15
```

6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal fffff local-server-group servergroup-east
```

Results

From configuration mode, confirm the results of your configuration by issuing the `show` statement at the `[edit forwarding-options]` hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
    relay-option {
        option-number 60;
        equals {
            ascii video-gold {
                forward-only;
            }
        }
        equals {
            ascii video-bronze {
                local-server-group servergroup-15;
            }
        }
        default-action {
            drop;
        }
        starts-with {
            hexadecimal fffff {
                local-server-group servergroup-east;
            }
        }
```

```
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the Status of DHCP Relay Agent Selective Traffic Processing | **184**

To verify the status of DHCP relay agent selective traffic processing, perform this task:

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose

Verify the DHCP relay agent selective traffic processing status.

Action

Display statistics for DHCP relay agent.

```
user@host> show dhcp relay statistics
Packets dropped:
    Total                     30
    Bad hardware address       1
    Bad opcode                 1
    Bad options                3
    Invalid server address     5
    No available addresses     1
    No interface match         2
    No routing instance match  9
    No valid local address     4
    Packet too short           2
    Read error                 1
    Send error                 1
    Option 60                  1
    Option 82                  2
```

```
Messages received:
    BOOTREQUEST                 116
    DHCPDECLINE                 0
    DHCPDISCOVER                11
    DHCPINFORM                  0
    DHCPRELEASE                 0
    DHCPREQUEST                 105

Messages sent:
    BOOTREPLY                   0
    DHCPOFFER                   2
    DHCPACK                     1
    DHCPNAK                     0
    DHCPFORCERENEW              0

Packets forwarded:
    Total                       4
    BOOTREQUEST                 2
    BOOTREPLY                   2
```

Meaning

The `Packets forwarded` field in the `show dhcp relay statistics` command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of `BOOTREQUEST` and `BOOTREPLY` packets forwarded.

Verifying and Managing DHCP Relay Configuration

IN THIS SECTION

- Purpose | **186**
- Action | **186**

Purpose

View or clear address bindings or statistics for DHCP relay agent clients.

Action

- To display the address bindings for DHCP relay agent clients:

```
user@host> show dhcp relay binding
```

- To display DHCP relay agent statistics:

```
user@host> show dhcp relay statistics
```

- To clear the binding state of DHCP relay agent clients:

```
user@host> clear dhcp relay binding
```

- To clear all DHCP relay agent statistics:

```
user@host> clear dhcp relay statistics
```

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp relay binding routing instance <routing-instance name>`
- `show dhcp relay statistics routing instance <routing-instance name>`
- `clear dhcp relay binding routing instance <routing-instance name>`
- `clear dhcp relay statistics routing instance <routing-instance name>`

NOTE: On all SRX Series Firewalls, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

SEE ALSO

Minimum DHCP Relay Agent Configuration

Extended DHCP Relay Agent Overview

IN THIS SECTION

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers | 188
- DHCP Liveness Detection | 189

You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.

NOTE: The extended DHCP relay agent options configured with the `dhcp-relay` statement are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.

For information about the DHCP/BOOTP relay agent, see Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents.

You can also configure the extended DHCP relay agent to support IPv6 clients. See *DHCPv6 Relay Agent Overview* for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level.

You can also include the `dhcp-relay` statement at the following hierarchy levels:

- `[edit logical-systems` *`logical-system-name`* `forwarding-options]`
- `[edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `forwarding-options]`
- `[edit routing-instances` *`routing-instance-name`* `forwarding-options]`

Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some differences in the details of usage.

On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.

4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

DHCP Liveness Detection

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: DHCP liveness detection either globally or per DHCP group.

RELATED DOCUMENTATION

DHCP Overview | 2

Secure DHCP Message Exchange | 355

DHCP Client | 245

Suppressing DHCP Routes | 365

DHCP and BOOTP Relay Agent

IN THIS SECTION

- DHCP and BOOTP Relay Overview for Switches | 190
- Configuring DHCP and BOOTP Relay | 194
- Configuring DHCP and BOOTP Relay on QFX Series | 194

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay.

You can also enable BOOTP support when the switch is configured as a DHCP server. For more details, read this topic.

DHCP and BOOTP Relay Overview for Switches

IN THIS SECTION

- DHCP Client and Server Model | 191
- DHCP Client, Server, and Relay Agent Model | 193

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

You can configure the switch to use the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent. For information on configuring this option, see the *source-address-giaddr* configuration statement.

You can also use smart DHCP relay, which enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure a Layer 3 interface, Layer 3 subinterface, or IRB interface with multiple IP addresses and configure that interface to be a relay agent.

NOTE: Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.

DHCP Client and Server Model

DHCP IP address allocation works on a client/server model in which the server, in this case a Junos OS, assigns the client reusable IP information from an address pool. A DHCP client might receive offer messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 12 on page 192.

Figure 12: DHCP Client/Server Model

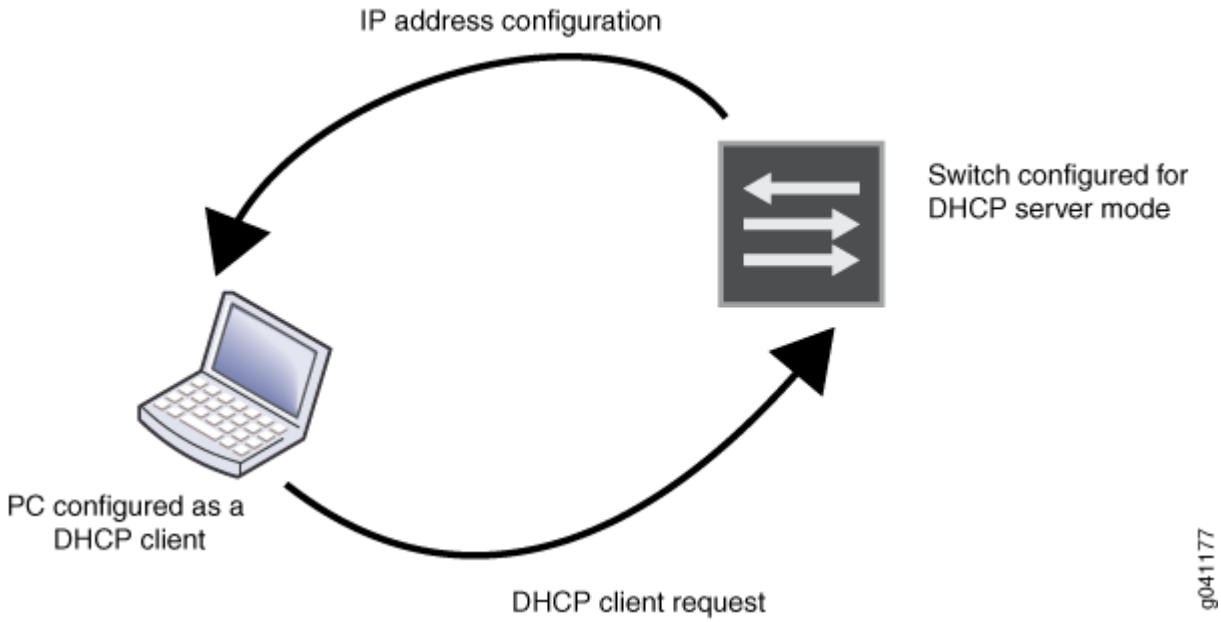
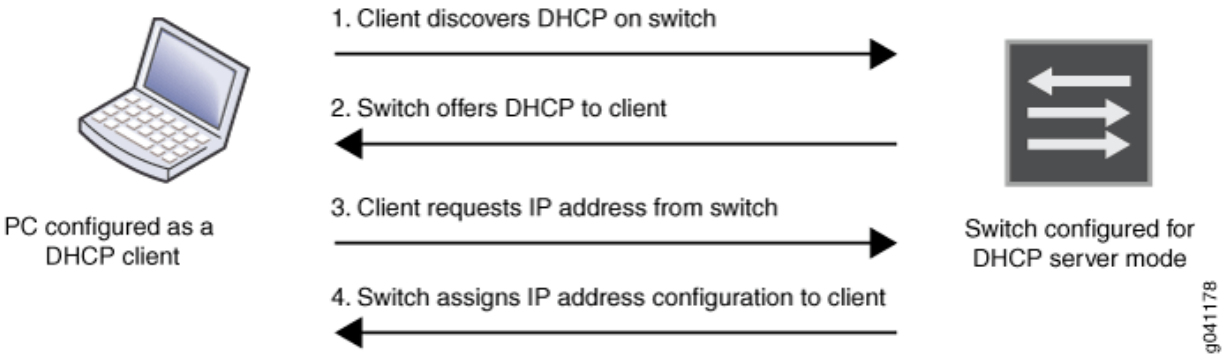


Figure 13: DHCP Four-Step Transfer



DHCP consists of a four-step transfer process beginning with a broadcast DHCP discovery message from the client. As the second step, the client receives a DHCP offer message from the server. This message includes the IP address and mask, and some other specific parameters. The client then sends a DHCP request message to accept the IP address and other parameters that it received from the server in the previous step. The DHCP server sends a DHCP response message and removes the now-allocated address from the DHCP address pool. See Figure 13 on page 192.

NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you

might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

DHCP Client, Server, and Relay Agent Model

The DHCP relay agent is located between a DHCP client and DHCP server and forwards DHCP messages between servers and clients as following:

1. The DHCP client sends a discover packet to find a DHCP server in the network from which to obtain configuration parameters for the subscriber (or DHCP client), including an IP address.
2. The DHCP relay agent receives the discover packet and forwards copies to each of the two DHCP servers. The DHCP relay agent then creates an entry in its internal client table to keep track of the client's state.
3. In response to receiving the discover packet, each DHCP server sends an offer packet to the client. The DHCP relay agent receives the offer packets and forwards them to the DHCP client.
4. On receipt of the offer packets, the DHCP client selects the DHCP server from which to obtain configuration information. Typically, the client selects the server that offers the longest lease time on the IP address.
5. The DHCP client sends a request packet that specifies the DHCP server from which to obtain configuration information.
6. The DHCP relay agent receives the request packet and forwards copies to each of the two DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client's configuration parameters.
8. The DHCP relay agent receives the ACK packet and forwards it to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay agent installs a host route and Address Resolution Protocol (ARP) entry for this client.
11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

Configuring DHCP and BOOTP Relay

You can configure a switch to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server or DHCP relay agent. When a switch is a relay agent, if a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style.If your switch runs software that does not support ELS, see "Configuring DHCP and BOOTP Relay" on page 194. For ELS details, see Using the Enhanced Layer 2 Software CLI.

To configure a switch to be a server, use the *dhcp-local-server* statement. To configure a switch to be a relay agent, use the *dhcp-relay* statement.

If you want to enable BOOTP support when the switch is configured to be a DHCP server, enter the following statement:

```
[edit system services dhcp-local-server]
user@switch# set overrides bootp-support
```

If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides bootp-support
```

Configuring DHCP and BOOTP Relay on QFX Series

IN THIS SECTION

- Configuring a DHCP and BOOTP Relay Agent on QFX Series | **195**
- Configuring DHCP Smart Relay on QFX Series | **197**

You can configure the QFX Series to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that if a locally attached host can issue a DHCP or BOOTP request as a broadcast message and the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see "Configuring DHCP and BOOTP Relay" on page 194. For ELS details, see Using the Enhanced Layer 2 Software CLI.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which allows you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent using the primary gateway address, the switch can resend the requests via the alternative gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 logical interface with multiple IP addresses and configure that interface to be a relay agent.

Configuring a DHCP and BOOTP Relay Agent on QFX Series

To configure a switch to act as a DHCP and BOOTP relay agent, include the `bootp` statement at the `[edit forwarding-options helpers]` hierarchy level:

```
[edit forwarding-options helpers]
bootp {
    apply-secondary-as-giaddr text-description;
    client-response-ttl number;
    description text-description;
    interface (interface-name | interface-group) {
        client-response-ttl number;
        description text-description;
        maximum-hop-count number;
        minimum-wait-time seconds;
        no-listen;
        server address
        apply-secondary-as-giaddr
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    relay-agent-option;
```

```
    server server-identifier
}
```

To include a description of the BOOTP service, DHCP service, or interface, use the `description` statement.

To configure a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the `interface` statement.

To stop packets from being forwarded, include the `no-listen` statement.

To set the maximum allowed number in the hops field of the BOOTP message, include the `maximum-hop-count` statement. BOOTP messages that have a larger number in the hops field than the maximum allowed are not forwarded. If you omit the `maximum-hop-count` statement, the default maximum number of hops is four.

To set the minimum allowed number of seconds in the `secs` field of the BOOTP message, include the `minimum-wait-time` statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the `secs` field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the `server` statement. You can include multiple `server` statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the `client-response-ttl` statement.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options
helpers {
    bootp {
        description "dhcp relay agent global parameters";
        server 192.168.55.44;
        server 172.16.0.3 routing-instance c3;
        maximum-hop-count 10;
        minimum-wait-time 8;
        interface {
            xe-0/0/1 {
                description "use this info for this interface";
                server 10.10.10.10;
                server 192.168.14.14;
                maximum-hop-count 11;
                minimum-wait-time 3;
            }
            xe-0/0/2 {
```

```
                no-listen;  ###ignore DHCPDISCOVER messages on this interface
            }
            all {
                description "globals apply to all other interfaces";
            }
        }
    }
}
```

SEE ALSO

bootp

Configuring DHCP Smart Relay on QFX Series

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See Configuring IRB Interfaces on Switches and Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface for information about this approach.
- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See Understanding Layer 3 Logical Interfaces and Configuring a Layer 3 Logical Interface for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- `set forwarding-options helpers bootp smart-relay-global`: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.
- `set forwarding-options helpers bootp interface` *`interface-name`* `smart-relay-agent`: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP

addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

SEE ALSO

bootp

RELATED DOCUMENTATION

DHCP Overview | **2**

DHCP Client | **245**

DHCP Server | **49**

DHCP Relay Agent Information Option (Option 82)

IN THIS SECTION

- Using DHCP Relay Agent Option 82 Information | **199**
- How DHCP Relay Agent Uses Option 82 for Auto Logout | **209**
- Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | **210**
- Check if Your Device Support DHCP Option-82 | **211**
- Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82 | **212**
- Example: Configure DHCP Relay in Forward Only Mode | **213**

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. You can configure the option 82 support globally or for a named group of interfaces. For more information, read this topic.

Using DHCP Relay Agent Option 82 Information

IN THIS SECTION

- Configuring Option 82 Information | 200
- Overriding Option 82 Information | 202
- Including a Prefix in DHCP Options | 203
- Including a Textual Description in DHCP Options | 206

Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the `relay-option-82` statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

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

  NOTE: If `relay-option-82` is configured, but none of the attributes under `relay-option-82` (that is, `circuit-id` | `remote-id` | `server-id-override`) are explicitly configured, then the default behavior is for the circuit-id (that is, suboption 1) to always be included in the option-82 value. This is true whether or not the `vendor-specific` attribute under `relay-option-82` is configured.

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

You can configure the option 82 support globally or for a named group of interfaces.

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the `delete relay-option-82` statement.

NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See *DHCPv6 Relay Agent Options*.

The following sections describe the option 82 operations you can configure:

Configuring Option 82 Information

You use the `relay-option-82` statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the `circuit-id` statement to include the Agent Circuit ID (suboption 1) in the packets, or the `remote-id` statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the `circuit-id` or `remote-id` statement without including any of the optional `prefix`, `use-interface-description`, `use-vlan-id`, `include-irb-and-l2`, or `no-vlan-interface-name` statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

```
(fe | ge)-fpc/pic/port.subunit
```

NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

```
(fe | ge)-fpc/pic/port:vlan-id
```

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:

```
(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

NOTE: Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

```
(fe | ge)-fpc/pic/port.subunit:bridge-domain-name
```

- IRB interfaces that use VLANs:

```
(fe | ge)-fpc/pic/port.subunit:vlan-name
```

To include the IRB interface name with the Layer 2 interface name, configure the `include-irb-and-l2` statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

```
(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit
```

- IRB interfaces that use VLANs:

```
(fe | ge)-fpc/pic/port:vlan-name+irb.subunit
```

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the `no-vlan-interface-name` statement. The format is as follows:

```
irb.subunit
```

To enable insertion of option 82 information:

1. Specify that you want to configure option 82 support.

   ```
   [edit forwarding-options dhcp-relay]
   user@host# edit relay-option-82
   ```

2. Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.

   - To insert the Agent Circuit ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set circuit-id
     ```

   - To insert the Agent Remote ID:

     ```
     [edit forwarding-options dhcp-relay relay-option-82]
     user@host# set remote-id
     ```

   - To insert both, configure both set commands.

3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.

   See *Including a Prefix in DHCP Options*.

4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.

   See *Including a Textual Description in DHCP Options*.

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

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

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the option 82 information in DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-option-82
```

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the `host-name`, `logical-system-name`, and `routing-instance-name` options. The DHCP relay agent obtains the values for the `host-name`, `logical-system-name`, and `routing-instance-name` as follows:

- If you include the `host-name` option, the DHCP relay agent uses the hostname of the device configured with the `host-name` statement at the `[edit system]` hierarchy level.
- If you include the `logical-system-name` option, the DHCP relay agent uses the logical system name configured with the `logical-system` statement at the `[edit logical-system]` hierarchy level.

- If you include the routing-instance-name option, the DHCP relay agent uses the routing instance name configured with the routing-instance statement at the [edit routing-instances] hierarchy level or at the [edit logical-system *logical-system-name* routing-instances] hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the DHCP option information when you specify the prefix statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
hostname:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name:routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the *vlan-id* value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.
   - To configure the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

   - To configure the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit remote-id
```

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.
   - To include the prefix with the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set prefix host-name logical-system-name
```

   - To include the prefix with the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82 remote-id]
user@host# set prefix host-name logical-system-name
```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

   - To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

   - To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

   - To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the `description` statement at the `[edit interfaces` *`interface-name`*`]` hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.

NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID . You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set use-interface-description device
```

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

   - To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

   - To include the textual description in option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description device
```

   - To include the textual description in option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description device
```

SEE ALSO

Configuring Interface Description

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 9 on page 209 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the Action Taken column.

Table 9: DHCP Relay Agent Option 82 Value for Auto Logout

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override “trust-option- 82”	Override “always-write-option-82”		
No	No	–	–	–	No secondary search performed
No	Yes	Yes	–	–	Use option 82 from packet
No	Yes	No	–	Zero	Drop packet
No	Yes	No	–	Non-zero	Use option 82 from packet
Yes	No	–	–	–	Use configured option 82
Yes	Yes	No	–	Zero	Drop packet
Yes	Yes	No	No	Non-zero	Use option 82 from packet

Table 9: DHCP Relay Agent Option 82 Value for Auto Logout *(Continued)*

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override “trust-option- 82”	Override “always-write-option-82”		
Yes	Yes	No	Yes	Non-zero	Overwrite the configured option 82
Yes	Yes	Yes	No	–	Use option 82 from packet
Yes	Yes	Yes	Yes	–	Overwrite the configured option 82

Enable Processing of Untrusted Packets So Option 82 Information Can Be Used

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set trust-option-82
```

Check if Your Device Support DHCP Option-82

To configure a switch with DHCP relay in forward-only mode, check whether your DHCP server supports DHCP Option 82.

Use the procedures in Table 10 on page 211 to confirm the support of Option-82 or required workaround.

Table 10: Verify support of Option-82 in DHCP Server

Problem	How to Verify ?	Solution
Verify if your DHCP server supports DHCP Option 82.	Use the `dhcp traceoptions` on the DHCP Relay. A message states the drop due to missing Option 82. If the DHCP Offer packet dropped because of Option-82 not included, you will receive the message like: `Feb 25 15:41:13.577519 [MSTR][NOTE] [default:default][RLY][INET][irb.6] jdhcpd_packet_handle: BOOTPREPLY could not find client table entry`	To fix the issue: • **Solution 1:** Upgrade the DHCP Server to Junos OS version that fully supports Option 82. • **Solution 2:** Change the DHCP Relay to a “stateful” mode (that is, DHCP Relay “binding” mode). • **Solution 3:** Move the DHCP Relay to a MX or to a non-ELS EX/QFX switch, so to enable the Legacy ‘helper bootp’ mode.

NOTE: Example: The DHCP Server in MS Windows Server 2019 fully supports Option 82, where as version 2016 has partial support.

SEE ALSO

DHCP Relay Agent | 153

DHCP and BOOTP Relay Agent | 190

Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82

Some PXE or BOOTP servers do not support Option-82, that is, their DHCP Offer messages do not include the Option-82 value added by the DHCP Relay. As a result, the DHCP Relay will drop the DHCP Offer and the PXE/BOOTP client will not be able to complete its boot sequence.

Following are the possible solution to resolve this issue:

Solution 1: Upgrade to a PXE Server that supports Option-82

Solution 2: Host the PXE server with a DHCP Server

- Ensure that the DHCP Server (that supports Option-82) run together with the PXE server.
- Configure an Option-60 on the DHCP Server.
  - Use the following CLI to configure Option-60 an a Microsoft WS DHCP Server:

```
netsh dhcp server dhcp-server-address add optiondef 60 ClientIdentifier STRING 0 PXEClient
```

  - Activate the option in the user interface of the DHCP server.

This way, the PXE/BOOTP clients will receive proper DHCP Offer with Option-60 “PXEClient” and will reach the PXE server at the same IP address of the DHCP Server.

Solution 3: Include Option-60 and Option-43 DHCP Server Message

If the PXE Server is not hosted together with the DHCP Server, you need the DHCP Server to send an Option-43 also in its DHCP Offer. The Option-43 provides the IP address of the PXE server. Note that, the older PXE or BOOTP clients might ignore Option-43 and will therefore try to get the software from the DHCP Server. Enter the Option-43 in the DHCP Server configuration in a hexadecimal mode.

For is a sample option-43 message:

```
06 01 07 08 07 00 01 01 0A 0B 0C 0D 09 0B 00 01 09 53 65 72 76 65 72 50 58 45 0A 02 00 53
```

The above message indicates the following information to the PXE client:

- Disable broadcast and multicast discovery
- Accept only the PXE Server provided in this text
- PXE Server IP is 10.11.12.13 (see the bytes '0A 0B 0C 0D' in the above text)
- Boot menu on the PXE client (to present to the end user):
  - just one line, “ServerPXE”
  - Autoselect the first Boot option, prompt “S”, no timeout (that is, immediately boot unless you press F8)

DHCP Packets on Non-Configured Interfaces

Once you enable DHCP-Relay on the MX Series routers, QFX or EX Series switches, the DHCP Snooping feature gets enabled and all DHCP packets incoming through any interface (both configured and unconfigured interface) of the device are analyzed. The interfaces that are not listed under the DHCP configuration are considered ‘unconfigured’.

Depending on the configuration, DHCP packets received on unconfigured interfaces are dropped.

If the DHCP packets are dropped on ‘unconfigured’ interface, you will receive the following message:

```
May 25 18:26:31.796241 [MSTR][NOTE] [default:default][RLY][INET][irb.82] jdhcpd_packet_handle:
BOOTPREQUEST irb.82 arrived on unconfigured interface DISCOVER, flags 23, config 0x0
```

SEE ALSO

DHCP Relay Agent | 153

DHCP and BOOTP Relay Agent | 190

Example: Configure DHCP Relay in Forward Only Mode

IN THIS SECTION

Requirements | 214

Overview | 214

Configuration | 215
Verification | 218

The example shows how to configure a “stateless” (“forward-only”) DHCP Relay on Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches. If your switch runs software that does not support ELS, see Configuring Interface Ranges. For ELS details, see Using the Enhanced Layer 2 Software CLI.

Requirements

This example uses the following hardware and software components:

- QFX or EX Series Switches (ELS mode).
- Junos OS Release 18.4R3.

Before you configure forward-only DHCP relay on EX Series and QFX Series switches, lets understand about Option 82 support on DHCP.

To verify whether your device supports DHCP Option-82, see "Check if Your Device Support DHCP Option-82" on page 211.

The following messages from the DHCP server include a copy of the Option 82 information on sent by the DHCP Relay in the Discover and Request messages:

- Offer
- Acknowledgement (ACK)
- Negative acknowledgment (NACK)

The DHCP relay discards any OFFER, ACK, and NACK messages that do not include a valid Option 82 information.

On how to avoid dropping of DHCP offer message when PXE or BOOTP servers do not support Option-82, see "Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82" on page 212.

Overview

In this example, we are configuring a switching device to act as DHCP relay agent by completing the following steps:

1. Add a set of DHCP server IP addresses configured as active server groups.
2. Configure the option 82 support for a named group of interfaces.

After you configure the example, the DHCP relay agent includes option 82 information in the DHCP packets that it receives from the clients and forwards to the DHCP server.

Configuration

IN THIS SECTION

- CLI Quick Configuration | **215**
- Configure forward-only' DHCP Relay Agent | **215**
- Results | **217**

To configure a forward-only DHCP relay agent on a ELS supported EX or QFX switches, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

```
set forwarding-options dhcp-relay server-group SV1 dhcp-server-1-address
set forwarding-options dhcp-relay server-group SV2 dhcp-server-2-address
set forwarding-options dhcp-relay active-server-group SV1
set forwarding-options dhcp-relay group DHCP-FO forward-only
set forwarding-options dhcp-relay group DHCP-FO relay-option-82 circuit-id use-interface-
description device
set forwarding-options dhcp-relay group DHCP-FO interface interface1
set forwarding-options dhcp-relay group DHCP-FO interface interface2
```

Configure forward-only' DHCP Relay Agent

Step-by-Step Procedure

To configure forward-only DHCP relay:

1. Specify the name of the server group, SV1 and SV2.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group SV1
user@host# set server-group SV2
```

2. Add the IP addresses of the DHCP servers belonging to the group.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group SV1 dhcp-server-1-address
user@host# set server-group SV2 dhcp-server-2-address
```

3. (Optional) In enterprise scenario, you can use the Preboot Execution Environment (PXE) or BOOTP for a PC (or other devices) to get its Junos OS from a server.

   - If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@host# set overrides bootp-support
```

   - Add a DHCP or PXE Servers to the DHCP Servers group

```
[edit forwarding-options dhcp-relay]
user@host# server-group SV1 dhcp-server-3-address
```

4. Apply the server group as an active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group SV1
```

5. Define DHCP-FO as interface group on your switching device acting as DHCP relay. Configure:

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO forward-only
```

6. Add a list of interfaces to the interface group.

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO interface interface1
user@host# set group DHCP-FO interface interface2
```

7. Set relay option 82 to interfaces and specify Agent circuit ID. Agent Circuit ID identifies the interface on which the client DHCP packet is received. When you configure circuit ID, the include the textual interface description in the message.

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO group relay-option-82 circuit-id use-interface-description device
```

Results

From configuration mode, confirm the results of your configuration by issuing the `show` statement at the `[edit forwarding-options]` hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host> show
dhcp-relay {
    server-group {
        SV1 {
            dhcp-server-1-address;
        }
        SV2 {
            dhcp-server-2-address;
        }
    }
    active-server-group SV1;
    group DHCP-FO {
        relay-option-82 {
            circuit-id {
                use-interface-description device;
            }
        }
        forward-only;
        interface interface1;
        interface interface2;
```

```
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the Offer message with Option-82 | 218

Verify if the messages from the DHCP server includes a copy of the Option 82 information sent by the DHCP relay.

Verifying the Offer message with Option-82

Purpose

Verify the “forward-only” DHCP Relay by enabling the dhcp traceoptions on the DHCP Relay.

Action

- Receive the output of the tracing operation in the specified file.

```
user@host# set system processes dhcp-service traceoptions file dhcp_logfile size 10m
user@host# set system processes dhcp-service traceoptions level all
user@host# set system processes dhcp-service traceoptions flag all
Feb 25 15:41:11.454186 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_io_process_ip_packet: LOCAL: recv pkt; sa 10.42.6.20; da 10.42.59.251; src_port 67;
dst_port 67; len 410
Feb 25 15:41:11.454218 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
from == 10.42.6.20, port == 67 ]--
Feb 25 15:41:11.454228 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
size == 410, op == 2 ]--
Feb 25 15:41:11.454250 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
flags == 8000 ]--
Feb 25 15:41:11.454271 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
htype == 1, hlen == 6 ]--
Feb 25 15:41:11.454292 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
```

```
hops == 0, xid == e50f52a1 ]--
Feb 25 15:41:11.454313 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
secs == 0, flags == 8000 ]--
Feb 25 15:41:11.454347 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
ciaddr == 0.0.0.0 ]--
Feb 25 15:41:11.454428 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
yiaddr == 10.42.58.21 ]--
Feb 25 15:41:11.454461 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
siaddr == 10.42.6.20 ]--
Feb 25 15:41:11.454472 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
giaddr == 10.42.59.251 ]--
Feb 25 15:41:11.454486 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
chaddr == 34 48 ed 27 e2 29 00 00 00 00 00 00 00 00 00 00 ]--
Feb 25 15:41:11.454508 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
sname ==  ]--
Feb 25 15:41:11.454535 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
file ==  ]--
Feb 25 15:41:11.454560 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  53,
len   1, data DHCP-OFFER ]--
Feb 25 15:41:11.454603 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   1,
len   4, data ff ff fc 00 ]--
Feb 25 15:41:11.454616 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  58,
len   4, data 00 05 46 00 ]--
Feb 25 15:41:11.454638 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  59,
len   4, data 00 09 3a 80 ]--
Feb 25 15:41:11.454675 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  51,
len   4, data 00 0a 8c 00 ]--
Feb 25 15:41:11.454701 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  54,
len   4, data 0a 2a 06 14 ]--
Feb 25 15:41:11.454724 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   3,
len   4, data 0a 2a 3b fe ]--
Feb 25 15:41:11.454748 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   4,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454778 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   6,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454805 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  15,
len  15, data 6c 69 73 65 63 2e 69 6e 74 65 72 6e 61 6c 00 ]--
Feb 25 15:41:11.454829 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  42,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454858 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code 128,
len  29, data 61 74 73 65 2d 65 6d 70 69 72 75 6d 31 2e 6c 69 73 65 63 2e 69 6e 74 65 72 6e
61 6c 00 ]--
Feb 25 15:41:11.454888 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code 129,
```

```
len  29, data 61 74 73 65 2d 65 6d 70 69 72 75 6d 31 2e 6c 69 73 65 63 2e 69 6e 74 65 72 6e
61 6c 00 ]--
Feb 25 15:41:11.454902 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  82,
len  19, data 01 11 49 52 42 2d 69 72 62 2e 35 36 3a 61 65 33 30 2e 30 ]--
Feb 25 15:41:11.454924 [MSTR][INFO] [default:default][RLY][INET][irb.56] --[ OPTION code 255,
len   0 ]--
Feb 25 15:41:11.454939 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_find_client_from_server_pdu: Using yiaddr from BOOTPREPLY for lookup
Feb 25 15:41:11.454962 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_platform_client_v4_app_get_l3_index:  safd is not client type
Feb 25 15:41:11.454992 [MSTR][DEBUG] client_key_compose: Composing key (0xb294380) for cid_l
0, cid NULL, mac 34 48 ed 27 e2 29, htype 1, subnet 10.42.59.251, ifindx 0, opt82_l 0, opt82
NULL
Feb 25 15:41:11.455016 [MSTR][DEBUG] client_key_compose: Successfully composed
CK_TYPE_HW_ADDR_ON_SUBNET (2) client key object.
Feb 25 15:41:11.455028 [MSTR][DEBUG] client_key_print: key_type CK_TYPE_HW_ADDR_ON_SUBNET
(2): subnet 10.42.59.251, MAC htype 1, Addr 34 48 ed 27 e2 29
Feb 25 15:41:11.455050 [MSTR][DEBUG] client_key_print: key_type CK_TYPE_HW_ADDR_ON_SUBNET (2)
other fields: subnet 10.42.59.251, ifindex 0, opt82_len 0, -
Feb 25 15:41:11.455081 [MSTR][INFO] [default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Safd irb.56 in routing context default:default - forward
only or drop processing
Feb 25 15:41:11.455114 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Removing option-82
Feb 25 15:41:11.455124 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Length of option 82 = 21 bytes
Feb 25 15:41:11.455146 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Moving 2 bytes, which were after option 82 and parse again
Feb 25 15:41:11.455169 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Safd irb.56 in routing context default:default - config
supports fwd only relaying packet
Feb 25 15:41:11.455193 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Result of forward-only: packet_consumed Yes,
packet_dropped No, message_type OFFER
Feb 25 15:41:11.455217 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_relay_forward_only_packet: Broadcast BOOTPREPLY OFFER for 10.42.58.21 on safd irb.56
```

- You can use the following commands to search for problems in the DHCP traceoptions log file (in this example, **'dhcp_logfile'**).

- To get an overview of most common problems, use:

```
user@host>  show log dhcp_logfile | match "dropp|fail|unconf" | except "packet_dropped No"
```

- To investigate a specific problem, use:

```
user@host>  show log dhcp_logfile | find " arrived on unconfigured interface"
```

  The `find` command is similar to Linux `less` command. It will reach the first entry in the log and allow you to scroll up/down the message.

- (Optional) To query the traceoptions logs on a Linux sever (or from the Junos shell), you can use both the following commands:

```
user@host> egrep -i "dropp|fail|unconf" dhcp_logfile | egrep -v "packet_dropped No" | more
```

```
user@host> egrep -i -b 5 " arrived on unconfigured interface" dhcp_logfile | more
```

Meaning

The above sample confirms that the messages from the DHCP server includes a copy of the Option 82 information sent by the DHCP relay and the sample also displays the textual description of the interface.

RELATED DOCUMENTATION

Secure DHCP Message Exchange | 355

DHCP Server | 49

DHCP Server Configuration | 52

DHCP Access Service Overview | 9

Secure DHCP Message Exchange | 355

DHCP Active Server Groups | 360

DHCPv6 Server | 104

DHCP Auto Logout | 308

DHCPv6 Relay Agent

IN THIS SECTION

- DHCPv6 Relay Agent Overview | 222
- Configuring DHCPv6 Relay Agent | 223
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets | 235
- Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets | 236
- Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets | 238
- Verifying and Managing DHCPv6 Relay Configuration | 239

The DHCPv6 relay agent enhances the DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agent supports an IPv4 network. DHCPv6 relay agents eliminate the necessity of having a DHCPv6 server on each physical network. For more information about inserting DHCPv6 Interface-ID (Option 18), Remote-ID (Option 37) or Client MAC Address (Option 79) in DHCPv6 packets, and verifying the DHCPv6 configuration, read this topic.

DHCPv6 Relay Agent Overview

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

NOTE: The following DHCPv6 functionalities are not supported on ACX Series routers:

- Subscriber authentication for DHCPv6 relay agents
- DHCP snooping
- DHCPv6 client
- Liveness detection
- Dynamic profiles
- Option 37 support for remote ID insertion
- Bidirectional Forwarding Detection (BFD) for DHCPv6 relay

The DHCPv6 relay agent is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the DHCP local server or DHCP relay agent.

To configure the DHCPv6 relay agent on the router (or switch), you include the `dhcpv6` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems` *`logical-system-name`* `forwarding-options dhcp-relay]`
- `[edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `forwarding-options dhcp-relay]`
- `[edit routing-instances` *`routing-instance-name`* `forwarding-options dhcp-relay]`

See *DHCPv6 Monitoring and Management* for commands specific to viewing and clearing DHCPv6 bindings and statistics.

Configuring DHCPv6 Relay Agent

IN THIS SECTION

- Requirements | **224**
- Overview | **224**
- Configuration | **226**

The DHCPv6 relay agent operates as the interface to relay messages between DHCPv6 clients and the DHCPv6 server on different IP networks.

The example describes how to configure the DHCPv6 relay agent on the SRX Series Firewall. SRX Series Firewall acting as DHCPv6 relay agent is responsible for forwarding the requests and responses between the DHCPv6 clients and the server which are part of different routing instances.

Requirements

The example DHCPv6 relay agent configuration has been tested on the following hardware and software components:

- SRX Series Firewalls with Junos OS 22.3R1 or later.

Overview

IN THIS SECTION

- Topology | **224**

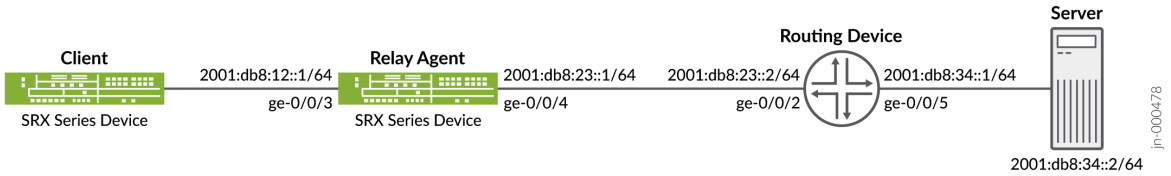
You can configure DHCPv6 relay agent to provide additional security when exchanging DHCPv6 messages between a DHCPv6 server and DHCPv6 clients that reside in different virtual routing instances. This type of configuration is for DHCPv6 relay connection between a DHCPv6 server and a DHCPv6 client, when the DHCPv6 server resides in a network that is isolated from the client network.

Topology

To exchange DHCPv6 messages between different routing instances, you must enable both the server-facing interface and the client-facing interface of the DHCPv6 relay agent to recognize and forward DHCPv6 packets.

The following Figure 14 on page 225 shows DHCPv6 performance as DHCPv6 local server, DHCPv6 client, and DHCPv6 relay agent

Figure 14: Understanding DHCPv6 Services in a Routing Instance



The following list provides an overview of the tasks required to create the DHCPv6 message exchange between the different routing instances:

- Configure the client-facing side of the DHCPv6 relay agent.
- Configure the server-facing side of the DHCPv6 relay agent.
- Configure the Security Zone to Allow the DHCPv6 protocol.

  Table1: DHCPv6 Relay Parameters:

Parameters	Client-Side-Details	Server-Side-Details
interface	ge-0/0/3.0	ge-0/0/4.0
routing interface	trust-vr	untrust-vr
ip address	2001:db8:12::1/64	2001:db8:23::1/64

NOTE: In order to make this setup work, the DHCPv6 server connecting route and relay agent interface route must be in both routing-instances. For example, in the above topology, the server route 2001:db8:34::/64 needs to be shared with the dhcp-relay VR, and the dhcp-relay interface route 2001:db8:12::/64 exact needs to be shared with the default routing instance.

Also, a dummy dhcp-relay config must be added in the routing instance with the DHCPv6 server. If this is not configured, dhcp-relay will not be able to receive packets from the DHCPv6 server.

Configuration

IN THIS SECTION

- CLI Quick Configuration | 226
- Procedure | 227
- Procedure | 228
- Procedure | 229
- Procedure | 230
- Results | 231

CLI Quick Configuration

The following procedures describe the configuration tasks for creating the DHCPv6 message exchange between the DHCPv6 server and clients in different routing instances. To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Quick configuration for Client-Facing Support:

```
set routing-instances trust-vr instance-type virtual-router
set routing-instances trust-vr interface ge-0/0/3.0
set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:12::1/64
```

Quick configuration for Server-Facing Support:

```
set routing-instances untrust-vr instance-type virtual-router
set routing-instances untrust-vr interface ge-0/0/4.0
set routing-instances untrust-vr forwarding-options dhcp-relay dhcpv6 forward-only-replies
set interfaces ge-0/0/4 unit 0 family inet6 address 2001:db8:23::1/64
```

Quick configuration for DHCPv6 Relay Support:

```
set routing-instances untrust-vr forwarding-options dhcp-relay dhcpv6 server-group dummy-config
set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
set routing-instances untrust-vr routing-options static route 2001:db8:34::/64 next-hop
```

```
2001:db8:23::2
set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 server-group server-1
2001:db8:34::2
set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 active-server-group server-1
set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 group relay-in-vr interface
ge-0/0/3.0
set routing-instances trust-vr routing-options instance-import export_dhcp_server_route
set policy-options policy-statement export_dhcp_server_route term 1 from instance untrust-vr
set policy-options policy-statement export_dhcp_server_route term 1 from route-filter
2001:db8:34::/64 exact
set policy-options policy-statement export_dhcp_server_route term 1 then accept
set policy-options policy-statement export_dhcp_server_route term 2 then reject
set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance trust-vr
set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter
2001:db8:12::/64 exact
set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
set policy-options policy-statement import_relay_route_to_server_vr term 2 then reject
set routing-options static route 2001:db8:34::2/64 next-table untrust-vr.inet.0
```

Quick configuration for Security Zone to Allow the DHCPv6 Protocol:

```
set security policies default-policy permit-all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic system-
services all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic system-
services all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic protocols all
```

Procedure

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the *CLI User Guide*.

To configure support on the client-facing side of the DHCPv6 relay agent:

1. Set a routing instance type as virtual router.

```
[edit]
user@host# set routing-instances trust-vr instance-type virtual-router
```

2. Set an interface to the virtual router

```
[edit]
user@host# set routing-instances trust-vr interface ge-0/0/3.0
```

3. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/3 unit 0 family inet6 address 2001:db8:12::1/64
```

Procedure

Step-by-Step Procedure

To configure support on the server-facing side of the DHCPv6 relay agent:

1. Set a virtual router.

```
[edit]
user@host# set routing-instances untrust-vr instance-type virtual-router
```

2. Set an interface to the virtual router.

```
[edit]
user@host# set routing-instances untrust-vr interface ge-0/0/4.0
```

3. Set the forward-only-replies option.

```
[edit]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay dhcpv6 forward-only-
replies
```

4. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/4 unit 0 family inet6 address 2001:db8:23::1/64
```

Procedure

Step-by-Step Procedure

To configure the DHCPv6 local server to support:

1. Set the configuration in dhcp-relay for untrust-vr routing instance

```
[edit ]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay dhcpv6 server-group
dummy-config
user@host# set routing-instances untrust-vr routing-options instance-import
import_relay_route_to_server_vr
user@host# set routing-instances untrust-vr routing-options static route 2001:db8:34::/64
next-hop 2001:db8:23::2
```

2. Set the configuration in dhcp-relay for trust-vr routing instance

```
[edit ]
user@host# set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 server-group
server-1 2001:db8:34::2
user@host# set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 active-server-
group server-1
user@host# set routing-instances trust-vr forwarding-options dhcp-relay dhcpv6 group relay-in-
vr interface ge-0/0/3.0
user@host# set routing-instances trust-vr routing-options instance-import
export_dhcp_server_route
```

3. Set the configuration to share routes between routing instances.

```
[edit ]
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from instance
untrust-vr
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from route-
```

```
filter 2001:db8:34::/64 exact
user@host# set policy-options policy-statement export_dhcp_server_route term 1 then accept
user@host# set policy-options policy-statement export_dhcp_server_route term 2 then reject
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from
instance trust-vr
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from
route-filter 2001:db8:12::/64 exact
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 then
accept
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 2 then
reject
user@host# set routing-options static route 2001:db8:34::2/64 next-table untrust-vr.inet.0
```

NOTE: You can enable an SRX Series Firewall to function as a DHCPv6 local server. The DHCPv6 local server provides an IP address and other configuration information in response to a client request.

Procedure

Step-by-Step Procedure

To configure the security zone to allow the DHCPv6 Protocol:

1. Set the default security policy to permit all traffic.

```
[edit ]
user@host# set security policies default-policy permit-all
```

2. Set all system services and protocols on interface ge-0/0/4.0.

```
[edit ]
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic protocols all
```

3. Set all system services and protocols on interface ge-0/0/3.0.

```
[edit ]
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
protocols all
```

Results

- Result for Client-facing Support:

From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
    instance-type virtual-router;
    interface ge-0/0/3.0;
}
```

- Result for Server-Facing Support:

  From configuration mode, confirm your configuration by entering the `show routing-instances` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
untrust-vr {
    instance-type virtual-router;
    interface ge-0/0/4.0;
    forwarding-options {
        dhcp-relay {
            forward-only-replies;
        }
    }
}
```

- Result for DHCPv6 Local Server Support:

  From configuration mode, confirm your configuration by entering the `show routing-instances`, `show policy-options` and `show routing-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
    routing-options {
        instance-import export_dhcp_server_route;
    }
    forwarding-options {
        dhcp-relay {
            server-group {
                server-1 {
                    2001:db8:34::2;
                }
            }
            active-server-group server-1;
            group relay-in-vr {
                interface ge-0/0/3.0;
            }
        }
    }
}
untrust-vr {
    routing-options {
        static {
            route 2001:db8:34::/64 next-hop 2001:db8:23::2;
        }
        instance-import import_relay_route_to_server_vr;
    }
    forwarding-options {
        dhcp-relay {
            server-group {
                dummy-config;
            }
        }
    }
}
[edit]
```

```
user@host# show policy-options
policy-statement export_dhcp_server_route {
    term 1 {
        from {
            instance untrust-vr;
            route-filter 2001:db8:34::/64 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
policy-statement import_relay_route_to_server_vr {
    term 1 {
        from {
            instance trust-vr;
            route-filter 2001:db8:12::/64 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
[edit]
user@host#  show routing-options
    static {
        route 2001:db8:34::2/64 next-table untrust-vr.inet.0;
    }
```

- Result for Security Zone to Allow the DHCPv6 Protocol:

  From configuration mode, confirm your configuration by entering the `show security policies` and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
```

```
[edit]
user@host# show security zones
    security-zone HOST {
        interfaces {
            all;
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/4.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone trust {
        interfaces {
            ge-0/0/3.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
```

If you are done configuring the device, enter `commit` from configuration mode.

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

- Prefix—Specify the `prefix` option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the `use-interface-description` option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Circuit ID suboption (suboption 1)—Specify the `use-option-82` option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the `logical` interface description or the `device` interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-option-82
```

SEE ALSO

> *Including a Prefix in DHCP Options*
>
> *Including a Textual Description in DHCP Options*

Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets

Starting in Junos OS Release 14.1, you can configure DHCPv6 relay agent to insert DHCPv6 Remote-ID (option 37) in the packets that the relay sends to a DHCPv6 server. You can configure option 37 support at either the DHCPv6 global or group level.

When you configure option 37 support, you can optionally include the following information:

- Prefix—Specify the `prefix` option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the `use-interface-description` option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Remote-ID suboption (suboption 2)—Specify the `use-option-82` option to use the value of the DHCPv4 option 82 Remote-ID suboption (suboption 2). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 2 value and inserts it into the outgoing packets.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Remote-ID option (option 37) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 37.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

2. (Optional) Specify the prefix to include with the option 37 information.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 37 include the textual description of the interface. You can specify either the `logical` interface description or the `device` interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 37 use the DHCPv4 option 82 Remote-ID suboption (suboption 2) value.

   If no DHCPv4 binding exists, or if the binding does not include an option 82 suboption 2 value, by default the router sends the packets without adding option 37. However, you can use the optional `strict` keyword to specify that the router drop packets that do not have a suboption 2 value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-option-82 strict
```

SEE ALSO

Extracting an Option 82 or Option 37 Substring to Create an Interface Set

Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets

The incremental deployment of IPv6 to existing IPv4 networks can result in a dual-stack network environment in which devices act as both DHCPv4 and DHCPv6 clients. In dual-stack scenarios, operators need to be able to associate DHCPv4 and DHCPv6 messages with the same client interface, based on an identifier that is common to the interface.

You can configure a DHCPv6 relay agent to insert the DHCPv6 client MAC address in the packets that the relay sends to a DHCPv6 server. The client MAC address is used to associate DHCPv4 and DHCPv6 messages with the same client interface.

In addition to associating DHCPv4 and DHCPv6 messages from a dual-stack client, having the client MAC address in DHCPv6 packets provides additional information for event debugging and logging related to the client at the relay agent and the server.

When DHCPv6 option 79 is enabled, the DHCPv6 relay agent reads the source MAC address of DHCPv6 Solicit and DHCPv6 Request messages that it receives from a client. The relay agent encapsulates the Solicit and Request messages within a DHCPv6 Relay-Forward message, and inserts the client MAC address as option 79 in the Relay-Forward header before relaying the message to the server.

If the DHCPv6 packet already has a Relay-Forward header, the DHCPv6 relay agent adds the client MAC address if the packet meets the following conditions: the packet has only one Relay-Forward header, the Relay-Forward header was added by an LDRA, and the Relay-Forward header does not already include option 79 information.

You can also configure DHCPv6 option 79 for a lightweight DHCPv6 relay agent (LDRA). An LDRA resides on the same IPv6 link as the DHCPv6 client and relay agent or server and acts as a layer 2 relay agent, without performing the routing function necessary to forward messages to a server or relay agent that resides on a different IPv6 link.

- To configure DHCPv6 option 79 for a DHCPv6 relay agent (layer 3):

```
[edit]
user@host# set forwarding-options dhcp-relay dhcpv6 relay-agent-option-79
```

- To configure DHCPv6 option 79 for an LDRA (layer 2):

```
[edit]
user@host# set vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-79
```

SEE ALSO

DHCPv6 Relay Agent Options

Configuring DHCPv6 Relay Agent Options

Using Lightweight DHCPv6 Relay Agent (LDRA)

DHCP Active Server Groups | 360

Verifying and Managing DHCPv6 Relay Configuration

IN THIS SECTION

- Purpose | 239
- Action | 239

Purpose

View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

Action

- To display the address bindings for extended DHCPv6 relay agent clients:

```
user@host> show dhcpv6 relay binding
```

- To display extended DHCPv6 relay agent statistics:

```
user@host> show dhcpv6 relay statistics
```

- To clear the binding state of DHCPv6 relay agent clients:

```
user@host> clear dhcpv6 relay binding
```

- To clear all extended DHCPv6 relay agent statistics:

```
user@host> clear dhcpv6 relay statistics
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1	Starting in Junos OS Release 14.1, you can configure DHCPv6 relay agent to insert DHCPv6 Remote-ID (option 37) in the packets that the relay sends to a DHCPv6 server.

RELATED DOCUMENTATION

- Centrally Configure DHCP Options on a RADIUS Server | 288
- DHCP Snooping | 299
- DHCP Liveness Detection | 327
- DHCP Relay Agent Information Option (Option 82) | 198
- DHCP Client | 245
- DHCP Server | 49

DHCP Relay Proxy

IN THIS SECTION

- DHCP Relay Proxy Overview | 241
- Enabling DHCP Relay Proxy Mode | 243

A DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers. The DHCP relay agent is configured on the router or switch, which operates between the DHCP client and one or more DHCP servers. For more information, read this topic.

DHCP Relay Proxy Overview

IN THIS SECTION

- Benefits of Using DHCP Relay Proxy | 241
- Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers | 242

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

NOTE: You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

Benefits of Using DHCP Relay Proxy

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is

automatically removed when the lease time expires or when the client releases the address. Note that DHCP Relay support for unnumbered Ethernet interfaces is not available on ACX7000 Devices (ACX7024, ACX7100, ACX7100, and ACX7509).

- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
   a. Selects the first offer received as the offer to sent to the client
   b. Replaces the DHCP server address with the address of the DHCP relay proxy
   c. Forwards the offer to the DHCP client.
4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.

10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.

11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set proxy-mode
```

5
CHAPTER

DHCP Client

DHCP Client | 245

DHCPv6 Client | 266

DHCP Client

IN THIS SECTION

- Understanding DHCP Client Operation | 245
- Minimum DHCP Client Configuration | 246
- Configuring a DHCP Client | 246
- Example: Configuring the Device as a DHCP Client | 249
- Verifying and Managing DHCP Client Configuration | 256
- Example: Configuring as a DHCP Client in Chassis Cluster Mode | 257

SRX Series device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. For more information, read this topic.

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a *logical interface* on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series Firewalls in chassis cluster mode.

Minimum DHCP Client Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
    ge-0/0/0 {
        unit 0 {
            family inet {
                dhcp-client
        }
    }
}
```

NOTE: To configure a DHCP client in a routing instance, add the interface in a routing instance using the `[edit routing-instances]` hierarchy.

Configuring a DHCP Client

A Dynamic Host Configuration Protocol (DHCP) server can provide many valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients, and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see "Configuring a DHCP Server on Switches" on page 67 or "Configuring a Switch as a DHCP Server" on page 63.

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

```
[edit]
user@switch# set interfaces interface-name unit number family  inet dhcp
 configuration-statement
```

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

The options that you can configure are listed in Table 11 on page 247. Replace the variable *configuration-statement* with one or more of the statements listed in this table. If you do not explicitly configure these options, the switch uses default values for them.

Table 11: DHCP Client Settings

Configuration Statement	Description
`client-identifier`	Unique client ID—By default this consists of the hardware type (01 for Ethernet) and the MAC address (a.b.c.d). For this example, the value would be 01abcd.
`lease-time`	Time in seconds that a client holds the lease for an IP address assigned by a DHCP server. If a client does not request a specific lease time, then the server sends the default lease time. The default lease time on a Junos OS DHCP server is 1 day. **NOTE**: Starting in Junos OS Release 23.4R1, the DHCP client silently discards the DHCP OFFER which has a lease-time less than 15 seconds.
`retransmission-attempt`	Number of times the client attempts to retransmit a DHCP packet.
`retransmission-interval`	Time between transmission attempts.
`server-address`	IP address of the server that the client queries for an IP address.

Table 11: DHCP Client Settings *(Continued)*

Configuration Statement	Description
`update-server`	TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch are propagated.
`vendor-option`	Vendor class ID (CPU's manufacturer ID string) for the DHCP client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

NOTE: To configure the DHCP client in a routing instance, configure the interface in the `[edit routing-instances]` hierarchy.

Example: Configuring the Device as a DHCP Client

IN THIS SECTION

- Requirements | 249
- Overview | 250
- Configuration | 251
- Verification | 254

This example shows how to configure the device as a DHCP client.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. You can use the `show system services dhcp pool` CLI command to view information on DHCP address pools.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/2, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 50,000, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Set the force-discover option if you want to force the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series Firewalls is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

NOTE: Starting with Junos OS Release 17.3R1, on all SRX Series Firewalls and vSRX Virtual Firewall instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to align with other Junos platforms. There is no change in the functionality.

Configuration

IN THIS SECTION

- Procedure | 251

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet dhcp-client client-identifier prefix host-name
set interfaces ge-0/0/2 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/2 unit 0 family inet dhcp-client force-discover
set interfaces ge-0/0/2 unit 0 family inet dhcp-client server-address 192.168.2.1
set interfaces ge-0/0/2 unit 0 family inet dhcp-client vendor-id ether
set interfaces ge-0/0/2 unit 0 family inet dhcp-client options no-hostname
```

GUI Quick Configuration

Step-by-Step Procedure

To configure the device as a DHCP client:

1. In the J-Web interface, select **Configure** > **Services** > **DHCP** > **DHCP Client**.
2. Under Interfaces, add `ge-0/0/2.0`.
3. Configure the DHCP client identifier as either an ASCII or hexadecimal value.
4. From the Client identifier choice list, select `hexadecimal`.
5. In the Hexadecimal box, type the client identifier—`00:0a:12:00:12:12`.

6. Set the DHCP lease time in seconds. This is the lease time in seconds requested in a DHCP client protocol packet; the range is 60 through 2,147,483,647. Type **86400**.
7. Set the retransmission number of attempts to 6. This is the number of attempts to retransmit the DHCP client protocol packet. The range is 0 through 6.
8. Set the retransmission interval in seconds to 5. This is the number of seconds between successive transmissions. The range is 4 through 64. The default is 4 seconds.
9. Configure the force-discover option to force the DHCP client to send a DHCP discover packet after one to three failed `dhcp-request` attempts.
10. Set the IPv4 address of the preferred DHCP server. Type **192.168.2.1**.
11. Set the vendor class ID. This is the vendor class identification for the DHCP client. Type **ether**.
12. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).
13. Click **OK**.
14. If you are done configuring the device, click **Commit** >.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/2 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Configure the force-discover option.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set force-discover.
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set server-address 192.168.2.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

9. Configure options no-hostname if you do not want the client to send the hostname in packets.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

Results

From configuration mode, confirm your configuration by entering the `show interfaces ge-0/0/2 unit 0 family inet` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/2 unit 0 family inet
dhcp-client {
    client-identifier hexadecimal 00:0a:12:00:12:12;
    options no-hostname;
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    force-discover;
    server-address 192.168.2.1;
    update-server;
    vendor-id ether;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Client | **254**

Confirm that the configuration is working properly.

Verifying the DHCP Client

Purpose

Verify that the DHCP client information has been configured.

Action

From operational mode, enter these commands:

- `show dhcp client binding` command to display the binding state of a Dynamic Host Configuration Protocol (DHCP) client.
- `show dhcp client statistics` command to display client statistics.

These commands produce the following sample output:

```
user@host> show dhcp client binding
```

```
IP address        Hardware address   Expires     State      Interface
192.168.2.2       88:a2:5e:0a:d6:03  2419093     BOUND      ge-0/0/2.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     2
    Send error                2

Messages received:
    BOOTREPLY                 6
    DHCPOFFER                 4
    DHCPACK                   2
    DHCPNAK                   0
    DHCPFORCERENEW            0

Messages sent:
    BOOTREQUEST               39
    DHCPDECLINE               0
    DHCPDISCOVER              23
    DHCPREQUEST               16
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 0
    DHCPREBIND                0
```

Verifying and Managing DHCP Client Configuration

IN THIS SECTION

- Purpose | 256
- Action | 256

Purpose

View or clear information about client address bindings and statistics for the DHCP client on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

Action

- To display the address bindings in the client table on the DHCP client:

```
user@host> show dhcp client binding
```

- To display DHCP client statistics:

```
user@host> show dhcp client statistics
```

- To clear the binding state of a DHCP client from the client table on the DHCP client:

```
user@host> clear dhcp client binding
```

- To clear all DHCP client statistics:

```
user@host> clear dhcp client statistics
```

NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- show dhcp client binding routing instance *<routing-instance name>*
- show dhcp client statistics routing instance *<routing-instance name>*
- clear dhcp client binding routing instance *<routing-instance name>*
- clear dhcp client statistics routing instance *<routing-instance name>*

Example: Configuring as a DHCP Client in Chassis Cluster Mode

IN THIS SECTION

- Requirements | **257**
- Overview | **258**
- Configuration | **258**
- Verification | **264**

This example shows how to configure the device as a DHCP client in chassis cluster mode.

Requirements

This example uses the following hardware and software components:

- Two SRX Series Firewalls as DHCP client
- One SRX Series Firewall as DHCP server
- Junos OS Release 12.1X47-D10 or later for SRX Series Firewalls

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.

- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series Firewalls as DHCP clients and a third SRX Series Firewall as a DHCP server. Configure the two DHCP clients in chassis cluster mode.

For DHCP clients, you specify the interface as reth1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds. You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 203.0.113.1 and the vendor class ID to ether.

For the DHCP server, configure the SRX Series Firewall as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface ge-0/0/2.0.

Configuration

IN THIS SECTION

- Procedure | 258

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Configure DHCP Client 1 and Client 2:

```
set interfaces reth1 unit 0 family inet dhcp-client
set interfaces reth1 unit 0 family inet dhcp-client client-identifier user-id ascii
00:0a:12:00:12:12
set interfaces reth1 unit 0 family inet dhcp-client options no-hostname
set interfaces reth1 unit 0 family inet dhcp-client lease-time 86400
```

```
set interfaces reth1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces reth1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces reth1 unit 0 family inet dhcp-client server-address 203.0.113.1
set interfaces reth1 unit 0 family inet dhcp-client vendor-id ether
```

Configure chassis cluster on Client 1 and Client 2:

```
set chassis cluster reth-count 2
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 1000
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-4/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
```

Configure the DHCP server:

```
set system service dhcp-local-server group g1 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
set access address-assignment pool p1 family inet network 203.0.113.0/24
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the devices as DHCP clients:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces reth1 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```

3. Set the hostname if you do not want the DHCP client to send hostname in the packets (RFC option code 12).

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

4. Set the DHCP lease time.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

5. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

6. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set server-address 203.0.113.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

Step-by-Step Procedure

To configure the DHCP clients in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 2
```

2. Enable control link recovery.

```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```

3. Configure heartbeat settings.

```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 1000
```

4. Configure the redundancy groups.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 node 0 priority 100
user@host# set chassis cluster redundancy-group 1 node 1 priority 1
user@host# set chassis cluster redundancy-group 0 node 0 priority 100
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

5. Configure redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
```

Step-by-Step Procedure

To configure the device as DHCP server:

1. Configure the DHCP local server.

```
[edit system services]
user@host# set dhcp-local-server group g1 interface ge-0/0/2.0
```

2. Configure IP address of the server.

```
[edit interfaces]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
```

3. Configure an address pool.

```
[edit access]
user@host# set address-assignment pool p1 family inet network 203.0.113.0/24
user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Results

From configuration mode, confirm your configuration by entering the `show` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces reth1 unit 0 family inet
dhcp-client {
    client-identifier user-id ascii 00:0a:12:00:12:12;
    options no-hostname;
```

```
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    server-address 203.0.113.1;
    vendor-id ether;
}
```

```
[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 2;
heartbeat-interval 1000;
redundancy-group 0 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 1{
    node 0 priority 100;
    node 1 priority 1;
}
```

```
[edit]
user@host# show interfaces reth1
redundant-ether-options {

    redundancy-group 1;
}
```

```
[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
        network 203.0.113.0/24;
        range r1 {
            low 203.0.113.5;
            high 203.0.113.20;
        }
```

```
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Client in Chassis Cluster Mode | 264

Verifying the DHCP Client in Chassis Cluster Mode

Purpose

Verify that the DHCP client is working in chassis cluster mode.

Action

From operational mode, enter the `show dhcp client binding`, `show dhcp client statistics` and `show dhcp client binding interface reth1 detail` commands.

```
user@host> show dhcp client binding
```

```
IP address     Hardware address   Expires     State      Interface
 203.0.113.14      00:1f:12:e3:34:01  84587       BOUND      reth1.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     4
    Send error                4

Messages received:
    BOOTREPLY                 3
```

```
    DHCPOFFER                   1
    DHCPACK                     2
    DHCPNAK                     0
    DHCPFORCERENEW              0

Messages sent:
    BOOTREQUEST                 0
    DHCPDECLINE                 0
    DHCPDISCOVER                5
    DHCPREQUEST                 8
    DHCPINFORM                  0
    DHCPRELEASE                 1
    DHCPRENEW                   0
    DHCPREBIND                  0
```

```
user@host> show dhcp client binding interface reth1 detail
```

```
Client Interface: reth1.0
     Hardware Address:             00:10:db:ff:10:01
     State:                        BOUND(LOCAL_CLIENT_STATE_BOUND)
     Lease Expires:                2013-12-18 10:15:36 CST
     Lease Expires in:             30 seconds
     Lease Start:                  2013-12-17 10:15:36 CST
     Server Identifier:            203.0.113.1
     Client IP Address:            10.1.1.14
     Update Server                 No

DHCP options:
    Name: dhcp-lease-time, Value: 1 day
    Name: server-identifier, Value: 10.1.1.1
    Name: subnet-mask, Value: 255.255.255.0
```

Meaning

The sample output shows that DHCP clients configured in the example work in a chassis cluster.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.3R1	Starting with Junos OS Release 17.3R1, on all SRX Series Firewalls and vSRX Virtual Firewall instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to align with other Junos platforms.
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series Firewalls is being deprecated and only the new JDHCP CLI is supported.

RELATED DOCUMENTATION

- DHCP Server | 49
- DHCP Relay Agent | 153
- Suppressing DHCP Routes | 365
- DHCP Overview | 2
- DHCP Access Service Overview | 9
- Legacy DHCP and Extended DHCP | 16

DHCPv6 Client

IN THIS SECTION

- DHCPv6 Client Overview | 267
- Understanding DHCPv6 Client and Server Identification | 268
- Minimum DHCPv6 Client Configuration on SRX Series Devices | 269
- Configuring DHCP Client-Specific Attributes | 271
- DHCPv6 Client Configuration Options | 271
- Configuring the DHCPv6 Client Rapid Commit Option | 273
- Configuring a DHCPv6 Client in Autoconfig Mode | 274

Configuring TCP/IP Propagation on a DHCPv6 Client | 275

SRX Series device can act as a DHCPv6 client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. To enable a device to operate as a DHCPv6 client, you must configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. For more information, read this topic.

DHCPv6 Client Overview

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a *logical interface* on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the `dhcpv6-client` statement at the [`edit interfaces`] hierarchy level.

NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the [`edit routing-instances`] hierarchy.

NOTE: On all SRX Series Firewalls, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Understanding DHCPv6 Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or server. DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-llt)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Llayer address (duid-ll)

The duid-llt DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

SEE ALSO

DHCPv6 Client Overview | **267**

Minimum DHCPv6 Client Configuration on SRX Series Devices

This topic describes the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the DHCPv6 client type. The client type can be autoconfig or statefull.

   - To enable DHCPv6 auto configuration mode, configure the client type as `autoconfig`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

- For stateful address assignment, configure the client type as `statefull`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the identity association type.

   - To configure identity association for nontemporary address (IA_NA) assignment, specify the `client-ia type` as `ia-na`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

   - To configure identity association for prefix delegation (IA_PD), specify the `client-ia-type` as `ia-pd`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:

   - Link Layer address (duid-ll)
   - Link Layer address plus time (duid-llt)
   - Vendor-assigned unique ID based on enterprise number (vendor)

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [`edit routing-instances`] hierarchy.

Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

You use the `dhcp-attributes` statement to configure DHCPv6 client-specific attributes for address-assignment pools at the `[edit access address-assignment pool` *`pool-name`* `family inet6] hierarchy`.

Table 12 on page 271 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 12: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
`dns-server`	IPv6 address of DNS server to which clients can send DNS queries	23
`grace-period`	Grace period offered with the lease	–
`maximum-lease-time`	Maximum lease time allowed by the DHCPv6 server	–
`option`	User-defined options	–
`sip-server-address`	IPv6 address of SIP outbound proxy server	22
`sip-server-domain-name`	Domain name of the SIP outbound proxy server	21

DHCPv6 Client Configuration Options

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the

retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:
   - dns-server
   - domain
   - ntp-server
   - sip-domain
   - sip-server

   For example, to specify the DHCPv6 client requested option as `dns-server`:

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set req-option dns-server
   ```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set retransmission-attempt 6
   ```

3. Configure the `update-server` option on the DHCPv6 client.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-server
   ```

4. Specify the interface used to delegate prefixes.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set update-router-advertisement interface ge-0/0/0
   ```

5. Configure the two-message (rapid commit) exchange option for address assignment.

   ```
   [edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
   user@host# set rapid-commit
   ```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [`edit routing-instances`] hierarchy.

NOTE: On all SRX Series Firewalls, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, and SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Configuring the DHCPv6 Client Rapid Commit Option

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```

Configuring a DHCPv6 Client in Autoconfig Mode

A DHCPv6 client configured in autoconfig mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in autoconfig mode on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as `autoconfig`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

2. Specify the identity association type as `ia-na` for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the interface on which to configure router advertisement.

```
[edit protocols router-advertisement]
user@host# set interface ge-0/0/0
```

Configuring TCP/IP Propagation on a DHCPv6 Client

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the `update-server` option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

2. Configure the address pool to specify the interface (where `update-server` is configured) from which TCP/IP settings can be propagated.

```
[edit access]
user@host# set address-assignment pool 2 family inet6 dhcp-attributes propagate-settings ge-0/0/0
```

RELATED DOCUMENTATION

DHCP Client | **245**

DHCPv6 Client | **266**

Understanding DHCPv6 Client and Server Identification | **268**

CHAPTER 6

DHCP with External Authentication Server

DHCP with External Authentication Server | 277

Centrally Configure DHCP Options on a RADIUS Server | 288

DHCP with External Authentication Server

IN THIS SECTION

- Using External AAA Authentication Services to Authenticate DHCP Clients | 277
- Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | 279
- Example-Configuring DHCP with External Authentication Server | 280
- Specifying Authentication Support | 281
- Creating Unique Usernames for DHCP Clients | 282
- Grouping Interfaces with Common DHCP Configurations | 285

Extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. For more information, read this topic.

This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

Using External AAA Authentication Services to Authenticate DHCP Clients

IN THIS SECTION

- Steps to Configure DHCP with External Authentication Server | 278

The authentication, authorization, and accounting (AAA) Service Framework provides a single point of contact for all the authentication, authorization, accounting, address assignment, and dynamic request services that the router supports for network access.

In extended DHCP applications, both DHCP server and the DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. The support id available for DHCPv6 local server and DHCPv6 relay agent.

Junos OS devices use the AAA infrastructure for authenticating (the DHCP client for DHCP service with the assigned DHCP server. The following high-level steps are involved in DHCP client authentication:

- DHCP local server or relay agent receives a discover PDU from a client
- DHCP service contacts the AAA server to authenticate the DHCP client.
- DHCP service can obtain client addresses and DHCP configuration options from the external AAA authentication server.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command.

All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the `authentication-server` statement at the `[edit access profile profile-name]` hierarchy level.

Steps to Configure DHCP with External Authentication Server

To configure DHCP local server and DHCP relay agent for authentication support:

1. Specify that you want to configure authentication by including authentication keyword at respective hierarchy levels.
2. (Optional) Configure optional features to create a unique username.
3. (Optional) Configure a password that authenticates the username to the external authentication service.

Example:

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
```

```
        user-prefix user-prefix-string;
    }
}
```

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The DHCP service uses the information and sends it to the DHCP client.

The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications.

For example, if the authentication response includes an address pool name and a local configuration specifies DHCP attributes for that pool, the DHCP service merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client.

When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 13 on page 279 lists the information that RADIUS might include in the authentication grant. See *RADIUS Attributes and Juniper Networks VSAs Supported by the AAA Service Framework* for a complete list of RADIUS attributes and Juniper Networks VSAs that the extended DHCP applications supports for subscriber access management or DHCP management.

Table 13: Information in Authentication Grant

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address

Table 13: Information in Authentication Grant *(Continued)*

Attribute Number	Attribute Name	Description
RADIUS attribute 9	Framed-IP-Netmask	Subnet mask for client IP address (DHCP option 1)
Juniper Networks VSA 26-4	Primary-DNS	Primary domain server (DHCP option 6)
Juniper Networks VSA 26-5	Secondary-DNS	Secondary domain server (DHCP option 6)
Juniper Networks VSA 26-6	Primary-WINS	Primary WINS server (DHCP option 44)
Juniper Networks VSA 26-7	Secondary-WINS	Secondary WINS server (DHCP option 44)
RADIUS attribute 27	Session-Timeout	Lease time
RADIUS attribute 88	Framed-Pool	Address assignment pool name
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Example-Configuring DHCP with External Authentication Server

To configure authentication at DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent levels.

1. Specify that you want to configure authentication.

```
[edit system services dhcp-local-server]
user@host# edit authentication
```

2. (Optional) Specify the optional information you want to include in the username.

```
[edit system services dhcp-local-server authentication username-include]
user@host# set username-include circuit-type
user@host# set username-include domain-name example.com
user@host# set username-include mac-address
user@host# set username-include user-prefix wallybrown
```

3. Configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

```
[edit system services dhcp-local-server authentication]
user@host# set password $ABC123
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
    username-include {
        circuit-type;
        domain-name example.com;
        mac-address 2001:db8::/32;
        user-prefix wallybrown;
    }
}
```

The resulting unique username is:

```
wallybrown.2001:db8::/32.enet@example.com
```

Specifying Authentication Support

Include the `authentication` statement at hierarchy levels given in Table 14 on page 282. You can configure either global authentication support or group-specific support.

Table 14: Supported Hierarchy Levels for Authentication Support

Supported Hierarchy Level	Hierarchy Level
DHCP local server	`[edit system services dhcp-local-server]`
DHCP relay agent	`[edit forwarding-options dhcp-relay]`
DHCPv6 local server	`[edit system services dhcp-local-server dhcpv6]`
DHCPv6 relay agent	`[edit forwarding-options dhcp-relay dhcpv6]`

Creating Unique Usernames for DHCP Clients

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers (DHCP clients).

To configure unique usernames, use the `username-include` statement. You can include any or all of the additional statements.

```
authentication {
    username-include {
        circuit-type;
        client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
```

```
    }
}
```

NOTE: If you do not include a username in the authentication configuration, the router (or switch) does not perform authentication; however, the IP address is provided by the local pool if it is configured.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.

The following list describes the optional information that you can include as part of the username:

- `circuit-type`—The circuit type used by the DHCP client, for example `enet`.
- `client-id`—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- `delimiter`—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- `domain-name`—The client domain name as a string. The router adds the @ delimiter to the username.
- `interface-description`—The description of the device (physical) interface or the logical interface.
- `interface-name`—The interface name, including the interface device and associated VLAN IDs.
- `logical-system-name`—The name of the logical system, if the receiving interface is in a logical system.
- `mac-address`—The client MAC address, in a string of the format *xxxx.xxxx.xxxx*.
- `option-60`—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- `option-82 <circuit-id> <remote-id>`—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
  - `circuit-id`—The payload of the Agent Circuit ID suboption.
  - `remote-id`—The payload of the Agent Remote ID suboption.
  - Both `circuit-id` and `remote-id`—The payloads of both suboptions, in the format: `circuit-id[delimiter]remote-id`.
  - Neither `circuit-id` or `remote-id`—The raw payload of the option 82 from the PDU is concatenated to the username.

> **NOTE**: For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

- `relay-agent-interface-id`—The Interface-ID option (option 18). (DHCPv6 local server or DHCPv6 relay agent only)
- `relay-agent-remote-id`—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server or DHCPv6 relay agent only)
- `relay-agent-subscriber-id`—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server or DHCPv6 relay agent only)
- `routing-instance-name`—The name of the routing instance, if the receiving interface is in a routing instance.
- `user-prefix`—A string indicating the user prefix.
- `vlan-tags`—The subscriber VLAN tags. Includes the outer VLAN tag and, if present, the inner VLAN tag. You can use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

The router (switch) creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

For DHCP local server and DHCP relay agent:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]routing-instance-
name[delimiter]circuit-type[delimiter]interface-
name[delimiter]option-82[delimiter]option-60@domain-name
```

For DHCPv6 local server:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]routing-instance-
name[delimiter]circuit-type[delimiter]interface-name[delimiter]relay-agent-remote-
id[delimiter]relay-agent-subscriber-id[delimiter]relay-agent-interface-id[delimiter]client-
id@domain-name
```

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the *interface interface-name* statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the `upto` option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

Example- 2

To configure an interface group, use the `group` statement.

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface` *`interface-name`* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

1. The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

```
group boston {
    interface 192.168.10.1;
    interface 192.168.15.5;
}
```

2. You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
    interface 192.168.10.1 upto 192.168.10.255;
}
```

3.

You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
    interface 192.168.100.1 exclude;
    interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

Example:

```
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    interface interface-name <upto upto-interface-name> <exclude>;
}
```

RELATED DOCUMENTATION

Centrally Configure DHCP Options on a RADIUS Server | 288

IP Address Assignment Pool | 27

Centrally Configure DHCP Options on a RADIUS Server

IN THIS SECTION

- RADIUS-Sourced Options | 288
- Client-Sourced Options Configuration | 289
- Data Flow for RADIUS-Sourced DHCP Options | 289
- Multiple VSA 26-55 Instances Configuration | 291
- DHCP Options That Cannot Be Centrally Configured | 292

DHCP management on Junos OS devices support central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options) and traditional client-sourced options configuration. Read the following sections for information on central configuration of DHCP options on the RADIUS server.

RADIUS-Sourced Options

Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

Client-Sourced Options Configuration

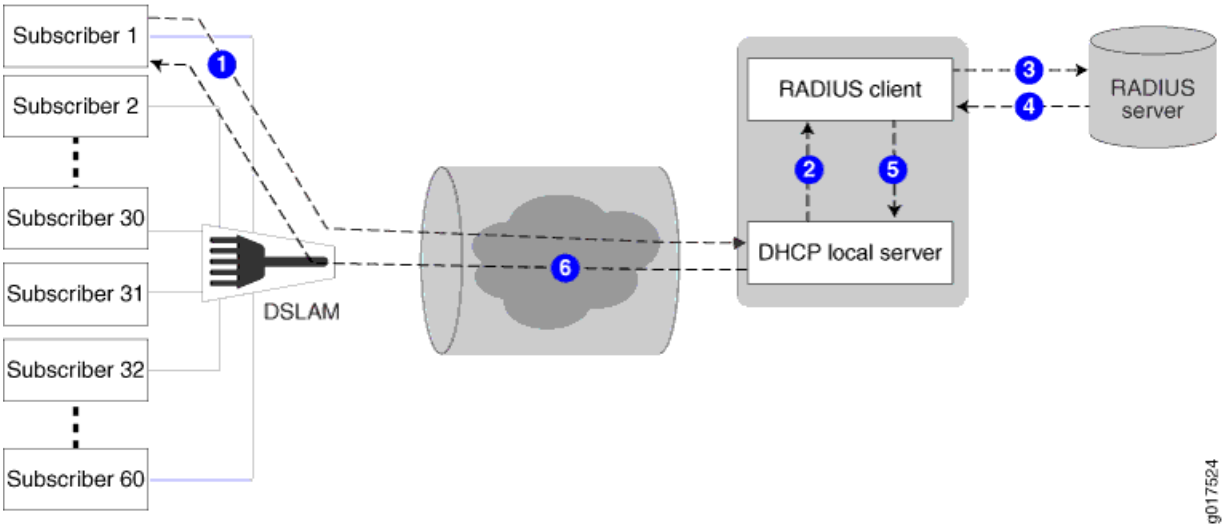
In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router's (switch's) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

Data Flow for RADIUS-Sourced DHCP Options

Figure 15 on page 290 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 15: DHCP Options Data Flow



The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.
2. The DHCP local server initiates authentication with the Junos OS RADIUS client.
3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber's (DHCP client's) client-sourced DHCP options.
4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.
5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.
6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).
7. The subscriber (DHCP client) is configured with the DHCP options.
8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:

- Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
- Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
- Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to by reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

BEST PRACTICE: For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

NOTE: If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the `RO` flags in the Subscriber Management RADIUS dictionary file. The `R` value indicates a multivalued reply attribute and the `O` value indicates an ordered attribute.

DHCP Options That Cannot Be Centrally Configured

Table 15 on page 292 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 15: Unsupported Opaque DHCP Options

DHCP Option	Option Name	Comments
Option 0	Pad Option	Not supported.
Option 51	IP Address Lease Time	Value is provided by RADIUS attribute 27 (Session-Timeout).
Option 52	Option Overload	Not supported.
Option 53	DHCP Message Type	Value is provided by DHCP local server.
Option 54	Server Identifier	Value is provided by DHCP local server.
Option 55	Parameter Request List	Value is provided by DHCP local server.
Option 255	End	Value is provided by DHCP local server.
–	DHCP magic cookie	Not supported.

RELATED DOCUMENTATION

- DHCP with External Authentication Server
- DHCP Overview
- IP Address Assignment Pool

CHAPTER 7

Managing DHCP Services

Group-Specific DHCP Configurations | 294

DHCP Snooping | 299

DHCP Auto Logout | 308

Additional Configurations for DHCP Clients | 312

Dynamic Reconfiguration of DHCP Servers and Clients | 317

DHCP Liveness Detection | 327

Secure DHCP Message Exchange | 355

DHCP Active Server Groups | 360

Suppressing DHCP Routes | 365

Group-Specific DHCP Configurations

IN THIS SECTION

- Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces | **294**
- Configuring Group-Specific DHCP Local Server Options | **296**
- Configuring Group-Specific DHCP Relay Options | **296**
- Configuring DHCP Server Configuration with Optional Pool Matching Using Groups | **298**

You use the group feature to group a set of interfaces and then apply a common DHCP configuration such as extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent to the named interface group. For more information, read this topic.

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following *configuration statement*:

```
user@host# set interface  interface-name upto upto-interface-name
```

- The start subunit, `interface` *`interface-name`*, serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit `.0` subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, `interface ge-2/2/2` is treated as `interface ge-2/2/2.0`.
- Ranged entries contain the `upto` option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a `0` (zero) subunit acts as a wildcard.

- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because `ge-1/0/0.10` is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface `ge-1/0/0.26` is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

  In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface `ge-1/0/0.20` takes precedence and enforces an interface client limit of `5`.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the `[edit system services dhcp-local-server group` *`group-name`*`]` hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the `[edit system services dhcp-local-server group` *`group-name`*`]` hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the `[edit system services dhcp-local-server]` hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the `dynamic-profile` statement.

- `authentication` —Configure the parameters the router sends to the external AAA server.
- `dynamic-profile` —Specify the dynamic profile that is attached to a group of interfaces.
- `interface` —Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- `liveness-detection` —Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see DHCP Liveness Detection Overview.
- `overrides` —Override the default configuration settings for the extended DHCP local server. For information, see *Overriding the Default DHCP Local Server Configuration Settings*.
- `interface-tag`—(Optional) Specifies a tag name for the interface that will be associated with a DHCP configuration. Use the tag to identify subscribers associated with this DHCP local server group.

Configuring Group-Specific DHCP Relay Options

You can include the following statements at the `[edit forwarding-options dhcp-relay group` *`group-name`*`]` hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements

apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level to configure group-specific options for DHCPv6 relay agent.

- `active-server-group` —Configure an active server group to apply a common DHCP relay agent configuration for a named group of DHCP server addresses. For information, see *Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups*.
- `authentication` —Configure the parameters the router (or switch) sends to the external AAA server.
- `dynamic-profile` —Specify the dynamic profile that is attached to a group of interfaces.
- `interface` —Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- `liveness-detection` —Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see DHCP Liveness Detection Overview.
- `overrides` —Override the default configuration settings for the extended DHCP relay agent. For information, see *Overriding the Default DHCP Relay Configuration Settings*.
- `relay-agent-interface-id` —(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.
- `relay-agent-remote-id` —(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.
- `relay-option` —Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see *Using DHCP Option Information to Selectively Process DHCP Client Traffic*.
- `relay-option-82` —(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see *Using DHCP Relay Agent Option 82 Information*.
- `service-profile` —Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see *Default Subscriber Service Overview* .
- `interface-tag`—(Optional) Specifies a tag name for the interface that will be associated with a DHCP configuration. Use the tag to identify subscribers associated with this DHCP relay agent.

Configuring DHCP Server Configuration with Optional Pool Matching Using Groups

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching must also be included in the address-assignment pool configuration. The DHCP local server uses the default pool match configuration of `ip-address-first`.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        ip-address-first:
        option-82:
    }
}
```

RELATED DOCUMENTATION

- DHCP Server Configuration | **52**
- DHCP Server Options | **77**
- DHCP Relay Agent | **153**
- DHCP Relay Agent Information Option (Option 82) | **198**

DHCP Snooping

IN THIS SECTION

- DHCP Snooping Support | 299
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent | 302
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | 305

DHCP snooping on Junos OS device validates DHCP messages and drops invalid traffic. You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives. For more information, read this topic.

DHCP Snooping Support

IN THIS SECTION

- What is DHCP Snooping | 299
- Benefits of DHCP Snooping | 300
- Activating DHCP Snooping | 300
- Configuring DHCP Snooping | 301

DHCP snooping provides additional security by identifying the incoming DHCP packets and rejecting DHCP traffic determined to be unacceptable from untrusted devices in the network.

What is DHCP Snooping

DHCP allocates IP addresses dynamically, leasing addresses to devices so that the addresses can be reused when they are no longer needed by the devices to which they were assigned. Hosts and end

devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping looks into incoming DHCP packets and examines DHCP messages. It extracts their IP addresses and lease information allocated to clients and builds up a database. Using this database, it can determine if the packets arriving are from the valid clients—that is—the IP addresses of the clients was assigned by the DHCP server. In this way, DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

Benefits of DHCP Snooping

- DHCP snooping provides an extra layer of security via dynamic IP source filtering.
- DHCP snooping can prevent rogue DHCP activity in the network by filtering out DHCP packets that are arriving on the wrong ports, or with incorrect contents.

Activating DHCP Snooping

When you are using the DHCP snooping feature, it is important that you understand about enabling the DHCP snooping feature.

On Junos OS device, you cannot configure DHCP snooping feature as an independent feature. Whenever you configure DHCP security or DHCP relay or DHCP server for a specific VLAN or interface or routing instance of the device, the DHCP snooping is automatically enabled on that VLAN/interface/ routing instance to perform it's task.

For example:

- When you enable DHCP Relay on a given list of interfaces of a specific routing instance
- DHCP snooping gets automatically enabled on those interfaces for that routing instance.
- When you enable DHCP security on a specific VLAN, DHCP snooping gets automatically enabled on that VLAN.

Junos OS enables DHCP snooping on a switch/router/firewall in:

- A routing instance when you configure the following options in that routing instance:
  - `dhcp-relay` statement at the [`edit forwarding-options`] hierarchy level.
  - `dhcp-local-server` statement at the [`edit system services`] hierarchy level.
- A switch when you configure the following option for any port security features:
  - `dhcp-security` statement at the [`edit vlans vlan-name forwarding-options`] hierarchy level.

TIP: If you need to configure DHCP relay, use the `forward-only` statement unless you need subscriber management or class-of-service (CoS).

We recommend you read the DHCP documentation and use a lab with DHCP traceoptions enabled to check and understand the configuration.

Configuring DHCP Snooping

In the default DHCP snooping configuration, all traffic is snooped.

On Junos OS device, DHCP snooping is enabled in a routing instance when you configure the following options in that routing instance:

- `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level
- `dhcp-local-server` statement at the `[edit system services]` hierarchy level
- You can optionally use the `forward-snooped-clients` statement to evaluate the snooped traffic and to determine if the traffic is forwarded or dropped, based on whether or not the interface is configured as part of a group.

The router discards snooped packets by default if there is no subscriber associated with the packet. To enable normal processing of snooped packets, you must explicitly configure the `allow-snooped-clients` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can configure DHCP snooping support for a specific routing instance for the following:

- DHCPv4 relay agent—Override the router's (or switch's) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets. A renew request may be unicast directly to the DHCP server. This is a BOOTPREQUEST packet and is snooped.

- DHCPv6 relay agent—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and

the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- DHCP local server—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.
- You can also disable snooping filters. In the preceding configurations, all DHCP traffic is forwarded to the slower routing plane of the routing instance before it is either forwarded or dropped. Disabling snooping filters causes DHCP traffic that can be forwarded directly from the faster hardware control plane to bypass the routing control plane.

Example: Configuring DHCP Snooping Support for DHCP Relay Agent

IN THIS SECTION

- Requirements | 302
- Overview | 302
- Configuration | 303

This example shows how to configure DHCP snooping support for DHCP relay agent.

Requirements

- Configure DHCP relay agent. See *Extended DHCP Relay Agent Overview*.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

- Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group **frankfurt**.

- Configure DHCP relay agent to forward snooped packets to only configured interfaces.

Configuration

IN THIS SECTION

- Procedure | 303

Procedure

Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Specify the named group of interfaces on which DHCP snooping is supported.

```
[edit forwarding-options dhcp-relay]
user@host# edit group frankfurt
```

3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

4. Specify that you want to override the default configuration for the group.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# edit overrides
```

5. Enable DHCP snooping support for the group.

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# set allow-snooped-clients
```

6. Return to the `[edit forwarding-options dhcp-relay]` hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group `frankfurt`).

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```

Results

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
    forward-snooped-clients configured-interfaces;
    group frankfurt {
        overrides {
            allow-snooped-clients;
        }
        interface fe-1/0/1.3 {
```

```
            upto fe-1/0/1.9;
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the `forward-snooped-clients` statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, you enable or disable the DHCP relay snooping feature.

Table 16 on page 305 shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the `allow-snooped-clients` statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets.

Table 16: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
`forward-snooped-clients` not configured	snooped packets result in subscriber (DHCP client) creation	dropped
`all-interfaces`	forwarded	forwarded
`configured-interfaces`	forwarded	dropped
`non-configured-interfaces`	snooped packets result in subscriber (DHCP client) creation	forwarded

Table 17 on page 306 shows the action the router (or switch) takes on snooped packets when DHCP snooping is disabled by the `no-allow-snooped-clients` statement.

Table 17: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
`forward-snooped-clients` not configured	dropped	dropped
`all-interfaces`	dropped	forwarded
`configured-interfaces`	dropped	dropped
`non-configured-interfaces`	dropped	forwarded

Table 18 on page 306 shows the action the router (or switch) takes for the snooped BOOTREPLY packets.

Table 18: Actions for Snooped BOOTREPLY Packets

forward-snooped-clients Configuration	Action
`forward-snooped-clients` not configured	snooped **BOOTREPLY** packets dropped if client is not found
`forward-snooped-clients` all configurations	snooped **BOOTREPLY** packets forwarded if client is not found

Configured interfaces have been configured with the **group** statement in the `[edit forwarding-options dhcp-relay]` hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the **group** statement.

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Enable DHCP snooped packet forwarding.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
    dhcp-relay {
        forward-snooped-clients configured-interfaces;
    }
}
```

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- Security Services Administration Guide
- DHCP Server | **49**
- DHCP Relay Agent | **153**
- DHCP Client | **245**

DHCP Auto Logout

IN THIS SECTION

- DHCP Auto Logout Overview | 308
- Automatically Logging Out DHCP Clients | 310

DHCP local server and DHCP relay agent support Auto logout feature. Auto logout releases and returns IP addresses to the address pool if DHCP clients are no longer using these addresses. It improves the efficiency of DHCP IP address assignment. For more information, read this topic.

DHCP Auto Logout Overview

IN THIS SECTION

- Auto Logout Overview | 308
- How DHCP Identifies and Releases Clients | 309
- Option 60 and Option 82 Requirements | 310

This topic provides an introduction to the DHCP auto logout feature and includes the following sections:

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the address pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address— the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful— the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method— DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.

  NOTE: The incoming interface method differs from the `overrides interface-client-limit 1` statement, which retains the existing binding and rejects the newly connected client.

- Option 60 and option 82 method— DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client' s existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, the DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in DHCP Relay Agent Option 82 Value for Auto Logout.

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet from a client whose identity matches an existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.
   - For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable auto logout and specify the secondary identification method you want to use when the primary identification method is unsuccessful.

   - For example, to configure DHCP local server to use the incoming interface method:

```
[edit system services dhcp-local-server overrides]
user@host# set client-discover-match incoming-interface
```

   - For example, to configure DHCP relay agent to use the option 60 and option 82 method:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set client-discover-match option60-and-option82
```

NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information | 199

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

Additional Configurations for DHCP Clients

IN THIS SECTION

- Specifying the Maximum Number of DHCP Clients Per Interface | 312
- DHCP Local Server Handling of Client Information Request Messages | 313
- Enabling Processing of Client Information Requests | 314
- Sending Release Messages When Clients Are Deleted | 315

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

NOTE: The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the `interface-client-limit` statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.
   - For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit overrides
```

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the `interface-client-limit` statement.)

```
[edit system services dhcp-local-server overrides]
user@host# set interface-client-limit number
```

NOTE: For DHCP local server and DHCP relay agent, you can use either the `interface-client-limit` statement or the `client-discover-match incoming-interface` statement to set a limit of one client per interface. The `interface-client-limit` statement with a value of 1 retains the existing client and rejects any new client connections. The `client-discover-match incoming-interface` statement deletes the existing client and allows a new client to connect.

DHCP Local Server Handling of Client Information Request Messages

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP inform or DHCPv6 information-request message that indicates what information is desired. These message types can be collectively referred to as information request messages. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients is typically configured with the `dhcp-attributes` statement for an address pool defined by the `address-assignment pool` *`pool-name`* statement at the `[edit access]` hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify the name of the pool from which the local server retrieves the requested configuration information for the client. If you do not do specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.

NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data can be used to select the pool from which the response information is taken. Additionally other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap exists between RADIUS attributes and local pool attributes, the RADIUS values are used instead of the local configuration data. If no RADIUS information is received from the underlying PPP interface, then the behavior is the same as described previously for non-PPP interfaces.

Enabling Processing of Client Information Requests

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See DHCPv6 Address-Assignment Pools. For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See *Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address* for details about how to configure the information sought by clients that send information request messages.

By default, DHCP local server and DHCPv6 local server do not respond to information request (DHCP inform and DHCPv6 information-request) messages from the client. You can enable DHCP local server

and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

To enable processing of DHCP client information request messages:

1. Specify that you want to configure override options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides]
     user@host# set process-inform
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides]
     user@host# set process-inform
     ```

2. (Optional) Specify a pool name from which DHCP information is returned to the client.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides process-inform]
     user@host# set pool pool-name
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides process-inform]
     user@host# set pool pool-name
     ```

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a

release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.

NOTE: You must include the `send-release-on-delete` statement to configure DHCP relay and relay proxy to send the release message when the `client-discover-match` statement is included.

You can use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.
   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set send-release-on-delete
   ```

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

DHCP Client | 245

Dynamic Reconfiguration of DHCP Servers and Clients

IN THIS SECTION

- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients | 317
- Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview | 321
- Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings | 322
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients | 323
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails | 324
- Configuring a Token for DHCP Local Server Authentication | 325
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | 326

Junos OS allows you to perform different types of DHCP services such as attaching dynamic profiles, using external authentication services with DHCP, specifying maximum number of clients, managing client information request messages, dynamic reconfiguration of clients and so on. For more information, read this topic.

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

IN THIS SECTION

- Default Client/Server Interaction | 318
- Dynamic Client/Server Interaction for DHCPv4 | 319
- Dynamic Client/Server Interaction for DHCPv6 | 319
- Manually Forcing the Local Server to Initiate the Reconfiguration Process | 320
- Action Taken for Events That Occur During a Reconfiguration | 320
- Benefits of Dynamic Reconfiguration of DHCP Local Server Clients | 321

Dynamic reconfiguration of clients enables the extended DHCP local server to initiate a client update without waiting for the client to initiate a request.

Default Client/Server Interaction

Typically the DHCP client initiates all of the basic DHCP client/server interactions. The DHCP server sends information to a client only in response to a request from that client. This behavior does not enable a client to be quickly updated with its network address and configuration in the event of server changes:

> **NOTE**: Technically, the DHCP client/server interactions are the same on routers and switches. However, the primary usage of this technology on the routers is for subscriber management. The switches are not used for subscriber management. Therefore, this topic provides two sample scenarios. The actions are the same, but the implementation details are different.

- On routers—Suppose a service provider restructures its addressing scheme or changes the server IP addresses that it provided to clients. Without dynamic reconfiguration, the service provider typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, the provider can wait for customers to make a service call about the network failures and then instruct them to power cycle their customer premises equipment to reinitiate the connection. Neither of these actions is timely or convenient for customers.

- On switches—Suppose you restructure the addressing scheme or change the server IP addresses that the DHCP server provides to clients. Without dynamic reconfiguration, the network typically clears the DHCP server binding table, but cannot inform the DHCP clients that their bindings have been cleared. Consequently, the DHCP client operates as though its IP address is still valid, but it is now unable to communicate over the access network, resulting in an outage. The DHCP local server needs to wait for the client to send a message to renew its lease or rebind to the server. In response, the server sends a NAK message to the client to force it to begin the DHCP connection process again. Alternatively, you can wait for users to notify you of the network failures and then instruct them to power cycle their equipment to reinitiate the connection. Neither of these actions is timely or convenient for users.

Dynamic Client/Server Interaction for DHCPv4

Dynamic reconfiguration for DHCPv4 is available through a partial implementation of RFC 3203, *DHCP Reconfigure Extension* for DHCPv4. It enables the DHCPv4 local server to send a message to the client to force reconfiguration.

The server sends a forcerenew message to a DHCPv4 client, initiating a message exchange. In response, DHCPv4 clients that support the forcerenew message then send a lease renewal message to the server. The server rejects the lease renewal request and sends a NAK to the client, causing the client to reinitiate the DHCP connection. A successful reconnection results in the reconfiguration of the DHCP client. Only the exchange of forcerenew, renew, and NAK messages is supported from RFC 3202. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to forcerenew messages other than to forward them to the client.

When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfiguring state and the local server sends a forcerenew message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber services or DHCP-managed services, such as forwarding and statistics, continue to work. Client statistics are not maintained in the interval between a successful reconfiguration and the subsequent client binding. When the server responds to the client renewal request with a NAK, the client entry is removed from the binding table and final statistics are reported. New statistics are collected when the client sends a discover message to establish a new session.

Dynamic Client/Server Interaction for DHCPv6

Dynamic reconfiguration for DHCPv6 is available through a partial implementation of RFC 3315, *Dynamic Host Configuration Protocol for IPv6 (DHCPv6)*. It enables the DHCPv6 local server to send a message to the client to force reconfiguration.

DHCPv6 servers send reconfigure messages to DHCPv6 clients, initiating a message exchange. In response, DHCPv6 clients that support the reconfigure message transition to the renewing state and send a renew message to the server. The server returns a reply message with a lifetime of zero (0). The client transitions to the init state and sends a solicit message. The server sends an advertise message to indicate that it is available for service. The client sends a request for configuration parameters, which the server then includes in its reply. DHCP relay and DHCP relay proxy do not participate in the client reconfiguration or react to reconfigure messages other than to forward them to the client.

When a DHCPv6 server is triggered to initiate reconfiguration on a bound DHCPv6 client, the client transitions to the reconfigure state. All subscriber services, such as forwarding and statistics, continue to work. The server then sends the reconfigure message to the client. If the DHCPv6 client is already in the reconfigure state, the DHCPv6 server ignores the reconfiguration trigger. For clients in any state other than bound or reconfigure, the server clears the binding state of the client, as if the `clear dhcpv6 server binding` command had been issued.

Manually Forcing the Local Server to Initiate the Reconfiguration Process

You can force the local server to initiate the reconfiguration process for clients by issuing the `request dhcp server reconfigure` command for DHCPv4 clients, and the `request dhcpv6 server reconfigure` command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Action Taken for Events That Occur During a Reconfiguration

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. Table 19 on page 320 lists the actions taken in response to several different events.

Table 19: Action Taken for Events That Occur During a Reconfiguration

Event	Action
Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.	Server drops packet and deletes client.
Server receives a request, renew, rebind, or init-reboot message from the client.	DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).
Server receives a release or decline message from the client.	Server deletes client.
The client lease times out.	Server deletes client.
The `clear dhcp server binding` command is issued.	Server deletes client.
The `request dhcp server reconfigure` (DHCPv4) or `request dhcpv6 server reconfigure` (DHCPv6) command is issued.	Command is ignored.
GRES or DHCP restart occurs.	Reconfiguration process is halted.

Benefits of Dynamic Reconfiguration of DHCP Local Server Clients

- Enable the DHCP local server to dynamically reconfigure DHCP clients, avoiding extended outages because of server configuration changes that otherwise require the server to wait for the client to renews its lease or rebind to the server.

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements. You can provide the statements at the `[edit system services dhcp-local-server reconfigure]` hierarchy level for all DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 reconfigure]` hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the `[edit system services dhcp-local-server group` *`group-name`* `reconfigure]` hierarchy level for DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 group` *`group-name`* `reconfigure]` hierarchy level for DHCPv6 clients.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

   For DHCPv4:

   ```
   [edit system services dhcp-local-server]
   user@host# set reconfigure
   ```

   For DHCPv6:

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set reconfigure
   ```

2. (Optional) Enable dynamic reconfiguration for only the clients serviced by a group of interfaces.

For DHCPv4:

```
[edit system services dhcp-local-server group-name]
user@host# set reconfigure
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name]
user@host# set reconfigure
```

3. (Optional) Configure how the server attempts reconfiguration.

   See *Configuring Dynamic Reconfiguration Attempts for DHCP Clients*.

4. (Optional) Configure the response to a failed reconfiguration.

   See *Configuring Deletion of the Client When Dynamic Reconfiguration Fails*.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

   See *Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect*.

6. (Optional) Configure a token for rudimentary server authentication.

   See *Configuring a Token for DHCP Local Server Authentication*.

7. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

   See *Preventing Binding of Clients That Do Not Support Reconfigure Messages*.

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the `all` option.

```
user@host> request dhcp server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCPv4 client.

```
user@host> request dhcp server reconfigure 192.168.27.3
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 00:00:5E:00:53:67
```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

```
user@host> request dhcp server reconfigure all logical-system ls-bldg5
```

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

```
user@host> request dhcp server reconfigure all routing-instance ri-boston
```

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending forcerenew or reconfigure messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

   For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set timeout 8
```

   For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set timeout 8
```

To override the global configuration for a particular group of clients, include the statements at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-terminate
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-terminate
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Configuring a Token for DHCP Local Server Authentication

You can configure an authentication token to provide rudimentary protection against inadvertently instantiated DHCP servers. You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. If the service provider has previously configured the DHCP client with a token, then the client can compare that token against the newly received token. If the tokens do not match, the DHCP client discards the forcerenew message. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.

  For DHCPv4:

  ```
  [edit system services dhcp-local-server reconfigure]
  user@host# set token token-value
  ```

  For DHCPv6:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set token token-value
  ```

(Optional) For only a particular group of clients:

- Specify the token.

  For DHCPv4:

```
[edit system services dhcp-local-server group group-name reconfigure]
user@host# set token token-value
```

  For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set token token-value
```

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

  For DHCPv4:

```
[edit system services dhcp-local-server reconfigure trigger]
user@host# set radius-disconnect
```

  For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure trigger]
user@host# set radius-disconnect
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure trigger]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger]` hierarchy level.

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.1	Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements.

RELATED DOCUMENTATION

- DHCP Overview | 2
- IP Address Assignment Pool | 27
- DHCP Server | 49
- DHCP Relay Agent | 153
- DHCP Client | 245

DHCP Liveness Detection

IN THIS SECTION

- DHCP Liveness Detection Overview | 328
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD | 330
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 332
- Configuring Detection of DHCP Local Server Client Connectivity with BFD | 336
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 338
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 343

DHCP liveness detection for DHCP client IP sessions utilizes an active liveness detection protocol to conduct liveness detection checks for relevant clients. When configured with a liveness detection protocol, if a given client fails to respond to a configured number of consecutive liveness detection requests, the client binding is deleted and its resources released. For more information, read this topic.

DHCP Liveness Detection Overview

IN THIS SECTION

- Benefits of DHCP Liveness Detection | 329

Unlike PPP, DHCP does not define a native keepalive mechanism as part of either the DHCPv4 or DHCPv6 protocols. Without a keepalive mechanism, DHCP local server, DHCP relay, and DHCP relay proxy are unable to quickly detect if any of them has lost connectivity with a subscriber or a DHCP client. Instead, they must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages before exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often insufficient when serving as session health checks for clients in a DHCP subscriber access or a DHCP-managed network. Because DHCP lease times are typically too long to provide an adequate response time for a session health failure, and configuring short DHCP lease times can pose an undue burden on control plane processing, implementing a DHCP liveness detection mechanism enables better monitoring of bound DHCP clients. When configured with a liveness detection protocol, if a given subscriber (or client) fails to respond to a configured number of consecutive liveness detection requests, the subscriber (or client) binding is deleted and its resources released.

DHCP liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

Examples of liveness detection protocols include Bidirectional Forwarding Detection (BFD) for both DHCPv4 and DHCPv6 subscribers, IPv4 Address Resolution Protocol (ARP) for DHCPv4 subscribers, and IPv6 Neighbor Unreachability Detection (NUD) using Neighbor Discovery (ND) packets for DHCPv6 subscribers.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. In earlier releases, only BFD is supported for all platforms.

The two liveness detection methods are mutually exclusive.

When configuring BFD liveness detection, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 liveness detection either globally or per DHCPv4 or DHCPv6 group.
- DHCPv4 or DHCPv6 subscriber access clients that do not support BFD are not affected by the liveness detection configuration. These clients can continue to access the network (after they are validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for clients that support BFD when those clients enter a bound state.
- After protocol-specific messages are initiated for a BFD client, they are periodically sent to the subscriber (or client) IP address of the client and responses to those liveness detection requests are expected within a configured amount of time.
- If liveness detection responses are not received from clients that support BFD within the configured amount of time for a configured number of consecutive attempts, the liveness detection check is deemed to have failed. A configured failure action to clear the client binding is applied.
- The only failure action supported for Layer 2 Liveness detection is `clear-binding`.

When configuring DHCP ARP and ND Layer 2 liveness detection on MX Series, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 ARP and ND liveness detection globally, per DHCPv4 or DHCPv6 group, and per dual-stack group.
- ARP/ND liveness detection applies only to DHCP clients that:
  - Are directly connected over dynamic VLANs.
  - Have permanent Layer 2 entries.
- DHCPv6 clients must have a unique source MAC address and link-local address. Only single liveness detection entry is used for all IPv6 addresses associated with a specific client session.

Benefits of DHCP Liveness Detection

Using DHCP liveness detection, IP sessions are acted upon as soon as liveness detection checks fail. This faster response time serves to:

- Provide more accurate time-based accounting of subscriber (or DHCP client) sessions.
- Better preserve router (switch) resources.

- Help to reduce the window of vulnerability to some security attacks.

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP relay clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection
     ```

   - For DHCP group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit liveness-detection
     ```

   NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name` hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.

   ```
   [edit forwarding-options dhcp-relay group group-name]
   user@host# set overrides proxy-mode
   ```

3. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit method
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit method
```

4. Specify the liveness detection method that you want DHCP to use.

> **NOTE**: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.
>
> Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit bfd
```

5. Configure the liveness detection method as desired.

   See "Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients" on page 332 for an example of how to globally configure DHCP relay liveness detection with BFD.

6. Configure the action the router takes when a liveness detection failure occurs.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

IN THIS SECTION

- Requirements | 332
- Overview | 333
- Configuration | 333

This example shows how to configure liveness detection for DHCP relay agent subscribers using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers.
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP relay agent. See *Extended DHCP Relay Agent Overview*.

Overview

In this example, you configure liveness detection for DHCP relay agent subscribers by completing the following operations:

1. Enable liveness detection globally for DHCP relay subscribers.
2. Specify BFD as the liveness detection method for all dynamically created DHCP relay subscribers.
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level.

Configuration

IN THIS SECTION

- Procedure | 333

Procedure

Step-by-Step Procedure

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.

```
[edit forwarding-options dhcp-relay]
user@host# edit liveness-detection
```

2. Specify that you want to configure the liveness detection method.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit method
```

3. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

4. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set detection-time threshold 50000
```

5. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set holddown-interval 50
```

6. Configure the BFD minimum transmit and receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-interval 45000
```

7. Configure the minimum receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

8. Configure a multiplier value for the detection time.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set multiplier 100
```

9. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set no-adaptation
```

10. Configure the BFD session mode.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set session-mode automatic
```

11. Configure the threshold and minimum interval for the BFD transmit interval.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

12. Configure the BFD protocol version you want to detect.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set version automatic
```

13. Configure the action the router takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

Results

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
    liveness-detection {
```

```
        failure-action clear-binding-if-interface-up;
        method {
            bfd {
                version automatic;
                minimum-interval 45000;
                minimum-receive-interval 60000;
                multiplier 100;
                no-adaptation;
                transmit-interval {
                    minimum-interval 45000;
                    threshold 60000;
                }
                detection-time {
                    threshold 50000;
                }
                session-mode automatic;
                holddown-interval 50;
            }
        }
    }
    }
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring Detection of DHCP Local Server Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP local server clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: You can also configure DHCP liveness detection for DHCP relay.

To configure liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

- For DHCP global configuration:

```
[edit system services dhcp-local-server]
user@host# edit liveness-detection
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name]
user@host# edit liveness-detection
```

NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

2. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit method
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit method
```

3. Specify the liveness detection method that you want DHCP to use.

NOTE: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit bfd
```

4. Configure the liveness detection method as desired.

   See *Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients* for an example of how to configure DHCPv4 groups for DHCP local server liveness detection with BFD.

5. Configure the action the router takes when a liveness detection failure occurs.

   - For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit failure-action action
```

   - For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

IN THIS SECTION

- Requirements | 339
- Overview | 339
- Configuration | 339

This example shows how to configure group liveness detection for DHCP local server subscribers or DHCP clients using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP local server. See *Understanding Differences Between Legacy DHCP and Extended DHCP*.

Overview

In this example, you configure group liveness detection for DHCP local server subscribers (clients) by completing the following operations:

1. Enable liveness detection for DHCP local server subscriber (or DHCP client) groups.
2. Specify BFD as the liveness detection method for all dynamically created DHCP local server subscribers (clients).
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router (switch) takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

Configuration

IN THIS SECTION

- Procedure | 340

Procedure

Step-by-Step Procedure

To configure group liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

```
[edit system services dhcp-local-server ]
user@host# edit liveness-detection
```

2. Specify that you want to configure liveness detection for a specific DHCP local server group.

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit group local_group_1
```

3. Specify that you want to configure the liveness detection method.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit method
```

4. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method]
user@host# edit bfd
```

5. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set detection-time threshold 30000
```

6. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set holddown-interval 50
```

7. Configure the BFD minimum transmit and receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum transmit and receive interval if you configure the `minimum-interval` for the BFD `transmit-interval` statement and the `minimum-receive-interval`.

```
[edit system services dhcp-local-servergroup local_group_1  liveness-detection method bfd]
user@host# set minimum-interval 45000
```

8. Configure the minimum receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum receive interval if you configure the BFD minimum transmit and receive interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

9. Configure a multiplier value for the detection time.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set multiplier 100
```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set no-adaptation
```

11. Configure the BFD session mode.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set session-mode automatic
```

12. Configure the threshold and minimum interval for the BFD transmit interval.

NOTE: You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

13. Configure the BFD protocol version you want to detect.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set version automatic
```

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit failure-action action
```

Results

From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.

```
[edit]
user@host# show system
services {
    dhcp-local-server {
        group local_group_1 {
            liveness-detection {
                failure-action clear-binding-if-interface-up;
                method {
                    bfd {
                        version automatic;
                        minimum-interval 45000;
                        minimum-receive-interval 60000;
                        multiplier 100;
```

```
                    no-adaptation;
                    transmit-interval {
                        minimum-interval 45000;
                        threshold 60000;
                    }
                    detection-time {
                        threshold 30000;
                    }
                    session-mode automatic;
                    holddown-interval 50;
                }
            }
        }
    }
}
}
```

If you are done configuring the device, enter `commit` from configuration mode.

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

IN THIS SECTION

- How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works | **343**
- Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets | **348**
- Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets | **351**
- Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets | **354**

How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works

IN THIS SECTION

- Send Functionality | **344**

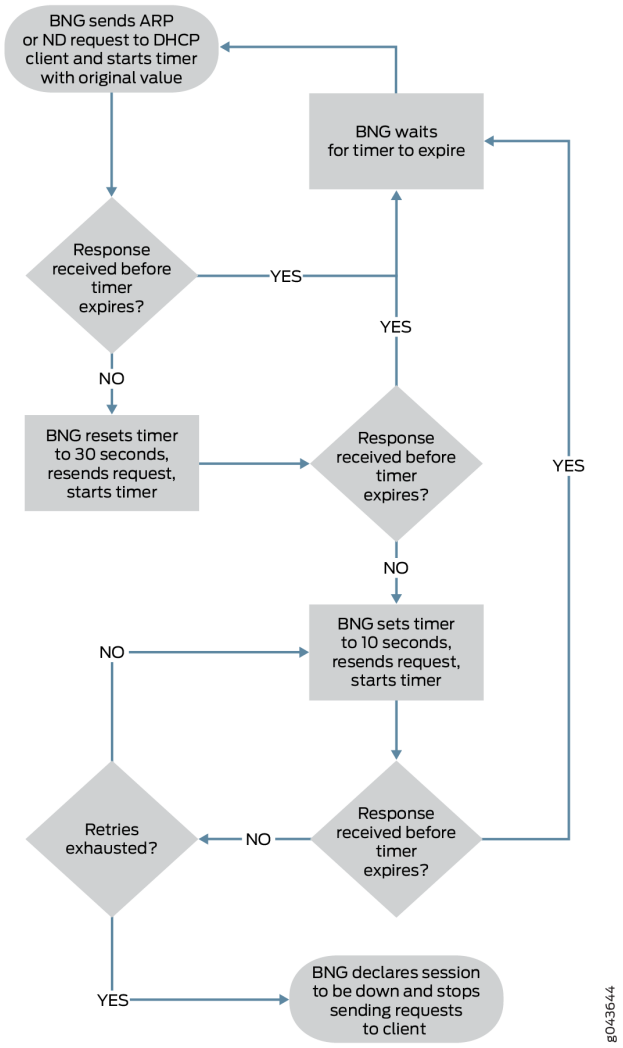
- Receive Functionality | 346

Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients. This Layer 2 liveness detection offers separate mechanisms for the DHCP client host and for the router acting as a broadband network gateway (BNG) to determine the validity and state of the DHCP client sessions. These mechanisms are referred to as the *send* functionality and the *receive* functionality. You can configure Layer 2 liveness detection for DHCP local server and DHCP relay clients.

Send Functionality

The BNG uses the send functionality to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions. Figure 1 illustrates the send functionality.

Figure 16: Layer 2 Liveness Detection Send Behavior Flow



1. The BNG sends request packets to the each DHCP client at a configurable interval, then waits for a response. The BNG retries the requests when it does not receive a timely response. It sends ARP requests for DHCPv4 clients and Neighbor Discovery (ND) requests for DHCPv6 clients.

2. If the BNG receives a response from the client before the interval times out, it waits for the timer to expire and then sends another request to that client.

3. If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt; the timer is not configurable.

4. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

5. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This timer value is not configurable.

6. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

7. If the BNG does not receive a response within the 10-second interval, it sends another request and starts the 10-second timer again. The BNG continues to send requests at 10-second intervals until it receives a response from the client before the interval times out or it exhausts the number of retry attempts.

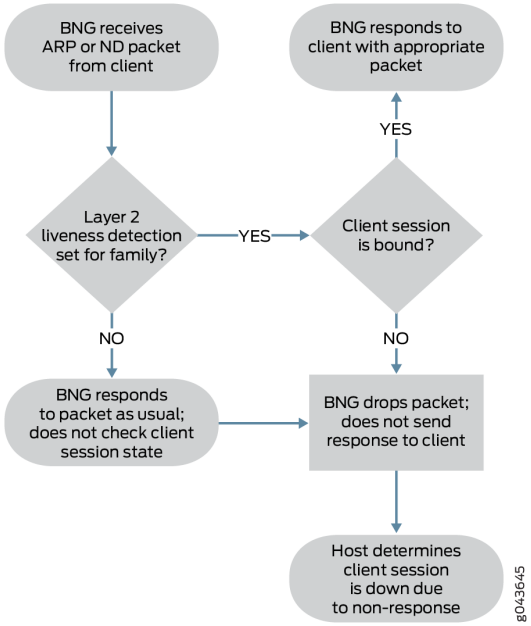
   The first retry attempt uses the 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

8. If the BNG never sends a response from a client within the interval before the retries are exhausted, then the liveness detection check fails and the clear-binding failure action is implemented. The client session is cleared.

Receive Functionality

The receive functionality enables a DHCP client host to determine the state of the DHCPv4 or DHCPv6 client session from the perspective of a BNG. The BNG conducts a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients when it receives ARP or ND packets. Figure 2 illustrates the receive functionality.

Figure 17: Layer 2 Liveness Detection Receive Behavior Flow



When the BNG receives either of these packets, it does the following:

1. Checks whether Layer 2 liveness detection for subscriber management is enabled globally for the relevant address family, inet or inet6.
2. If Layer 2 liveness detection is not enabled, then the BNG responds as usual to the received packets without checking the state of the client session.
3. If liveness detection is enabled for the family, then the BNG checks whether the client session is still in the bound state.
4. If the client session is bound, the BNG responds to the client with the appropriate ARP or ND packet.
5. If the session is not bound, the BNG drops the received packet. It does not send an ARP or ND response packet to the host, enabling the host to determine that the BNG considers the session to be down.

The usefulness of the receive functionality depends on the ability of the DHCP client host to reclaim resources from the stale client based on the absence of a response packet from the BNG for an unbound client session. If this capability requires a change in the client implementation, you may want to use the send functionality.

Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 local server liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

- For DHCPv4 group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv4 dual-stack-group configuration:

```
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv4 global configuration:

```
[edit system services dhcp-local-server liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 dual-stack-group configuration:

```
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 local server liveness detection:

1. Specify that you want to configure the liveness detection method.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit liveness-detection method
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6 liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6 liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP relay clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 relay liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

- For DHCPv4 group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv4 dual-stack-group configuration:

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv4 global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 dual-stack-group configuration:

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 relay liveness detection:

1. Specify that you want to configure the liveness detection method.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit liveness-detection method
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the receive functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The receive functionality enables the DHCP client host to determine whether a client session is down based on a lack of response from the BNG to the ARP or ND packets it sends to the BNG. You configure the receive functionality globally for DHCP per address family as an override to the global subscriber management configuration.

Enable Layer 2 liveness detection globally per address family.

- For DHCPv4:

```
[edit system services subscriber-management overrides]
user@host# set interfaces family inet layer2-liveness-detection
```

- For DHCPv6:

```
[edit system services subscriber-management overrides]
user@host# set interfaces family inet6 layer2-liveness-detection
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

DHCPv6 Server | 104

DHCPv6 Relay Agent | 222

Secure DHCP Message Exchange

IN THIS SECTION

- DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs | 355
- Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances | 356

Junos OS allows you to use the DHCP relay agent to provide secure message exchange between different virtual routing and forwarding instances (VRFs). To enable secure exchange of DHCP messages, you must configure both the server side and the client side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information. For more information, read this topic.

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs

In some service provider networks, the service network in which the DHCP server resides is isolated from the actual subscriber network. This separation of the service and subscriber networks can sometimes introduce potential security issues, such as route leaking.

Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different virtual routing and forwarding instances (VRFs). The DHCP relay agent can ensure that there is no direct routing between the client VRF and the DHCP

server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. Subscriber management supports the cross-VRF message exchange for both DHCP and DHCPv6 packets.

To exchange DHCP messages between different VRFs, you must enable both the server-side and the client-side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information in the packets. The message exchange uses the following DHCP options to identify the traffic to be relayed.

- Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets
- Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets

Statistics for DHCP packets using the cross-VRF message exchange are counted in the client VRF.

The following list describe how DHCP relay agent exchanges messages between the DHCP clients and DHCP server in different VRFs:

- Packets from DHCP client to DHCP server—DHCP relay agent receives the DHCP packet from the client in the client VRF, and then inserts the appropriate DHCP option 82 suboption 1 or DHCPv6 option 18 attribute into the packet. The relay agent then forwards the packet to the DHCP server in the server's VRF.
- Packets from DHCP server to DHCP client—DHCP relay agent receives the DHCP reply message from the DHCP server in the server VRF. The relay agent derives the client's interface, including VRF, from the DHCP option 82 suboption 1 or DHCPv6 option 18 attribute in the packet in the DHCP server VRF. The relay agent then forwards the reply message to the DHCP client in the client's VRF.

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances

IN THIS SECTION

- Client-Side Support | 358
- Server-Side Support | 358
- DHCP Local Server Support | 359

Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for a *stateless* DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that must be isolated from the client network.

A stateless DHCP relay agent does not maintain dynamic state information about the DHCP clients and does not maintain a static route for the traffic to flow between the client and server routing instances.

To enable the DHCP message exchange between the two VRFs, you configure each side of the DHCP relay to recognize and forward acceptable traffic based on the DHCP option information in the packets. The acceptable traffic is identified by either the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets or the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets.

The following list provides an overview of the tasks required to create the DHCP message exchange between the different VRFs:

- Client-side support—Configure the DHCP relay agent `forward-only` statement to specify the VRF location of the DHCP server, to which the DHCP relay agent forwards the client packets with the appropriate DHCP option information. The `forward-only` statement ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations (such as creating dynamic interfaces or maintaining leases).

  You can optionally configure a specific logical system and routing instance for the server VRF. If you do not specify a logical system or routing instance, then DHCP uses the local logical system and routing instance from which the configuration is added.

- Server-side support—Configure the DHCP relay agent `forward-only-replies` statement so the DHCP relay agent forwards the reply packets that have the appropriate DHCP option information. This statement also ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations.

  NOTE: You do not need to configure the `forward-only-replies` statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

- DHCP local server support—Configure the DHCP local server to support option 82 information in DHCP NAK and forcerenew messages. By default, the two message types do not support option 82.

- Additional support—Ensure that the following required support is configured:

  - Proxy ARP support must be enabled on the server-facing interface in the DHCP server VRF so that the DHCP relay agent can receive and respond to the ARP requests for clients and the client-facing interface in the DHCP server VRF.

  - Routes must be available to receive the DHCP packets from the DHCP server in the server VRF for the clients reachable in the client VRF.

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different VRFs.

Client-Side Support

To configure support on the client side of the DHCP relay agent:

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP server VRF to which the DHCP relay agent forwards the packets from the DHCP client. DHCP relay agent forwards the acceptable packets that have the appropriate DHCP option information, but does not perform any additional subscriber management operations. You can configure the `forward-only` statement globally or for a named group of interfaces, and for DHCPv4 or DHCPv6. You can specify the current, default, or a specific logical system or routing instance for the server VRF.

   The following example configures the `forward-only` statement globally for DHCPv4, and specifies the default logical system and routing instance:

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only logical-system default routing-instance default
```

NOTE: For local DHCPv4 clients, the DHCP relay agent adds the Agent Circuit ID option. However, if the Agent Circuit ID option is already present in the packet, you must ensure that the DHCP server supports the option 82 Vendor-Specific Information suboption (suboption 9).

If the `forward-only` statement is configured at the `[edit forwarding-options dhcp-relay relay-option]` hierarchy level, then that relay-option action takes precedence over the configuration of the `forward-only` statement for the DHCP cross-VRF message exchange.

Server-Side Support

To configure the cross-VRF message exchange support on the server side of the DHCP relay:

NOTE: You do not need to configure the `forward-only-replies` statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Configure the DHCP relay agent to forward the DHCP packets from the DHCP server VRF to the client. DHCP relay agent only forwards the packets, and does not perform any additional subscriber management operations. You can configure the `forward-only-replies` statement globally for DHCPv4 and DHCPv6.

   The following example configures the `forward-only-replies` statement globally for DHCPv4.

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only-replies
```

DHCP Local Server Support

To configure the DHCP local server to support option 82 information in NAK and forcerenew messages; the cross-VRF message exchange feature uses the option 82 or DHCPv6 option 18 information to determine the client VRF:

1. Enable DHCP local server configuration.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Specify that you want to configure an override option.

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

3. Configure DHCP local server to override the default behavior and support option 82 information in DHCP NAK and forcerenew messages. You can configure the override action globally, for a group of interfaces, or for a specific interface.

```
[edit system services dhcp-local-server overrides]
user@host# set include-option-82 forcerenew nak
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
14.2	Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different virtual routing and forwarding instances (VRFs).
14.2	Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information

DHCP Server | 49

DHCP Relay Agent | 153

DHCP Client | 245

DHCPv6 Server | 104

DHCPv6 Relay Agent | 222

DHCPv6 Client | 266

DHCP Active Server Groups

IN THIS SECTION

- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups | 361

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group. For this, you must configure a group of DHCP server addresses, and apply them as an active server group. For more information, read this topic.

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups

You can apply a common DHCP or DHCPv6 relay configuration to a set of IP addresses configured as a server group. An active server group is sometimes referred to as a trusted group of servers.

You can configure active server groups globally or at the group level (configured with the `group`. When you apply the active server group at the group level, it overrides a global active server group configuration.

To configure a group of DHCP server addresses and apply them as an active server group:

1. Specify the name of the server group.
   - For DHCPv4 servers:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# set server-group server-group-name
     ```

   - For DHCPv6 servers:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# set server-group server-group-name
     ```

2. Add the IP addresses of the DHCP servers belonging to the group.
   - For DHCPv4 servers:

     ```
     [edit forwarding-options dhcp-relay server-group server-group-name]
     user@host# set ip-address1
     user@host# set ip-address2
     ```

   - For DHCPv6 servers:

     ```
     [edit forwarding-options dhcp-relay dhcpv6 active-server-group]
     user@host# set ip-address1
     user@host# set ip-address2
     ```

NOTE: Starting in Junos OS Release 18.4R1, up to 32 server IP addresses are supported per DHCPv4 server group. In earlier releases, a maximum of 5 server IP addresses are supported for DHCPv4 servers. Configuring more than the maximum number of server addresses results in a commit check failure.

3. Apply the server group as an active server group.
   - At global level (DHCPv4)

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group server-group-name
```

   - At group-level (DHCPv4)

```
[edit forwarding-options dhcp-relay group interface-group-name]
user@host# set active-server-group server-group-name
```

   - At global level (DHCPv6)

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set active-server-group server-group-name
```

   - At group-level (DHCPv6)

```
[edit forwarding-options dhcp-relay dhcpv6 group interface-group-name]
user@host# set active-server-group server-group-name
```

Example: Configuring Active Server Groups in DHCP Relay Agent Configuration

For example, you might want to direct certain DHCP client traffic to a DHCP server. You can configure an interface group for each set of clients, specifying the DHCP relay interfaces for the group. In each of these groups, you specify an active server group to which each client groups traffic is forwarded. After a DHCP server group is created and server IP addresses are added to the group, the device used as the DHCP relay agent can forward messages to specific servers.

- Three groups of DHCP server addresses are configured, Default, Campus-A, and Campus-B.

- The Default group is applied as the global active server group for the overall DHCP relay configuration.
- The Campus-A server group is assigned as the active server group for interface group Campus-A-v10-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-A-v10-DHCP-RELAY is forwarded to DHCP servers 198.51.100.100 and 198.51.100.101.
- The Campus-B server group is assigned as the active server group for interface group Campus-B-v200-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-B-v200-DHCP-RELAY is forwarded to DHCP servers 198.51.100.55 and 198.51.100.56.
- All other DHCP traffic is forwarded to DHCP server 203.0.113.1.

```
[edit forwarding-options dhcp-relay]
#
# Server groups
user@host# set server-group Default 203.0.113.1
user@host# set server-group Campus-A 198.51.100.100
user@host# set server-group Campus-A 198.51.100.101
user@host# set server-group Campus-B 198.51.100.55
user@host# set server-group Campus-B 198.51.100.56
#
# Default server group applied globally.
user@host# set active-server-group Default
#
# Interface groups with application of active server groups
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.1
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.2
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.3
user@host# set group Campus-A-v10-DHCP-RELAY active-server-group Campus-A
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.4
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.5
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/1/0.6
user@host# set group Campus-B-v200-DHCP-RELAY active-server-group Campus-B
```

Note the following:

- In some configurations, servers in an active server group maintain redundant information about the DHCP clients. If the binding server later becomes inaccessible, the client is unable to renew the lease from that server. When the client attempts to rebind to a server, other servers in the group with the client information can reply with an ACK message. By default, instead of forwarding the ACK to the DHCP client, the relay agent drops any such ACKs that it receives from any server other than the

binding server because the new server address does not match the expected server address in the DHCP client entry. Consequently the lease cannot be extended by any of the redundant servers.

- Starting in Junos OS Release 16.2R1, you can enable a DHCPv4 relay agent to forward DHCP request (renew or rebind) ACKs from any server in the active server group (thus, any trusted server). The relay agent updates the client entry with the new server address. Because the servers in the group are expected to mirror the client information exactly, the lease option is expected to be the same as for the original server and the relay agent does not need to verify the lease option.
- Starting in Junos OS Release 18.4R1, this capability is extended to allow a DHCP relay agent to forward DHCP information request (DHCPINFORM) ACK messages from any server in the active server group.

To enable ACK forwarding from any server in the active server group:

- Enable forwarding for the active server group.

```
[edit forwarding-options dhcp-relay active-server-group]
user@host# set allow-server-change
```

Change History Table

Feature support is determined by the platform and release you are using. Use Feature Explorer to determine if a feature is supported on your platform.

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1
16.2R1	Starting in Junos OS Release 16.2R1

RELATED DOCUMENTATION

Group-Specific DHCP Configurations | 294

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 153

DHCPv6 Server | 104

DHCPv6 Relay Agent | 222

Suppressing DHCP Routes

IN THIS SECTION

- Suppressing DHCP Access, Access-Internal, and Destination Routes | 365
- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | 366

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. However, you can override the default behavior and prevent DHCP from automatically installing the route information. For more information, read this topic.

Suppressing DHCP Access, Access-Internal, and Destination Routes

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds the following routes:

- DHCPv4 sessions—access-internal and destination routes.
- DHCPv6 sessions—access-internal and access routes.

An access route represents a network behind an attached video services router, and is set to a preference of 13.

An access internal route is a /32 route that represents a directly attached end user, and is set to a preference of 12.

These routes are used by the DHCP application on a video services router to represent either the end users or the networks behind the attached video services router.

In some scenarios, you might want to override the default behavior and prevent DHCP from automatically installing the route information.

For example, DHCP relay installs destination (host) routes by default—this action is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of destination routes might cause a conflict when you configure DHCP relay with static subscriber interfaces.

To avoid such configuration conflicts you can override the default behavior and prevent DHCP relay from installing the routes.

Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default

You can use the route suppression option to override the default route installation behavior. You can configure route suppression and prevent DHCP from installing specific types of routes for:

- DHCP local server and DHCP relay agent
- DHCPv4 and DHCPv6 sessions
- Globally or for named interface groups

For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both.

Example:

- For DHCP local server route suppression (for example, a global configuration):

```
[edit system services dhcp-local-server]
user@host# set route-suppression access-internal
```

- For DHCP relay (for example, a group-specific configuration):

```
[edit forwarding-options dhcp-relay group southeast]
user@host# set route-suppression destination
```

- For DHCPv6 local server (for example, a group-specific configuration):

```
[edit system services dhcp-local-server group southern3]
user@host# set dhcpv6 route-suppression access access-internal
```

- For DHCPv6 relay (for example, a global configuration):

```
[edit forwarding-options dhcp-relay]
user@host# set dhcpv6 route-suppression access
```

Note the following while configuring route suppression option:

- You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.
- The `no-arp` statement supported in legacy DHCP is replaced by the `route-suppression` statement.

RELATED DOCUMENTATION

DHCP Server | 49

DHCP Client | 245

DHCP Relay Agent | 153

DHCP Overview | 2

8
CHAPTER

Configuration Statements and Operational Commands

Junos CLI Reference Overview | 369

Junos CLI Reference Overview

We've consolidated all Junos CLI commands and configuration statements in one place. Learn about the syntax and options that make up the statements and commands and understand the contexts in which you'll use these CLI elements in your network configurations and operations.

- Junos CLI Reference

Click the links to access Junos OS and Junos OS Evolved configuration statement and command summary topics.

- Configuration Statements
- Operational Commands