



Junos[®] OS

DHCP Local Server Feature Guide for Subscriber Management

Release

14.1



Published: 2014-04-25

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

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, 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 Local Server Feature Guide for Subscriber Management

14.1

Copyright © 2014, 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 <http://www.juniper.net/support/eula.html>. By downloading, installing or using such software, you agree to the terms and conditions of that EULA.

Table of Contents

	About the Documentation	xiii
	Documentation and Release Notes	xiii
	Supported Platforms	xiii
	Using the Examples in This Manual	xiii
	Merging a Full Example	xiv
	Merging a Snippet	xiv
	Documentation Conventions	xv
	Documentation Feedback	xvii
	Requesting Technical Support	xvii
	Self-Help Online Tools and Resources	xvii
	Opening a Case with JTAC	xviii
Part 1	Overview	
Chapter 1	DHCP Local Server	3
	Extended DHCP Local Server Overview	4
	Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools	6
	Providing DHCP Client Configuration Information	7
	Minimal Configuration for Clients	8
	DHCP Local Server and Address-Assignment Pools	8
	DHCP Liveness Detection	9
	DHCPv6 Local Server Overview	10
	DHCP Local Server Handling of Client Information Request Messages	11
	Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview	12
	Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface	13
	Primary Dynamic Profile	13
	Default Subscriber Service Overview	14
	DHCP Duplicate Client In Subnet Overview	15
	Group-Specific DHCP Local Server Options	16
	DHCP Access, Access-Internal, and Destination Route Suppression	16
	Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients	17
	Default Client/Server Interaction	17
	Dynamic Client/Server Interaction for DHCPv4	18
	Dynamic Client/Server Interaction for DHCPv6	18
	Dynamic Configuration Options	19
	DHCP Snooping Support	21
	DHCP Auto Logout Overview	22
	Auto Logout Overview	22
	How DHCP Identifies and Releases Clients	22

Option 60 and Option 82 Requirements	23
Subscriber Binding Retention During Interface Delete Events	24
Address-Assignment Pools Overview	25
Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address	25
Multiple Address Assignment for DHCPv6 Clients	26
Multiple Address Assignment Using Local Address Pools or RADIUS	26
Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment	26
DHCPv6 Options in a DHCPv6 Multiple Address Environment	27
Centrally Configured Opaque DHCP Options	28
Data Flow for RADIUS-Sourced DHCP Options	30
Multiple VSA 26-55 Instances Configuration	31
DHCP Options That Cannot Be Centrally Configured	31
DHCP Lease-Time Validation Overview	32
Graceful Routing Engine Switchover	33
Port Number Requirements for DHCP Firewall Filters	34

Part 2

Chapter 2

Configuration

Configuration Tasks for DHCP Local Server	39
Using External AAA Authentication Services with DHCP	40
Guidelines for Configuring Support for DHCP Duplicate Clients	41
Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information	42
Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces	43
Configuring a Default Subscriber Service	45
Grouping Interfaces with Common DHCP Configurations	45
Guidelines for Configuring Interface Ranges	46
Overriding Default DHCP Local Server Configuration Settings	48
Specifying the Maximum Number of DHCP Clients Per Interface	49
Allowing Only One DHCP Client Per Interface	50
Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default	52
Automatically Logging Out DHCP Clients	53
Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events	54
Configuring the Router to Strictly Enforce the Subscriber Scaling License	54
Enabling Processing of Client Information Requests	55
Specifying the Delegated Address Pool for IPv6 Prefix Assignment	56
Enabling DHCPv6 Rapid Commit Support	57
Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment	57
Deleting DHCP Local Server and DHCP Relay Override Settings	58
Configuring Extended DHCP Local Server Dynamic Client Reconfiguration	58
Configuring Dynamic Reconfiguration Attempts for DHCP Clients	60
Configuring Deletion of the Client When Dynamic Reconfiguration Fails	61
Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect	61

	Configuring a Token for DHCP Local Server Authentication	62
	Preventing Binding of Clients That Do Not Support Reconfigure Messages	62
	Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings	63
	DHCP Liveness Detection Overview	64
	Configuring Detection of DHCP Local Server Client Connectivity	65
	Configuring a DHCP Lease-Time Threshold	67
	Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces	68
	Attaching a Dynamic Profile to All DHCP Subscriber or All DHCP Client Interfaces	68
	Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces or a Group of DHCP Client Interfaces	69
	Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server	70
	Configuring Passwords for Usernames	71
	Creating Unique Usernames for DHCP Clients	72
	Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use	74
	Specifying the Subnet for DHCP Client Address Assignment	75
Chapter 3	DHCP Local Server Examples	77
	Example: Minimum Extended DHCP Local Server Configuration	77
	Example: Extended DHCP Local Server Configuration with Optional Pool Matching	78
	Example: Extended DHCPv6 Local Server Configuration	78
	Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine	79
	Example: Configuring Group Liveness Detection for DHCP Local Server Clients	83
Chapter 4	Configuration Statements	89
	[edit system services dhcp-local-server] Hierarchy Level	91
	[edit system services subscriber-management] Hierarchy Level	94
	aggregate-clients (DHCP Local Server)	96
	attempts (DHCP Local Server)	97
	authentication (DHCP Local Server)	98
	bfd	99
	circuit-type (DHCP Local Server)	100
	clear-on-abort (DHCP Local Server)	101
	client-discover-match (DHCP Local Server)	102
	client-id (DHCP Local Server)	103
	delegated-pool (DHCP Local Server)	104
	delimiter (DHCP Local Server)	105
	detection-time	106
	dhcp-local-server	107
	dhcpv6 (DHCP Local Server)	112
	domain-name (DHCP Local Server)	115
	duplicate-clients-in-subnet (DHCP Local Server and DHCP Relay Agent)	116
	dynamic-profile (DHCP Local Server)	117
	enforce-strict-scale-limit-license (Subscriber Management)	118
	external-authority	118

failure-action	119
forward-snooped-clients (DHCP Local Server)	120
group (DHCP Local Server)	121
holddown-interval	123
interface (DHCP Local Server)	124
interface-client-limit (DHCP Local Server)	126
interface-delete (Subscriber Management or DHCP Client Management)	127
interface-name (DHCP Local Server)	128
ip-address-first	129
lease-time-threshold (DHCP Local Server and DHCP Relay Agent)	130
lease-time-validation (DHCP Local Server and DHCP Relay Agent)	131
liveness-detection	132
logical-system-name (DHCP Local Server)	133
ltv-syslog-interval (System Process)	133
mac-address (DHCP Local Server)	134
maintain-subscriber (Subscriber Management)	135
method	136
minimum-interval	137
minimum-receive-interval	138
multi-address-embedded-option-response (DHCP Local Server)	139
multiplier	140
no-adaptation	141
option-60 (DHCP Local Server)	142
option-82 (DHCP Local Server Authentication)	143
option-82 (DHCP Local Server Pool Matching)	144
overrides (DHCP Local Server)	145
password (DHCP Local Server)	147
pool (DHCP Local Server Overrides)	148
pool-match-order	149
process-inform	150
radius-disconnect (DHCP Local Server)	152
rapid-commit (DHCPv6 Local Server)	153
reconfigure (DHCP Local Server)	154
relay-agent-interface-id (DHCP Local Server)	155
relay-agent-remote-id (DHCP Local Server)	156
relay-agent-subscriber-id (DHCP Local Server)	157
requested-ip-network-match (DHCP Local Server)	158
route-suppression (DHCP Local Server and Relay Agent)	159
routing-instance-name (DHCP Local Server)	160
service-profile (DHCP Local Server)	161
session-mode	162
strict (DHCP Local Server)	163
subscriber-management (Subscriber Management)	164
threshold (detection-time)	165
threshold (transmit-interval)	166
timeout (DHCP Local Server)	167
token (DHCP Local Server)	168
transmit-interval	169
trigger (DHCP Local Server)	170

	use-primary (DHCP Local Server)	171
	user-prefix (DHCP Local Server)	172
	username-include (DHCP Local Server)	173
	version (BFD)	174
	violation-action (DHCP Local Server and DHCP Relay Agent)	175
Part 3	Administration	
Chapter 5	Verifying and Managing Configurations	179
	Clearing DHCP Bindings for Subscriber Access	179
	Monitoring DHCP Options Configured on RADIUS Servers	181
	Verifying and Managing DHCP Local Server Configuration	183
	Verifying and Managing DHCPv6 Local Server Configuration	183
	Verifying and Managing the DHCP Maintain Subscribers Feature	184
Chapter 6	Monitoring Commands	185
	clear dhcp server binding	186
	clear dhcp server statistics	189
	clear dhcpv6 server binding	191
	clear dhcpv6 server statistics	193
	request dhcp server reconfigure	194
	request dhcpv6 server reconfigure	196
	request system reboot	198
	show dhcp server binding	203
	show dhcp server statistics	208
	show dhcpv6 server binding	211
	show dhcpv6 server statistics	217
	show subscribers	220
	show subscribers summary	238
Part 4	Troubleshooting	
Chapter 7	Acquiring Troubleshooting Information	245
	Tracing Extended DHCP Operations	245
	Configuring the Extended DHCP Log Filename	247
	Configuring the Number and Size of Extended DHCP Log Files	247
	Configuring Access to the Extended DHCP Log File	248
	Configuring a Regular Expression for Extended DHCP Messages to Be Logged	248
	Configuring the Extended DHCP Tracing Flags	249
	Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged	249
	Tracing Extended DHCP Operations for Specific Interfaces	250
	Tracing Extended DHCP Operations for Specific Interfaces	251
	Collecting Subscriber Access Logs Before Contacting Juniper Technical Support	252
Chapter 8	Troubleshooting Configuration Statements	255
	interface-traceoptions (DHCP)	256
	trace (DHCP Local Server)	258

	traceoptions (DHCP)	259
Part 5	Index	
	Index	263

List of Figures

Part 1	Overview	
Chapter 1	DHCP Local Server	3
	Figure 1: DHCP Options Data Flow	30

List of Tables

	About the Documentation	xiii
	Table 1: Notice Icons	xv
	Table 2: Text and Syntax Conventions	xv
Part 1	Overview	
Chapter 1	DHCP Local Server	3
	Table 3: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server	5
	Table 4: Information in Authentication Grant	7
	Table 5: RADIUS Attributes and VSAs for DHCPv6 Local Server	10
	Table 6: Action Taken for Events That Occur During a Reconfiguration	20
	Table 7: Unsupported Opaque DHCP Options	32
	Table 8: Lease-Time Violation Event Logging	33
Part 2	Configuration	
Chapter 2	Configuration Tasks for DHCP Local Server	39
	Table 9: Actions for DHCP Local Server Snooped Packets	70
Part 3	Administration	
Chapter 5	Verifying and Managing Configurations	179
	Table 10: DHCP Options Description	182
Chapter 6	Monitoring Commands	185
	Table 11: show dhcp server binding Output Fields	204
	Table 12: show dhcp server statistics Output Fields	209
	Table 13: show dhcpv6 server binding Output Fields	212
	Table 14: show dhcpv6 server statistics Output Fields	218
	Table 15: show subscribers Output Fields	223
	Table 16: show subscribers Output Fields	239

About the Documentation

- Documentation and Release Notes on page xiii
- Supported Platforms on page xiii
- Using the Examples in This Manual on page xiii
- Documentation Conventions on page xv
- Documentation Feedback on page xvii
- Requesting Technical Support on page xvii

Documentation and Release Notes

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

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

Juniper Networks Books publishes books by Juniper Networks engineers and subject matter experts. These books go beyond the technical documentation to explore the nuances of network architecture, deployment, and administration. The current list can be viewed at <http://www.juniper.net/books>.

Supported Platforms

For the features described in this document, the following platforms are supported:

- MX Series

Using the Examples in This Manual

If you want to use the examples in this manual, you can use the **load merge** or the **load merge relative** command. These commands cause the software to merge the incoming configuration into the current candidate configuration. The example does not become active until you commit the candidate configuration.

If the example configuration contains the top level of the hierarchy (or multiple hierarchies), the example is a *full example*. In this case, use the **load merge** command.

If the example configuration does not start at the top level of the hierarchy, the example is a *snippet*. In this case, use the **load merge relative** command. These procedures are described in the following sections.

Merging a Full Example

To merge a full example, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration example into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following configuration to a file and name the file **ex-script.conf**. Copy the **ex-script.conf** file to the **/var/tmp** directory on your routing platform.

```
system {
  scripts {
    commit {
      file ex-script.xml;
    }
  }
}
interfaces {
  fxp0 {
    disable;
    unit 0 {
      family inet {
        address 10.0.0.1/24;
      }
    }
  }
}
```

2. Merge the contents of the file into your routing platform configuration by issuing the **load merge** configuration mode command:

```
[edit]
user@host# load merge /var/tmp/ex-script.conf
load complete
```

Merging a Snippet

To merge a snippet, follow these steps:

1. From the HTML or PDF version of the manual, copy a configuration snippet into a text file, save the file with a name, and copy the file to a directory on your routing platform.

For example, copy the following snippet to a file and name the file **ex-script-snippet.conf**. Copy the **ex-script-snippet.conf** file to the **/var/tmp** directory on your routing platform.

```
commit {
  file ex-script-snippet.xml; }
```

2. Move to the hierarchy level that is relevant for this snippet by issuing the following configuration mode command:

```
[edit]
user@host# edit system scripts
[edit system scripts]
```

3. Merge the contents of the file into your routing platform configuration by issuing the **load merge relative** configuration mode command:

```
[edit system scripts]
user@host# load merge relative /var/tmp/ex-script-snippet.conf
load complete
```

For more information about the **load** command, see the *CLI User Guide*.

Documentation Conventions

Table 1 on page xv defines notice icons used in this guide.

Table 1: Notice Icons

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

Table 2 on page xv defines the text and syntax conventions used in this guide.

Table 2: Text and Syntax Conventions

Convention	Description	Examples
Bold text like this	Represents text that you type.	To enter configuration mode, type the configure command: user@host> configure

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

Convention	Description	Examples
Fixed-width text like this	Represents output that appears on the terminal screen.	user@host> show chassis alarms No alarms currently active
<i>Italic text like this</i>	<ul style="list-style-type: none">Introduces or emphasizes important new terms.Identifies guide names.Identifies RFC and Internet draft titles.	<ul style="list-style-type: none">A policy <i>term</i> is a named structure that defines match conditions and actions.<i>Junos OS CLI User Guide</i>RFC 1997, <i>BGP Communities Attribute</i>
<i>Italic text like this</i>	Represents variables (options for which you substitute a value) in commands or configuration statements.	Configure the machine's domain name: [edit] root@# set system domain-name <i>domain-name</i>
Text like this	Represents names of configuration statements, commands, files, and directories; configuration hierarchy levels; or labels on routing platform components.	<ul style="list-style-type: none">To configure a stub area, include the stub statement at the [edit protocols ospf area area-id] hierarchy level.The console port is labeled CONSOLE.
< > (angle brackets)	Encloses optional keywords or variables.	stub <default-metric <i>metric</i>>;
(pipe symbol)	Indicates a choice between the mutually exclusive keywords or variables on either side of the symbol. The set of choices is often enclosed in parentheses for clarity.	broadcast multicast (<i>string1</i> <i>string2</i> <i>string3</i>)
# (pound sign)	Indicates a comment specified on the same line as the configuration statement to which it applies.	rsvp { # Required for dynamic MPLS only
[] (square brackets)	Encloses a variable for which you can substitute one or more values.	community name members [<i>community-ids</i>]
Indentation and braces ({ })	Identifies a level in the configuration hierarchy.	[edit] routing-options { static { route default { nexthop <i>address</i> ; retain; } } }
;(semicolon)	Identifies a leaf statement at a configuration hierarchy level.	
GUI Conventions		
Bold text like this	Represents graphical user interface (GUI) items you click or select.	<ul style="list-style-type: none">In the Logical Interfaces box, select All Interfaces.To cancel the configuration, click Cancel.

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

Convention	Description	Examples
> (bold right angle bracket)	Separates levels in a hierarchy of menu selections.	In the configuration editor hierarchy, select Protocols>Ospf .

Documentation Feedback

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

- Document or topic name
- URL or page number
- Software release version (if applicable)

Requesting Technical Support

Technical product support is available through the Juniper Networks Technical Assistance Center (JTAC). If you are a customer with an active J-Care or JNASC support contract, or are covered under warranty, and need post-sales technical support, you can access our tools and resources online or open a case with JTAC.

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

Self-Help Online Tools and Resources

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

- Find CSC offerings: <http://www.juniper.net/customers/support/>
- Search for known bugs: <http://www2.juniper.net/kb/>
- Find product documentation: <http://www.juniper.net/techpubs/>
- Find solutions and answer questions using our Knowledge Base: <http://kb.juniper.net/>
- Download the latest versions of software and review release notes: <http://www.juniper.net/customers/csc/software/>

- Search technical bulletins for relevant hardware and software notifications:
<http://kb.juniper.net/InfoCenter/>
- Join and participate in the Juniper Networks Community Forum:
<http://www.juniper.net/company/communities/>
- Open a case online in the CSC Case Management tool: <http://www.juniper.net/cm/>

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

Opening a Case with JTAC

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

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

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

PART 1

Overview

- [DHCP Local Server on page 3](#)

CHAPTER 1

DHCP Local Server

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [DHCP Local Server Handling of Client Information Request Messages on page 11](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 12](#)
- [Default Subscriber Service Overview on page 14](#)
- [DHCP Duplicate Client In Subnet Overview on page 15](#)
- [Group-Specific DHCP Local Server Options on page 16](#)
- [DHCP Access, Access-Internal, and Destination Route Suppression on page 16](#)
- [Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 17](#)
- [DHCP Snooping Support on page 21](#)
- [DHCP Auto Logout Overview on page 22](#)
- [Subscriber Binding Retention During Interface Delete Events on page 24](#)
- [Address-Assignment Pools Overview on page 25](#)
- [Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 25](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 26](#)
- [DHCPv6 Options in a DHCPv6 Multiple Address Environment on page 27](#)
- [Centrally Configured Opaque DHCP Options on page 28](#)
- [DHCP Lease-Time Validation Overview on page 32](#)
- [Graceful Routing Engine Switchover on page 33](#)
- [Port Number Requirements for DHCP Firewall Filters on page 34](#)

Extended DHCP Local Server Overview

Junos OS includes an extended DHCP local server that enhances traditional DHCP server operation by providing additional address assignment and client configuration functionality and flexibility in a subscriber-aware environment. The 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. The address-assignment pools are considered external because they are external to the DHCP local server. The pools are managed independently of the DHCP local server, and can be shared by different client applications, such as DHCP or PPPoE access. [Table 3 on page 5](#) provides a comparison of the extended DHCP local server and a traditional DHCP local server.

The extended DHCP local server provides an IP address and other configuration information in response to a client request. The 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 DHCP client authentication. You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.

Table 3: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server

Feature	Extended DHCP Local Server	Traditional 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

You can also configure the extended DHCP local server to support 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.



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 overview covers:

- [Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools on page 6](#)
- [Providing DHCP Client Configuration Information on page 7](#)
- [Minimal Configuration for Clients on page 8](#)
- [DHCP Local Server and Address-Assignment Pools on page 8](#)
- [DHCP Liveness Detection on page 9](#)

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.

Providing DHCP Client Configuration Information

When the extended 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 extended DHCP application uses the information from the authentication grant for the response the DHCP application sends 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 grant includes an address pool name and a local configuration specifies DHCP attributes for that pool (such as, DNS server address), the extended DHCP application 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 might need to configure the local address-assignment pool to provide the configuration information, such as DNS server, 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 4 on page 7](#) 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 4: Information in Authentication Grant

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address
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

Table 4: Information in Authentication Grant (*continued*)

Attribute Number	Attribute Name	Description
RADIUS attribute 88	Framed-Pool	Address assignment pool name
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Minimal Configuration for Clients

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.

DHCP Local Server and Address-Assignment Pools

In the traditional DHCP server operation, 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 external address-assignment pools (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.

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.



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.

DHCP Liveness Detection

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 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. You can configure

Related Documentation

- [Address-Assignment Pools Overview on page 25](#)
- [Configuring Address-Assignment Pools](#)
- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 12](#)
- [Using External AAA Authentication Services with DHCP on page 40](#)
- [Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 25](#)
- [Graceful Routing Engine Switchover on page 33](#)
- [Subscriber Management Unified ISSU Support](#)
- [Tracing Extended DHCP Operations on page 245](#)
- [Verifying and Managing DHCP Local Server Configuration on page 183](#)
- [Example: Minimum Extended DHCP Local Server Configuration on page 77](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 78](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 79](#)

DHCPv6 Local Server Overview

The DHCPv6 local server enhances the extended DHCP local server by providing support for IPv6. 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.

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



NOTE: 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.

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in [Table 5 on page 10](#) to configure the client:

Table 5: 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

The DHCPv6 local server is compatible with the extended DHCP local server and the extended 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 extended 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

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. See the “[edit system services dhcp-local-server] Hierarchy Level” on page 91 for the complete DHCP local server syntax, including the DHCPv6 syntax.

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]**

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)
- [Using External AAA Authentication Services with DHCP on page 40](#)
- [Grouping Interfaces with Common DHCP Configurations on page 45](#)
- [Group-Specific DHCP Local Server Options on page 16](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Configuring Passwords for Usernames on page 71](#)
- [Creating Unique Usernames for DHCP Clients on page 72](#)
- [Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address on page 25](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 183](#)
- [Example: Extended DHCPv6 Local Server Configuration on page 78](#)

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 information request that indicates what information is desired. 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. Include the **process-inform** statement at the **[edit system services dhcp-local-server overrides]** or **[edit system services dhcp-local-server dhcpv6 overrides]** hierarchy level.

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 has typically been 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 specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.

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.



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.

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Enabling Processing of Client Information Requests on page 55](#)

Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview

The router's DHCP support enables you to attach a dynamic profile to a DHCP subscriber interface. When a DHCP subscriber logs in, the router instantiates the specified dynamic profile and then applies the services defined in the profile to the interface.

You can attach dynamic profiles to all interfaces or you can specify a particular group of interfaces to which the profile is attached. Both the DHCP local server and the DHCP relay agent support the attachment of dynamic profiles to interfaces.

You can enable the following optional features when the dynamic profile is attached. The two options cannot be used together.

- Enable multiple DHCP subscribers to share the same VLAN logical interface. The firewall filters, CoS schedulers, and IGMP configuration of the clients are merged.
- Specify the primary dynamic profile that is instantiated when the first subscriber logs in.

Multiple DHCP Subscribers Sharing the Same VLAN Logical Interface

The **aggregate-clients** statement specifies that the router merge the firewall filters, CoS schedulers, and IGMP configuration of multiple DHCP clients that are on the same VLAN logical interface (for example, multiple clients belonging to the same household). You can configure the aggregate-clients support for all interfaces or for a group of interfaces. The **aggregate-clients** statement provides the option of either merging (chaining) or replacing software components for each client.

By default, the feature is disabled and a single DHCP client is allowed per VLAN when a dynamic profile is associated with the VLAN logical interface.

When you specify the **merge** option, the router aggregates the software components for multiple subscribers as follows:

- Firewall filters—The filters are chained together using the precedence as the order of execution. If the same firewall filter is attached multiple times, the filter is executed only once.
- CoS schedulers—The different CoS schedulers are merged as if the scheduler map has multiple schedulers. The merge operation for the individual traffic-control-profiles parameters (shaping-rate, delay-buffer-rate, guaranteed-rate) preserves the maximum value for each parameter.
- IGMP configuration—The current IGMP configuration is replaced with the configuration of the newest DHCP client.

When you specify the **replace** option, the entire logical interface is replaced whenever a new client logs in to the network using the same VLAN logical interface. For example, if a customer subscribes to voice, video, and data services on the network, when a voice client logs in, instead of applying a specific voice filter for only that service, the entire voice, video, and data filter chain is applied.



NOTE: You cannot use a dynamic demux interface to represent multiple subscribers in a dynamic profile attached to an interface. One dynamic demux interface represents one subscriber. Do not configure the **aggregate-clients** option when attaching a dynamic profile to a demux interface for DHCP.

Primary Dynamic Profile

The **use-primary** option enables you to specify the primary dynamic profile that is instantiated when the first subscriber logs in. Subsequent subscribers are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber logs out, the next subscriber that logs in is assigned the primary dynamic profile.

This feature can conserve logical interfaces in a network where dynamic IP demux interfaces are used to represent subscribers. To conserve interfaces, make sure the primary profile that you specify does not create a demux interface, but provides the initial policies for the primary interface subscriber.

- Related Documentation**
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68](#)

Default Subscriber Service Overview

Subscriber management enables you to specify a default subscriber service for DHCP subscribers. The default service (dynamic profile) is applied to subscribers when the subscriber logs in. By configuring a default service, you can apply a particular service (for example, a basic service) to subscribers who are not explicitly assigned a service.

When a subscriber logs in, the configured default service is always activated, even when remote service provisioning or RADIUS service activation is configured for the subscriber. The default service is deactivated only when the subscriber is successfully provisioned by the PCRF by means of the GX-Plus application. (Remote provisioning is configured by the **provisioning-order** statement at the **[edit access profile]** hierarchy level.)

In all other cases, the default service remains active. For example, if RADIUS authentication is configured but service activation is not, the default subscriber service remains activated. Likewise, if RADIUS authentication is not configured, the default subscriber service remains activated.

Default services can also be deactivated either with a RADIUS CoA deactivate request or with the **request network-access aaa subscriber delete session-id** command.

To create and assign a default subscriber service, you must complete the following operations:

- Create the service—Ensure that the service you want to use has been configured in a dynamic profile. The actual service is no different than any other service used for subscriber management.
- Specify the default service—Use the Junos OS CLI to specify the service that is used as the default service.
- Specify the interfaces on which the default service is assigned —Use the Junos OS CLI to specify that the default service is used globally, for a group of interfaces, or for a specific interface.

- Related Documentation**
- [Configuring a Default Subscriber Service on page 45](#)
 - *CLI-Activated Subscriber Services*
 - *Activating and Deactivating Subscriber Services Locally with the CLI*
 - *Understanding Gx-Plus Interactions Between the Router and the PCRF*

DHCP Duplicate Client In Subnet Overview

In some network environments, client IDs and hardware addresses (MAC addresses) might not be unique, resulting in duplicate clients. A duplicate DHCP client occurs when a client attempts to get a lease, and that client has the same client ID or the same hardware address as an existing DHCP client—the existing client and the new client cannot exist simultaneously, unless you have configured the optional duplicate client support.



NOTE: This document describes an enhanced method for providing support for duplicate clients. The enhanced method is mutually exclusive with the previously existing method, which used the `duplicate-clients-on-interface` statement at the `[edit forwarding-options dhcp-relay]` and `[edit system services dhcp-local-server]` hierarchy levels. If you attempt to configure both methods, the commit operation fails.

By default, DHCP local server and DHCP relay agent use the subnet information to differentiate between duplicate clients. However, in some cases, this level of differentiation is not adequate. For example, when multiple subinterfaces share the same underlying loopback interface with the same preferred source address, the interfaces appear to be on the same subnet.

You can enable support for duplicate clients in a subnet by configuring DHCP to use additional information to uniquely identify clients—the additional information is either the client incoming interface or the option 82 information in the DHCP packets. Using the option 82 information provides the following important benefits:

- You can configure DHCP relay to preserve and use the remotely created option 82.
- DHCP local server can support an environment in which an aggregation device is present between the client and the DHCP server.

When configured to support duplicate clients in the subnet, DHCP uses the following information to distinguish between the duplicate clients:

- The subnet on which the client resides
- The client ID or hardware address
- The duplicate clients option you configure—either the client incoming interface or the option 82 information in the client's incoming DHCP packets

Related Documentation

- [Guidelines for Configuring Support for DHCP Duplicate Clients on page 41](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces on page 43](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information on page 42](#)

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, and at the **[edit system services dhcp-local-server]** hierarchy level to set global 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.
- **overrides**—Override the default configuration settings for the extended DHCP local server. For information, see “[Overriding Default DHCP Local Server Configuration Settings](#)” on page 48.

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 45](#)

DHCP Access, Access-Internal, and Destination Route Suppression

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds access-internal and destination routes for DHCPv4 sessions, and access-internal and access routes for DHCPv6 sessions. 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.



NOTE: 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.

You can configure both DHCP local server and DHCP relay agent to override the default route installation behavior, and you can specify the override for both DHCPv4 and DHCPv6 sessions. You can override the route installation 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.



NOTE: In Junos OS releases prior to Release 13.2, the `no-arp` statement was used to override the default installation of host routes. In Junos OS Release 13.2 and later, the `no-arp` statement is deprecated and the function is replaced by the `route-suppression` statement.

Related Documentation

- [Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 52](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Extended DHCP Relay Agent Overview](#)
- [DHCPv6 Relay Agent Overview](#)

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

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.

Dynamic Configuration Options

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.

- To enable dynamic reconfiguration with default reconfiguration values for all DHCP clients, include the **reconfigure** statement at the **[edit system services dhcp-local-server]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level for DHCPv6 clients.
- Alternatively, to enable dynamic reconfiguration for only the DHCP clients serviced by a specified group of interfaces, include the **reconfigure** statement at the **[edit system services dhcp-local-server group group-name]** hierarchy level for DHCPv4 clients, and at the **[edit system services dhcp-local-server dhcpv6 group group-name]** hierarchy level for DHCPv6 clients.

You can optionally modify the behavior of the reconfiguration process by including the appropriate 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.

Include the **attempts** statement to specify how many times the local server sends the **forcerenew** or **reconfigure** message to initiate client reconfiguration. Include the **timeout** statement to set the interval between the first and second attempts. The interval between each subsequent attempt doubles the previous value. 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.

By default, the DHCP client's original configuration is restored if all of the reconfiguration attempts fail. Include the **clear-on-abort** statement to delete the client instead.

You can configure an authentication token by including the **token** statement. The DHCP local server then includes this token inside the authentication option when it sends

forcerenew or reconfigure messages. If the service provider has previously configured the DHCP client with this token, then the client can compare that token against the newly received token, and reject the message if the tokens do not match. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

In the event of a RADIUS-initiated disconnect (RID), the client is deleted by default. You can configure the client to be reconfigured instead of deleted by including the **radius-disconnect** statement. The client is deleted if all attempts to reconfigure the client fail.

For the DHCPv6 server only, you can include the **strict** statement. By default, the server accepts solicit messages from clients that do not support server-initiated reconfiguration. Including this statement causes the server to discard solicit messages from nonsupporting clients; consequently the server does not bind these clients.

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.

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. [Table 6 on page 20](#) lists the actions taken in response to several different events.

Table 6: 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.

- Related Documentation**
- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)

DHCP Snooping Support

DHCP snooping provides DHCP security on the router or switch by filtering incoming messages. When DHCP snooping is enabled, the router differentiates between trusted and untrusted interfaces, and forwards messages from trusted sources while rejecting the untrusted messages.

In Junos OS, DHCP snooping is enabled in a routing instance when you configure either the **dhcp-relay** statement at the **[edit forwarding-options]** hierarchy level, or the **dhcp-local-server** statement at the **[edit system services]** hierarchy level in that routing instance. However, depending on the Junos OS release, the router processes the snooped packets differently, as described in the following list:

- In Junos OS Release 10.0 and earlier, the router processes snooped packets normally.
- In Junos OS Release 10.1 and later, the router discards snooped packets by default. To enable normal processing of snooped packets in Junos OS Release 10.1 and later, 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 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.

- 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.

**Related
Documentation**

- [Configuring DHCP Snooping for DHCP Relay Agent](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 70](#)
- [Example: Configuring DHCP Snooping Support for DHCP Relay Agent](#)

DHCP Auto Logout Overview

This topic provides an introduction to the optional DHCP auto logout feature and includes the following sections:

- [Auto Logout Overview on page 22](#)
- [How DHCP Identifies and Releases Clients on page 22](#)
- [Option 60 and Option 82 Requirements on page 23](#)

Auto Logout Overview

Auto logout is an optional configuration for DHCP local server and DHCP relay agent that improves the efficiency of DHCP IP address assignment. Auto logout enables IP addresses to be immediately released and returned to the address pool when the addresses are no longer used by DHCP clients. 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 different 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, 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*.

- Related Documentation**
- [Automatically Logging Out DHCP Clients on page 53](#)
 - [DHCP Relay Agent Option 82 Value for Auto Logout](#)
 - [Allowing Only One DHCP Client Per Interface on page 50](#)
 - [Clearing DHCP Bindings for Subscriber Access on page 179](#)

Subscriber Binding Retention During Interface Delete Events

You can configure the router to maintain DHCP subscribers when an event occurs that normally results in the router deleting the subscriber. For example, by default, the router logs out DHCP subscribers when an interface delete event occurs, such as a DPC reboot or failure. However, if you configure the router to maintain subscribers, the router identifies each subscriber that was on the deleted interface, and resumes normal packet processing for the subscriber when the interface is restored.



NOTE: Subscribers are logged off as usual when their lease expires, even if the router is configured to maintain subscribers and the subscriber is on a deleted interface that has not yet been restored.

You configure the router to maintain subscribers on a global basis— the configuration applies to DHCP local server, DHCPv6 local server, and DHCP relay clients in all logical routers and routing instances. When you enable the maintain subscribers feature, the router applies the feature to existing subscribers as well as subscribers who later connect.

If the maintain subscribers feature is enabled on the router, you can explicitly delete a subscriber binding and log out the subscriber by either specifying a lease expiration timeout or using one of the following commands, as appropriate:

- [clear dhcp server binding](#)
- [clear dhcpv6 server binding](#)
- [clear dhcp relay binding](#)

- Related Documentation**
- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54](#)
 - [Verifying and Managing the DHCP Maintain Subscribers Feature on page 184](#)

Address-Assignment Pools Overview

The address-assignment pool feature supports subscriber management and DHCP management functionality by enabling you to create centralized IPv4 and IPv6 address pools independently 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.

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.

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.

You can link address-assignment pools together to provide backup pools for address assignment. When the primary pool is fully allocated, the router or switch automatically switches to the linked, or secondary, pool and begins allocating addresses from that pool.

You can also explicitly identify that an address-assignment pool is used for ND/RA.

Related Documentation

- *Configuring Address-Assignment Pools*
- *DNS Address Assignment Precedence*
- *Address-Assignment Pools Licensing Requirements*
- *Example: Configuring an Address-Assignment Pool*
- *Configuring an Extended DHCP Server with DHCPv6 on EX Series Switches (CLI Procedure)*

Use of DHCP Option 50 and DHCPv6 IA_NA Option to Request a Specific IP Address

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.

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)

Multiple Address Assignment for DHCPv6 Clients

Subscriber management (on the routers) or DHCP management (on the switches) enables you to 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 subscriber (or 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 in a networking environment in which a customer premises equipment (CPE) device requires a host address and a delegated prefix. In such an environment, you can configure subscriber management to assign both a DHCPv6 IA_NA (Identity Association for Non-Temporary Addresses) and an IA_PD (Identity Association for Prefix Delegation) address to the client (the CPE device).

- [Multiple Address Assignment Using Local Address Pools or RADIUS on page 26](#)
- [Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment on page 26](#)

Multiple Address Assignment Using Local Address Pools or RADIUS

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 router or switch creates a subscriber (or DHCP client) entry and binds the entry to the assigned address. If both addresses are successfully allocated, the router (or switch) creates a single subscriber (or 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 subscriber management (or DHCP management) uses to assign IPv6 prefixes for subscribers (or DHCP clients).

Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment



NOTE: EX Series switches do not support demux.

(On the routers only) Subscriber management provides a predefined variable that you can use to dynamically configure DHCPv6 multiple address assignment. You apply the Junos OS predefined variable, `$junos-subscriber-ipv6-multi-address`, as a demux source address in a dynamic profile. When the dynamic profile is attached to a subscriber, the variable is expanded to include both the host and prefix addresses. You use this variable instead of the `$junos-subscriber-ipv6-address` variable, which supports a single IPv6 address.

You include the `$junos-subscriber-ipv6-multi-address` variable at the `[edit dynamic-profile profile-name interfaces interface-name unit logical-unit-number family inet6 demux-source]` hierarchy level.

**Related
Documentation**

- [Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 56](#)
- [Junos OS Predefined Variables](#)

DHCPv6 Options in a DHCPv6 Multiple Address Environment

In a DHCPv6 environment, DHCPv6 clients can use a single DHCPv6 Solicit message to request multiple addresses (for example, IA_NA address, IA_PD address, or both), as well as the DNS server address (DHCPv6 attribute 23). When a client requests multiple addresses, DHCPv6 uses the following guidelines to determine how options are returned to the client.

- **DNS server address**—Whenever a client requests an IA_PD address (either alone or with an IA_NA address) and also requests a DNS server address, DHCPv6 returns a DNS address only when one is specified in the IA_PD pool. If the IA_PD pool does not include a DNS address, DHCPv6 ignores any DNS address configured in the IA_NA pool.
If the client requests an IA_NA address (but not an IA_PD address) and also a DNS server address, DHCPv6 returns a DNS address if one is configured in the IA_NA pool.
- **Lease time**—DHCPv6 returns the shortest value of the lease times configured in the IA_NA pool, the IA_PD pool, and `authd`. DHCPv6 uses this value to set the lifetimes and the Renew and Rebind timers.



NOTE: By default, DHCPv6 local server returns the DNS server address as a global DHCPv6 option. However, in releases prior to 12.3R3, and in releases 13.1 and 13.2, the default behavior was for DHCPv6 to return the DNS server address as a suboption inside the DHCPv6 IA_NA and IA_PD headers rather than as a global option. You can override the current default behavior if you want DHCPv6 to return the DNS server address at the suboption level.

**Related
Documentation**

- [Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 57](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 26](#)

Centrally Configured Opaque DHCP 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.

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).



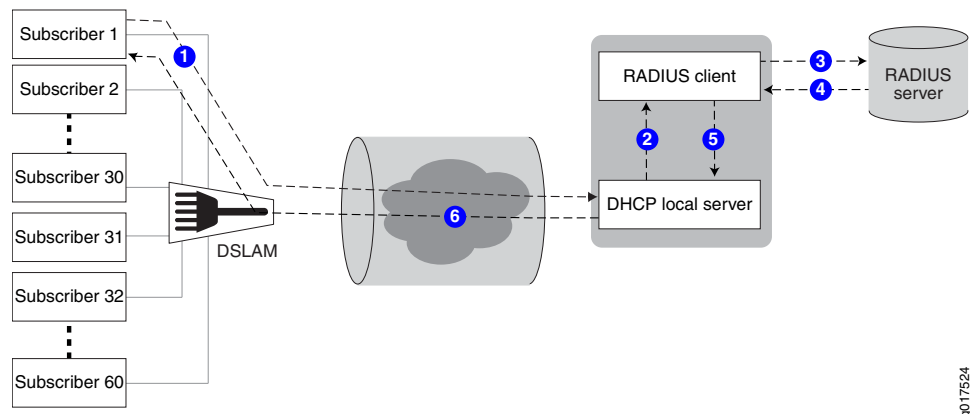
NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

- [Data Flow for RADIUS-Sourced DHCP Options on page 30](#)
- [Multiple VSA 26-55 Instances Configuration on page 31](#)
- [DHCP Options That Cannot Be Centrally Configured on page 31](#)

Data Flow for RADIUS-Sourced DHCP Options

Figure 1 on page 30 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 1: 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 be 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 7 on page 32 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 7: 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 • [Monitoring DHCP Options Configured on RADIUS Servers on page 181](#)

DHCP Lease-Time Validation Overview

In a subscriber access environment, a DHCP server obtains an address lease from either local configuration or from an external DHCP server, and assigns the lease to the DHCP client address.

Obtaining leases from external sources can present issues when the external source is owned or managed by a third party—the third party might configure the external source to provide address leases that are unsuitable for the subscriber access environment. For example, extremely short lease times can create unnecessary traffic that results in reduced performance in the network.

To avoid potential issues caused by short DHCP lease times, subscriber management provides a lease-time validation feature. Lease-time validation enables you to explicitly configure a threshold for the minimum lease time allowed in your subscriber access environment, and to specify a violation action (such as dropping the lease offer) the router takes when a short lease time is offered by a third party. You can specify the following violation actions:

- **drop**—(DHCPv4 and DHCPv6 relay agent) The third-party lease offer is dropped and the client binding fails.
- **override-lease**—(DHCPv4 and DHCPv6 local server) The third-party lease time is overridden by the specified threshold value.

- **strict**—(DHCPv4 and DHCPv6 local server) The third-party lease is ignored and the client binding fails.
- **no action**—If you do not specify a violation action, DHCP binds the client using the third-party lease but marks the binding as lease-time violating.

A lease-time violation can occur during the initial lease grant or during a rebinding or renewal operation. To reduce excessive and redundant log messages, the router consolidates lease-time violation reporting, as shown in [Table 8 on page 33](#).

Table 8: Lease-Time Violation Event Logging

Event	syslog	Extended DHCP Traceoptions
Initial lease-time violation for the specific DHCP server	warning	warning
Number of lease-time violations return to zero for the specific DHCP server	warning	warning
Status of lease-time violations caused by specific DHCP server, reported in the interval configured in ltv-syslog-interval command	warning	—
Violation action of drop occurred, or the DHCP packet was not generated	—	warning
Violation action of override-lease occurred (DHCP local server only)	—	warning
Lease-time violation	—	warning

Related Documentation

- [Configuring a DHCP Lease-Time Threshold on page 67](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Extended DHCP Relay Agent Overview](#)
- [DHCPv6 Relay Agent Overview](#)

Graceful Routing Engine Switchover

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 in the Junos OS*.

- Related Documentation**
- [Extended DHCP Local Server Overview on page 4](#)
 - *Extended DHCP Relay Agent Overview*
 - *Subscriber Management Unified ISSU Support*

Port Number Requirements for DHCP Firewall Filters

When you configure a firewall filter to perform some action on DHCP packets at the Routing Engine, such as protecting the Routing Engine by allowing only proper DHCP packets, you must specify both port 67 (bootps) and port 68 (bootpc) for both the source and destination. The firewall filter acts at both the line cards and the Routing Engine.

This requirement applies to both DHCP local server and DHCP relay, but it applies only when DHCP is provided by the `jdhcpd` process. MX Series routers, M120 routers, and M320 routers use `jdhcpd`. For DHCP relay, that means the configuration is required only at the **[edit forwarding-options dhcp-relay]** hierarchy level and not at the **[edit forwarding-options helpers bootp]** hierarchy level.

DHCP packets received on the line cards are encapsulated by `jdhcpd` with a new UDP header where their source and destination addresses are set to port 68 before being forwarded to the Routing Engine.

For DHCP relay and DHCP proxy, packets sent to the DHCP server from the router have both the source and destination UDP ports set to 67. The DHCP server responds using the same ports. However, when the line card receives these DHCP response packets, it changes both port numbers from 67 to 68 before passing the packets to the Routing Engine. Consequently the filter needs to accept port 67 for packets relayed from the client to the server, and port 68 for packets relayed from the server to the client.

Failure to include both port 67 and port 68 as described here results in most DHCP packets not being accepted.

For information about firewall filters, see *Firewall Filters Overview*.

**Related
Documentation**

- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 79](#)
- [Extended DHCP Local Server Overview on page 4](#)
- *Extended DHCP Relay Agent Overview*
- *Dynamic Firewall Filters Overview*

PART 2

Configuration

- [Configuration Tasks for DHCP Local Server on page 39](#)
- [DHCP Local Server Examples on page 77](#)
- [Configuration Statements on page 89](#)

CHAPTER 2

Configuration Tasks for DHCP Local Server

- [Using External AAA Authentication Services with DHCP on page 40](#)
- [Guidelines for Configuring Support for DHCP Duplicate Clients on page 41](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information on page 42](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces on page 43](#)
- [Configuring a Default Subscriber Service on page 45](#)
- [Grouping Interfaces with Common DHCP Configurations on page 45](#)
- [Guidelines for Configuring Interface Ranges on page 46](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Specifying the Maximum Number of DHCP Clients Per Interface on page 49](#)
- [Allowing Only One DHCP Client Per Interface on page 50](#)
- [Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 52](#)
- [Automatically Logging Out DHCP Clients on page 53](#)
- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54](#)
- [Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 54](#)
- [Enabling Processing of Client Information Requests on page 55](#)
- [Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 56](#)
- [Enabling DHCPv6 Rapid Commit Support on page 57](#)
- [Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 57](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 60](#)
- [Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 61](#)

- [Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 61](#)
- [Configuring a Token for DHCP Local Server Authentication on page 62](#)
- [Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 62](#)
- [Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 63](#)
- [DHCP Liveness Detection Overview on page 64](#)
- [Configuring Detection of DHCP Local Server Client Connectivity on page 65](#)
- [Configuring a DHCP Lease-Time Threshold on page 67](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 70](#)
- [Configuring Passwords for Usernames on page 71](#)
- [Creating Unique Usernames for DHCP Clients on page 72](#)
- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74](#)
- [Specifying the Subnet for DHCP Client Address Assignment on page 75](#)

Using External AAA Authentication Services with DHCP

The extended DHCP local server, including DHCPv6 local server, and the extended DHCP relay agent, including DHCPv6 relay agent, support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. When the extended DHCP local server or relay agent receives a discover PDU from a client, the extended DHCP application contacts the AAA server to authenticate the DHCP client. The extended DHCP application can obtain client addresses and DHCP configuration options from the external AAA authentication server.



.....

NOTE: This section uses the term *extended DHCP application* to refer to both the extended DHCP local server and the extended DHCP relay agent.

.....

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 responds as though it were 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.

You can configure either global authentication support or group-specific support.

You must configure the **username-include** statement to enable the use of authentication. The **password** statement is not required and does not cause DHCP to use authentication if the **username-include** statement is not included.

To configure DHCP local server and DHCP relay agent authentication support:

1. Specify that you want to configure authentication options.

- For DHCP local server:

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

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

- For DHCPv6 local server:

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit authentication
```

2. (Optional) Configure a password that authenticates the username to the external authentication service.

See [“Configuring Passwords for Usernames” on page 71](#).

3. (Optional) Configure optional features to create a unique username.

See [“Creating Unique Usernames for DHCP Clients” on page 72](#).

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [DHCPv6 Relay Agent Overview](#)

Guidelines for Configuring Support for DHCP Duplicate Clients

When configuring DHCP duplicate client support, consider the following guidelines:

- The DHCP duplicate client support feature is used for DHCPv4 clients only.
- If you want to preserve the remotely-created option 82 information, use the **option 82** option with the **duplicate-clients-in-subnet** statement to distinguish between duplicate clients. If there is no remotely created option 82 in the incoming DHCP packets, the router locally creates the option 82 information.
- If you want to use the locally-created option-82, use the **incoming-interface** option with the **duplicate-clients-in-subnet** statement to distinguish between duplicate clients.

- DHCP relay agent and DHCP local server in the same routing instance must have the same the **duplicate-clients-in-subnet** configuration.
- For the Layer 3 wholesale model:
 - The wholesaler and retailer logical system/routing instances must have the same **duplicate-clients-in-subnet** statement configuration.
 - For DHCP relay, the wholesaler and the retailer routing contexts must both have the **relay-option-82** statement configured with the Agent Circuit ID suboption (suboption 1) in option 82.

**Related
Documentation**

- [DHCP Duplicate Client In Subnet Overview on page 15](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces on page 43](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information on page 42](#)

Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information

Duplicate clients occur when two clients in a subnet have the same hardware address or the same client ID.

The following two procedures describe how to configure the router to use the option 82 information in the incoming packets to differentiate between duplicate clients. The first procedure describes the configuration for DHCP relay agent. The second procedure is for DHCP local server.

To configure the DHCP relay agent to differentiate between duplicate clients based on option 82 information:

1. Specify that you want to configure DHCP relay agent.

```
[edit forwarding-options]  
user@host# edit dhcp-relay
```

2. Configure DHCP relay to insert option 82 information if there is no remotely created option 82. Use the default setting, which inserts the interface ID rather than the optional interface description.

```
[edit forwarding-options dhcp-relay]  
user@host# set relay-option-82 circuit-id
```

3. Configure the router to always accept DHCP client packets that contain option 82 information.

```
[edit forwarding-options dhcp-relay]  
user@host# set overrides trust-option-82
```



NOTE: The `trust-option-82` statement must always be enabled so the router can process incoming DHCP client packets that contain option 82 information when the packets have a gateway IP address (giaddr) of 0 (zero).

4. Configure DHCP relay to use the remotely created option 82 information to distinguish between duplicate clients. If there is no remotely created option 82 in the traffic, the router locally creates the option 82 information.

```
[edit forwarding-options dhcp-relay]
user@host# set duplicate-clients-in-subnet option-82
```



NOTE: Make sure that the `always-write-option-82` statement is *not* enabled, as the statement will overwrite the remotely created option 82.

To configure the DHCP local server to differentiate between duplicate clients based on the option 82 information:

1. Specify that you want to configure DHCP local server.

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

2. Configure the duplicate client support with the `option-82` option.

```
[edit system services dhcp-local-server]
user@host# set duplicate-clients-in-subnet option-82
```

Related Documentation

- [DHCP Duplicate Client In Subnet Overview on page 15](#)
- [Guidelines for Configuring Support for DHCP Duplicate Clients on page 41](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces on page 43](#)

Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces

Duplicate clients occur when two clients in a subnet have the same hardware address or the same client ID.

The following two procedures describe how to configure the router to use the clients' incoming interface to differentiate between duplicate clients. The first procedure describes the configuration for DHCP relay agent; the second procedure is for DHCP local server.

To configure the DHCP relay agent to differentiate between duplicate clients based on the client incoming interface:

1. Specify that you want to configure DHCP relay agent.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Configure the duplicate client support with the **incoming-interface** option.

```
[edit forwarding-options dhcp-relay]
user@host# set duplicate-clients-in-subnet incoming-interface
```

3. Configure DHCP relay to insert option 82 information if the information is not specified remotely. Use the default setting, which inserts the interface ID rather than the optional interface description.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option-82 circuit-id
```

4. Configure the router to overwrite any remotely supplied option 82 information in incoming packets.

```
[edit forwarding-options dhcp-relay]
user@host# set overrides always-write-option-82
```

5. Configure the router to always accept DHCP client packets that contain option 82 information.

```
[edit forwarding-options dhcp-relay]
user@host# set overrides trust-option-82
```



NOTE: The *trust-option-82* statement must always be enabled so the router can process incoming DHCP client packets that contain option 82 information when the packets have a gateway IP address (giaddr) of 0 (zero).

To configure the DHCP local server to differentiate between duplicate clients based on the client incoming interface:

1. Specify that you want to configure DHCP local server.

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

2. Configure the duplicate client support with the **incoming-interface** option.

```
[edit system services dhcp-local-server]
user@host# set duplicate-clients-in-subnet incoming-interface
```

Related Documentation

- [DHCP Duplicate Client In Subnet Overview on page 15](#)
- [Guidelines for Configuring Support for DHCP Duplicate Clients on page 41](#)
- [Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information on page 42](#)

Configuring a Default Subscriber Service

Subscriber management enables you to specify a default subscriber service for DHCP (and DHCPv6) local server and DHCP relay agent. The default service is the service (dynamic profile) that is applied to subscribers when they log in.

Default services are subsequently deactivated in any of the following circumstances:

- A PCRF responds to AAA for the subscriber.
- A RADIUS CoA deactivation request is issued.
- You deactivate the service manually through the CLI.

To configure a default subscriber service:

1. Ensure that the service you want to use as the default has been configured in a dynamic profile.
2. Specify the default service.

The following example configures the default service for DHCP local server subscribers.

```
[edit system services dhcp-local-server]
user@host# set service-profile retailer1-subscriber
```

3. Attach the default service—you can attach the profile globally, for a group of interfaces, or for a specific interface.

The following example attaches the profile to a named group of interfaces for DHCP local server.

- Specify the group to which the default service is attached.

```
[edit system services dhcp-local-server]
user@host# set group subscriber-svl
```

- Specify the dynamic profile that defines the default service.

```
[edit system services dhcp-local-server group subscriber-svl]
user@host# set dynamic-profile retailer1-subscriber
```

Related Documentation

- [Default Subscriber Service Overview on page 14](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68](#)

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group together 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
```

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [DHCPv6 Relay Agent Overview](#)
- [Group-Specific DHCP Local Server Options on page 16](#)
- [Group-Specific DHCP Relay Options](#)
- [Guidelines for Configuring Interface Ranges on page 46](#)

Guidelines for Configuring Interface Ranges

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
```

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 45](#)

Overriding Default DHCP Local Server Configuration Settings

Subscriber management enables you to override certain default DHCP and DHCPv6 local server configuration settings. You can override 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]** or **[edit system services dhcp-local-server dhcpv6]** 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]** or **[edit system services dhcp-local-server dhcpv6 group]** 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]** or **[edit system services dhcp-local-server dhcpv6 group group-name interface]** hierarchy level.

To override default DHCP local server configuration settings:

1. Specify that you want to configure override options.

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 boston overrides
```

Per-interface override:

```
[edit system services dhcp-local-server]
user@host# edit group boston overrides interface fe-1/0/1.1
```

2. (Optional) Override the maximum number of DHCP clients allowed per interface.
See [“Specifying the Maximum Number of DHCP Clients Per Interface” on page 49](#).
3. (Optional) Configure DHCP client auto logout.
See [“Automatically Logging Out DHCP Clients” on page 53](#).
4. (Optional) Enable processing of information requests from clients.
See [“Enabling Processing of Client Information Requests” on page 55](#).
5. (Optional, DHCPv6 only) Specify a delegated pool name to use for DHCPv6 multiple address assignment.
See [“Specifying the Delegated Address Pool for IPv6 Prefix Assignment” on page 56](#).
6. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.
See [“Enabling DHCPv6 Rapid Commit Support” on page 57](#).

7. (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](#)” on page 57.

8. (Optional) Delete DHCP override settings.

See “[Deleting DHCP Local Server and DHCP Relay Override Settings](#)” on page 58.

Related Documentation

- [Group-Specific DHCP Local Server Options](#) on page 16
- [Deleting DHCP Local Server and DHCP Relay Override Settings](#) on page 58

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.

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Allowing Only One DHCP Client Per Interface on page 50](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)

Allowing Only One DHCP Client Per Interface

Subscriber management provides two methods that you can use to configure DHCP local server and DHCP relay agent to allow only one DHCP client per interface. The two methods differ on which client is allowed on the interface—the new client or the existing client. The two methods are supported by both DHCP local server and DHCP relay agent, and can be configured globally, for a group of interfaces, or for a specific interface.

- **Accept new client**—Delete the existing client binding and allow the new client to connect. To configure this action, use the ... **overrides client-discover-match incoming-interface** statement.
- **Keep existing client**—Retain the existing client binding on the interface and reject any requests from new DHCP clients. To configure this action, use the ... **overrides interface-client-limit 1** statement to specify a maximum of one client.

To configure the router to delete the existing client binding on the interface and allow the new client to connect:

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. Configure the router to view all client connections on the interface as coming from the same client, which allows a new client to replace the existing client. This example shows the DHCP local server configuration. The DHCP relay agent configuration is similar.

[edit system services dhcp-local-server overrides]

user@host# set **client-discover-match** incoming-interface

To configure the router to keep the existing client binding on the interface and refuse connections from new clients:

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. Set the maximum number of clients allowed per interface to one. This example shows the DHCP local server configuration. The DHCP relay agent configuration is similar.

[edit system services dhcp-local-server overrides]

user@host# set **interface-client-limit** 1

**Related
Documentation**

- [DHCP Auto Logout Overview on page 22](#)
- [Automatically Logging Out DHCP Clients on page 53](#)

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

You can configure both DHCP local server and DHCP relay agent to override the default installation of access, access-internal, and destination routes. 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. You can configure the override globally or for named interface groups.



NOTE: 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.



NOTE: In Junos OS releases prior to Release 13.2, the `no-arp` statement was used to override the default installation of host routes. In Junos OS Release 13.2 and later, the `no-arp` statement is deprecated and the function is replaced by the `route-suppression` statement.

To configure route suppression and prevent DHCP from installing specific types of routes:

- 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
```

Related Documentation

- [DHCP Access, Access-Internal, and Destination Route Suppression on page 16](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Extended DHCP Relay Agent Overview](#)
- [DHCPv6 Relay Agent Overview](#)

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 Auto Logout Overview on page 22](#)
- [DHCP Relay Agent Option 82 Value for Auto Logout](#)
- [Allowing Only One DHCP Client Per Interface on page 50](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Extended DHCP Local Server Overview on page 4](#)

- *Extended DHCP Relay Agent Overview*

Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events

You can specify a configuration in which the router does not log out a subscriber when the subscriber's interface is deleted.

To configure the router to maintain DHCP subscribers when the subscriber interface is deleted:

1. Specify that you want to configure subscriber management.

```
[edit system services]
user@host# edit subscriber-management
```

2. Configure the router to support the maintain-subscriber feature.

```
[edit system services subscriber-management]
user@host# edit maintain-subscriber
```

3. Configure the router to enable the maintain-subscriber feature when an interface-delete event occurs.

```
[edit system services subscriber-management maintain-subscriber]
user@host# set interface-delete
```

- Related Documentation**
- [Subscriber Binding Retention During Interface Delete Events on page 24](#)
 - [Verifying and Managing the DHCP Maintain Subscribers Feature on page 184](#)

Configuring the Router to Strictly Enforce the Subscriber Scaling License

You can configure the router to strictly enforce the subscriber scaling feature, which is part of the Junos Subscriber Access Feature Pack license. The subscriber scaling feature specifies the maximum number of subscribers that can be logged in at any one time.

When you configure strict scaling license support, the router performs the following actions:

- Strictly enforces the subscriber scaling license and does not allow any grace period. When the number of logged-in subscriber reaches the number allowed by the scaling license, no additional subscribers are allowed to log in.
- Creates the informational log message, "90 percent of installed subscriber scale licenses in use" in `/var/log/messages`, to inform you when you have 10 percent of the total allowed licenses remaining. The router clears this condition when license usage falls below 90 percent. The log message is created again if the 90 percent usage is later reached.

To configure the router to strictly enforce the subscriber scaling license:

1. Specify that you want to configure subscriber management.


```
[edit system services]
user@host# edit subscriber-management
```

2. Configure the router to enforce the scaling license.

```
[edit system services subscriber-management]
user@host# set enforce-strict-scale-limit-license
```

**Related
Documentation**

- *Subscriber Access Licensing Overview*
- *Junos OS Feature Licenses*
- *Verifying Junos OS License Installation*

Enabling Processing of Client Information Requests

By default, DHCP local server and DHCPv6 local server do not respond to 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.

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See *Configuring an Address-Assignment Pool Name and Addresses*. 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* for details about how to configure the information sought by clients that send 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
```

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)

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
```

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)

Enabling DHCPv6 Rapid Commit Support

You can configure the extended DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled on the extended DHCPv6 local server, 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 override 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
```

Related Documentation

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 58](#)
- [Extended DHCP Local Server Overview on page 4](#)

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

In a DHCPv6 environment, DHCPv6 clients can use a single Solicit message to request multiple addresses (an IA_NA address, an IA_PD address, or both), as well as the DNS server address (DHCPv6 attribute 23). By default, the DHCPv6 local server returns the DNS server address as a global DHCPv6 option.

You can override the default behavior and specify that the DHCPv6 local server returns DNS server addresses as their respective IA_NA and IA_PD suboptions. You can configure the DHCPv6 local server to support the override globally, for a specific group, or for a specific interface.



CAUTION: Some customer premises equipment (CPE) cannot recognize the DNS server address when the address is returned as an IA_NA or IA_PD suboption, which can create interoperability issues.

To configure the DHCPv6 local server to return the DNS server address as an IA_NA or IA_PD suboption.

1. Specify that you want to configure DHCPv6 override options.

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

2. Override the default behavior. DHCPv6 local server now returns DNS server addresses as the respective IA_PD or IA_NA suboption.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set multi-address-embedded-option-response
```

**Related
Documentation**

- [DHCPv6 Options in a DHCPv6 Multiple Address Environment on page 27](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 26](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)

Deleting DHCP Local Server and DHCP Relay Override Settings

You can delete override settings for DHCP local server and DHCP relay globally, for a named group, or for a specific interface within a named group. You can delete a specific override setting or all overrides.

- To delete a specific DHCP override setting at a particular hierarchy level, include the **overrides** statement with the appropriate subordinate statements. For example, to delete the DHCP local server override **interface-client-limit** setting for a group named **marin20**:

```
[edit system services dhcp-local-server]
user@host# delete group marin20 overrides interface-client-limit
```

- To delete all DHCP override settings at a hierarchy level, include the **overrides** statement without any subordinate statements. For example, to delete all DHCP relay overrides for interface **fxp0.0**, which is in group **marin20**:

```
[edit forwarding-options dhcp-relay]
user@host# delete group marin20 interface fxp0.0 overrides
```

**Related
Documentation**

- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)

Configuring Extended DHCP Local Server Dynamic Client Reconfiguration

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. In addition to requesting that the DHCP local server initiate reconfiguration, you can specify the reconfiguration behavior.

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) Override the global configuration for a particular group of clients.

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” on page 60](#).

4. (Optional) Configure the response to a failed reconfiguration.

See [“Configuring Deletion of the Client When Dynamic Reconfiguration Fails” on page 61](#).

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

See [“Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect” on page 61](#).

6. (Optional) Configure a token for rudimentary server authentication.

See [“Configuring a Token for DHCP Local Server Authentication” on page 62](#).

7. (Optional) Initiate reconfiguration of some or all client bindings.

See [“Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings” on page 63](#).

8. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

See [“Preventing Binding of Clients That Do Not Support Reconfigure Messages” on page 62](#).

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` 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.

Related Documentation

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [attempts on page 97](#)
- [timeout on page 167](#)

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-abort
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-abort
```

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.

Related Documentation

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [clear-on-abort on page 101](#)

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.

**Related
Documentation**

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [radius-disconnect on page 152](#)
- [trigger on page 170](#)

Configuring a Token for DHCP Local Server Authentication

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. The client compares the received token with a token already configured on the client. If the tokens do not match, the DHCP client discards the forcerenew message. Use of the token provides rudimentary protection against inadvertently instantiated DHCP servers.

(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 8ysIU9E32k8r
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set token 8ysIU9E32k8r
```

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.

**Related
Documentation**

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [token on page 168](#)

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.

(Optional) To configure the DHCPv6 local server to require that all clients accept reconfiguration:

- Specify strict reconfiguration.

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

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]` hierarchy level.

The `show dhcpv6 server statistics` command displays a count of solicit messages that the server has discarded.

Related Documentation

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [strict on page 163](#)

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.

For DHCPv4:

```
user@host> request dhcp server reconfigure all
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCP client.

For DHCPv4:

```
user@host> request dhcp server reconfigure 192.168.27.3
```

For DHCPv6:

```
user@host> request dhcpv6 server reconfigure 2001:bd8:1111:2222::
```

- Specify the client ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure
LL_TIME0x1-0x2e159c0-00:10:94:00:00:02
```

- Specify the session ID of a DHCPv6 client.

```
user@host> request dhcpv6 server reconfigure 5
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 12:23:34:45:56:67
```

- 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
```

**Related
Documentation**

- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
- [request dhcp server reconfigure on page 194](#)

DHCP Liveness Detection Overview

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, or DHCP relay proxy is unable to quickly detect if it has lost connectivity with a subscriber or a DHCP client; and it must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages prior to exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often considered 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.

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.

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 for DHCPv6 subscribers.



NOTE: This release supports only BFD for DHCPv4 and DHCPv6 liveness detection.

When configuring BFD liveness detection, keep the following in mind:

- 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 (once validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for relevant clients (that is, 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 and a configured failure action is implemented.

Related Documentation

- [Configuring Detection of DHCP Local Server Client Connectivity on page 65](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity](#)

Configuring Detection of DHCP Local Server Client Connectivity

Liveness detection for DHCP subscriber IP sessions 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.



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 this release, the only method supported for liveness detection is Bidirectional Forwarding Detection (BFD).

- 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 for DHCP Local Server Clients” on page 83](#) for an example of how to configure DHCPv4 groups for DHCP local server liveness detection.

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
```

Related Documentation

- [DHCP Liveness Detection Overview on page 64](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83](#)
- [Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients](#)

Configuring a DHCP Lease-Time Threshold

Subscriber management provides a lease-time validation feature that enables you to specify the minimum DHCP lease time allowed in your subscriber access environment. When you configure lease-time validation, you specify the lease-time threshold and the action the router performs when an offered lease time is less than the threshold (such as dropping the lease).

Lease-time validation ensures that leases that are offered by third-party DHCP servers or address assignment pools always meet the requirements of your network. For example, you want short leases to be rejected because they can result in excessive renewal traffic that can impact network performance.

You can configure lease-time validation on DHCPv4 and DHCPv6 local servers, and DHCPv4 and DHCPv6 relay agents, and for individual interfaces or interface groups. DHCP relay proxy also supports lease-time validation.

The following procedure describes the steps you use to configure lease-time validation. This example describes a configuration for DHCP relay agent. You use similar steps at the appropriate hierarchy levels for DHCP local server, DHCPv6 local server, and DHCPv6 relay agent.

To configure lease time validation for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent support.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify that you want to configure the DHCP lease time validation feature.

```
[edit forwarding-options dhcp-relay]
user@host# set lease-time-validation
```

3. Configure the threshold that specifies the minimum DHCP client lease time allowed in your network.

```
[edit forwarding-options dhcp-relay lease-time-validation]
user@host# set lease-time-threshold 3600
```

4. Configure the action the router takes when a lease time violation occurs.

```
[edit forwarding-options dhcp-relay lease-time-validation]
user@host# set violation-action drop
```



NOTE: DHCP relay agent and DHCP local server support different violation actions. See the [violation-action](#) statement for descriptions of the actions.

If you do not specify a violation action, DHCP binds the client using the third-party lease but marks the binding as lease-time violating.

5. (Optional) Configure how often you want the router to consolidate and log syslog warning messages.

```
[edit system processes dhcp-service]
user@host# set ltv-syslog-interval 3600
```

Related Documentation

- [DHCP Lease-Time Validation Overview on page 32](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Extended DHCP Relay Agent Overview](#)

Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

This topic describes how to attach a dynamic profile to a DHCP subscriber interface or a DHCP client interface. When a DHCP subscriber or DHCP client logs in, the specified dynamic profile is instantiated and the services defined in the profile are applied to the interface.

This topic contains the following sections:

- [Attaching a Dynamic Profile to All DHCP Subscriber or All DHCP Client Interfaces on page 68](#)
- [Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces or a Group of DHCP Client Interfaces on page 69](#)

Attaching a Dynamic Profile to All DHCP Subscriber or All DHCP Client Interfaces

To attach a dynamic profile to all DHCP subscriber or all DHCP client interfaces:

1. At the DHCP configuration hierarchy, use the **dynamic-profile** statement to specify the name of the dynamic profile to attach to all interfaces.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set dynamic-profile vod-profile-22
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# set dynamic-profile vod-profile-west
```

2. (Routers only) Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The **aggregate-clients** option does not apply to demux subscriber interfaces. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients merge
```

- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```

Attaching a Dynamic Profile to a Group of DHCP Subscriber Interfaces or a Group of DHCP Client Interfaces

Before you begin:

- Configure the interface group.

See “[Grouping Interfaces with Common DHCP Configurations](#)” on page 45.

To attach a dynamic profile to a group of interfaces:

1. At the DHCP configuration hierarchy, specify the name of the interface group and the dynamic profile to attach to the group.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set group boston dynamic-profile vod-profile-42
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# set group quebec dynamic-profile vod-profile-east
```

2. (Routers only) Optionally, you can configure the attribute to use when attaching the specified profile.

You can include either the **aggregate-clients** option to enable multiple DHCP subscribers to share the same VLAN logical interface, or the **use-primary** option to specify that the primary dynamic profile is used. The **aggregate-clients** option does not apply to demux subscriber interfaces. The two options are mutually exclusive.

- To enable multiple subscribers to share the same VLAN logical interface:

```
[edit system services dhcp-local-server dynamic-profile]
user@host# set aggregate-clients merge
```

- To use the primary dynamic profile:

```
[edit forwarding-options dhcp-relay dynamic-profile]
user@host# set use-primary subscriber_profile
```

Related Documentation

- [Dynamic Profiles Overview](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview on page 12](#)
- [Example: Configuring Dynamic Subscriber Interfaces on IP Demux Interfaces](#)

Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server

You can configure how DHCP local server handles DHCP snooped packets. Depending on the configuration, DHCP local server either forwards or drops the snooped packets it receives.

[Table 9 on page 70](#) indicates the action the router takes for DHCP local server snooped packets.



NOTE: Configured interfaces are those interfaces that have been configured with the `group` statement in the `[edit system services dhcp-local-server]` hierarchy. Non-configured interfaces are those that are in the logical system/routing instance but have not been configured by the `group` statement.

Table 9: Actions for DHCP Local Server Snooped Packets

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
forward-snooped-clients not configured	dropped	dropped
all-interfaces	forwarded	forwarded
configured-interfaces	forwarded	dropped
non-configured-interfaces	dropped	forwarded

To configure DHCP snooped packet forwarding for DHCP local server:

1. Specify that you want to configure DHCP local server.

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

2. Enable DHCP snooped packet forwarding for DHCP local server.

```
[edit system services dhcp-local-server]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.


```
[edit system services dhcp-local-server forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP local server to forward DHCP snooped packets on only configured interfaces:

```
[edit]
system {
  services {
    dhcp-local-server {
      forward-snooped-clients configured-interfaces;
    }
  }
}
```

Related Documentation

- [DHCP Snooping Support on page 21](#)

Configuring Passwords for Usernames

You can configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

To configure a password that authenticates the username:

1. Specify that you want to configure authentication options.

- For DHCP local server:

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

- For DHCPv6 local server:

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

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

2. Configure the password. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the **password** statement.)

```
[edit system services dhcp-local-server authentication]
user@host# set password myPassword1234
```

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Extended DHCP Relay Agent Overview](#)
- [Using External AAA Authentication Services with DHCP on page 40](#)
- [Special Requirements for Junos OS Plain-Text Passwords](#)

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).



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-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**. (Not supported for DHCPv6 local server)
- **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 relay agent)
- **relay-agent-remote-id**—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server or relay agent)
- **relay-agent-subscriber-id**—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server or relay agent)
- **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.

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]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
```

To configure a unique username:

1. Specify that you want to configure authentication.

- For DHCP local server:

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

- For DHCPv6 local server:

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

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit authentication
```

2. Specify that you want to include optional information in the username. (DHCP local server, DHCPv6 local server, and DHCP relay agent all support the **username-include** statement.)

```
[edit system services dhcp-local-server authentication]
user@host# set username-include
```

3. (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 isp55.com
user@host# set username-include mac-address
user@host# set username-include user-prefix wallybrown
```

The previous **username-include** configuration produces this unique username:

wallybrown.0090.1a01.1234.enet@isp55.com

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Extended DHCP Relay Agent Overview](#)
- [Using External AAA Authentication Services with DHCP on page 40](#)

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. You use the **pool-match-order** statement to specify the match order. If you do not specify the **pool-match-order**, the router (or switch) uses the default **ip-address-first** matching to select the address pool. After DHCP local server determines the address assignment pool to use, the server performs the matching based on the criteria you specified in the pool configuration.

In the default **ip-address-first** matching, 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 there is no giaddr in the request, then the DHCP local server matches the IP address of the receiving interface to the address of the address-assignment pool.

In **external-authority** matching, 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.

For IPv4 address-assignment pools, you can optionally configure the extended DHCP local server to match the DHCP relay agent information option (option 82) in the client DHCP packets to a named range in the address-assignment pool used for the client. Named ranges are subsets within the overall address-assignment pool address range, which you can configure when you create the address-assignment pool.



NOTE: 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.

To configure the matching order the extended DHCP local server uses to determine the address-assignment pool used for a client:

1. Access the **pool-match-order** configuration.

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

2. Specify the pool matching methods in the order in which the router (switch) performs the methods. You can specify the methods in any order. All methods are optional—the router (switch) uses the **ip-address-first** method by default.

- Configure the router (switch) to use an external addressing authority.

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

- Configure the router (switch) to use the ip-address-first method.

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

- (IPv4 address-assignment pools only) Specify the option 82 matching method.

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

Related Documentation

- [Address-Assignment Pools Overview on page 25](#)
- [Configuring Address-Assignment Pools](#)
- [Extended DHCP Local Server Overview on page 4](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 78](#)

Specifying the Subnet for DHCP Client Address Assignment

Subscriber management enables you to explicitly specify the subnet to which the DHCP local server matches the requested IP address. The server accepts and uses an active client's requested IP address for address assignment only when the requested address and the IP address of the DHCP server interface are in the same subnet. The server accepts and uses a passive client's requested IP address only when the requested address and the IP address of the relay interface are in the same subnet. The DHCPv6 local server supports the same process for DHCPv6 clients and addresses.

To specify the subnet used for client address assignment:

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# set requested-ip-network-match 10
```

- For DHCPv6 local server:

```
[edit forwarding-options dhcp-local-server dhcpv6]
user@host# set requested-ip-network-match 30
```

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 4](#)
- [requested-ip-network-match on page 158](#)

CHAPTER 3

DHCP Local Server Examples

- [Example: Minimum Extended DHCP Local Server Configuration on page 77](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 78](#)
- [Example: Extended DHCPv6 Local Server Configuration on page 78](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine on page 79](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83](#)

Example: Minimum Extended DHCP Local Server Configuration

This example shows the minimum configuration you need to use for the extended DHCP local server on the router or switch:

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



NOTE: The interface type in this topic is just an example. The **fe-** interface type is not supported by EX Series switches.

This example creates the server group named **group_one**, and specifies that the DHCP local server is enabled on interface **fe-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.

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)

Example: Extended DHCP Local Server Configuration with Optional Pool Matching

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;
  }
}
```



NOTE: The interface type in this topic is just an example. The fe- interface type is not supported by EX Series switches.

- Related Documentation**
- [Extended DHCP Local Server Overview on page 4](#)
 - [Address-Assignment Pools Overview on page 25](#)

Example: Extended DHCPv6 Local Server Configuration

This example shows a sample extended DHCPv6 local server configuration. The second part of the example shows a sample RADIUS authentication configuration—authentication must be configured for DHCPv6 local server operations.

```
[edit system services]
dhcp-local-server {
  dhcpv6 {
    authentication {
      password v679M8vt;
      username-include {
        user-prefix wallybrown;
        domain-name isp55.com;
      }
    }
  }
}
```



```

    }
  }
  group group_two {
    authentication {
      password P$55qw4$$;
      username-include {
        user-prefix south5;
        domain-name isp55.com;
      }
    }
  }
  interface ge-1/0/3.0;
}
}
}

```

The following is a sample RADIUS authentication configuration.

```

[edit access]
radius-server {
  192.168.1.250 {
    port 1812;
    secret &tlUEl*7688+;
  }
}
profile isp-bos-metro-fiber-basic {
  accounting-order radius;
  authentication-order radius;
  radius {
    authentication-server 192.168.1.250;
    accounting-server 192.168.1.250;
  }
  accounting {
    order radius;
    accounting-stop-on-failure;
    accounting-stop-on-access-deny;
    update-interval 10;
    statistics time;
  }
}

```

Related Documentation

- [DHCPv6 Local Server Overview on page 10](#)

Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine

This example shows how to configure a firewall filter to ensure that proper DHCP packets can reach the Routing Engine on MX Series routers.

- [Requirements on page 80](#)
- [Overview on page 80](#)
- [Configuration on page 80](#)
- [Verification on page 83](#)

Requirements

This configuration example applies only to routers where DHCP local server and DHCP relay agent services are provided by the `jdhcpd` process rather than the legacy `dhcpd` process or `fud` (UDP forwarding) process. MX Series routers, M120 routers, and M320 routers use `jdhcpd`. For DHCP relay, that means the configuration is required only at the `[edit forwarding-options dhcp-relay]` hierarchy level and not at the `[edit forwarding-options helpers bootp]` hierarchy level.

No special configuration beyond device initialization is required before you can configure this feature.

Overview

Firewall filters that perform some action on DHCP packets at the Routing Engine, such as a filter to protect the Routing Engine by allowing only proper DHCP packets, require that both port 67 (bootps) and port 68 (bootpc) are configured as both source and destination ports.

DHCP packets received on the line cards are encapsulated by `jdhcpd` with a new UDP header where their source and destination addresses are set to port 68 before being forwarded to the Routing Engine. For DHCP relay and DHCP proxy, packets sent to the DHCP server from the router have both the source and destination UDP ports set to 67. The DHCP server responds using the same ports. However, when the line card receives these DHCP response packets, it changes both port numbers from 67 to 68 before passing the packets to the Routing Engine. Consequently the filter needs to accept port 67 for packets relayed from the client to the server, and port 68 for packets relayed from the server to the client.

In this example, you configure two filter terms, **`dhcp-client-accept`** and **`dhcp-server-accept`**. The match conditions for **`dhcp-client-accept`** specify a source address and destination address for broadcast packets, the UDP protocol used for DHCP packets, and the bootpc (68) source port and bootps (67) destination port. Packets that match these conditions are counted and accepted.

The match conditions for **`dhcp-server-accept`** specify the UDP protocol used for DHCP packets, and both port 67 and 68 for both source port and destination port. Packets that match these conditions are counted and accepted.



NOTE: This example does not show all possible configuration choices, nor does it show how the filter is applied in your configuration. This example applies to both static application of the filter as well as dynamic application with a dynamic profile.

Configuration

CLI Quick Configuration

To quickly configure the sample Routing Engine DHCP filter, copy the following commands, paste them in a text file, remove any line breaks, and then copy and paste the commands into the CLI.

```

[edit]
edit firewall family inet filter RE-protect
edit term dhcp-client-accept
set from source-address 0.0.0.0/32
set from destination-address 255.255.255.255/32
set from protocol udp
set from source-port 68
set from destination-port 67
set then count dhcp-client-accept
set then accept
up
edit term dhcp-server-accept
set from protocol udp
set from source-port 67
set from source-port 68
set from destination-port 67
set from destination-port 68
set then count dhcp-server-accept
set then accept
top

```

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*.

To configure a DHCP firewall filter to protect the Routing Engine:

1. Create or specify a firewall filter.

```

[edit firewall]
user@host# edit family inet filter RE-protect

```

2. Create a filter term for the client.

```

[edit firewall family inet filter RE-protect]
user@host# edit term dhcp-client-accept

```

3. Specify the match conditions for DHCP packets.

```

[edit firewall family inet filter RE-protect term dhcp-client-accept]
user@host# set from source-address 0.0.0.0/32
user@host# set from destination-address 255.255.255.255/32
user@host# set from protocol udp
user@host# set from source-port 68
user@host# set from destination-port 67

```

4. Specify the action to take for matched packets.

```

[edit firewall family inet filter RE-protect term dhcp-client-accept]
user@host# set then count dhcp-client-accept
user@host# set then accept

```

5. Create a filter term for the server.

```

[edit firewall family inet filter RE-protect]
user@host# edit term dhcp-server-accept

```

6. Specify the match conditions for DHCP packets.

```

[edit firewall family inet filter RE-protect term dhcp-server-accept]

```

```
user@host# set from protocol udp
user@host# set from source-port [67 68]
user@host# set from destination-port [67 68]
```

7. Specify the action to take for matched packets.

```
[edit firewall family inet filter RE-protect term dhcp-server-accept]
user@host# set then count dhcp-client-accept
user@host# set then accept
```

Results From configuration mode, confirm your configuration by entering the **show firewall** command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show firewall
family inet {
  filter RE-protect {
    term dhcp-client-accept {
      from {
        source-address {
          0.0.0.0/32;
        }
        destination-address {
          255.255.255.255/32;
        }
        protocol udp;
        source-port 68;
        destination-port 67;
      }
      then {
        count dhcp-client-accept;
        accept;
      }
    }
    term dhcp-server-accept {
      from {
        protocol udp;
        source-port [ 67 68 ];
        destination-port [ 67 68 ];
      }
      then {
        count dhcp-server-accept;
        accept;
      }
    }
  }
}
```

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

Verification

To confirm that the Routing Engine DHCP protection filter is properly passing DHCP packets, perform these tasks:

- [Verifying the DHCP Filter Operation on page 83](#)

Verifying the DHCP Filter Operation

Purpose	Verify that both counters increment as DHCP traffic passes to the Routing Engine.
Action	<p>From operational mode, enter the show firewall family inet filter RE-protect command.</p> <pre> user@host> show firewall family inet filter RE-protect Filter: RE-protect Counters: Name Bytes Packets dhcp-client-accept 328 1 dhcp-server-accept 574 1 user@host> show firewall family inet filter RE-protect Filter: RE-protect Counters: Name Bytes Packets dhcp-client-accept 660 2 dhcp-server-accept 1152 2 </pre>
Meaning	The output lists both configured counters, dhcp-client-accept and dhcp-server-accept. By issuing the command more than once, you can see that the byte and packet fields both show that traffic is being accepted and counted.
Related Documentation	<ul style="list-style-type: none"> • Port Number Requirements for DHCP Firewall Filters on page 34 • <i>Dynamic Firewall Filters Overview</i> • <i>Firewall Filters Overview</i> • Extended DHCP Local Server Overview on page 4 • <i>Extended DHCP Relay Agent Overview</i>

Example: Configuring Group Liveness Detection for DHCP Local Server Clients

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 on page 84](#)
- [Overview on page 84](#)
- [Configuration on page 84](#)

Requirements

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1R1 or later
- Junos OS Release 12.3R2 or later for EX Series switches
- Configure DHCP local server. See [“Extended DHCP Local Server Overview” on page 4](#).

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

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-server group 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]
regress@montag# 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.

**Related
Documentation**

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCP Liveness Detection Overview on page 64](#)
- [Configuring Detection of DHCP Local Server Client Connectivity on page 65](#)

CHAPTER 4

Configuration Statements

- [\[edit system services dhcp-local-server\] Hierarchy Level on page 91](#)
- [\[edit system services subscriber-management\] Hierarchy Level on page 94](#)
- [aggregate-clients \(DHCP Local Server\) on page 96](#)
- [attempts \(DHCP Local Server\) on page 97](#)
- [authentication \(DHCP Local Server\) on page 98](#)
- [bfd on page 99](#)
- [circuit-type \(DHCP Local Server\) on page 100](#)
- [clear-on-abort \(DHCP Local Server\) on page 101](#)
- [client-discover-match \(DHCP Local Server\) on page 102](#)
- [client-id \(DHCP Local Server\) on page 103](#)
- [delegated-pool \(DHCP Local Server\) on page 104](#)
- [delimiter \(DHCP Local Server\) on page 105](#)
- [detection-time on page 106](#)
- [dhcp-local-server on page 107](#)
- [dhcpx6 \(DHCP Local Server\) on page 112](#)
- [domain-name \(DHCP Local Server\) on page 115](#)
- [duplicate-clients-in-subnet \(DHCP Local Server and DHCP Relay Agent\) on page 116](#)
- [dynamic-profile \(DHCP Local Server\) on page 117](#)
- [enforce-strict-scale-limit-license \(Subscriber Management\) on page 118](#)
- [external-authority on page 118](#)
- [failure-action on page 119](#)
- [forward-snooped-clients \(DHCP Local Server\) on page 120](#)
- [group \(DHCP Local Server\) on page 121](#)
- [holddown-interval on page 123](#)
- [interface \(DHCP Local Server\) on page 124](#)
- [interface-client-limit \(DHCP Local Server\) on page 126](#)
- [interface-delete \(Subscriber Management or DHCP Client Management\) on page 127](#)
- [interface-name \(DHCP Local Server\) on page 128](#)

- [ip-address-first](#) on page 129
- [lease-time-threshold](#) (DHCP Local Server and DHCP Relay Agent) on page 130
- [lease-time-validation](#) (DHCP Local Server and DHCP Relay Agent) on page 131
- [liveness-detection](#) on page 132
- [logical-system-name](#) (DHCP Local Server) on page 133
- [ltv-syslog-interval](#) (System Process) on page 133
- [mac-address](#) (DHCP Local Server) on page 134
- [maintain-subscriber](#) (Subscriber Management) on page 135
- [method](#) on page 136
- [minimum-interval](#) on page 137
- [minimum-receive-interval](#) on page 138
- [multi-address-embedded-option-response](#) (DHCP Local Server) on page 139
- [multiplier](#) on page 140
- [no-adaptation](#) on page 141
- [option-60](#) (DHCP Local Server) on page 142
- [option-82](#) (DHCP Local Server Authentication) on page 143
- [option-82](#) (DHCP Local Server Pool Matching) on page 144
- [overrides](#) (DHCP Local Server) on page 145
- [password](#) (DHCP Local Server) on page 147
- [pool](#) (DHCP Local Server Overrides) on page 148
- [pool-match-order](#) on page 149
- [process-inform](#) on page 150
- [radius-disconnect](#) (DHCP Local Server) on page 152
- [rapid-commit](#) (DHCPv6 Local Server) on page 153
- [reconfigure](#) (DHCP Local Server) on page 154
- [relay-agent-interface-id](#) (DHCP Local Server) on page 155
- [relay-agent-remote-id](#) (DHCP Local Server) on page 156
- [relay-agent-subscriber-id](#) (DHCP Local Server) on page 157
- [requested-ip-network-match](#) (DHCP Local Server) on page 158
- [route-suppression](#) (DHCP Local Server and Relay Agent) on page 159
- [routing-instance-name](#) (DHCP Local Server) on page 160
- [service-profile](#) (DHCP Local Server) on page 161
- [session-mode](#) on page 162
- [strict](#) (DHCP Local Server) on page 163
- [subscriber-management](#) (Subscriber Management) on page 164
- [threshold](#) (detection-time) on page 165
- [threshold](#) (transmit-interval) on page 166

- [timeout \(DHCP Local Server\)](#) on page 167
- [token \(DHCP Local Server\)](#) on page 168
- [transmit-interval](#) on page 169
- [trigger \(DHCP Local Server\)](#) on page 170
- [use-primary \(DHCP Local Server\)](#) on page 171
- [user-prefix \(DHCP Local Server\)](#) on page 172
- [username-include \(DHCP Local Server\)](#) on page 173
- [version \(BFD\)](#) on page 174
- [violation-action \(DHCP Local Server and DHCP Relay Agent\)](#) on page 175

[\[edit system services dhcp-local-server\]](#) Hierarchy Level

```

system {
  services {
    dhcp-local-server {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          delimiter delimiter-character;
          domain-name domain-name-string;
          interface-name;
          logical-system-name;
          mac-address;
          option-60;
          option-82 <circuit-id> <remote-id>;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
    }
    dhcpv6 {
      authentication {
        password password-string;
        username-include {
          circuit-type;
          client-id;
          delimiter delimiter-character;
          domain-name domain-name-string;
          interface-name;
          logical-system-name;
          relay-agent-interface-id;
          relay-agent-remote-id;
          relay-agent-subscriber-id;
          routing-instance-name;
          user-prefix user-prefix-string;
        }
      }
    }
    group group-name {
      authentication {
        password password-string;
        username-include {

```

```
    circuit-type;
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-name;
    logical-system-name;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
  }
}
interface interface-name {
  exclude;
  overrides {
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    rapid-commit;
  }
  service-profile dynamic-profile-name;
  trace;
  upto upto-interface-name;
}
overrides {
  delegated-pool;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
route-suppression;
service-profile dynamic-profile-name;
}
overrides {
  delegated-pool;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
}
```

```

    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name (aggregate-clients (merge | replace) | use-primary
    primary-profile-name);
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            overrides;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
}
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
interface interface-name {
    exclude;
    overrides {
        client-discover-match (option60-and-option82 | incoming-interface);
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;

```

```
        process-inform {
            pool pool-name;
        }
    }
    reconfigure {
        attempts attempt-count;
        clear-on-abort;
        timeout timeout-value;
        token token-value;
        trigger {
            radius-disconnect;
        }
    }
    requested-ip-network-match subnet-mask;
    route-suppression;
    service-profile dynamic-profile-name;
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
service-profile dynamic-profile-name;
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
}
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}
```

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)

[edit system services subscriber-management] Hierarchy Level

```
system {
  services {
    subscriber-management {
      enforce-strict-scale-limit-license;
    }
  }
}
```



```
gres-route-flush-delay;
maintain-subscriber {
  interface-delete;
}
traceoptions {
  file <filename> <files number> <match regular-expression > <size
    maximum-file-size> <world-readable | no-world-readable>;
  flag flag;
}
}
```

**Related
Documentation**

- [Subscriber Binding Retention During Interface Delete Events on page 24](#)
- [Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 54](#)
- *Delaying Removal of Access Routes and Access-Internal Routes After Graceful Routing Engine Switchover*

aggregate-clients (DHCP Local Server)

Syntax	aggregate-clients (merge replace);
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dynamic-profile profile-name],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile profile-name],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dynamic-profile profile-name],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile profile-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dynamic-profile profile-name],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile profile-name],</p> <p>[edit system services dhcp-local-server dynamic-profile profile-name],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> dynamic-profile profile-name]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Options merge and replace introduced in Junos OS Release 9.5.</p>
Description	<p>Specify that the router merge (chain) client attributes such as firewall filters and CoS attributes or replace them when multiple client sessions exist on the same underlying VLAN.</p> <p>Not supported for IP demux subscriber interfaces.</p>
Options	<p>merge—Aggregate multiple clients attributes for the same subscriber (logical interface)</p> <p>replace—Replace the entire logical interface whenever a new client logs in to the network using the same VLAN logical interface</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68

attempts (DHCP Local Server)

Syntax	<code>attempts attempt-count;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure how many attempts are made to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces before reconfiguration is considered to have failed. A group configuration takes precedence over a DHCP local server configuration.
Options	<p><i>attempt-count</i>—Maximum number of attempts.</p> <p>Range: 1 through 10</p> <p>Default: 8</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 60

authentication (DHCP Local Server)

Syntax	<pre> authentication { password <i>password-string</i>; username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; } }</pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay or DHCP local server configuration.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40

bfd

Syntax	<pre> bfd { version (0 1 automatic); minimum-interval <i>milliseconds</i>; minimum-receive-interval <i>milliseconds</i>; multiplier <i>number</i>; no-adaptation; transmit-interval { minimum-interval <i>milliseconds</i>; threshold <i>milliseconds</i>; } detection-time { threshold <i>milliseconds</i>; } session-mode (automatic multihop singlehop); holddown-interval <i>milliseconds</i>; } </pre>
Hierarchy Level	<p>[edit system services dhcp-local-server liveness-detection method], [edit system services dhcp-local-server dhcpv6 liveness-detection method], [edit forwarding-options dhcp-relay liveness-detection method], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients


circuit-type (DHCP Local Server)

Syntax	circuit-type;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40

clear-on-abort (DHCP Local Server)

Syntax	clear-on-abort;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Delete all DHCP clients or only the DHCP clients serviced by the specified group of interfaces when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success. A group configuration takes precedence over a DHCP local server configuration.
Default	Restores the original client configuration when reconfiguration fails.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 61

client-discover-match (DHCP Local Server)

Syntax	client-discover-match (option60-and-option82 incoming-interface);
Hierarchy Level	<p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ... overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Option incoming-interface introduced in Junos OS Release 13.3.</p>
Description	Configure the match criteria DHCP local server uses to uniquely identify DHCP subscribers or clients when primary identification fails. The options are mutually exclusive.
Options	<p>incoming-interface—Allow only one client device to connect on the interface. If the client device changes, the router deletes the existing client binding and creates a binding for the newly connected device.</p>
<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; text-align: center; margin-right: 10px;">  </div> <div> <p>NOTE: The overrides client-discover-match incoming-interface configuration deletes and replaces the existing binding when a new device connects. This action differs from the overrides interface-client-limit 1 statement, which retains the existing binding and rejects the newly connected client.</p> </div> </div>	
<p>option60-and-option82—Use option 60 and option 82 information to identify subscribers.</p>	
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Local Server Overview on page 4 • Overriding Default DHCP Local Server Configuration Settings on page 48 • DHCP Auto Logout Overview on page 22 • Allowing Only One DHCP Client Per Interface on page 50

client-id (DHCP Local Server)

Syntax	client-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the DHCPv6 Client-ID option (option 1) in the client PDU name is concatenated with the username during the subscriber authentication or client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 72

delegated-pool (DHCP Local Server)

Syntax	<code>delegated-pool <i>pool-name</i>;</code>
Hierarchy Level	<code>[edit system services dhcp-local-server dhcpv6 overrides],</code> <code>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</code> <code>[edit system services dhcp-local-server dhcpv6 group group-name interface <i>interface-name</i></code> <code>overrides],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system</code> <code>services dhcp-local-server dhcpv6 ...],</code> <code>[edit logical-systems <i>logical-system-name</i> system services system services dhcp-local-server</code> <code>dhcpv6 ...],</code> <code>[edit routing-instances <i>routing-instance-name</i> system services system services</code> <code>dhcp-local-server dhcpv6 ...]</code>
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify the address pool that assigns the IA_PD address. A pool specified by RADIUS VSA 26-161 takes precedence over the pool specified by this delegated-pool statement.
Options	<i>pool-name</i> —Name of the address-assignment pool.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 56• Overriding Default DHCP Local Server Configuration Settings on page 48

delimiter (DHCP Local Server)

Syntax	<code>delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the character used as the delimiter between the concatenated components of the username.
Options	<i>delimiter-character</i> —Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 40](#)

detection-time

Syntax	<pre>detection-time { threshold milliseconds; }</pre>
Hierarchy Level	[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Enable failure detection. The BFD failure detection timers are adaptive and can be adjusted to be faster or slower. For example, the timers can adapt to a higher value if the adjacency fails, or a neighbor can negotiate a higher value for a timer than the one configured.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

dhcp-local-server

```
Syntax  dhcp-local-server {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dhcpv6 {
        authentication {
            ...
        }
        group group-name {
            authentication {
                ...
            }
            interface interface-name {
                exclude;
                liveness-detection {
                    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                    method {
                        bfd {
                            version (0 | 1 | automatic);
                            minimum-interval milliseconds;
                            minimum-receive-interval milliseconds;
                            multiplier number;
                            no-adaptation;
                            transmit-interval {
                                minimum-interval milliseconds;
                                threshold milliseconds;
                            }
                        }
                        detection-time {
                            threshold milliseconds;
                        }
                    }
                    session-mode (automatic | multihop | singlehop);
                    holddown-interval milliseconds;
                }
            }
        }
    }
    overrides {
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
    }
}
```

```

    }
    rapid-commit;
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        bfd {
            version (0 | 1 | automatic);
            minimum-interval milliseconds;
            minimum-receive-interval milliseconds;
            multiplier number;
            no-adaptation;
            transmit-interval {
                minimum-interval milliseconds;
                threshold milliseconds;
            }
            detection-time {
                threshold milliseconds;
            }
            session-mode (automatic | multihop | singlehop);
            holddown-interval milliseconds;
        }
    }
}
}
overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {

```

```

        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}
duplicate-clients-in-subnet (incoming-interface | option-82);
dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
forward-snooped-clients (all-interfaces | configured-interfaces |
    non-configured-interfaces);
group group-name {
    authentication {
        ...
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
        primary-profile-name>;
    interface interface-name {
        exclude;
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                bfd {
                    version (0 | 1 | automatic);
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                    detection-time {
                        threshold milliseconds;
                    }
                }
                session-mode (automatic | multihop | singlehop);
                holddown-interval milliseconds;
            }
        }
    }
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
}

```

```

    }
  }
  requested-ip-network-match subnet-mask
  route-suppression;
  service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
    }
    session-mode (automatic | multihop | singlehop);
    holddown-interval milliseconds;
  }
}
}
overrides {
  client-discover-match (option60-and-option82 | incoming-interface);
  interface-client-limit number;
  process-inform {
    pool pool-name;
  }
}
pool-match-order {
  external-authority;
  ip-address-first;
  option-82;
}
reconfigure {
  attempts attempt-count;
  clear-on-abort;
  strict;
  timeout timeout-value;
  token token-value;
  trigger {
    radius-disconnect;
  }
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}

```


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

Release Information Statement introduced in Junos OS Release 9.0.
 Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch and enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and so is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the **[edit forwarding-options helpers]** hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The **dhcpv6** stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.



NOTE: When you configure the **dhcp-local-server** statement at the routing instance hierarchy level, you must use a routing instance type of **virtual-router**.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Extended DHCP Local Server Overview on page 4](#)
- [DHCPv6 Local Server Overview on page 10](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

dhcpv6 (DHCP Local Server)

```
Syntax  dhcpv6 {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    group group-name {
        authentication {
            ...
        }
        interface interface-name {
            exclude;
            liveness-detection {
                failure-action (clear-binding | clear-binding-if-interface-up | log-only);
                method {
                    bfd {
                        version (0 | 1 | automatic);
                        minimum-interval milliseconds;
                        minimum-receive-interval milliseconds;
                        multiplier number;
                        no-adaptation;
                        transmit-interval {
                            minimum-interval milliseconds;
                            threshold milliseconds;
                        }
                        detection-time {
                            threshold milliseconds;
                        }
                    }
                    session-mode (automatic | multihop | singlehop);
                    holddown-interval milliseconds;
                }
            }
        }
        overrides {
            interface-client-limit number;
            multi-address-embedded-option-response;
            process-inform {
                pool pool-name;
            }
            rapid-commit;
        }
        service-profile dynamic-profile-name;
        trace;
    }
}
```

```

    upto upto-interface-name;
  }
  overrides {
    delegated-pool;
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
      pool pool-name;
    }
    rapid-commit;
  }
  route-suppression;
  service-profile dynamic-profile-name;
}
liveness-detection {
  failure-action (clear-binding | clear-binding-if-interface-up | log-only);
  method {
    bfd {
      version (0 | 1 | automatic);
      minimum-interval milliseconds;
      minimum-receive-interval milliseconds;
      multiplier number;
      no-adaptation;
      transmit-interval {
        minimum-interval milliseconds;
        threshold milliseconds;
      }
      detection-time {
        threshold milliseconds;
      }
      session-mode (automatic | multihop | singlehop);
      holddown-interval milliseconds;
    }
  }
}
overrides {
  delegated-pool;
  interface-client-limit number;
  multi-address-embedded-option-response;
  process-inform {
    pool pool-name;
  }
  rapid-commit;
  reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
      radius-disconnect;
    }
  }
}
reconfigure {
  attempts attempt-count;

```

```
clear-on-abort;
strict;
timeout timeout-value;
token token-value;
trigger {
    radius-disconnect;
}
}
requested-ip-network-match subnet-mask;
route-suppression;
service-profile dynamic-profile-name;
}
```

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services [dhcp-local-server](#)],
[edit logical-systems *logical-system-name* system services [dhcp-local-server](#)],
[edit routing-instances *routing-instance-name* system services [dhcp-local-server](#)],
[edit system services [dhcp-local-server](#)]

Release Information Statement introduced in Junos OS Release 9.6.
Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Configure DHCPv6 local server options on the router or switch and enable the router or switch to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately.

Required Privilege Level system—To view this statement in the configuration.
system-control—To add this statement to the configuration.

Related Documentation


- [DHCPv6 Local Server Overview on page 10](#)

domain-name (DHCP Local Server)

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Options	<i>domain-name-string</i> —Domain name formatted string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 40](#)

duplicate-clients-in-subnet (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>duplicate-clients-in-subnet (incoming-interface option-82);</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]</p>
Release Information	Statement introduced in Junos OS Release 13.3.
Description	Configure how the router distinguishes between duplicate clients in the same subnet. Duplicate clients are defined as clients that have the same hardware address or client ID.
<div>  <p>NOTE: You must configure the <code>duplicate-clients-in-subnet</code> statement identically for both <code>[forwarding-options dhcp-relay]</code> and <code>[system services dhcp-local-server]</code> hierarchy levels.</p> </div>	
Options	<p>incoming-interface—Use the incoming interface information in packets to differentiate between duplicate clients.</p> <p>option-82—Use the option 82 information to differentiate between duplicate clients.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration.</p> <p>interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCP Duplicate Client In Subnet Overview on page 15 • Guidelines for Configuring Support for DHCP Duplicate Clients on page 41 • Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Their Incoming Interfaces on page 43 • Configuring the Router to Distinguish Between DHCP Duplicate Clients Based on Option 82 Information on page 42

dynamic-profile (DHCP Local Server)

Syntax	<pre>dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); use-primary <i>primary-profile-name</i>; }</pre>
Hierarchy Level	<pre>[edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options aggregate-clients and use-primary introduced in Junos OS Release 9.3.</p> <p>Support at the [edit ... interface] hierarchy levels introduced in Junos OS Release 11.2.</p>
Description	Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.
Options	<p>profile-name—Name of the dynamic profile.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68 • Configuring a Default Subscriber Service on page 45

enforce-strict-scale-limit-license (Subscriber Management)

Syntax	enforce-strict-scale-limit-license;
Hierarchy Level	[edit system services subscriber-management]
Release Information	Statement introduced in Junos OS Release 11.2.
Description	Configure the router to strictly enforce the subscriber scaling license, and to not allow the normal grace period. No additional subscribers are allowed to log in after the number of subscribers reaches the maximum allowed for the license.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 54

external-authority

Syntax	external-authority;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order]
Release Information	Statement introduced in Junos OS Release 10.0. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment. When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74• Extended DHCP Local Server Overview on page 4• Address-Assignment Pools Overview on page 25

failure-action

Syntax	failure-action (clear-binding clear-binding-if-interface-up log-only);
Hierarchy Level	[edit system services dhcp-local-server liveness-detection], [edit system services dhcp-local-server dhcpv6 liveness-detection], [edit forwarding-options dhcp-relay liveness-detection], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the action the router (or switch) takes when a liveness detection failure occurs.
Options	<p>clear-binding—The client session is cleared when a liveness detection failure occurs.</p> <p>clear-binding-if-interface-up—The client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up.</p> <p>log-only—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.</p>
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • DHCP Liveness Detection Overview on page 64 • Configuring Detection of DHCP Local Server Client Connectivity on page 65 • Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

forward-snooped-clients (DHCP Local Server)

Syntax	forward-snooped-clients (all-interfaces configured-interfaces non-configured-interfaces);
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]
Release Information	Statement introduced in Junos OS Release 10.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure how the DHCP local server handles DHCP snooped packets on specific interfaces.
Options	all-interfaces —Perform the action on all interfaces. configured-interfaces —Perform the action only on configured interfaces. non-configured-interfaces —Perform the action only on nonconfigured interfaces.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• DHCP Snooping Support on page 21• Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 70

group (DHCP Local Server)

```
Syntax  group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            relay-agent-interface-id
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary
    primary-profile-name>;
    interface interface-name {
        exclude;
        overrides {
            client-discover-match (option60-and-option82 | incoming-interface);
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit;
        }
        service-profile dynamic-profile-name;
        trace;
        upto upto-interface-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            bfd {
                version (0 | 1 | automatic);
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
            }
            detection-time {
                threshold milliseconds;
            }
        }
        session-mode (automatic | multihop | singlehop);
    }
}
```

```

        holddown-interval milliseconds;
    }
}
overrides {
    client-discover-match (option60-and-option82 | incoming-interface);
    delegated-pool;
    interface-client-limit number;
    process-inform {
        pool pool-name;
    }
    rapid-commit;
}
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
route-suppression;
service-profile dynamic-profile-name;
}

```


Hierarchy Level	<p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.
Options	<p>group-name—Name of the group.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Extended DHCP Local Server Overview on page 4](#)
 - [Grouping Interfaces with Common DHCP Configurations on page 45](#)
 - [Using External AAA Authentication Services with DHCP on page 40](#)
 - [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68](#)
 - [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

holddown-interval

Syntax	<code>holddown-interval <i>milliseconds</i>;</code>
Hierarchy Level	[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.
Options	<i>milliseconds</i> —Interval specifying how long a BFD session must remain up before a state change notification is sent. Range: 0 through 255,000 Default: 0
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

interface (DHCP Local Server)

Syntax	<pre> interface <i>interface-name</i> { exclude; overrides { client-discover-match (option60-and-option82 incoming-interface); interface-client-limit <i>number</i>; rapid-commit; } service-profile <i>dynamic-profile-name</i>; trace; upto <i>upto-interface-name</i>; } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server <i>group group-name</i>], [edit system services dhcp-local-server <i>dhcpv6 group group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services <i>dhcp-local-server ...</i>], [edit logical-systems <i>logical-system-name</i> system services <i>dhcp-local-server ...</i>], [edit routing-instances <i>routing-instance-name</i> system services <i>dhcp-local-server ...</i>] </pre>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options upto and exclude introduced in Junos OS Release 9.1.</p>
Description	<p>Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP local server is enabled. You can repeat the interface <i>interface-name</i> statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. Also, you cannot use an interface that is being used by the DHCP relay agent.</p>
<div style="display: flex; align-items: flex-start;"> <div style="flex: 1; text-align: center; margin-right: 10px;">  </div> <div> <p>NOTE: DHCP values are supported in Integrated Routing and Bridging (IRB) configurations. When you configure an IRB interface in a network that is using DHCP, the DHCP information (for example, authentication, address assignment, and so on) is propagated in the associated bridge domain. This enables the DHCP server to configure client IP addresses residing within the bridge domain. IRB currently only supports static DHCP configurations. For additional information about how to configure IRB, see <i>Configuring Integrated Routing and Bridging for Bridge Domains</i>.</p> </div> </div>	
Options	<p>exclude—Exclude an interface or a range of interfaces from the group. This option and the overrides option are mutually exclusive.</p> <p><i>interface-name</i>—Name of the interface. You can repeat this option multiple times.</p> <p><i>upto-interface-name</i>—Upper end of the range of interfaces; the lower end of the range is the <i>interface-name</i> entry. The interface device name of the <i>upto-interface-name</i> must be the same as the device name of the <i>interface-name</i>.</p>

The remaining statements are explained separately.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Extended DHCP Local Server Overview on page 4• Grouping Interfaces with Common DHCP Configurations on page 45• Using External AAA Authentication Services with DHCP on page 40

interface-client-limit (DHCP Local Server)

Syntax	<code>interface-client-limit <i>number</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group interface <i>interface-name</i> <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Set the maximum number of DHCP subscribers or DHCP clients per interface allowed for a specific group or for all groups. A group specification takes precedence over a global specification for the members of that group.
Default	No limit
Options	<i>number</i> —Maximum number of clients allowed.

Range: 1 through 500,000

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Specifying the Maximum Number of DHCP Clients Per Interface on page 49](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 48](#)

interface-delete (Subscriber Management or DHCP Client Management)

Syntax interface-delete;

Hierarchy Level [edit system services subscriber-management [maintain-subscriber](#)]

Release Information Statement introduced in Junos OS Release 11.1.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description On router—Configure the router to maintain, rather than log out, subscribers when the subscriber interface is deleted. By default, the router logs out subscribers when the subscriber interface is deleted.

On switch—Configure the switch to maintain rather than log out DHCP clients when the client interface is deleted. By default, the switch logs out DHCP clients when the client interface is deleted.

Required Privilege Level system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

Related Documentation

- [Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54](#)

interface-name (DHCP Local Server)

Syntax	interface-name;
Hierarchy Level	[edit system services dhcp-local-server authentication username-include], [edit system services dhcp-local-server dhcpv6 authentication username-include], [edit system services dhcp-local-server dhcpv6 group group-name authentication username-include], [edit system services dhcp-local-server group group-name authentication username-include] [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Required Privilege Level	interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Creating Unique Usernames for DHCP Clients on page 72

ip-address-first

Syntax	ip-address-first;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order],</p> <p>[edit system services dhcp-local-server pool-match-order]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.0.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Configure the extended DHCP local server to use the IP address method to determine which address-assignment pool to use. The local server uses the IP address in the gateway IP address if one is present in the DHCP client PDU. If no gateway IP address is present, the local server uses the IP address of the receiving interface to find the address-assignment pool. The DHCP local server uses this method by default when no method is explicitly specified.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74 • Extended DHCP Local Server Overview on page 4 • Address-Assignment Pools Overview on page 25 • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

lease-time-threshold (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>lease-time-threshold seconds;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> lease-time-validation],</code> <code>[edit logical-systems <i>logical-system-name</i> ...],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...],</code> <code>[edit routing-instances <i>routing-instance-name</i> ...],</code> <code>[edit system services dhcp-local-server lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 lease-time-validation],</code> <code>[edit system services dhcp-local-server group <i>group-name</i> lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> lease-time-validation]</code>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure the minimum DHCP lease time allowed in your subscriber access network. If a third-party DHCP server or address pool provides a client lease that is less than the configured threshold, the router performs the action specified by the violation-action statement.
Options	seconds —Minimum client lease time allowed. Range: 60 through 2,147,483,647 seconds
Required Privilege Level	system —To view this statement in the configuration. system-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring a DHCP Lease-Time Threshold on page 67

lease-time-validation (DHCP Local Server and DHCP Relay Agent)

Syntax	<pre>lease-time-validation { lease-time-threshold seconds; violation-action action; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group group-name], [edit forwarding-options dhcp-relay dhcpv6 group group-name], [edit logical-systems logical-system-name ...], [edit logical-systems logical-system-name routing-instances routing-instance-name...], [edit routing-instances routing-instance-name ...], [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server group group-name], [edit system services dhcp-local-server dhcpv6 group group-name]</pre>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	<p>Enable the lease-time validation feature on the router. You can then configure the lease-time threshold and an optional action to take when a lease-time violation occurs.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Lease-Time Threshold on page 67

liveness-detection

Syntax	<pre> liveness-detection { failure-action (clear-binding clear-binding-if-interface-up log-only); method { bfd { version (0 1 automatic); minimum-interval milliseconds; minimum-receive-interval milliseconds; multiplier number; no-adaptation; transmit-interval { minimum-interval milliseconds; threshold milliseconds; } detection-time { threshold milliseconds; } session-mode (automatic multihop singlehop); holddown-interval milliseconds; } } } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit system services dhcp-local-server group group-name], [edit system services dhcp-local-server dhcpv6 group group-name], [edit forwarding-options dhcp-relay group group-name], [edit forwarding-options dhcp-relay dhcpv6 group group-name] </pre>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure bidirectional failure detection timers and authentication criteria for static routes.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • DHCP Liveness Detection Overview on page 64 • Configuring Detection of DHCP Local Server Client Connectivity on page 65 • Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

logical-system-name (DHCP Local Server)

Syntax	logical-system-name;
Hierarchy Level	[edit system services dhcp-local-server authentication username-include], [edit system services dhcp-local-server dhcpv6 authentication username-include], [edit system services dhcp-local-server dhcpv6 group group-name authentication username-include], [edit system services dhcp-local-server group group-name authentication username-include] [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...] [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40


ltv-syslog-interval (System Process)

Syntax	ltv-syslog-interval <i>seconds</i> ;
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure how often the router logs consolidated syslog messages for DHCP lease-time violations.
Options	seconds —Time interval that specifies how often the router logs syslog messages. Range: 600 through 86,400 seconds
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Lease-Time Threshold on page 67 • <i>processes</i>

mac-address (DHCP Local Server)

Syntax	mac-address;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 40

maintain-subscriber (Subscriber Management)

Syntax	<code>maintain-subscriber { interface-delete; }</code>
Hierarchy Level	[edit system services subscriber-management]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	Configure the router to maintain, rather than log out, subscribers when the specified type of event occurs (such as when an interface is deleted).
<div>  <p>NOTE: The <code>maintain-subscriber</code> statement and <code>remove-when-no-subscribers</code> statement are mutually exclusive. You cannot specify that dynamically configured VLAN interfaces are removed when no subscribers exist when the router is also configured to maintain subscribers.</p> </div>	
The remaining statement is explained separately.	
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54

method

Syntax	<pre> method { bfd { version (0 1 automatic); minimum-interval <i>milliseconds</i>; minimum-receive-interval <i>milliseconds</i>; multiplier <i>number</i>; no-adaptation; transmit-interval { minimum-interval <i>milliseconds</i>; threshold <i>milliseconds</i>; } detection-time { threshold <i>milliseconds</i>; } session-mode (automatic multihop singlehop); holddown-interval <i>milliseconds</i>; } } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server <i>liveness-detection</i>], [edit system services dhcp-local-server dhcpv6 <i>liveness-detection</i>], [edit forwarding-options dhcp-relay <i>liveness-detection</i>], [edit forwarding-options dhcp-relay dhcpv6 <i>liveness-detection</i>], [edit system services dhcp-local-server group <i>group-name</i> <i>liveness-detection</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> <i>liveness-detection</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> <i>liveness-detection</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> <i>liveness-detection</i>] </pre>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the liveness detection method.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

minimum-interval

Syntax	<code>minimum-interval <i>milliseconds</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd transmit-interval], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd transmit-interval]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the minimum intervals at which the local routing device transmits hello packets and then expects to receive a reply from a neighbor with which it has established a BFD session. This value represents the minimum interval at which the local routing device transmits hello packets as well as the minimum interval that the routing device expects to receive a reply from a neighbor with which it has established a BFD session. Optionally, instead of using this statement, you can specify the minimum transmit and receive intervals separately using the transmit-interval minimal-interval and minimum-receive-interval statements.</p>
Options	<p><i>milliseconds</i> — Specify the minimum interval value for BFD liveliness detection.</p> <p>Range: 1 through 255,000</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

minimum-receive-interval

Syntax	<code>minimum-receive-interval <i>milliseconds</i>;</code>
Hierarchy Level	<code>[edit system services dhcp-local-server liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],</code> <code>[edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options</code> <code> dhcp-relay dhcpv6 liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method</code> <code> bfd],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method</code> <code> bfd]</code>
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the minimum interval at which the local routing device (or switch) must receive a reply from a neighbor with which it has established a BFD session.
Options	<i>milliseconds</i> — Specify the minimum receive interval value. Range: 1 through 255,000
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

multi-address-embedded-option-response (DHCP Local Server)

Syntax	multi-address-embedded-option-response;
Hierarchy Level	<p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services system services dhcp-local-server dhcpv6 ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services system services dhcp-local-server dhcpv6 ...]</p>
Release Information	Statement introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases. Statement supported in Junos OS Release 13.3 and later releases. (Not supported in Junos OS 13.1 and 13.2.)
Description	Configure DHCPv6 local server to return the DNS server address (DHCPv6 attribute 23) as a suboption in the respective IA_NA or IA_PD headers.
Default	DHCPv6 local server returns the DNS server address as a global DHCPv6 option.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Overriding How the DNS Server Address Is Returned in a DHCPv6 Multiple Address Environment on page 57 • Overriding Default DHCP Local Server Configuration Settings on page 48

multiplier

Syntax	<code>multiplier <i>number</i>;</code>
Hierarchy Level	<code>[edit system services dhcp-local-server liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd],</code> <code>[edit forwarding-options dhcp-relay liveness-detection method bfd],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd],</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method</code> <code>bfd],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method</code> <code>bfd]</code>
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the number of hello packets not received by the neighbor before Bidirectional Forwarding Detection (BFD) declares the neighbor down.
Options	number —Maximum allowable number of hello packets missed by the neighbor. Range: 1 through 255 Default: 3
Required Privilege Level	routing —To view this statement in the configuration. routing-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

no-adaptation

Syntax	no-adaptation;
Hierarchy Level	[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure Bidirectional Forwarding Detection (BFD) sessions to not adapt to changing network conditions.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • <i>Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients</i>

option-60 (DHCP Local Server)

Syntax	option-60;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the payload of Option 60 (Vendor Class Identifier) from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Using External AAA Authentication Services with DHCP on page 40

option-82 (DHCP Local Server Authentication)

Syntax	<code>option-82 <circuit-id> <remote-id>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Specify the type of Option 82 information from the client PDU that is concatenated with the username during the subscriber authentication or DHCP client authentication process. You can specify either, both, or neither of the Agent Circuit ID and Agent Remote ID suboptions. If you specify both, the Agent Circuit ID is supplied first, followed by a delimiter, and then the Agent Remote ID. If you specify that neither suboption is supplied, the raw payload of Option 82 from the PDU is concatenated to the username.</p>
Options	<p>circuit-id—(Optional) Agent Circuit ID suboption (suboption 1).</p> <p>remote-id—(Optional) Agent Remote ID suboption (suboption 2).</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40

option-82 (DHCP Local Server Pool Matching)

Syntax	option-82;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server pool-match-order], [edit system services dhcp-local-server pool-match-order]
Release Information	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the extended DHCP local server to use the option 82 value in the DHCP client DHCP PDU together with the ip-address-first method to determine which address-assignment pool to use. You must configure the ip-address-first statement before configuring the option-82 statement. The DHCP local server first determines which address-assignment pool to use based on the ip-address-first method. Then, the local server matches the option 82 value in the client PDU with the option 82 configuration in the address-assignment pool. This statement is supported for IPv4 address-assignment pools only.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74• Extended DHCP Local Server Overview on page 4• Address-Assignment Pools Overview on page 25

overrides (DHCP Local Server)

Syntax	<pre> overrides { client-discover-match (option60-and-option82 incoming-interface); delegated-pool; interface-client-limit <i>number</i>; multi-address-embedded-option-response; process-inform { pool <i>pool-name</i>; } rapid-commit; } </pre>
Hierarchy Level	<pre> [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Override the default configuration settings for the extended DHCP local server. Specifying the overrides statement with no subordinate statements removes all DHCP local server overrides at that hierarchy level.</p> <ul style="list-style-type: none"> To override global 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 configuration options for a named group of interfaces, include the statements at the [edit system services dhcp-local-server group <i>group-name</i>] hierarchy level. To override configuration options for a specific interface within a named group of interfaces, include the statements at the [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>] hierarchy level. Use the [edit system services dhcp-local-server dhcpv6] hierarchy level to override DHCPv6 configuration options. <p>The remaining statements are explained separately.</p> <p>The interface-client-limit statement is not supported in the [edit system services dhcp-local-server dhcpv6] hierarchy level.</p>

The [delegated-pool](#), [multi-address-embedded-option-response](#), and the [rapid-commit](#) statements are supported in the `[edit system services dhcp-local-server dhcpv6 ...]` hierarchy level only.

Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Extended DHCP Local Server Overview on page 4• Overriding Default DHCP Local Server Configuration Settings on page 48• Deleting DHCP Local Server and DHCP Relay Override Settings on page 58• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>
------------------------------	--

password (DHCP Local Server)

Syntax	<code>password password-string;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication],</p> <p>[edit system services dhcp-local-server authentication],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit system services dhcp-local-server group group-name authentication]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40

pool (DHCP Local Server Overrides)

Syntax `pool pool-name;`

Hierarchy Level [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit logical-systems *logical-system-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 group *group-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server dhcpv6 group *group-name* interface *interface-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server group *group-name* overrides [process-inform](#)],
 [edit system services dhcp-local-server group *group-name* interface *interface-name* overrides [process-inform](#)]

Release Information Statement introduced in Junos OS Release 11.4.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.

Description	Configure DHCP or DHCPv6 local server to reply to DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) with information taken from the specified pool without interacting with AAA.
Options	pool-name —Name of the address pool, which must be configured within family inet for DHCP local server and within family inet6 for DHCPv6 local server.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Enabling Processing of Client Information Requests on page 55 • Overriding Default DHCP Local Server Configuration Settings on page 48

pool-match-order

Syntax	<pre>pool-match-order { external-authority; ip-address-first; option-82; }</pre>
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server], [edit system services dhcp-local-server]
Release Information	Statement introduced in Junos OS Release 9.0. Statement introduced in Junos OS Release 12.1.
Description	Configure the order in which the DHCP local server uses information in the DHCP client PDU to determine how to obtain an address for the client. The remaining statements are explained separately.
Default	DHCP local server uses the ip-address-first method to determine which address pool to use.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 74 • Extended DHCP Local Server Overview on page 4 • Configuring a DHCP Server on Switches (CLI Procedure)

process-inform

Syntax	<pre>process-inform { pool pool-name; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit system services dhcp-local-server overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> overrides],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Enable the processing of DHCP information request messages (DHCPINFORM for DHCPv4 and INFORMATION-REQUEST for DHCPv6) sent from the client to request DHCP options. For DHCP local servers, the messages are also passed to the configured server list.</p>

The remaining statement is explained separately.

Default	Information request messages are not processed.
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Enabling Processing of Client Information Requests on page 55• Overriding Default DHCP Local Server Configuration Settings on page 48• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

radius-disconnect (DHCP Local Server)

Syntax	radius-disconnect;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure trigger],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure trigger],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure trigger]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces to be reconfigured when a RADIUS-initiated disconnect is received by the DHCP client or group of clients. A group configuration takes precedence over a DHCP local server configuration.
Default	The client is deleted when a RADIUS-initiated disconnect is received.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 61

rapid-commit (DHCPv6 Local Server)

Syntax	rapid-commit;
Hierarchy Level	<p>[edit system services dhcp-local-server dhcpv6 overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name overrides],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure DHCPv6 local server to recognize the Rapid Commit option (DHCPv6 option 14) in DHCPv6 solicit messages sent from the DHCPv6 client. When rapid commit is enabled for both DHCPv6 local server and the DHCPv6 client, a two-message handshake is used instead of the standard four-message handshake. You can enable rapid commit support on DHCPv6 local server globally, for a named group, or for a specific interface.</p>
Default	Rapid commit support is not enabled.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Enabling DHCPv6 Rapid Commit Support on page 57 • Overriding Default DHCP Local Server Configuration Settings on page 48

reconfigure (DHCP Local Server)

Syntax

```
reconfigure {
    attempts attempt-count;
    clear-on-abort;
    strict;
    timeout timeout-value;
    token token-value;
    trigger {
        radius-disconnect;
    }
}
```

Hierarchy Level

[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services **dhcp-local-server**],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6**],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server **group** *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit logical-systems *logical-system-name* system services **dhcp-local-server**],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **dhcpv6**],
 [edit logical-systems *logical-system-name* system services dhcp-local-server **group** *group-name*],
 [edit logical-systems *logical-system-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit routing-instances *routing-instance-name* system services **dhcp-local-server**],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **dhcpv6**],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server **group** *group-name*],
 [edit routing-instances *routing-instance-name* system services dhcp-local-server dhcpv6 **group** *group-name*],
 [edit system services **dhcp-local-server**],
 [edit system services dhcp-local-server **dhcpv6**],
 [edit system services dhcp-local-server **group** *group-name*],
 [edit system services dhcp-local-server dhcpv6 **group** *group-name*]

Release Information

Statement introduced in Junos OS Release 10.0.
 Support at the [edit ... **dhcpv6** ...] hierarchy levels introduced in Junos OS Release 10.4.
 Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description

Enable dynamic reconfiguration triggered by the DHCP local server of all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. A group configuration takes precedence over a DHCP local server configuration. The **strict** statement is available only for DHCPv6.

The remaining statements are explained separately.

Required Privilege Level

system—To view this statement in the configuration.
 system-control—To add this statement to the configuration.

- Related Documentation**
- [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)
 - [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

relay-agent-interface-id (DHCP Local Server)

Syntax	relay-agent-interface-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the DHCPv6 Relay Agent Interface-ID option (option 18) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 72

relay-agent-remote-id (DHCP Local Server)

Syntax	relay-agent-remote-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>For MX Series routers only, enterprise-id and remote-id options introduced in Junos OS Release 12.3R3.</p> <p>For MX Series routers only, the enterprise-id and remote-id options are obsoleted starting in Junos OS Releases 12.3R7, 13.2R4, 13.3R2, and 14.1R1.</p>
Description	Specify that the DHCPv6 Relay Agent Remote-ID option (option 37) in the client PDU name is concatenated with the username during the subscriber authentication or DHCP client authentication process. In order to generate an ASCII version of the username, the router concatenates only the remote-id portion of option 37 to the username, and ignores the enterprise number.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 72


relay-agent-subscriber-id (DHCP Local Server)

Syntax	relay-agent-subscriber-id;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	Statement introduced in Junos OS Release 9.6.
Description	Specify that the DHCPv6 Relay Agent Subscriber-ID option (option 38) in the client PDU name is concatenated with the username during the subscriber authentication process.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Creating Unique Usernames for DHCP Clients on page 72

requested-ip-network-match (DHCP Local Server)

Syntax	<code>requested-ip-network-match <i>subnet-mask</i>;</code>
Hierarchy Level	<code>[edit system services dhcp-local-server]</code> <code>[edit system services dhcp-local-server dhcpv6],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system</code> <code>services dhcp-local-server ...],</code> <code>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</code> <code>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</code>
Release Information	Statement introduced in Junos OS Release 12.2.
Description	Configure the subnet to which the DHCP local server matches the requested IP address (IPv6 address for DHCPv6 local server). The server accepts and uses the active client's requested address for address assignment only when the requested address and the IP address of the DHCP server interface (or IPv6 address of the DHCPv6 local server) are in the same subnet. The server accepts and uses the passive client's requested address for address assignment only when the requested address and the address of the relay interface are in the same subnet.
Options	<i>subnet-mask</i> —Length of the subnet mask. Range: <ul style="list-style-type: none">• DHCP: 0 through 15• DHCPv6: 0 through 127 Default: <ul style="list-style-type: none">• DHCP: 8• DHCPv6: 16
Required Privilege Level	<code>system</code> —To view this statement in the configuration. <code>system-control</code> —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Specifying the Subnet for DHCP Client Address Assignment on page 75

route-suppression (DHCP Local Server and Relay Agent)

Syntax	route-suppression (access access-internal destination);
Hierarchy Level	[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> ...], [edit routing-instances <i>routing-instance-name</i> ...], [edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>]
Release Information	Statement introduced in Junos OS Release 13.2.
Description	Configure the jdhcpd process to suppress the installation of access, access-internal, or destination routes during client binding.
<div>  <p>NOTE: 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.</p> </div>	
Options	<p>access—(DHCPv6 only) Suppress installation of access routes. You can use the access and access-internal options in the same statement for DHCPv6.</p> <p>access-internal—In a DHCPv4 hierarchy, suppress installation of both access-internal and destination routes. In a DHCPv6 hierarchy, suppress access-internal routes only. Can be configured in the same statement with the access option.</p> <p>destination—(DHCPv4 only) Suppress installation of destination routes. This option and the access-internal option are mutually exclusive; however, the access-internal option also suppresses destination routes.</p>
Required Privilege Level	system—To view this statement in the configuration. system-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 52

routing-instance-name (DHCP Local Server)

Syntax	routing-instance-name;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify that the routing instance name be concatenated with the username during the subscriber authentication or DHCP client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 40](#)

service-profile (DHCP Local Server)

Syntax	<code>service-profile <i>dynamic-profile-name</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit system services dhcp-local-server group <i>group-name</i>], [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.2.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Specify the default subscriber service or DHCP client management service, which is activated when the subscriber or client logs in and no other service is activated by a RADIUS server or a provisioning server.</p> <ul style="list-style-type: none"> • To specify the default service for all DHCP local server clients, include the service-profile statement at the [edit system services dhcp-local-server] hierarchy level. • To specify the default service for a named group of interfaces, include the service-profile statement at the [edit system services dhcp-local-server group <i>group-name</i>] hierarchy level. • To specify the default service for a particular interface within a named group of interfaces, include the service-profile statement at the [edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>] hierarchy level. • For DHCPv6 clients, use the service-profile statement at the [edit system services dhcp-local-server dhcpv6] hierarchy level.
Options	<i>dynamic-profile-name</i> —Name of the dynamic profile that defines the service.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Local Server Overview on page 4 • Default Subscriber Service Overview on page 14 • Configuring a Default Subscriber Service on page 45

session-mode

Syntax	session-mode (automatic multihop singlehop);
Hierarchy Level	[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd]
Release Information	Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Configure the session mode.
Options	automatic —Configure single-hop BFD sessions if the peer is directly connected to the router interface and multihop BFD sessions if the peer is not directly connected to the router interface. multihop —Configure multihop BFD sessions. single-hop —Configure single hop BFD sessions.
Required Privilege Level	routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83• <i>Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients</i>


strict (DHCP Local Server)

Syntax	strict;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify whether the server denies a client to bind when the client does not indicate that it accepts reconfigure messages. This feature is available only for DHCPv6.
Default	Accept solicit messages from clients that do not support reconfiguration and permit them to bind.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 62


subscriber-management (Subscriber Management)

Syntax	<pre>subscriber-management { enforce-strict-scale-limit-license; gres-route-flush-delay; maintain-subscriber { interface-delete; } traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } }</pre>
Hierarchy Level	[edit system services]
Release Information	Statement introduced in Junos OS Release 11.1.
Description	<p>Configure global services for subscriber management, such as maintaining subscribers and tracing operations.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Configuring the Router to Strictly Enforce the Subscriber Scaling License on page 54• <i>Delaying Removal of Access Routes and Access-Internal Routes After Graceful Routing Engine Switchover</i>• Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54• <i>Tracing Subscriber Management Database Operations for Subscriber Access</i>

threshold (detection-time)

Syntax	<code>threshold <i>milliseconds</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server liveness-detection method bfd detection-time], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd detection-time], [edit forwarding-options dhcp-relay liveness-detection method bfd detection-time], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd detection-time], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd detection-time], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd detection-time], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd detection-time], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd detection-time]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the threshold for the adaptation of the detection time. When the BFD session detection time adapts to a value equal to or greater than the threshold, a single trap and a single system log message are sent.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The threshold time must be greater than or equal to the <code>minimum-interval</code> or the <code>minimum-receive-interval</code>.</p> </div> </div>	
Options	<p><i>milliseconds</i>— Value for the detection time adaptation threshold.</p> <p>Range: 1 through 255,000</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

threshold (transmit-interval)

Syntax	<code>threshold <i>milliseconds</i>;</code>
Hierarchy Level	<p>[edit system services dhcp-local-server liveness-detection method bfd transmit-interval],</p> <p>[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval],</p> <p>[edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd transmit-interval],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd transmit-interval],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd transmit-interval],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd transmit-interval],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd transmit-interval]</p>
Release Information	Statement introduced in Junos OS Release 12.1.
Description	Specify the threshold for detecting the adaptation of the transmit interval. When the BFD session transmit interval adapts to a value greater than the threshold, a single trap and a single system message are sent.
Options	<p><i>milliseconds</i> — Threshold value.</p> <p>Range: 0 through 4,294,967,295 ($2^{32} - 1$)</p>
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The threshold value specified in the <code>threshold</code> statement must be greater than the value specified in the <code>minimum-interval</code> statement for the <code>transmit-interval</code> statement.</p> </div> </div>	
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

timeout (DHCP Local Server)

Syntax	<code>timeout <i>timeout-value</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	Configure the initial value in seconds between attempts to reconfigure all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.
Options	<p><i>timeout-value</i>—Initial retry timeout value.</p> <p>Range: 1 through 10 seconds</p> <p>Default: 2 seconds</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 60

token (DHCP Local Server)

Syntax	<code>token <i>token-value</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	<p>Configure a plain-text token for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces. The token enables rudimentary entity authentication to protect against inadvertently instantiated DHCP servers. A null token (empty string) indicates that the configuration token functionality is not enabled. A group configuration takes precedence over a DHCP local server configuration. For more information about tokens, see RFC 3118, <i>Authentication for DHCP Messages</i>, section 4.</p>
Options	<p><i>token-value</i>—Plain-text alphanumeric string.</p> <p>Default: null (empty string)</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 Configuring a Token for DHCP Local Server Authentication on page 62

transmit-interval

Syntax	<pre>transmit-interval { threshold milliseconds; minimum-interval milliseconds; }</pre>
Hierarchy Level	<p>[edit system services dhcp-local-server liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd], [edit forwarding-options dhcp-relay liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method bfd]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the Bidirectional Forwarding Detection (BFD) transmit interval.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>routing—To view this statement in the configuration. routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

trigger (DHCP Local Server)

Syntax	<pre>trigger { radius-disconnect; }</pre>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 reconfigure],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> reconfigure],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.</p>
Description	<p>Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.</p> <p>The remaining statement is explained separately.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58 • Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 61 • radius-disconnect on page 152

use-primary (DHCP Local Server)

Syntax	<code>use-primary <i>primary-profile-name</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dynamic-profile <i>profile-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dynamic-profile <i>profile-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> dynamic-profile <i>profile-name</i>],</p> <p>[edit system services dhcp-local-server dynamic-profile <i>profile-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> dynamic-profile <i>profile-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile is instantiated when the first subscriber or DHCP client logs in. Subsequent subscribers (or clients) are not assigned the primary dynamic profile; instead, they are assigned the dynamic profile specified for the interface. When the first subscriber (or client) logs out, the next subscriber (or client) that logs in is assigned the primary dynamic profile.
Options	<i>primary-profile-name</i> —Name of the dynamic profile to configure as the primary dynamic profile
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces on page 68

user-prefix (DHCP Local Server)

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication username-include],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],</p> <p>[edit system services dhcp-local-server group group-name authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.
Options	<i>user-prefix-string</i> —User prefix string.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>

- Related Documentation**
- [Using External AAA Authentication Services with DHCP on page 40](#)

username-include (DHCP Local Server)

Syntax	<pre>username-include { circuit-type; client-id; delimiter <i>delimiter-character</i>; domain-name <i>domain-name-string</i>; interface-name; logical-system-name; mac-address; option-60; option-82 <circuit-id> <remote-id>; relay-agent-interface-id; relay-agent-remote-id; relay-agent-subscriber-id; routing-instance-name; user-prefix <i>user-prefix-string</i>; }</pre>
Hierarchy Level	<p>[edit system services dhcp-local-server authentication],</p> <p>[edit system services dhcp-local-server dhcpv6 authentication],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name authentication],</p> <p>[edit system services dhcp-local-server group group-name authentication],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Configure the username that the router or switch passes to the external AAA server. You must include at least one of the optional statements for the username to be valid. If you do not configure a username, the router (or switch) accesses the local authentication service only and does not use external authentication services, such as RADIUS.</p> <p>The statements are explained separately. The option-60 and option-82 statements are not supported in the DHCPv6 hierarchy levels. The client-id, relay-agent-interface-id, relay-agent-remote-id and relay-agent-subscriber-id statements are supported in the DHCPv6 hierarchy levels only.</p>
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Using External AAA Authentication Services with DHCP on page 40 • Creating Unique Usernames for DHCP Clients on page 72

version (BFD)

Syntax	version (0 1 automatic);
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols ldp oam bfd-liveness-detection], [edit logical-systems <i>logical-system-name</i> protocols ldp oam fec <i>address</i> bfd-liveness-detection], [edit system services dhcp-local-server liveness-detection method <i>bfd</i>], [edit system services dhcp-local-server dhcpv6 liveness-detection method <i>bfd</i>], [edit forwarding-options dhcp-relay liveness-detection method <i>bfd</i>], [edit forwarding-options dhcp-relay dhcpv6 liveness-detection method <i>bfd</i>], [edit system services dhcp-local-server group <i>group-name</i> liveness-detection method <i>bfd</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method <i>bfd</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method <i>bfd</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method <i>bfd</i>], [edit protocols ldp oam bfd-liveness-detection], [edit protocols ldp oam fec <i>address</i> bfd-liveness-detection]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Configure the BFD protocol version to detect.
Options	<p>0—Use BFD protocol version 0.</p> <p>1—Use BFD protocol version 1.</p> <p>automatic—Autodetect the BFD protocol version.</p> <p>Default: automatic</p>
Required Privilege Level	<p>routing—To view this statement in the configuration.</p> <p>routing-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none">• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 83• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients• Configuring BFD for LDP LSPs

violation-action (DHCP Local Server and DHCP Relay Agent)

Syntax	<code>violation-action <i>action</i>;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name</i> lease-time-validation],</code> <code>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> lease-time-validation],</code> <code>[edit logical-systems <i>logical-system-name</i> ...],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...],</code> <code>[edit routing-instances <i>routing-instance-name</i> ...],</code> <code>[edit system services dhcp-local-server lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 lease-time-validation],</code> <code>[edit system services dhcp-local-server group <i>group-name</i> lease-time-validation],</code> <code>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> lease-time-validation]</code>
Release Information	Statement introduced in Junos OS Release 14.1.
Description	Configure the action that the router performs when a DHCP lease-time violation occurs. The violation occurs when a third-party DHCP server or address-assignment pool offers a DHCP lease time that is less than the threshold specified by the lease-time-threshold statement.
Options	<p><i>action</i>—Action taken by the router when a lease-time violation occurs.</p> <ul style="list-style-type: none"> • drop—(Optional) For DHCPv4 and DHCPv6 relay agent, the third-party lease is dropped and the client binding fails. • override-lease—(Optional) For DHCPv4 and DHCPv6 local server, the third-party lease is overridden with the value specified by the lease-time-threshold statement and binds the client using the new value. • strict—(Optional) For DHCPv4 and DHCPv6 local server, DHCP ignores the third-party lease and the client binding fails.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Configuring a DHCP Lease-Time Threshold on page 67

PART 3

Administration

- [Verifying and Managing Configurations on page 179](#)
- [Monitoring Commands on page 185](#)

CHAPTER 5

Verifying and Managing Configurations

- [Clearing DHCP Bindings for Subscriber Access on page 179](#)
- [Monitoring DHCP Options Configured on RADIUS Servers on page 181](#)
- [Verifying and Managing DHCP Local Server Configuration on page 183](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 183](#)
- [Verifying and Managing the DHCP Maintain Subscribers Feature on page 184](#)

Clearing DHCP Bindings for Subscriber Access

This topic provides the procedure you use to display current DHCP bindings, clear selected bindings, and verify that the specified bindings are successfully cleared.

Subscriber management enables you to clear DHCP bindings at several different levels for DHCP local server and DHCP relay agent. For example, you can clear the DHCP bindings on all interfaces, a group of interfaces, or a specific interface. You can also clear DHCP bindings based on IP address, MAC address, session-ID, DHCPv6 prefix, DHCPv6 Client ID, FPC, PIC, port, VLAN, or stacked VLAN (S-VLAN).

This topic includes examples to show several variations of the clear DHCP binding feature. The examples use DHCP local server commands; however, the procedure and commands are similar for DHCP relay agent, DHCPv6 local server, and DHCPv6 relay agent.

To clear bindings and verify the results for a specific IP address:

1. Display current bindings. Issue the appropriate variation of the **show dhcp server binding** command.

```
user@host> show dhcp server binding
2 clients, (2 bound, 0 selecting, 0 renewing, 0 rebinding)

IP address      Hardware address  Type    Lease expires at
192.168.32.1    90:00:00:01:00:01 active    2011-10-17 11:38:47 PST
192.168.32.3    90:00:00:02:00:01 active    2011-00-17 11:38:41 PST
```

2. Clear the binding you want to remove.

```
user@host> clear dhcp server binding 192.168.32.1
```

3. Verify that the binding has been cleared.

```
user@host> show dhcp server binding
1 clients, (1 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
192.168.32.3	90:00:00:02:00:01	active	2011-00-17 11:38:41 PST

The following examples show variations of the clear DHCP binding feature. The examples use the DHCP local server version of the commands.



NOTE: IP demux interfaces are not supported by the show and clear DHCP bindings commands for DHCP local server and DHCP relay agent.

To clear all bindings:

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

To clear bindings on a specific interface:

```
user@host> clear dhcp server binding interface fe-0/0/2
```

To clear all bindings over an interface. This example uses the wildcard option.

```
user@host> clear dhcp server binding ge-1/0/0. *
```

To clear bindings on top of a specific VLAN. This example clears all bindings on top of VLAN 100.

```
user@host> clear dhcp server binding ge-1/0/0:100
```

To clear bindings for a specific S-VLAN. This example clears bindings on S-VLAN 100-200.

```
user@host> clear dhcp server binding ge-1/0/0:100-200
```

To clear all bindings on top of all demux VLANs:

```
user@host> clear dhcp server binding demux0
```

To clear all bindings on top of an underlying interface. This example clears the bindings on all demux VLANs on top of interface ae0:

```
user@host> clear dhcp server binding ae0
```

To clear PPP bindings. This example uses the wildcard feature and clears the PPP bindings over interface pp0.100 and pp0.200.

```
user@host> clear dhcp server binding pp0.*
```

To clear all bindings on an FPC. This example uses the wildcard feature and clears all DHCP bindings on FPC 1.

```
user@host> clear dhcp server binding ge-1/*
```

To clear all bindings on a PIC. This example uses the wildcard feature and clears all DHCP bindings on FPC 1, PIC 0.

```
user@host> clear dhcp server binding ge-1/0/*
```

To clear all bindings on a port. This example uses the wildcard feature and clears all DHCP bindings on FPC 1, PIC 0, port 0.

```
user@host> clear dhcp server binding ge-1/0/0.*
```

- Related Documentation**
- [DHCP Auto Logout Overview on page 22](#)
 - [Automatically Logging Out DHCP Clients on page 53](#)

Monitoring DHCP Options Configured on RADIUS Servers

Purpose View information for DHCP options that are centrally configured on a RADIUS server and that are distributed using Juniper Networks VSA 26-55 (DHCP-Options).

Action To display information for opaque DHCP options:

```
user@host> show subscribers detail
Type: DHCP
IP Address: 192.168.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-prof-23
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Session Timeout (seconds): 3600
Idle Timeout (seconds): 600
Login Time: 2011-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
```

Meaning DHCP Options: len 52
 35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
 00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
 33 2d 37 2d 30 37 05 01 06 0f 21 2c

The DHCP options output provides the following information:

- The **len** field is the total number of hex values in the message.
- The hex values specify the type, length, and value (TLV) of DHCP options, and are converted to decimal to identify the DHCP options, as defined in RFC 2132.

The number of hex values that make up a particular DHCP option varies, depending on the length of the option. For example, the first DHCP option specified in the output includes three sets of hex values (**35 01 01**). The first hex value (**35**) identifies the option type, the second value (**01**) indicates the length of the value entry, which in this case is one set of hex values. The third hex value (**01**) specifies the value for the DHCP option.

In the second DHCP option specification (**39 02 02 40**), the hex value **39** is the type, and the length of **02** specifies that two sets of hex entries make up the value for the option. Therefore, this option specification uses four sets of hex entries; one for the type (**39**), one to specify the length (**02**), and two for the option value (**02 40**).

The third DHCP option is specified by the hex values **3d 07 01 00 10 94 00 00 08**. The hex value **3d** is the type, followed by the length (**07**), which specifies that the next seven sets of hex entries make up the value for the option. Therefore, this option specification uses a total of nine sets of hex entries; one for the type (**3d**), one to specify the length (**07**), and seven for the value of the DHCP option (**01 00 10 94 00 00 08**).

[Table 10 on page 182](#) describes the first two options in more detail.

Table 10: DHCP Options Description

Option	Type	Length	Value
35 01 01	35 = decimal 53 (Code 53 in RFC 2132 is the DHCP Message Type option)	01 = the length of the option is one set of hex values (the next set in the list)	01 = value of the message type that is described in RFC 2132. The code 01 specifies a message type of DHCPDISCOVER.
39 02 02 40	39 = decimal 57 (Code 57 is the Maximum DHCP Message Size option)	02 = the length of the option is two sets of hex values (the next two sets in the list)	0240 = converted to a length of 576 octets

Related Documentation

- [Centrally Configured Opaque DHCP Options on page 28](#)
- [show subscribers on page 220](#)

Verifying and Managing DHCP Local Server Configuration

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 routing-instance customer routing instance
```

• To display extended DHCP local server statistics:

```
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:

```
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 routing-instance customer routing instance
```

Related Documentation • [CLI Explorer](#)

Verifying and Managing DHCPv6 Local Server Configuration

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
```

Related Documentation • [CLI Explorer](#)

Verifying and Managing the DHCP Maintain Subscribers Feature

Purpose	Display information related to the DHCP maintain-subscribers feature and explicitly log out maintained clients.
Action	<ul style="list-style-type: none">• To display DHCP local server binding information for the DHCP maintain subscribers feature: <code>user@host>show dhcp server binding detail</code>• To display DHCPv6 local server binding information for the DHCP maintain subscribers feature: <code>user@host>show dhcpv6 server binding detail</code>• To display DHCP relay binding information for the DHCP maintain subscribers feature: <code>user@host>show dhcp relay binding detail</code>• To explicitly log out a DHCP local server subscriber when the maintain subscriber feature is enabled: <code>user@host>clear dhcp server binding <i>binding-type</i></code>• To explicitly log out a DHCPv6 local server subscriber when the maintain subscriber feature is enabled: <code>user@host>clear dhcpv6 server binding <i>binding-type</i></code>• To explicitly log out a DHCP relay subscriber when the maintain subscriber feature is enabled: <code>user@host>clear dhcp relay binding <i>binding-type</i></code>
Related Documentation	<ul style="list-style-type: none">• Subscriber Binding Retention During Interface Delete Events on page 24• Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events on page 54

CHAPTER 6

Monitoring Commands

- clear dhcp server binding
- clear dhcp server statistics
- clear dhcpv6 server binding
- clear dhcpv6 server statistics
- request dhcp server reconfigure
- request dhcpv6 server reconfigure
- request system reboot
- show dhcp server binding
- show dhcp server statistics
- show dhcpv6 server binding
- show dhcpv6 server statistics
- show subscribers
- show subscribers summary

clear dhcp server binding

Syntax `clear dhcp server binding`
 `<address>`
 `<all>`
 `<interface interface-name>`
 `<interfaces-vlan>`
 `<interfaces-wildcard>`
 `<logical-system logical-system-name>`
 `<routing-instance routing-instance-name>`

Release Information Command introduced in Junos OS Release 9.0.
 Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Description Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on 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.

Options *address*—(Optional) Clear the binding state for the DHCP client, using one of the following entries:

- *ip-address*—The specified IP address.
- *mac-address*—The specified MAC address.
- *session-id*—The specified session ID.

all—(Optional) Clear the binding state for all DHCP clients.

interface interface-name—(Optional) Clear the binding state for DHCP clients on the specified interface.



NOTE: This option clears all bindings whose initial login requests were received over the specified interface. Dynamic demux login requests are not received over the dynamic demux interface, but rather the underlying interface of the dynamic demux interface. To clear a specific dynamic demux interface, use the *ip-address* or *mac-address* options.

interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.

interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Clear the binding state for DHCP clients on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- [Clearing DHCP Bindings for Subscriber Access on page 179](#)
- [show dhcp server binding on page 203](#)

List of Sample Output

- [clear dhcp server binding <ip-address> on page 187](#)
- [clear dhcp server binding all on page 187](#)
- [clear dhcp server binding interface on page 188](#)
- [clear dhcp server binding <interfaces-vlan> on page 188](#)
- [clear dhcp server binding <interfaces-wildcard> on page 188](#)

Output Fields See [show dhcp server binding](#) for an explanation of output fields.

Sample Output

clear dhcp server binding <ip-address>

The following sample output displays the address bindings in the DHCP client table on the extended DHCP local server before and after the **clear dhcp server binding** command is issued.

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

```
2 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
100.20.32.1	90:00:00:01:00:01	active	2007-01-17 11:38:47 PST
100.20.32.3	90:00:00:02:00:01	active	2007-01-17 11:38:41 PST

```
user@host> clear dhcp server binding 10.20.32.1
```

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

```
1 clients, (0 bound, 0 selecting, 0 renewing, 0 rebinding)
```

IP address	Hardware address	Type	Lease expires at
100.20.32.3	90:00:00:02:00:01	active	2007-01-17 11:38:41 PST

clear dhcp server binding all

The following command clears all DHCP local server bindings:

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

clear dhcp server binding interface

The following command clears DHCP local server bindings on a specific interface:

```
user@host> clear dhcp server binding interface fe-0/0/2
```

clear dhcp server binding <interfaces-vlan>

The following command uses the *interfaces-vlan* option to clear all DHCP local server bindings on top of the underlying interface **ae0**, which clears DHCP bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcp server binding ae0
```

clear dhcp server binding <interfaces-wildcard>

The following command uses the *interfaces-wildcard* option to clear all DHCP local server bindings over a specific interface:

```
user@host> clear dhcp server binding ge-1/0/0.*
```

clear dhcp server statistics

Syntax	<code>clear dhcp server statistics</code> <code><interface <i>interface-name</i>></code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Clear all extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Clear the statistics for DHCP clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the statistics for DHCP clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	view
List of Sample Output	clear dhcp server statistics on page 189
Output Fields	See show dhcp server statistics for an explanation of output fields.

Sample Output

clear dhcp server statistics

The following sample output displays the extended DHCP local server statistics before and after the **clear dhcp server statistics** command is issued.

```

user@host> show dhcp server statistics
Packets dropped:
    Total                1
    Lease Time Violation 1

Messages received:
    BOOTREQUEST          89163
    DHCPDECLINE           0
    DHCPDISCOVER          8110
    DHCPINFORM            0
    DHCPRELEASE           0
    DHCPREQUEST           81053

Messages sent:
    BOOTREPLY             32420
    DHCPOFFER             8110
    DHCPACK                8110
    DHCPNAK                8100

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

```

Packets dropped:	
Total	0
Messages received:	
BOOTREQUEST	0
DHCPDECLINE	0
DHCPDISCOVER	0
DHCPINFORM	0
DHCPRELEASE	0
DHCPREQUEST	0
Messages sent:	
BOOTREPLY	0
DHCPOFFER	0
DHCPACK	0
DHCPNAK	0

clear dhcpv6 server binding

Syntax	<pre>clear dhcpv6 server binding <address> <all> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p>
Description	Clear the binding state of a Dynamic Host Configuration Protocol for IPv6 (DHCPv6) client from the client table on the extended DHCPv6 local server.
Options	<p>address—(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:</p> <ul style="list-style-type: none"> • <i>CID</i>—The specified Client ID (CID). • <i>ipv6-prefix</i>—The specified IPv6 prefix. • <i>session-id</i>—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCPv6 clients.</p> <p>interface interface-name—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</p> <p>interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) Clear bindings on a set of interfaces. This option supports the use of the wildcard character (*).</p> <p>logical-system logical-system-name—(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 179 • show dhcpv6 server binding on page 211
List of Sample Output	<p>clear dhcpv6 server binding all on page 192</p> <p>clear dhcpv6 server binding <ipv6-prefix> on page 192</p>

[clear dhcpv6 server binding interface on page 192](#)
[clear dhcpv6 server binding <interfaces-vlan> on page 192](#)
[clear dhcpv6 server binding <interfaces-wildcard> on page 192](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

`clear dhcpv6 server binding all`

The following command clears all DHCPv6 local server bindings:

```
user@host> clear dhcpv6 server binding all
```

`clear dhcpv6 server binding <ipv6-prefix>`

The following command clears DHCPv6 local server bindings for a specific IPv6 prefix:

```
user@host> clear dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
```

`clear dhcpv6 server binding interface`

The following command clears DHCPv6 local server bindings on a specific interface:

```
user@host> clear dhcpv6 server binding interface fe-0/0/2
```

`clear dhcpv6 server binding <interfaces-vlan>`

The following command uses the *interfaces-vlan* option to clear all DHCPv6 local server bindings on top of the underlying interface **ae0**, which clears DHCPv6 bindings on all demux VLANs on top of **ae0**:

```
user@host> clear dhcpv6 server binding interface ae0
```

`clear dhcpv6 server binding <interfaces-wildcard>`

The following command uses the *interfaces-wildcard* option to clear all DHCPv6 local server bindings over a specific interface:

```
user@host> clear dhcpv6 server binding ge-1/0/0.*
```

clear dhcpv6 server statistics


Syntax	clear dhcpv6 server statistics <interface <i>interface-name</i> > <logical-system <i>logical-system-name</i> > <routing-instance <i>routing-instance-name</i> >
Release Information	Command introduced in Junos OS Release 9.6.
Description	Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified logical system. If you do not specify a logical system, statistics are cleared for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the statistics for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, statistics are cleared for the default routing instance.</p>
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none"> • show dhcpv6 server statistics on page 217
List of Sample Output	clear dhcpv6 server statistics on page 193
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear dhcpv6 server statistics

```
user@host> clear dhcpv6 server statistics
```

request dhcp server reconfigure

Syntax	<code>request dhcp server reconfigure (all <i>address</i> interface <i>interface-name</i> logical-system <i>logical-system-name</i> routing-instance <i>routing-instance-name</i>)</code>
Release Information	Command introduced in Junos OS Release 10.0. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Initiate reconfiguration processing for the specified DHCP clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcp server binding command.</p> <p>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 (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the forcerenew message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.</p>
Options	<p>all—Initiate reconfiguration for all DHCP clients.</p> <p><i>address</i>—Initiate reconfiguration for DHCP client with the specified IP address or MAC address.</p> <p>interface <i>interface-name</i>—Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).</p> <div style="border: 1px solid #ccc; padding: 10px; margin: 10px 0;"> <p> NOTE: You cannot use the interface <i>interface-name</i> option with the request dhcp server reconfigure command for DHCP passive clients (clients that are added as a result of DHCP snooped packets). For passive clients, the interface is not guaranteed to be the next-hop interface to the client, as is the case for active clients.</p> </div> <p>logical-system <i>logical-system-name</i>—Initiate reconfiguration for all DHCP clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.</p>
Required Privilege Level	view

Related Documentation • [Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58](#)

List of Sample Output [request dhcp server reconfigure on page 195](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

[request dhcp server reconfigure](#)

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

request dhcpv6 server reconfigure

Syntax	request dhcpv6 server reconfigure (all address client-id interface <i>interface-name</i> logical-system <i>logical-system-name</i> routing-instance <i>routing-instance-name</i> session-id)
Release Information	Command introduced in Junos OS Release 10.4. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Initiate reconfiguration processing for the specified DHCPv6 clients if they are in the bound state. If the clients are in the reconfiguring state, this command has no effect. If the clients are in any state other than bound or reconfiguring, this command has the same effect as the clear dhcpv6 server binding command.</p> <p>When the local server state machine starts the reconfiguration process on a bound client, the client transitions to the reconfigure state and the local server sends a reconfigure message to the client. Because the client was in the bound state before entering the reconfiguring state, all subscriber (or DHCP client) services, such as forwarding and statistics, continue to work. An exponential back-off timer determines the interval at which the reconfigure message is sent. If the final attempt is unsuccessful, the client is returned to its original state by default. You can optionally include the clear-on-abort statement to configure the client to be cleared when reconfiguration fails.</p>
Options	<p>all—Initiate reconfiguration for all DHCPv6 clients.</p> <p>address—Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.</p> <p>client-id—Initiate reconfiguration for DHCPv6 client with the specified client ID.</p> <p>interface <i>interface-name</i>—Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).</p> <p>logical-system <i>logical-system-name</i>—Initiate reconfiguration for all DHCPv6 clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.</p> <p>session-id—Initiate reconfiguration for DHCPv6 client with the specified session ID.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• Configuring Extended DHCP Local Server Dynamic Client Reconfiguration on page 58
List of Sample Output	request dhcpv6 server reconfigure on page 197
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request dhcpv6 server reconfigure

```
user@host> request dhcpv6 server reconfigure 2001::2/16
```

request system reboot

Syntax	request system reboot <at <i>time</i> > <both-routing-engines> <in <i>minutes</i> > <media (compact-flash disk removable-compact-flash usb)> <message " <i>text</i> "> <other-routing-engine>
Syntax (EX Series Switches)	request system reboot <all-members> <at <i>time</i> > <both-routing-engines> <in <i>minutes</i> > <local> <media (external internal)> <member <i>member-id</i> > <message " <i>text</i> "> <other-routing-engine> <slice <i>slice</i> >
Syntax (TX Matrix Router)	request system reboot <all-chassis all-lcc lcc <i>number</i> scc> <at <i>time</i> > <both-routing-engines> <in <i>minutes</i> > <media (compact-flash disk)> <message " <i>text</i> "> <other-routing-engine>
Syntax (TX Matrix Plus Router)	request system reboot <all-chassis all-lcc lcc <i>number</i> sfc <i>number</i> > <at <i>time</i> > <both-routing-engines> <in <i>minutes</i> > <media (compact-flash disk)> <message " <i>text</i> "> <other-routing-engine> <partition (1 2 alternate)>
Syntax (MX Series Router)	request system reboot <all-members> <at <i>time</i> > <both-routing-engines> <in <i>minutes</i> > <local> <media (external internal)> <member <i>member-id</i> > <message " <i>text</i> "> <other-routing-engine>
Release Information	Command introduced before Junos OS Release 7.4.

Option **other-routing-engine** introduced in Junos OS Release 8.0.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Option **sfc** introduced for the TX Matrix Plus router in Junos OS Release 9.6.
 Option **both-routing-engines** introduced in Junos OS Release 12.1.

Description Reboot the software.

Options **none**—Reboot the software immediately.

all-chassis—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all routers connected to the TX Matrix or TX Matrix Plus router, respectively.

all-lcc—(TX Matrix routers and TX Matrix Plus routers only) (Optional) On a TX Matrix router or TX Matrix Plus router, reboot all line card chassis connected to the TX Matrix or TX Matrix Plus router, respectively.

all-members—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.

at time—(Optional) Time at which to reboot the software, specified in one of the following ways:

- **now**—Stop or reboot the software immediately. This is the default.
- **+minutes**—Number of minutes from now to reboot the software.
- **yymmddhhmm**—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute.
- **hh:mm**—Absolute time on the current day at which to stop the software, specified in 24-hour time.

both-routing-engines—(Optional) Reboot both Routing Engines at the same time.

in minutes—(Optional) Number of minutes from now to reboot the software. This option is an alias for the **at +minutes** option.

lcc number—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.

Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

local—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the local Virtual Chassis member.

media (compact-flash | disk | removable-compact-flash | usb)—(Optional) Boot medium for next boot. (The options **removable-compact-flash** and **usb** pertain to the J Series routers only.)

media (external | internal)—(EX Series switches and MX Series routers only) (Optional) Reboot the boot media:

- **external**—Reboot the external mass storage device.
- **internal**—Reboot the internal flash device.

member *member-id*—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on the specified member of the Virtual Chassis configuration. For EX4200 switches, replace ***member-id*** with a value from 0 through 9. For an MX Series Virtual Chassis, replace ***member-id*** with a value of 0 or 1.

message "*text*"—(Optional) Message to display to all system users before stopping or rebooting the software.

other-routing-engine—(Optional) Reboot the other Routing Engine from which the command is issued. For example, if you issue the command from the master Routing Engine, the backup Routing Engine is rebooted. Similarly, if you issue the command from the backup Routing Engine, the master Routing Engine is rebooted.

partition—(TX Matrix Plus routers only) (Optional) Reboot using the specified partition on the boot media. This option has the following suboptions:

- **1**—Reboot from partition 1.
- **2**—Reboot from partition 2.
- **alternate**—Reboot from the alternate partition.

scc—(TX Matrix routers only) (Optional) Reboot the Routing Engine on the TX Matrix switch-card chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted.

sfc *number*—(TX Matrix Plus routers only) (Optional) Reboot the Routing Engine on the TX Matrix Plus switch-fabric chassis. If you issue the command from re0, re0 is rebooted. If you issue the command from re1, re1 is rebooted. Replace ***number*** with 0.

slice *slice*—(EX Series switches only) (Optional) Reboot a partition on the boot media. This option has the following suboptions:

- **1**—Power off partition 1.
- **2**—Power off partition 2.
- **alternate**—Reboot from the alternate partition.

Additional Information Reboot requests are recorded in the system log files, which you can view with the **show log** command (see *show log*). Also, the names of any running processes that are scheduled to be shut down are changed. You can view the process names with the **show system processes** command (see *show system processes*).

On a TX Matrix or TX Matrix Plus router, if you issue the **request system reboot** command on the master Routing Engine, all the master Routing Engines connected to the routing matrix are rebooted. If you issue this command on the backup Routing Engine, all the backup Routing Engines connected to the routing matrix are rebooted.



NOTE: Before issuing the **request system reboot** command on a TX Matrix Plus router with no options or the **all-chassis**, **all-lcc**, **lcc number**, or **sfc** options, verify that master Routing Engine for all routers in the routing matrix are in the same slot number. If the master Routing Engine for a line-card chassis is in a different slot number than the master Routing Engine for a TX Matrix Plus router, the line-card chassis might become logically disconnected from the routing matrix after the **request system reboot** command.



NOTE: To reboot a router that has two Routing Engines, reboot the backup Routing Engine (if you have upgraded it) first, and then reboot the master Routing Engine.

Required Privilege Level maintenance

Related Documentation

- *clear system reboot*
- *request system halt*
- *request system reboot*
- *Rebooting and Halting a QFX Series Product*
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output

[request system reboot on page 202](#)
[request system reboot \(at 2300\) on page 202](#)
[request system reboot \(in 2 Hours\) on page 202](#)
[request system reboot \(Immediately\) on page 202](#)
[request system reboot \(at 1:20 AM\) on page 202](#)

Output Fields When you enter this command, you are provided feedback on the status of your request.

Sample Output

request system reboot

```
user@host> request system reboot
Reboot the system ? [yes,no] (no)
```

request system reboot (at 2300)

```
user@host> request system reboot at 2300 message ?Maintenance time!?
Reboot the system ? [yes,no] (no) yes
```

```
shutdown: [pid 186]
*** System shutdown message from root@berry.network.net ***
System going down at 23:00
```

request system reboot (in 2 Hours)

The following example, which assumes that the time is 5 PM (17:00), illustrates three different ways to request the system to reboot in two hours:

```
user@host> request system reboot at +120
user@host> request system reboot in 120
user@host> request system reboot at 19:00
```

request system reboot (Immediately)

```
user@host> request system reboot at now
```

request system reboot (at 1:20 AM)

To reboot the system at 1:20 AM, enter the following command. Because 1:20 AM is the next day, you must specify the absolute time.

```
user@host> request system reboot at 06060120
request system reboot at 120
Reboot the system at 120? [yes,no] (no) yes
```

show dhcp server binding

Syntax	<pre>show dhcp server binding <address> <interfaces-vlan><brief detail summary> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 9.0.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p>
Description	Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (DHCP) local server.
Options	<p>address—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:</p> <ul style="list-style-type: none"> • <i>ip-address</i>—The specified IP address. • <i>mac-address</i>—The specified MAC address. • <i>session-id</i>—The specified session ID. <p>brief detail summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcp server binding.</p> <p>interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.</p> <p>interfaces-vlan—(Optional) Show the binding state information on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) The set of interfaces on which to show the binding state information. This option supports the use of the wildcard character (*).</p> <p>logical-system logical-system-name—(Optional) Display information about active client bindings for DHCP clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 179 • Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration • clear dhcp server binding on page 186

List of Sample Output

- [show dhcp server binding on page 205](#)
- [show dhcp server binding detail on page 206](#)
- [show dhcp server binding detail \(ACI Interface Set Configured\) on page 206](#)
- [show dhcp server binding interface <vlan-id> on page 206](#)
- [show dhcp server binding interface <svlan-id> on page 206](#)
- [show dhcp server binding <ip-address> on page 207](#)
- [show dhcp server binding <session-id> on page 207](#)
- [show dhcp server binding summary on page 207](#)
- [show dhcp server binding <interfaces-vlan> on page 207](#)
- [show dhcp server binding <interfaces-wildcard> on page 207](#)

Output Fields [Table 11 on page 204](#) lists the output fields for the **show dhcp server binding** command. Output fields are listed in the approximate order in which they appear.

Table 11: show dhcp server binding Output Fields

Field Name	Field Description	Level of Output
<i>number</i> clients, (<i>number</i> init, <i>number</i> bound, <i>number</i> selecting, <i>number</i> requesting, <i>number</i> renewing, <i>number</i> releasing)	Summary counts of the total number of DHCP clients and the number of DHCP clients in each state.	summary
IP address	IP address of the DHCP client.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Hardware address	Hardware address of the DHCP client.	brief detail
Expires	Number of seconds in which lease expires.	brief detail
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • FORCERENEW—Client has received forcerenew message from server. • INIT—Initial state. • RELEASE—Client is releasing IP address lease. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCP server. • SELECTING—Client receiving offers from DHCP servers. 	brief detail
Interface	Interface on which the request was received.	brief

Table 11: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Lease Expires	Date and time at which the client's IP address lease expires.	detail
Lease Expires in	Number of seconds in which lease expires.	detail
Lease Start	Date and time at which the client's IP address lease started.	detail
Lease time violated	Lease time violation has occurred.	detail
Last Packet Received	Date and time at which the router received the last packet.	detail
Incoming Client Interface	Client's incoming interface.	detail
Client Interface Svlan Id	S-VLAN ID of the client's incoming interface.	detail
Client Interface Vlan Id	VLAN ID of the client's incoming interface.	detail
Demux Interface	Name of the IP demultiplexing (demux) interface.	detail
Server IP Address or Server Identifier	IP address of DHCP server.	detail
Server Interface	Interface of DHCP server.	detail
Client Pool Name	Name of address pool used to assign client IP address lease.	detail
ACI Interface Set Name	Internally generated name of the dynamic agent circuit identifier (ACI) interface set.	detail
ACI Interface Set Index	Index number of the dynamic ACI interface set.	detail
ACI Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.	detail

Sample Output

show dhcp server binding

```

user@host> show dhcp server binding
IP address      Session Id  Hardware address  Expires  State  Interface
100.20.20.15    6          00:10:94:00:00:01 86180    BOUND  ge-1/0/0.0
100.20.20.16    7          00:10:94:00:00:02 86180    BOUND  ge-1/0/0.0
100.20.20.17    8          00:10:94:00:00:03 86180    BOUND  ge-1/0/0.0
100.20.20.18    9          00:10:94:00:00:04 86180    BOUND  ge-1/0/0.0
100.20.20.19    10         00:10:94:00:00:05 86180    BOUND  ge-1/0/0.0

```

show dhcp server binding detail

```

user@host> show dhcp server binding detail
Client IP Address: 100.20.20.15
  Hardware Address:      00:10:94:00:00:01
  State:                 BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)

  Lease Expires:         2009-07-21 10:10:25 PDT
  Lease Expires in:      86151 seconds
  Lease Start:           2009-07-20 10:10:25 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address:     100.20.20.9
  Server Interface:      none
  Session Id:            6
  Client Pool Name:      6
  Client IP Address:     100.20.20.16
  Hardware Address:      00:10:94:00:00:02
  State:                 BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)

  Lease Expires:         2009-07-21 10:10:25 PDT
  Lease Expires in:      86151 seconds
  Lease Start:           2009-07-20 10:10:25 PDT
  Lease time violated:    yes
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address:     100.20.20.9
  Server Interface:      none
  Session Id:            7
  Client Pool Name:      7

```

show dhcp server binding detail (ACI Interface Set Configured)

```

user@host> show dhcp server binding detail
Client IP Address: 100.20.22.14
  Hardware Address:      00:00:64:34:01:02
  State:                 BOUND(LOCAL_SERVER_STATE_BOUND)
  Lease Expires:         2012-03-13 09:53:32 PDT
  Lease Expires in:      82660 seconds
  Lease Start:           2012-03-12 10:23:32 PDT
  Last Packet Received:  2012-03-12 10:23:32 PDT
  Incoming Client Interface: demux0.1073741827
  Client Interface Svlan Id: 1802
  Client Interface Vlan Id: 302
  Demux Interface:       demux0.1073741832
  Server Identifier:     100.20.200.202
  Session Id:            11
  Client Pool Name:      poolA
  Client Profile Name:    DEMUXprofile
  ACI Interface Set Name: aci-1002-demux0.1073741827
  ACI Interface Set Index: 2
  ACI Interface Set Session ID: 6

```

show dhcp server binding interface <vlan-id>

```

user@host> show dhcp server binding interface ge-1/1/0:100
IP address      Session Id  Hardware address  Expires  State  Interface
200.20.20.15    6          00:10:94:00:00:01  86124    BOUND  ge-1/1/0:100
ge-1/1/0:100

```

show dhcp server binding interface <svlan-id>

```

user@host> show dhcp server binding interface ge-1/1/0:10-100

```


IP address	Session Id	Hardware address	Expires	State	Interface
200.20.20.16	7	00:10:94:00:00:02	86124	BOUND	
ge-1/1/0:10-100					

show dhcp server binding <ip-address>

```
user@host> show dhcp server binding 100.20.20.19
```

IP address	Session Id	Hardware address	Expires	State	Interface
100.20.20.19	10	00:10:94:00:00:05	86081	BOUND	ge-1/0/0.0

show dhcp server binding <session-id>

```
user@host> show dhcp server binding 6
```

IP address	Session Id	Hardware address	Expires	State	Interface
200.20.20.15	6	00:10:94:00:00:01	86124	BOUND	ge-1/0/0.0

show dhcp server binding summary

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

3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

show dhcp server binding <interfaces-vlan>

```
user@host> show dhcp server binding ge-1/0/0:100-200
```

IP address	Session Id	Hardware address	Expires	State	Interface
192.168.0.17	42	00:10:94:00:00:02	86346	BOUND	
ge-1/0/0.1073741827					
192.168.0.16	41	00:10:94:00:00:01	86346	BOUND	
ge-1/0/0.1073741827					

show dhcp server binding <interfaces-wildcard>

```
user@host> show dhcp server binding ge-1/3/*
```

IP address	Session Id	Hardware address	Expires	State	Interface
192.168.0.9	24	00:10:94:00:00:04	86361	BOUND	
ge-1/3/0.110					
192.168.0.8	23	00:10:94:00:00:03	86361	BOUND	
ge-1/3/0.110					
192.168.0.7	22	00:10:94:00:00:02	86361	BOUND	
ge-1/3/0.110					

show dhcp server statistics

Syntax	show dhcp server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 9.0.
Description	Display extended Dynamic Host Configuration Protocol (DHCP) local server statistics.
Options	logical-system <i>logical-system-name</i> —(Optional) Display information about extended DHCP local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system. routing-instance <i>routing-instance-name</i> —(Optional) Display information about extended DHCP local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• clear dhcp server statistics on page 189
List of Sample Output	show dhcp server statistics on page 209
Output Fields	Table 12 on page 209 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.

Table 12: show dhcp server statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCP local server • Authentication—Number of packets discarded because they could not be authenticated • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Dynamic profile—Number of packets discarded due to dynamic profile information • Invalid server address—Number of packets discarded because an invalid server address was specified • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the extended DHCP local server could not send
Messages received	<p>Number of DHCP messages received.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) received • DHCPDECLINE—Number of DHCP PDUs of type DECLINE received • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received
Messages sent	<p>Number of DHCP messages sent.</p> <ul style="list-style-type: none"> • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP OFFER PDUs transmitted • DHCPACK—Number of DHCP ACK PDUs transmitted • DHCPNACK—Number of DHCP NACK PDUs transmitted • DHCPFORCERENEW—Number of DHCP FORCERENEW PDUs transmitted

Sample Output

show dhcp server statistics

```

user@host> show dhcp server statistics
Packets dropped:
    Total                  1

```

Lease Time Violation	1
Messages received:	
BOOTREQUEST	25
DHCPDECLINE	0
DHCPDISCOVER	10
DHCPINFORM	0
DHCPRELEASE	4
DHCPREQUEST	10
Messages sent:	
BOOTREPLY	20
DHCPOFFER	10
DHCPACK	10
DHCPNAK	0
DHCPFORCERENEW	0

show dhcpv6 server binding

Syntax	<pre>show dhcpv6 server binding <address> <brief detail summary> <interface interface-name> <interfaces-vlan> <interfaces-wildcard> <logical-system logical-system-name> <routing-instance routing-instance-name></pre>
Release Information	<p>Command introduced in Junos OS Release 9.6.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p>
Description	Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server.
Options	<p>address—(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show:</p> <ul style="list-style-type: none"> • <i>CID</i>—The specified Client ID (CID). • <i>ipv6-prefix</i>—The specified IPv6 prefix. • <i>session-id</i>—The specified session ID. <p>brief detail summary—(Optional) Display the specified level of output about active client bindings. The default is brief, which produces the same output as show dhcpv6 server binding.</p> <p>interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.</p> <p>interfaces-vlan—(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.</p> <p>interfaces-wildcard—(Optional) Set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).</p> <p>logical-system logical-system-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified logical system.</p> <p>routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Clearing DHCP Bindings for Subscriber Access on page 179 • clear dhcpv6 server binding on page 191

List of Sample Output

- [show dhcpv6 server binding on page 213](#)
- [show dhcpv6 server binding detail on page 213](#)
- [show dhcpv6 server binding interface on page 214](#)
- [show dhcpv6 server binding interface detail on page 214](#)
- [show dhcpv6 server binding \(IPv6 Prefix\) on page 215](#)
- [show dhcpv6 server binding \(Session ID\) on page 215](#)
- [show dhcpv6 server binding \(Interfaces VLAN\) on page 215](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 215](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 215](#)
- [show dhcpv6 server binding summary on page 216](#)

Output Fields [Table 13 on page 212](#) lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 13: show dhcpv6 server binding Output Fields

Field Name	Field Description	Level of Output
<i>number clients</i> , (<i>number init</i> , <i>number bound</i> , <i>number selecting</i> , <i>number requesting</i> , <i>number renewing</i> , <i>number releasing</i>)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary
Prefix	Client's DHCPv6 prefix, or prefix used to support multiple address assignment.	brief detail
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which lease expires.	brief detail
State	State of the address binding table on the extended DHCPv6 local server: <ul style="list-style-type: none"> • BOUND—Client has active IP address lease. • INIT—Initial state. • RECONFIGURE—Server has sent reconfigure message to client. • RELEASE—Client is releasing IP address lease. • RENEWING—Client sending request to renew IP address lease. • REQUESTING—Client requesting a DHCPv6 server. • SELECTING—Client receiving offers from DHCPv6 servers. 	brief detail
Interface	Interface on which the DHCPv6 request was received.	brief
Client IPv6 Address	Client's IPv6 address.	detail
Client IPv6 Prefix	Client's IPv6 prefix.	detail
Client DUID	Client's DHCP Unique Identifier (DUID).	brief detail
Lease expires	Date and time at which the client's IP address lease expires.	detail

Table 13: show dhcpv6 server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Lease expires in	Number of seconds in which lease expires.	detail
Preferred Lease Expires	Date and UTC time at which the client's IPv6 prefix expires.	detail
Preferred Lease Expires in	Number of seconds at which client's IPv6 prefix expires.	detail
Lease Start	Date and time at which the client's address lease was obtained.	detail
Lease time violated	Lease time violation has occurred.	detail
Incoming Client Interface	Client's incoming interface.	detail
Server IP Address	IP address of DHCPv6 server.	detail
Server Interface	Interface of DHCPv6 server.	detail
Client Pool Name	Address pool used to assign IPv6 address.	detail
Client Prefix Pool Name	Address pool used to assign IPv6 prefix.	detail
Client Id length	Length of the DHCPv6 client ID, in bytes.	detail
Client Id	ID of the DHCPv6 client.	detail

Sample Output

show dhcpv6 server binding

```

user@host> show dhcpv6 server binding
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
2002::1/74 11 86321 BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c1-00:10:94:00:00:06

```

show dhcpv6 server binding detail

```

user@host> show dhcpv6 server binding detail

```

```

Session Id: 6
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:01

  State:
  BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86308 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Lease time violated:    yes
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:      0.0.0.0
    Server Interface:       none
    Client Id Length:       14
    Client Id:
    /0x00010001/0x02e159c0/0x00109400/0x0001

```

```

Session Id: 7
  Client IPv6 Address:     2002::1/128
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:
  BOUND(LOCAL_SERVER_STATE_BOUND_ON_INTF_DELETE)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86308 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:      0.0.0.0
    Client Pool Name:       bos-v6-pool
    Client Prefix Pool Name: bos-v6-prefix-pool
    Client Id Length:       14
    Client Id:
    /0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding interface

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101
Prefix          Session Id Expires State Interface Client DUID
2001:bd8:1111:2222::/64 1      86055   BOUND   ge-1/0/0.100
LL_TIME0x1-0x4b0a53b9-00:10:94:00:00:01

```

show dhcpv6 server binding interface detail

```

user@host> show dhcpv6 server binding interface ge-1/0/0:10-101 detail
Session Id: 7
  Client IPv6 Prefix:      2001:bd8:1111:2222::/64
  Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

  State:
  BOUND(bound)
    Lease Expires:         2009-07-21 10:41:15 PDT
    Lease Expires in:      86136 seconds
    Preferred Lease Expires: 2012-07-24 00:18:14 UTC
    Preferred Lease Expires in: 600 seconds
    Lease Start:           2009-07-20 10:41:15 PDT
    Incoming Client Interface: ge-1/0/0.0
    Server Ip Address:      0.0.0.0

```



```

Server Interface:          none
Client Id Length:         14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding (IPv6 Prefix)

```

user@host> show dhcpv6 server binding 14/0x00010001/0x02b3be8f/0x00109400/0x0005
detail
Session Id: 7
Client IPv6 Prefix:      2001:bd8:1111:2222::/64
Client DUID:             LL_TIME0x1-0x2e159c0-00:10:94:00:00:02

State:                   BOUND(bound)
Lease Expires:           2009-07-21 10:41:15 PDT
Lease Expires in:        86136 seconds
Preferred Lease Expires: 2012-07-24 00:18:14 UTC
Preferred Lease Expires in: 600 seconds
Lease Start:             2009-07-20 10:41:15 PDT
Incoming Client Interface: ge-1/0/0.0
Server Ip Address:       0.0.0.0
Server Interface:        none
Client Id Length:        14
Client Id:
/0x00010001/0x02e159c0/0x00109400/0x0002

```

show dhcpv6 server binding (Session ID)

```

user@host> show dhcpv6 server binding 8
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  8          86235  BOUND ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03

```

show dhcpv6 server binding (Interfaces VLAN)

```

user@host> show dhcpv6 server binding ge-1/0/0:100-200
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  11          87583  BOUND ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  12          87583  BOUND ge-1/0/0.1073741827
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 server binding (Interfaces Wildcard)

```

user@host> show dhcpv6 server binding demux0
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  30          79681  BOUND demux0.1073741824
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  31          79681  BOUND demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:CB9::/32  32          79681  BOUND demux0.1073741826
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

show dhcpv6 server binding (Interfaces Wildcard)

```

user@host> show dhcpv6 server binding ge-1/3/*
Prefix          Session Id Expires State Interface Client DUID
2001:DB8::/32  22          79681  BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB9::/32  33          79681  BOUND ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01

```

```
2001:CB9::/32      24      79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
```

show dhcpv6 server binding summary

```
user@host> show dhcpv6 server binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)
```

show dhcpv6 server statistics

Syntax	show dhcpv6 server statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 9.6.
Description	Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Display information about extended DHCPv6 local server statistics on the specified logical system. If you do not specify a logical system, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Display information about extended DHCPv6 local server statistics on the specified routing instance. If you do not specify a routing instance, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 server statistics on page 193
List of Sample Output	show dhcpv6 server statistics on page 218
Output Fields	Table 14 on page 218 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.

Table 14: show dhcpv6 server statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCPv6 local server because of errors. Only nonzero statistics appear in the Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.</p> <ul style="list-style-type: none"> • Total—Total number of packets discarded by the extended DHCPv6 local server • Strict Reconfigure—Number of solicit messages discarded because the client does not support reconfiguration • Bad hardware address—Number of packets discarded because an invalid hardware address was specified • Bad opcode—Number of packets discarded because an invalid operation code was specified • Bad options—Number of packets discarded because invalid options were specified • Invalid server address—Number of packets discarded because an invalid server address was specified • Lease Time Violation—Number of packets discarded because of a lease time violation • No available addresses—Number of packets discarded because there were no addresses available for assignment • No interface match—Number of packets discarded because they did not belong to a configured interface • No routing instance match—Number of packets discarded because they did not belong to a configured routing instance • No valid local address—Number of packets discarded because there was no valid local address • Packet too short—Number of packets discarded because they were too short • Read error—Number of packets discarded because of a system read error • Send error—Number of packets that the extended DHCPv6 local server could not send
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> • DHCPV6_CONFIRM—Number of DHCPv6 CONFIRM PDUs received. • DHCPV6_DECLINE—Number of DHCPv6 DECLINE PDUs received. • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 INFORMATION-REQUEST PDUs received. • DHCPV6_REBIND—Number of DHCPv6 REBIND PDUs received. • DHCPV6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received. • DHCPV6_RELAY_REPL—Number of DHCPv6 RELAY-REPL PDUs received. • DHCPV6_RELEASE—Number of DHCPv6 RELEASE PDUs received. • DHCPV6_RENEW—Number of DHCPv6 RENEW PDUs received. • DHCPV6_REQUEST—Number of DHCPv6 REQUEST PDUs received. • DHCPV6_SOLICIT—Number of DHCPv6 SOLICIT PDUs received.
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> • DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHCPV6_REPLY—Number of DHCPv6 ADVERTISE PDUs transmitted. • DHC6_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
```

Dhcpv6 Packets dropped:

Total	1
Lease Time Violation	1

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
DHCPV6_RELAY_REPL	0

Messages sent:

DHCPV6_ADVERTISE	9
DHCPV6_REPLY	5
DHCPV6_RECONFIGURE	0

show subscribers

Syntax show subscribers
 <detail | extensive | terse>
 <aci-interface-set-name *aci-interface-set-name*>
 <address *address*>
 <agent-circuit-identifier *agent-circuit-identifier-substring*>
 <client-type *client-type*>
 <count>
 <id>
 <interface *interface*>
 <logical-system *logical-system*>
 <mac-address *mac-address*>
 <physical-interface *physical-interface-name*>
 <profile-name *profile-name*>
 <routing-instance *routing-instance*>
 <stacked-vlan-id *stacked-vlan-id*>
 <subscriber-state *subscriber-state*>
 <user-name *user-name*>
 <vci *vci-identifier*>
 <vpi *vpi-identifier*>
 <vlan-id *vlan-id*>

Release Information Command introduced in Junos OS Release 9.3.
 Command introduced in Junos OS Release 9.3 for EX Series switches.
client-type, **mac-address**, **subscriber-state**, and **extensive** options introduced in Junos OS Release 10.2.
count option usage with other options introduced in Junos OS Release 10.2.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Options **aci-interface-set-name** and **agent-circuit-identifier** introduced in Junos OS Release 12.2.
 The **physical-interface** and **user-name** options introduced in Junos OS Release 12.3.
 Options **vci** and **vpi** introduced in Junos OS Release 12.3R3 and supported in later 12.3Rx releases.
 Options **vci** and **vpi** supported in Junos OS Release 13.2 and later releases. (Not supported in Junos OS Release 13.1.)

Description Display information for active subscribers.

Options **detail | extensive | terse**—(Optional) Display the specified level of output.

aci-interface-set-name—(Optional) Display all dynamic subscriber sessions that use the specified agent circuit identifier (ACI) interface set. Use the ACI interface set name generated by the router, such as aci-1003-ge-1/0/0.4001, and not the actual ACI value found in the DHCP or PPPoE control packets.

address—(Optional) Display subscribers whose IP address matches the specified address. You must specify the IPv4 or IPv6 address prefix without a netmask (for example, 192.168.17.1). If you specify the IP address as a prefix with a netmask (for example, 192.168.17.1/32), the router displays a message that the IP address is invalid, and rejects the command.

agent-circuit-identifier-substring—(Optional) Display all dynamic subscriber sessions whose ACI value matches the specified substring.

client-type—(Optional) Display subscribers whose client type matches the specified client type (DHCP, L2TP, PPP, PPPOE, VLAN, or static).

count—(Optional) Display the count of total subscribers and active subscribers for any specified option. You can use the ***count*** option alone or with the ***address***, ***client-type***, ***interface***, ***logical-system***, ***mac-address***, ***profile-name***, ***routing-instance***, ***stacked-vlan-id***, ***subscriber-state***, or ***vlan-id*** options.

id—(Optional) Display a specific subscriber session whose session id matches the specified subscriber ID. You can display subscriber IDs by using the ***show subscribers extensive*** or the ***show subscribers interface extensive*** commands.

interface—(Optional) Display subscribers whose interface matches the specified interface.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

mac-address—(Optional) Display subscribers whose MAC address matches the specified MAC address.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose physical interface matches the specified physical interface.

profile-name—(Optional) Display subscribers whose dynamic profile matches the specified profile name.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

stacked-vlan-id—(Optional) Display subscribers whose stacked VLAN ID matches the specified stacked VLAN ID.

subscriber-state—(Optional) Display subscribers whose subscriber state matches the specified subscriber state (ACTIVE, CONFIGURED, INIT, TERMINATED, or TERMINATING).

user-name—(M120, M320, and MX Series routers only) (Optional) Display subscribers whose username matches the specified subscriber name.

vci-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual circuit identifier (VCI) matches the specified VCI identifier. The range of values is **0** through **255**.

vpi-identifier—(MX Series routers with MPCs and ATM MICs with SFP only) (Optional) Display active ATM subscribers whose ATM virtual path identifier (VPI) matches the specified VPI identifier. The range of values is **0** through **65535**.

vlan-id—(Optional) Display subscribers whose VLAN ID matches the specified VLAN ID.



NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • show subscribers summary on page 238 • <i>Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration</i>
List of Sample Output	show subscribers (IPv4) on page 226 show subscribers (IPv6) on page 226 show subscribers (IPv4 and IPv6 Dual Stack) on page 226 show subscribers (LNS on MX Series Routers) on page 227 show subscribers (L2TP Switched Tunnels) on page 227 show subscribers client-type dhcp detail on page 227 show subscribers count on page 227 show subscribers address detail (IPv6) on page 227 show subscribers detail (IPv4) on page 228 show subscribers detail (IPv6) on page 228 show subscribers detail (IPv6 Static Demux Interface) on page 229 show subscribers detail (L2TP LNS Subscribers on MX Series Routers) on page 229 show subscribers detail (L2TP Switched Tunnels) on page 229 show subscribers detail (Tunneled Subscriber) on page 230 show subscribers detail (IPv4 and IPv6 Dual Stack) on page 230 show subscribers detail (ACI Interface Set Session) on page 231 show subscribers detail (PPPoE Subscriber Session with ACI Interface Set) on page 231 show subscribers extensive on page 231 show subscribers extensive (RPF Check Fail Filter) on page 232 show subscribers extensive (L2TP LNS Subscribers on MX Series Routers) on page 232 show subscribers extensive (IPv4 and IPv6 Dual Stack) on page 232 show subscribers extensive (Effective Shaping-Rate) on page 233 show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set) on page 234 show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring) on page 234 show subscribers interface extensive on page 235 show subscribers logical-system terse on page 235 show subscribers physical-interface count on page 236 show subscribers routing-instance inst1 count on page 236 show subscribers stacked-vlan-id detail on page 236 show subscribers stacked-vlan-id vlan-id detail (Combined Output) on page 236 show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface) on page 236 show subscribers user-name detail on page 236 show subscribers vlan-id on page 237

[show subscribers vlan-id detail on page 237](#)

[show subscribers vpi vci extensive \(PPPoE-over-ATM Subscriber Session\) on page 237](#)

Output Fields Table 15 on page 223 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 15: show subscribers Output Fields

Field Name	Field Description
Interface	Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface. The * character indicates a continuation of addresses for the same session.
IP Address/VLAN ID	Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> No IP address or VLAN ID is assigned to an L2TP tunnel-switched session. For these subscriber sessions the value is Tunnel-switched .
User Name	Name of subscriber.
LS:RI	Logical system and routing instance associated with the subscriber.
Type	Subscriber client type (DHCP, L2TP, PPP, PPPoE, STATIC-INTERFACE, VLAN).
IP Address	Subscriber IPv4 address.
IP Netmask	Subscriber IP netmask.
Primary DNS Address	IP address of primary DNS server.
Secondary DNS Address	IP address of secondary DNS server.
Primary WINS Address	IP address of primary WINS server.
Secondary WINS Address	IP address of secondary WINS server.
IPv6 Address	Subscriber IPv6 address, or multiple addresses.
IPv6 Prefix	Subscriber IPv6 prefix. If you are using DHCPv6 prefix delegation, this is the delegated prefix.
IPv6 User Prefix	IPv6 prefix obtained through ND/RA.
IPv6 Address Pool	Subscriber IPv6 address pool. The IPv6 address pool is used to allocate IPv6 prefixes to the DHCPv6 clients.
IPv6 Network Prefix Length	Length of the network portion of the IPv6 address.
IPv6 Prefix Length	Length of the subscriber IPv6 prefix.

Table 15: show subscribers Output Fields (*continued*)

Field Name	Field Description
Logical System	Logical system associated with the subscriber.
Routing Instance	Routing instance associated with the subscriber.
Interface Type	Whether the subscriber interface is Static or Dynamic .
Interface Set	Internally generated name of the dynamic ACI interface set used by the subscriber session.
Interface Set Type	Interface type of the ACI interface set: Dynamic . This is the only ACI interface set type currently supported.
Interface Set Session ID	Identifier of the dynamic ACI interface set entry in the session database.
Underlying Interface	Name of the underlying interface for the subscriber session.
Dynamic Profile Name	Dynamic profile used for the subscriber.
Dynamic Profile Version	Version number of the dynamic profile used for the subscriber.
MAC Address	MAC address associated with the subscriber.
State	Current state of the subscriber session (Init , Configured , Active , Terminating , Tunneled).
L2TP State	Current state of the L2TP session, Tunneled or Tunnel-switched . When the value is Tunnel-switched , two entries are displayed for the subscriber; the first entry is at the LNS interface on the LTS and the second entry is at the LAC interface on the LTS.
Tunnel switch Profile Name	Name of the L2TP tunnel switch profile that initiates tunnel switching.
Local IP Address	IP address of the local gateway (LAC).
Remote IP Address	IP address of the remote peer (LNS).
VLAN Id	VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
Stacked VLAN Id	Stacked VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i> .
RADIUS Accounting ID	RADIUS accounting ID associated with the subscriber.
Agent Circuit ID	Option 82 agent circuit ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
Agent Remote ID	Option 82 agent remote ID associated with the subscriber. The ID is displayed as an ASCII string unless the value has nonprintable characters, in which case it is displayed in hexadecimal format.
DHCP Relay IP Address	IP address used by the DHCP relay agent.

Table 15: show subscribers Output Fields (*continued*)

Field Name	Field Description
ATM VPI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual path identifier (VPI) on the subscriber's physical interface.
ATM VCI	(MX Series routers with MPCs and ATM MICs with SFP only) ATM virtual circuit identifier (VCI) for each VPI configured on the subscriber interface.
Login Time	Date and time at which the subscriber logged in.
Effective shaping-rate	Actual downstream traffic shaping rate for the subscriber, in kilobits per second.
IPv4 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv4 packets that fail the RPF check.
IPv6 rpf-check Fail Filter Name	Name of the filter applied by the dynamic profile to IPv6 packets that fail the RPF check.
DHCP Options	len = number of hex values in the message. The hex values specify the type, length, value (TLV) for DHCP options, as defined in RFC 2132.
Session ID	ID number for a subscriber service session.
Underlying Session ID	For DHCPv6 subscribers on a PPPoE network, displays the session ID of the underlying PPPoE interface.
Service Sessions	Number of service sessions (that is, a service activated using RADIUS CoA) associated with the subscribers.
Service Session Name	Service session profile name.
Session Timeout (seconds)	Number of seconds of access provided to the subscriber before the session is automatically terminated.
Idle Timeout (seconds)	Number of seconds subscriber can be idle before the session is automatically terminated.
IPv6 Delegated Address Pool	Name of the pool used for DHCPv6 prefix delegation.
IPv6 Delegated Network Prefix Length	Length of the prefix configured for the IPv6 delegated address pool.
IPv6 Interface Address	Address assigned by the Framed-Ipv6-Prefix AAA attribute.
IPv6 Framed Interface Id	Interface ID assigned by the Framed-Interface-Id AAA attribute.
ADF IPv4 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.

Table 15: show subscribers Output Fields (*continued*)

Field Name	Field Description
ADF IPv4 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv4 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Input Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 input filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
ADF IPv6 Output Filter Name	Name assigned to the Ascend-Data-Filter (ADF) interface IPv6 output filter (client or service session). The filter name is followed by the rules (in hexadecimal format) associated with the ADF filter and the decoded rule in Junos OS filter style.
IPv4 Input Filter Name	Name assigned to the IPv4 input filter (client or service session).
IPv4 Output Filter Name	Name assigned to the IPv4 output filter (client or service session).
IPv6 Input Filter Name	Name assigned to the IPv6 input filter (client or service session).
IPv6 Output Filter Name	Name assigned to the IPv6 output filter (client or service session).
IFL Input Filter Name	Name assigned to the logical interface input filter (client or service session).
IFL Output Filter Name	Name assigned to the logical interface output filter (client or service session).

Sample Output

show subscribers (IPv4)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/3/0.1073741824 100                 WHOLESALE-CLIENT  default:default
demux0.1073741824   100.0.0.10          RETAILER1-CLIENT  test1:retailer1
demux0.1073741825   101.0.0.3           RETAILER2-CLIENT  test1:retailer2
demux0.1073741826   102.0.0.3

```

show subscribers (IPv6)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/0/0.0         2001::c0:0:0:0/74  WHOLESALE-CLIENT  default:default
*                  2002::1/128        subscriber-25      default:default

```

show subscribers (IPv4 and IPv6 Dual Stack)

```

user@host> show subscribers
Interface          IP Address/VLAN ID  User Name
LS:RI
demux0.1073741834  0x8100.1002 0x8100.1
default:default
demux0.1073741835  0x8100.1001 0x8100.1
default:default
pp0.1073741836     61.1.1.1        dualstackuser1@ISP1.com

```

```

default:ASP-1
*                2041:1:1::/48
*                2061:1:1:1::/64
pp0.1073741837   23.1.1.3                dualstackuser2@ISP1.com
default:ASP-1
*                2001:1:2:5::/64

```

show subscribers (LNS on MX Series Routers)

```

user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-4/0/0.1     192.168.4.1         xyz@example.com default:default

```

show subscribers (L2TP Switched Tunnels)

```

user@host> show subscribers
Interface      IP Address/VLAN ID  User Name      LS:RI
si-2/1/0.1073741842 Tunnel-switched    ap@lts.com      default:default

si-2/1/0.1073741843 Tunnel-switched    ap@lts.com      default:default

```

show subscribers client-type dhcp detail

```

user@host> show subscribers client-type dhcp detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Login Time: 2009-08-25 14:43:52 PDT

Type: DHCP
IP Address: 100.20.10.7
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: demux0.1073744383
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:94:00:01:f3
State: Active
Radius Accounting ID: jnpr :2560
Login Time: 2009-08-25 14:43:56 PDT

```

show subscribers count

```

user@host> show subscribers count
Total Subscribers: 188, Active Subscribers: 188

```

show subscribers address detail (IPv6)

```

user@host> show subscribers address 100.16.12.137 detail

```

```
Type: PPPoE
User Name: pppoeTerV6User1Svc
IP Address: 100.16.12.137
IP Netmask: 255.0.0.0
IPv6 User Prefix: 1016:0:0:c88::/64
Logical System: default
Routing Instance: default
Interface: pp0.1073745151
Interface type: Dynamic
Underlying Interface: demux0.8201
Dynamic Profile Name: pppoe-client-profile
MAC Address: 00:0d:02:01:00:01
Session Timeout (seconds): 31622400
Idle Timeout (seconds): 86400
State: Active
Radius Accounting ID: jnpr demux0.8201:6544
Session ID: 6544
Agent Circuit ID: if13720
Agent Remote ID: if13720
Login Time: 2012-05-21 13:37:27 PDT
Service Sessions: 1
```

show subscribers detail (IPv4)

```
user@host> show subscribers detail
Type: DHCP
IP Address: 100.20.9.7
IP Netmask: 255.255.0.0
Primary DNS Address: 192.168.17.1
Secondary DNS Address: 192.168.17.2
Primary WINS Address: 192.168.22.1
Secondary WINS Address: 192.168.22.2
Logical System: default
Routing Instance: default
Interface: demux0.1073744127
Interface type: Dynamic
Dynamic Profile Name: dhcp-demux-prof
MAC Address: 00:10:95:00:00:98
State: Active
Radius Accounting ID: jnpr :2304
Idle Timeout (seconds): 600
Login Time: 2009-08-25 14:43:52 PDT
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 08 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 36 2f
33 2d 37 2d 30 37 05 01 06 0f 21 2c
Service Sessions: 2
```

show subscribers detail (IPv6)

```
user@host> show subscribers detail
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03
State: Active
Radius Accounting ID: 1
```

```

Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00

```

show subscribers detail (IPv6 Static Demux Interface)

```

user@host> show subscribers detail
Type: STATIC-INTERFACE
User Name: demux0.1@jnpr.net
IPv6 Prefix: 1:2:3:4:5:6:7:aa/128
Logical System: default
Routing Instance: default
Interface: demux0.1
Interface type: Static
Dynamic Profile Name: junos-default-profile
State: Active
Radius Accounting ID: 185
Login Time: 2010-05-18 14:33:56 EDT

```

show subscribers detail (L2TP LNS Subscribers on MX Series Routers)

```

user@host> show subscribers detail
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST

```

show subscribers detail (L2TP Switched Tunnels)

```

user@host> show subscribers detail
Type: L2TP
User Name: ap@example.com
Logical System: default
Routing Instance: default
Interface: si-2/1/0.1073741842
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.50.1.1
Remote IP Address: 192.168.20.3
Radius Accounting ID: 21
Session ID: 21
Login Time: 2013-01-18 03:01:11 PST

Type: L2TP
User Name: ap@example.com
Logical System: default

```

```
Routing Instance: default
Interface: si-2/1/0.1073741843
Interface type: Dynamic
Dynamic Profile Name: dyn-lts-profile
State: Active
L2TP State: Tunnel-switched
Tunnel switch Profile Name: ce-lts-profile
Local IP Address: 10.30.1.1
Remote IP Address: 172.20.1.10
Session ID: 22
Login Time: 2013-01-18 03:01:14 PST
```

show subscribers detail (Tunneled Subscriber)

```
user@host> show subscribers detail
Type: PPPoE
User Name: user1@example.com
Logical System: default
Routing Instance: default
Interface: pp0.1
State: Active, Tunneled
Radius Accounting ID: 512
```

show subscribers detail (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
```



```

State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00 00
00 00

```

show subscribers detail (ACI Interface Set Session)

```

user@host> show subscribers detail
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0
Interface Set: aci-1001-ge-1/0/0.2800
Interface Set Session ID: 0
Underlying Interface: ge-1/0/0.2800
Dynamic Profile Name: aci-vlan-set-profile-2
Dynamic Profile Version: 1
State: Active
Session ID: 1
Agent Circuit ID: aci-ppp-dhcp-20
Login Time: 2012-05-26 01:54:08 PDT

```

show subscribers detail (PPPoE Subscriber Session with ACI Interface Set)

```

user@host> show subscribers detail
Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.5
Logical System: default
Routing Instance: default
Interface: pp0.1073741825
Interface type: Dynamic
Interface Set: aci-1001-demux0.1073741824
Interface Set Type: Dynamic
Interface Set Session ID: 2
Underlying Interface: demux0.1073741824
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:64:39:01:02
State: Active
Radius Accounting ID: 3
Session ID: 3
Agent Circuit ID: aci-ppp-dhcp-dvlan-50
Login Time: 2012-03-07 13:46:53 PST

```

show subscribers extensive

```

user@host> show subscribers extensive
Type: DHCP
User Name: pd-user1
IPv6 Prefix: 2002:db2:ffff:1::/64
Logical System: default
Routing Instance: default
Interface: ge-3/1/3.2
Interface type: Static
MAC Address: 00:51:ff:ff:00:03

```

```
State: Active
Radius Accounting ID: 1
Session ID: 1
Login Time: 2011-08-25 12:12:26 PDT
DHCP Options: len 42
00 08 00 02 00 00 00 01 00 0a 00 03 00 01 00 51 ff ff 00 03
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
IPv6 Address Pool: pd_pool
IPv6 Network Prefix Length: 48
```

show subscribers extensive (RPF Check Fail Filter)

```
user@host> show subscribers extensive
...
Type: VLAN
Logical System: default
Routing Instance: default
Interface: ae0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof
State: Active
Session ID: 9
VLAN Id: 100
Login Time: 2011-08-26 08:17:00 PDT
IPv4 rpf-check Fail Filter Name: rpf-allow-dhcp
IPv6 rpf-check Fail Filter Name: rpf-allow-dhcpv6
...
```

show subscribers extensive (L2TP LNS Subscribers on MX Series Routers)

```
user@host> show subscribers extensive
Type: L2TP
User Name: user1@jnpr.net
IP Address: 10.1.32.58
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: si-5/2/0.1073749824
Interface type: Dynamic
Dynamic Profile Name: dyn-lns-profile2
Dynamic Profile Version: 1
State: Active
Radius Accounting ID: 8001
Session ID: 8001
Login Time: 2011-04-25 20:27:50 IST
IPv4 Input Filter Name: classify-si-5/2/0.1073749824-in
IPv4 Output Filter Name: classify-si-5/2/0.1073749824-out
```

show subscribers extensive (IPv4 and IPv6 Dual Stack)

```
user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlanProfile
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.1001
VLAN Id: 0x8100.1
```

```

Login Time: 2011-11-30 00:18:04 PST

Type: PPPoE
User Name: dualstackuser1@ISP1.com
IP Address: 61.1.1.1
IPv6 Prefix: 2041:1:1::/48
IPv6 User Prefix: 2061:1:1:1::/64
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Dynamic
Dynamic Profile Name: dualStack-Profile1
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
Login Time: 2011-11-30 00:18:05 PST
IPv6 Delegated Network Prefix Length: 48
IPv6 Interface Address: 2061:1:1:1::1/64
IPv6 Framed Interface Id: 1:1:2:2
IPv4 Input Filter Name: FILTER-IN-pp0.1073741825-in
IPv4 Output Filter Name: FILTER-OUT-pp0.1073741825-out
IPv6 Input Filter Name: FILTER-IN6-pp0.1073741825-in
IPv6 Output Filter Name: FILTER-OUT6-pp0.1073741825-out

Type: DHCP
IPv6 Prefix: 2041:1:1::/48
Logical System: default
Routing Instance: ASP-1
Interface: pp0.1073741825
Interface type: Static
MAC Address: 00:00:64:03:01:02
State: Active
Radius Accounting ID: jnpr :3
Session ID: 3
Underlying Session ID: 2
Login Time: 2011-11-30 00:18:35 PST
DHCP Options: len 42
00 08 00 02 0b b8 00 01 00 0a 00 03 00 01 00 00 64 03 01 02
00 06 00 02 00 19 00 19 00 0c 00 00 00 00 00 00 00 00 00
00 00
IPv6 Delegated Network Prefix Length: 48

```

show subscribers extensive (Effective Shaping-Rate)

```

user@host> show subscribers extensive
Type: VLAN
Logical System: default
Routing Instance: default
Interface: demux0.1073741837
Interface type: Dynamic
Interface Set: ifset-1
Underlying Interface: ae1
Dynamic Profile Name: svlan-dhcp-test
State: Active
Session ID: 1
Stacked VLAN Id: 0x8100.201
VLAN Id: 0x8100.201
Login Time: 2011-11-30 00:18:04 PST

```

Effective shaping-rate: 31000000k

...

show subscribers aci-interface-set-name detail (Subscriber Sessions Using Specified ACI Interface Set)

```
user@host> show subscribers aci-interface-set-name aci-1003-ge-1/0/0.4001 detail
```

Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001
Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT

show subscribers agent-circuit-identifier detail (Subscriber Sessions Using Specified ACI Substring)

```
user@host> show subscribers agent-circuit-identifier aci-ppp-vlan detail
```

Type: VLAN
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-set-profile
Dynamic Profile Version: 1
State: Active
Session ID: 13
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:56 PDT

Type: PPPoE
User Name: ppphint2
IP Address: 10.10.1.7
Logical System: default
Routing Instance: default
Interface: pp0.1073741834
Interface type: Dynamic
Interface Set: aci-1003-ge-1/0/0.4001

```

Interface Set Type: Dynamic
Interface Set Session ID: 13
Underlying Interface: ge-1/0/0.4001
Dynamic Profile Name: aci-vlan-pppoe-profile
Dynamic Profile Version: 1
MAC Address: 00:00:65:26:01:02
State: Active
Radius Accounting ID: 14
Session ID: 14
Agent Circuit ID: aci-ppp-vlan-10
Login Time: 2012-03-12 10:41:57 PDT

```

show subscribers interface extensive

```

user@host> show subscribers interface demux0.1073741826 extensive
Type: VLAN
User Name: test1@test.com
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Dynamic
Dynamic Profile Name: profile-vdemux-relay-23qos
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 12
Session ID: 12
Stacked VLAN Id: 0x8100.1500
VLAN Id: 0x8100.2902
Login Time: 2011-10-20 16:21:59 EST

Type: DHCP
User Name: test1@test.com
IP Address: 172.16.200.6
IP Netmask: 255.255.255.0
Logical System: default
Routing Instance: testnet
Interface: demux0.1073741826
Interface type: Static
MAC Address: 00:00:6e:56:01:04
State: Active
Radius Accounting ID: 21
Session ID: 21
Login Time: 2011-10-20 16:24:33 EST
Service Sessions: 2

Service Session ID: 25
Service Session Name: SUB-QOS
State: Active

Service Session ID: 26
Service Session Name: service-cb-content
State: Active
IPv4 Input Filter Name: content-cb-in-demux0.1073741826-in
IPv4 Output Filter Name: content-cb-out-demux0.1073741826-out

```

show subscribers logical-system terse

```

user@host> show subscribers logical-system test1 terse

```

Interface	IP Address/VLAN ID	User Name	LS:RI
demux0.1073741825	101.0.0.3	RETAILER1-CLIENT	test1:retailer1
demux0.1073741826	102.0.0.3	RETAILER2-CLIENT	test1:retailer2

show subscribers physical-interface count

```
user@host> show subscribers physical-interface ge-1/0/0 count
Total subscribers: 3998, Active Subscribers: 3998
```

show subscribers routing-instance inst1 count

```
user@host> show subscribers routing-instance inst1 count
Total Subscribers: 188, Active Subscribers: 183
```

show subscribers stacked-vlan-id detail

```
user@host> show subscribers stacked-vlan-id 101 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id detail (Combined Output)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers stacked-vlan-id vlan-id interface detail (Combined Output for a Specific Interface)

```
user@host> show subscribers stacked-vlan-id 101 vlan-id 100 interface ge-1/2/0.* detail
Type: VLAN
Interface: ge-1/2/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: svlan-prof
State: Active
Stacked VLAN Id: 0x8100.101
VLAN Id: 0x8100.100
Login Time: 2009-03-27 11:57:19 PDT
```

show subscribers user-name detail

```
user@host> show subscribers user-name larry1 detail
Type: DHCP
User Name: larry1
IP Address: 100.0.0.37
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: ge-1/0/0.1
Interface type: Static
Dynamic Profile Name: foo
MAC Address: 00:10:94:00:00:01
State: Active
Radius Accounting ID: 1
Session ID: 1
```

```

Login Time: 2011-11-07 08:25:59 PST
DHCP Options: len 52
35 01 01 39 02 02 40 3d 07 01 00 10 94 00 00 01 33 04 00 00
00 3c 0c 15 63 6c 69 65 6e 74 5f 50 6f 72 74 20 2f 2f 32 2f
37 2d 30 2d 30 37 05 01 06 0f 21 2c

```

show subscribers vlan-id

```

user@host> show subscribers vlan-id 100
Interface          IP Address          User Name
ge-1/0/0.1073741824
ge-1/2/0.1073741825

```

show subscribers vlan-id detail

```

user@host> show subscribers vlan-id 100 detail
Type: VLAN
Interface: ge-1/0/0.1073741824
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

Type: VLAN
Interface: ge-1/2/0.1073741825
Interface type: Dynamic
Dynamic Profile Name: vlan-prof-tpid
State: Active
VLAN Id: 100
Login Time: 2009-03-11 06:48:54 PDT

```

show subscribers vpi vci extensive (PPPoE-over-ATM Subscriber Session)

```

user@host> show subscribers vpi 40 vci 50 extensive
Type: PPPoE
User Name: testuser
IP Address: 100.0.0.2
IP Netmask: 255.255.0.0
Logical System: default
Routing Instance: default
Interface: pp0.0
Interface type: Static
MAC Address: 00:00:65:23:01:02
State: Active
Radius Accounting ID: 2
Session ID: 2
ATM VPI: 40
ATM VCI: 50
Login Time: 2012-12-03 07:49:26 PST
IP Address Pool: pool_1
IPv6 Framed Interface Id: 200:65ff:fe23:102

```

show subscribers summary

Syntax show subscribers summary
 <all>
 < detail | extensive | terse>
 <count>
 <physical-interface *physical-interface-name*>
 <logical-system *logical-system* pic | port | routing-instance *routing-instance* | slot>

Release Information Command introduced in Junos OS Release 10.2.

Description Display summary information for subscribers.

Options all—(Optional) Display full subscriber summary.

detail | extensive | terse—(Optional) Display the specified level of output.

count—(Optional) Display the count of total subscribers and active subscribers for any specified option.

logical-system—(Optional) Display subscribers whose logical system matches the specified logical system.

physical-interface-name—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers whose physical interface matches the specified physical interface, by subscriber state, client type and LS:RI.

pic—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by PIC number and the total number of subscribers.

port—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by port number and the total number of subscribers.

routing-instance—(Optional) Display subscribers whose routing instance matches the specified routing instance.

slot—(M120, M320, and MX Series routers only) (Optional) Display a count of subscribers by FPC slot number and the total number of subscribers.



NOTE: Due to display limitations, logical system and routing instance output values are truncated when necessary.

Required Privilege Level view

Related Documentation • [show subscribers on page 220](#)

List of Sample Output [show subscribers summary on page 240](#)

[show subscribers summary all on page 240](#)
[show subscribers summary physical-interface on page 240](#)
[show subscribers summary physical-interface pic on page 241](#)
[show subscribers summary physical-interface port on page 241](#)
[show subscribers summary physical-interface slot on page 241](#)
[show subscribers summary pic on page 241](#)
[show subscribers summary pic \(Aggregated Ethernet Interfaces\) on page 242](#)
[show subscribers summary port on page 242](#)
[show subscribers summary slot on page 242](#)
[show subscribers summary terse on page 242](#)

Output Fields Table 16 on page 239 lists the output fields for the **show subscribers** command. Output fields are listed in the approximate order in which they appear.

Table 16: show subscribers Output Fields

Field Name	Field Description
Subscribers by State	<p>Number of subscribers summarized by state. The summary information includes the following:</p> <ul style="list-style-type: none"> • Init—Number of subscriber currently in the initialization state. • Configured—Number of configured subscribers. • Active—Number of active subscribers. • Terminating—Number of subscribers currently terminating. • Terminated—Number of terminated subscribers. • Total—Total number of subscribers for all states.
Subscribers by Client Type	<p>Number of subscribers summarized by client type. Client types can include DHCP, L2TP, PPP, PPPOE, STATIC-INTERFACE, and VLAN. Also displays the total number of subscribers for all client types (Total).</p>
Subscribers by LS:RI	<p>Number of subscribers summarized by logical system:routing instance (LS:RI) combination. Also displays the total number of subscribers for all LS:RI combinations (Total).</p>
Interface	<p>Interface associated with the subscriber. The router or switch displays subscribers whose interface matches or begins with the specified interface.</p> <p>The * character indicates a continuation of addresses for the same session.</p> <p>For aggregated Ethernet interfaces, the output of the summary (pic port slot) options prefixes the interface name with ae0:.</p>
Count	<p>Count of subscribers displayed for each PIC, port, or slot when those options are specified with the summary option. For an aggregated Ethernet configuration, the total subscriber count does not equal the sum of the individual PIC, port, or slot counts, because each subscriber can be in more than one aggregated Ethernet link.</p>
Total Subscribers	<p>Total number of subscribers for all physical interfaces, all PICS, all ports, or all LS:RI slots.</p>
IP Address/VLAN ID	<p>Subscriber IP address or VLAN ID associated with the subscriber in the form <i>tpid.vlan-id</i></p>
User Name	<p>Name of subscriber.</p>
LS:RI	<p>Logical system and routing instance associated with the subscriber.</p>

Sample Output

show subscribers summary

```
user@host> show subscribers summary
```

Subscribers by State

Init	3
Configured	2
Active	183
Terminating	2
Terminated	1

TOTAL	191
-------	-----

Subscribers by Client Type

DHCP	107
PPP	76
VLAN	8

TOTAL	191
-------	-----

show subscribers summary all

```
user@host> show subscribers summary all
```

Subscribers by State

Init	3
Configured	2
Active	183
Terminating	2
Terminated	1

TOTAL	191
-------	-----

Subscribers by Client Type

DHCP	107
PPP	76
VLAN	8

TOTAL	191
-------	-----

Subscribers by LS:RI

default:default	1
default:ri1	28
default:ri2	16
ls1:default	22
ls1:riA	38
ls1:riB	44
logsysX:routinstY	42

TOTAL	191
-------	-----

show subscribers summary physical-interface

```
user@host> show subscribers summary physical-interface ge-1/0/0
```

Subscribers by State

Active:	3998
Total:	3998

Subscribers by Client Type

DHCP:	3998
-------	------

Total: 3998

Subscribers by LS:RI
 default:default: 3998
 Total: 3998

show subscribers summary physical-interface pic

```
user@host> show subscribers summary physical-interface ge-0/2/0 pic
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
 DHCP: 4825
 Total: 4825

Subscribers by LS:RI
 default:default: 4825
 Total: 4825

show subscribers summary physical-interface port

```
user@host> show subscribers summary physical-interface ge-0/3/0 port
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
 DHCP: 4825
 Total: 4825

Subscribers by LS:RI
 default:default: 4825
 Total: 4825

show subscribers summary physical-interface slot

```
user@host> show subscribers summary physical-interface ge-2/0/0 slot
Subscribers by State
Active: 4825
Total: 4825
```

Subscribers by Client Type
 DHCP: 4825
 Total: 4825

Subscribers by LS:RI
 default:default: 4825
 Total: 4825

show subscribers summary pic

```
user@host> show subscribers summary pic
Interface      Count
ge-1/0         1000
ge-1/3         1000

Total Subscribers: 2000
```

show subscribers summary pic (Aggregated Ethernet Interfaces)

```
user@host> show subscribers summary pic
Interface          Count
ae0: ge-1/0        801
ae0: ge-1/3        801

Total Subscribers: 801
```

show subscribers summary port

```
user@host> show subscribers summary port
Interface          Count
ge-1               2000

Total Subscribers: 2000
```

show subscribers summary slot

```
user@host> show subscribers summary slot
Interface          Count
ge-1               2000

Total Subscribers: 2000
```

show subscribers summary terse

```
user@host> show subscribers summary terse
Interface          IP Address/VLAN ID  User Name          LS:RI
ge-1/3/0.1073741824  100                WHOLESALE-CLIENT  default:default
demux0.1073741824    100.0.0.10         RETAILER1-CLIENT  test1:retailer1
demux0.1073741825    101.0.0.3          RETAILER2-CLIENT  test1:retailer2
demux0.1073741826    102.0.0.3          RETAILER2-CLIENT  test1:retailer2
```

PART 4

Troubleshooting

- [Acquiring Troubleshooting Information on page 245](#)
- [Troubleshooting Configuration Statements on page 255](#)

CHAPTER 7

Acquiring Troubleshooting Information

- [Tracing Extended DHCP Operations on page 245](#)
- [Tracing Extended DHCP Operations for Specific Interfaces on page 251](#)
- [Collecting Subscriber Access Logs Before Contacting Juniper Technical Support on page 252](#)

Tracing Extended DHCP Operations

Both the extended DHCP local server and the extended DHCP relay agent support tracing operations. DHCP tracing operations track extended DHCP operations and record them in a log file. The error descriptions captured in the log file provide detailed information to help you solve problems.

You can configure DHCP trace operations at the global level and at the interface level. Global DHCP tracing logs all DHCP-related events, whereas interface-level tracing logs only interface-specific DHCP events. If you configure interface-level trace operations, you can specify tracing for a range of interfaces or an individual interface. However, only a single interface-level log file is supported. That is, you cannot specify different interface-level log files for different interfaces or groups of interfaces.

By default, nothing is traced. When you enable the tracing operation, the default tracing behavior is as follows:

- Important events for both global and per-interface tracing are logged in a file located in the `/var/log` directory. By default, the router uses the filename, `jdhcpd`. You can specify a different filename, but you cannot change the directory in which trace files are located.
- When the trace log file ***filename*** reaches 128 kilobytes (KB), it is compressed and renamed ***filename.0.gz***. Subsequent events are logged in a new file called ***filename***, until it reaches capacity again. At this point, ***filename.0.gz*** is renamed ***filename.1.gz*** and ***filename*** is compressed and renamed ***filename.0.gz***. This process repeats until the number of archived files reaches the maximum file number. Then the oldest trace file—the one with the highest number—is overwritten.

You can optionally specify the number of trace files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB). (For more information about how log files are created, see the *Junos OS System Log Messages Reference*.)

- By default, only the user who configures the tracing operation can access log files. You can optionally configure read-only access for all users.

To configure global DHCP tracing operations.

- Specify tracing operations for DHCP local server and DHCP relay:

```
[edit system processes dhcp-service]
user@host# edit traceoptions
```

The tracing configuration is applied globally to all DHCP applications in every LS:RI. Configuration of event tracing on a per-LS:RI basis is not supported. DHCP tracing is configurable only in the default LS:RI. However, DHCP applications (local server or relay) do not have to be configured in the default LS:RI. This behavior was different in software releases before Junos OS Release 11.4, where you had to configure a DHCP application in the default LS:RI in order to configure DHCP tracing, even when you wanted to run DHCP and trace its operations only in a nondefault LS:RI.

In the earlier software releases, you configured tracing statements at the **[edit system services dhcp-local-server]** and **[edit forwarding-options dhcp-relay]** hierarchy levels. These statements have been deprecated and hidden in favor of the statements at the **[edit system processes dhcp-service]** hierarchy level.



NOTE: The deprecated statements may be removed from a future release; we recommend that you transition to the new statements.

Because you can configure DHCP tracing at three different hierarchy levels (one new and recommended, two old and deprecated), the following rules apply to manage the interaction:

- When you configure a filename or any other options for the trace log file, the configuration at the **[edit system processes dhcp-service]** hierarchy level has the highest precedence, followed by the configuration at the **[edit system services dhcp-local-server]** hierarchy level, and finally with the lowest precedence, the configuration at the **[edit forwarding-options dhcp-relay]** hierarchy level.
- The flag configurations for multiple hierarchy levels are merged and applied to all trace log events.
- The deprecated statements do not support filtering the generation of DHCP trace log events by severity level. If you use these statements, trace logging operates with an implicit severity of **all**, regardless of the severity level configured at the **[edit system processes dhcp-service]** hierarchy level.

For information about configuring per-interface tracing options, see [“Tracing Extended DHCP Operations for Specific Interfaces” on page 250](#).

The extended DHCP traceoptions operations are described in the following sections:

- [Configuring the Extended DHCP Log Filename on page 247](#)
- [Configuring the Number and Size of Extended DHCP Log Files on page 247](#)

- [Configuring Access to the Extended DHCP Log File on page 248](#)
- [Configuring a Regular Expression for Extended DHCP Messages to Be Logged on page 248](#)
- [Configuring the Extended DHCP Tracing Flags on page 249](#)
- [Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged on page 249](#)
- [Tracing Extended DHCP Operations for Specific Interfaces on page 250](#)

Configuring the Extended DHCP Log Filename

By default, the name of the file that records trace output is **jdhcpd**. You can specify a different name by including the **file** option. DHCP local server and DHCP relay agent both support the **file** option for the **traceoptions** statement and the **interface-traceoptions** statement.

To change the filename:

- Specify a filename for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set file filename
```

- Specify a filename for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set file filename
```

Configuring the Number and Size of Extended DHCP Log Files

You can optionally specify the number of compressed, archived trace log files to be from 2 through 1000. You can also configure the maximum file size to be from 10 KB through 1 gigabyte (GB); the default size is 128 kilobytes (KB).

The archived files are differentiated by a suffix in the format **.number.gz**. The newest archived file is **.0.gz** and the oldest archived file is **.(maximum number)-1.gz**. When the current trace log file reaches the maximum size, it is compressed and renamed, and any existing archived files are renamed. This process repeats until the maximum number of archived files is reached, at which point the oldest file is overwritten.

For example, you can 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 tracing operation, **filename**, reaches 2 MB, **filename** is compressed and renamed **filename.0.gz**, and a new file called **filename** is created. When the new **filename** reaches 2 MB, **filename.0.gz** is renamed **filename.1.gz** and **filename** is compressed and renamed **filename.0.gz**. This process repeats until there are 20 trace files. Then the oldest file, **filename.19.gz**, is simply overwritten when the next oldest file, **filename.18.gz** is compressed and renamed to **filename.19.gz**.

DHCP local server and DHCP relay agent both support the **files** and **size** options for the **traceoptions** statement and the **interface-traceoptions** statement. To configure the number and size of trace files:

- Specify the name, number, and size of the file used for the trace output for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename files number size maximum-file-size
```

- Specify the name, number, and size of the file used for the trace output for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename files number size maximum-file-size
```

Configuring Access to the Extended DHCP Log File

By default, only the user who configures the tracing operation can access the log files. You can enable all users to read the log file and you can explicitly set the default behavior of the log file.

DHCP local server and DHCP relay agent both support the **world-readable** option and the **no-world-readable** option for the **traceoptions** statement and the **interface-traceoptions** statement. To specify that all users can read the log file:

- Configure the log file to be world-readable for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename world-readable
```

- Configure the log file to be world-readable for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename world-readable
```

To explicitly set the default behavior, in which the log file can only be read by the user who configured tracing:

- Configure the log file to be no-world-readable for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename no-world-readable
```

- Configure the log file to be no-world-readable for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set file filename no-world-readable
```

Configuring a Regular Expression for Extended DHCP Messages to Be Logged

By default, the trace operation output includes all messages relevant to the logged events. You can refine the output by including regular expressions to be matched.

DHCP local server and DHCP relay agent both support the **match** option for the **traceoptions** statement and the **interface-traceoptions** statement. To configure regular expressions to be matched:

- Specify the regular expression for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set file filename match regular-expression
```

- Specify the regular expression for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set file filename match regular-expression
```

Configuring the Extended DHCP Tracing Flags

By default, only important events are logged. You can specify which events and operations are logged by specifying one or more tracing flags.

DHCP local server and DHCP relay agent both support the **flag** option for the **traceoptions** statement and the **interface-traceoptions** statement. A smaller set of flags is supported for interface-level tracing than for global tracing. To configure the flags for the events to be logged:

- Specify the flags for global tracing operations.

```
[edit system processes dhcp-service traceoptions]
user@host# set flag flag
```

- Specify the flags for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]
user@host# set flag flag
```

Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged

The messages associated with a logged event are categorized according to severity level. You can use the severity level to determine which messages are logged for the event type. A low severity level is less restrictive—filters out fewer messages—than a higher level. When you configure a severity level, all messages at that level and all higher (more restrictive) levels are logged.

The following list presents severity levels in order from lowest (least restrictive) to highest (most restrictive). This order also represents the significance of the messages; for example, **error** messages are of greater concern than **info** messages.

- **verbose**
- **info**
- **notice**
- **warning**
- **error**

The severity level that you configure depends on the issue that you are trying to resolve. In some cases you might be interested in seeing all messages relevant to the logged event, so you specify **all**. You can also specify **verbose** with the same result, because **verbose** is the lowest (least restrictive) severity level; it has nothing to do with the terseness or verbosity of the messages. Either choice generates a large amount of output. You can specify a more restrictive severity level, such as **notice** or **info** to filter the messages. By default, the trace operation output includes only messages with a severity level of **error**.

DHCP local server and DHCP relay agent both support the **level** option for the **traceoptions** statement and the **interface-traceoptions** statement. To configure the flags for the events to be logged:

- Specify the severity level for global tracing operations.

```
[edit system processes dhcp-service traceoptions]  
user@host# set level severity
```

- Specify the severity level for per-interface tracing operations.

```
[edit system processes dhcp-service interface-traceoptions]  
user@host# set level severity
```

Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



NOTE: Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in [“Tracing Extended DHCP Operations” on page 245](#).

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent:

```
[edit system processes dhcp-service]  
user@host# edit interface-traceoptions
```

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See [“Configuring the Extended DHCP Log Filename” on page 247](#).

- Configure the number and size of the log files.

See [“Configuring the Number and Size of Extended DHCP Log Files” on page 247](#).

- Configure access to the log file.

See [“Configuring Access to the Extended DHCP Log File” on page 248](#).

- Configure a regular expression to filter logging events.

See [“Configuring a Regular Expression for Extended DHCP Messages to Be Logged” on page 248](#).

- c. (Optional) Specify tracing flag options.

See [“Configuring the Extended DHCP Tracing Flags” on page 249](#).

- d. (Optional) Configure a severity level for messages to specify which event messages are logged.

See [“Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged” on page 249](#).

2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

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

- Enable tracing on a range of interfaces.

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

Tracing Extended DHCP Operations for Specific Interfaces

In addition to the global DHCP tracing operations, subscriber management enables you to trace extended DHCP operations for a specific interface or for a range of interfaces.

Configuring per-interface tracing is a two-step procedure. In the first step, you specify the tracing options that you want to use, such as file information and flags. In the second step, you enable the tracing operation on the specific interfaces.

To configure per-interface tracing operations:

1. Specify the tracing options you want to use.



NOTE: Per-interface tracing uses the same default tracing behavior as the global extended DHCP tracing operation. The default behavior is described in [“Tracing Extended DHCP Operations” on page 245](#).

- a. Specify that you want to configure per-interface tracing options.

- For DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent:

```
[edit system processes dhcp-service]
user@host# edit interface-traceoptions
```

- b. (Optional) Specify the tracing file options.

- Configure the name for the file used for the trace output.

See [“Configuring the Extended DHCP Log Filename”](#) on page 247.

- Configure the number and size of the log files.

See [“Configuring the Number and Size of Extended DHCP Log Files”](#) on page 247.

- Configure access to the log file.

See [“Configuring Access to the Extended DHCP Log File”](#) on page 248.

- Configure a regular expression to filter logging events.

See [“Configuring a Regular Expression for Extended DHCP Messages to Be Logged”](#) on page 248.

- c. (Optional) Specify tracing flag options.

See [“Configuring the Extended DHCP Tracing Flags”](#) on page 249.

- d. (Optional) Configure a severity level for messages to specify which event messages are logged.

See [“Configuring the Severity Level to Filter Which Extended DHCP Messages Are Logged”](#) on page 249.

2. Enable tracing on an interface or interface range.

The following examples show a DHCP local server configuration. You can also use the **trace** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level and at the **[edit system services dhcp-local-server dhcpv6]** hierarchy level.

- Enable tracing on a specific interface.

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

- Enable tracing on a range of interfaces.

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

**Related
Documentation**

- [Tracing Extended DHCP Operations](#) on page 245

Collecting Subscriber Access Logs Before Contacting Juniper Technical Support

Problem When you experience a subscriber access problem in your network, we recommend that you collect certain logs before you contact Juniper Technical Support. This topic shows you the most useful logs for a variety of network implementations. In addition to the relevant log information, you must also collect standard troubleshooting information and send it to Juniper Technical Support in your request for assistance.

Solution To collect standard troubleshooting information:

- Redirect the command output to a file.

```
user@host> request support information | save rsi-1
```

To configure logging to assist Juniper Technical Support:

1. Review the following blocks of statements to determine which apply to your configuration.

```
[edit]
set system syslog archive size 100m files 25
set system auto-configuration traceoptions file filename
set system auto-configuration traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions file filename size 100m files 25
set protocols ppp-service traceoptions level all
set protocols ppp-service traceoptions flag all
set protocols ppp traceoptions file filename size 100m files 25
set protocols ppp traceoptions level all
set protocols ppp traceoptions flag all
set protocols ppp monitor-session all
set interfaces pp0 traceoptions flag all
set demux traceoptions file filename size 100m files 25
set demux traceoptions level all
set demux traceoptions flag all
set system processes dhcp-service traceoptions file filename
set system processes dhcp-service traceoptions file size 100m
set system processes dhcp-service traceoptions file files 25
set system processes dhcp-service traceoptions flag all
set class-of-service traceoptions file filename
set class-of-service traceoptions file size 100m
set class-of-service traceoptions flag all
set class-of-service traceoptions file files 25
set routing-options traceoptions file filename
set routing-options traceoptions file size 100m
set routing-options traceoptions flag all
set routing-options traceoptions file files 25
set interfaces traceoptions file filename
set interfaces traceoptions file size 100m
set interfaces traceoptions flag all
set interfaces traceoptions file files 25
set system processes general-authentication-service traceoptions file filename
set system processes general-authentication-service traceoptions file size 100m
set system processes general-authentication-service traceoptions flag all
set system processes general-authentication-service traceoptions file files 25
```

2. Copy the relevant statements into a text file and modify the log filenames as you want.
3. Copy the statements from the text file and paste them into the CLI on your router to configure logging.
4. Commit the logging configuration to begin collecting information.



NOTE: The maximum file size for DHCP local server and DHCP relay log files is 1 GB. The maximum number of log files for DHCP local server and DHCP relay is 1000.



BEST PRACTICE: Enable these logs only to collect information when troubleshooting specific problems. Enabling these logs during normal operations can result in reduced system performance.

**Related
Documentation**

- *Compressing Troubleshooting Logs from /var/logs to Send to Juniper Technical Support*

CHAPTER 8

Troubleshooting Configuration Statements

- [interface-traceoptions \(DHCP\) on page 256](#)
- [trace \(DHCP Local Server\) on page 258](#)
- [traceoptions \(DHCP\) on page 259](#)

interface-traceoptions (DHCP)

Syntax	<pre>interface-traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; }</pre>
Hierarchy Level	[edit system processes dhcp-service]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	<p>Configure extended DHCP tracing operations that can be enabled on a specific interface or group of interfaces.</p> <p>Replaces deprecated interface-traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p> <p>To enable the tracing operation on the specific interfaces, you use the interface <i>interface-name</i> trace statement.</p>
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements</p> <ul style="list-style-type: none">• all—Trace all events• packet—Trace packet and option decoding operations• state—Trace changes in state <p>level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:</p> <ul style="list-style-type: none">• all—Match messages of all levels.• error—Match error messages.• info—Match informational messages.• notice—Match notice messages about conditions requiring special handling.

- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: *sizek* to specify KB, *sizem* to specify MB, or *sizeg* to specify GB

Range: 10240 through 1073741824

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration.
	trace-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • Tracing Extended DHCP Operations for Specific Interfaces on page 250

trace (DHCP Local Server)

Syntax	trace;
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> interface <i>interface-name</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Enable trace operations for a group of interfaces or for a specific interface within a group.
Required Privilege Level	<p>system—To view this statement in the configuration.</p> <p>system-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Tracing Extended DHCP Operations on page 245 • Tracing Extended DHCP Operations for Specific Interfaces on page 250

traceoptions (DHCP)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i> > <size <i>maximum-file-size</i>> <world-readable no-world-readable>; flag <i>flag</i>; level (all error info notice verbose warning); no-remote-trace; } </pre>
Hierarchy Level	[edit system processes dhcp-service]
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.</p> <p>Replaces deprecated traceoptions statements at the [edit forwarding-options dhcp-relay] and [edit system services dhcp-local-server] hierarchy levels.</p>
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory /var/log.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the size option.</p> <p>Range: 2 through 1000</p> <p>Default: 3 files</p> <p>flag <i>flag</i>—Tracing operation to perform. To specify more than one tracing operation, include multiple flag statements</p> <ul style="list-style-type: none"> • all—Trace all events. • auth—Trace authentication events. • 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 and option 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 events.
- **state**—Trace changes in state.
- **statistics**—Trace baseline statistics.
- **ui**—Trace user interface operations.

level—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- **all**—Match messages of all levels.
- **error**—Match error messages.
- **info**—Match informational messages.
- **notice**—Match notice messages about conditions requiring special handling.
- **verbose**—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure **verbose**, messages at all higher levels are traced. Therefore, the result is the same as when you configure **all**.
- **warning**—Match warning messages.

Default: error

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—Disable remote tracing.

no-world-readable—(Optional) Disable unrestricted file access, allowing only the user **root** and users who have the Junos OS **maintenance** permission to access the trace files.

size *maximum-file-size*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option.

Syntax: **sizek** to specify KB, **sizem** to specify MB, or **sizeg** to specify GB

Range: 10240 through 1073741824

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege Level	trace—To view this statement in the configuration. trace-control—To add this statement to the configuration.
---------------------------------	---

Related Documentation	• Tracing Extended DHCP Operations on page 245
------------------------------	--

PART 5

Index

- [Index on page 263](#)

Index

Symbols

#, comments in configuration statements.....	xvi
\$junos-subscriber-ipv6-multi-address predefined variable.....	26
(), in syntax descriptions.....	xvi
< >, in syntax descriptions.....	xvi
[], in configuration statements.....	xvi
{ }, in configuration statements.....	xvi
(pipe), in syntax descriptions.....	xvi

A

AAA directed logout	
DHCP authentication services.....	40
accounting	
opaque DHCP options.....	31
address-assignment pools	
DHCP local server.....	8
aggregate-clients statement	
DHCP local server.....	96
attempts statement	
DHCP local server.....	97
authentication services	
with DHCP.....	40
authentication statement	
DHCP local server.....	98
auto logout	
DHCP.....	22

B

bfd statement	
liveness detection method.....	99
binding state of DHCP client	
clearing.....	186
displaying.....	203
binding state of DHCPv6 client	
clearing.....	191
displaying.....	211
bindingst	
clearing DHCP.....	179
BOOTREPLY packets	
DHCP snooping.....	21

braces, in configuration statements.....	xvi
brackets	
angle, in syntax descriptions.....	xvi
square, in configuration statements.....	xvi

C

circuit-type statement	
DHCP local server.....	100
clear dhcp server binding command.....	186
clear dhcp server statistics command.....	189
clear dhcpv6 server binding command.....	191
clear dhcpv6 server statistics command.....	193
clear-on-abort statement	
DHCP local server.....	101
client configuration information	
DHCP.....	7
client usernames	
DHCP	
unique.....	72
client-discover-match statement	
DHCP local server.....	102
client-id statement.....	103
comments, in configuration statements.....	xvi
conventions	
text and syntax.....	xv
curly braces, in configuration statements.....	xvi
customer support.....	xvii
contacting JTAC.....	xvii

D

default subscriber service.....	14
configuring.....	45
delegated-pool statement	
DHCP local server.....	104
delimiter statement	
DHCP local server.....	105
detection-time statement	
liveness detection.....	106
DHCP	
allowing one client per interface.....	50
authentication services.....	40
AAA directed logout.....	40
auto logout.....	22
centrally-configured DHCP options.....	28, 181
clearing bindings.....	179
client configuration information.....	7
default route installation	
preventing.....	16, 52

distinguishing duplicate clients		default route installation	
based on interface.....	43	preventing.....	16, 52
based on option 82.....	42	delegated IPv6 pool.....	56
duplicate client IDs.....	15	DHCP snooping.....	21, 70
duplicate clients		DHCPv6.....	10
configuration guidelines.....	41	DHCPv6 rapid commit.....	57
duplicate hardware addresses.....	15	dynamic client reconfiguration	
extended server binding		authentication token configuration.....	62
clearing.....	186	behavior on failure configuration.....	61
displaying.....	203	configuration overview.....	58
extended server statistics		number of attempts configuration.....	60
clearing.....	189	preventing binding of nonsupporting	
displaying.....	208	clients.....	62
firewall filters on routers using the jdhcpd		RADIUS-initiated disconnect	
process.....	34	configuration.....	61
example.....	79	requesting.....	63
grouping interfaces.....	45	dynamic profile attachment	
configuration guidelines.....	46	multiple subscribers.....	68
information request processing		overview.....	12
overriding.....	55	use primary profile.....	68
maximum clients per interface		graceful Routing Engine switchover.....	33
overriding.....	49	grouping interfaces	
message severity levels for tracing		options.....	16
operations.....	249	information request message processing.....	11
override settings		information request processing	
deleting.....	58	overriding.....	55
rapid commit.....	57	interaction	
regular expressions for tracing		address-assignment pools.....	6
operations.....	248	DHCP clients.....	6
unique client usernames.....	72	lease time thresholds.....	32
user passwords.....	71	liveness detection.....	9, 65
DHCP client		maximum clients per interface	
binding state		overriding.....	49
clearing.....	186	minimal configuration	
displaying.....	203	default settings.....	8
statistics		option 50.....	25
clearing.....	189	override settings	
displaying.....	208	deleting.....	58
DHCP lease thresholds		overriding default configuration.....	48
configuring.....	67	overriding third-party leases.....	67
DHCP lease time thresholds		overview.....	4
DHCP.....	32	per-interface tracing operations.....	250, 251
DHCP lease-time validation.....	32	processing client information requests.....	11
DHCP local server		reconfigure client bindings.....	194
address-assignment pool selection.....	74	specific address.....	25
address-assignment pools.....	8	subnet for client addresses.....	75
allowing one client per interface.....	50	tracing operations.....	245
client auto logout.....	53	verifying configuration.....	183

DHCP local server statements	
attempts.....	97
circuit-type.....	100
clear-on-abort.....	101
client-discover-match.....	102
client-id.....	103
delegated-pool	104
delimiter.....	105
dhcp-local-server.....	107
dhcpv6.....	112
domain-name.....	115
duplicate-clients-in-subnet.....	116
dynamic-profile.....	117
forward-snooped-clients.....	120
group.....	121
interface.....	124
interface-client-limit.....	126
interface-name.....	128
interface-traceoptions.....	256
ip-address-first.....	129
lease-time-threshold.....	130
lease-time-validation.....	131
logical-system-name.....	133
mac-address.....	134
option-60.....	142
option-82.....	143, 144
overrides.....	145
password.....	147
pool.....	148
pool-match-order.....	149
process-inform.....	150
rapid-commit.....	153
relay-agent-interface-id.....	155
relay-agent-remote-id.....	156
relay-agent-subscriber-id.....	157
requested-ip-network-match.....	158
route-suppression.....	159
routing-instance-name.....	160
service-profile.....	161
strict.....	163
timeout.....	167
trace.....	258
traceoptions.....	259
trigger.....	170
username-include.....	173
violation-action.....	175
DHCP options	
accounting.....	31
configuring on RADIUS.....	28
opaque.....	28
RADIUS-sourced.....	28
renewing.....	31
verifying.....	181
DHCP relay	
allowing one client per interface.....	50
client auto logout.....	53
default route installation	
preventing.....	16, 52
DHCP snooping.....	21
dynamic profile attachment	
multiple subscribers.....	68
overview.....	12
use primary profile.....	68
graceful Routing Engine switchover.....	33
lease time thresholds.....	32
maximum clients per interface	
overriding.....	49
override settings	
deleting.....	58
overriding third-party leases.....	67
per-interface tracing operations.....	250, 251
tracing operations.....	245
DHCP relay agent statements	
duplicate-clients-in-subnet.....	116
interface-traceoptions.....	256
lease-time-threshold.....	130
lease-time-validation.....	131
route-suppression.....	159
traceoptions.....	259
use-primary.....	171
user-prefix.....	172
violation-action.....	175
DHCP snooping	
BOOTREPLY packets.....	21
DHCP local server.....	21, 70
disabling interfaces.....	21
enabling interfaces.....	21
example of DHCP relay agent	
configuration.....	83
DHCP subscriber	
auto logout.....	53
liveness detection.....	65
dhcp-local-server statement.....	107

DHCPv6	
DNS address	
multiple addresses.....	27, 57
extended server binding	
clearing.....	191
displaying.....	211
extended server statistics	
clearing.....	193
displaying.....	217
multiple address assignment.....	26
DHCPv6 client	
binding state	
clearing.....	191
displaying.....	211
statistics	
clearing.....	193
displaying.....	217
DHCPv6 local server	
IA_NA.....	25
overview.....	10
reconfigure client bindings.....	196
specific address.....	25
verifying configuration.....	183
DHCPv6 local server statements	
multi-address-embedded-option-response.....	139
dhcpcv6 statement.....	112
directed logout	
AAA.....	40
DNS address assignment	
DHCPv6 multiple addresses.....	27, 57
documentation	
comments on.....	xvii
domain-name statement	
DHCP local server.....	115
duplicate clients	
DHCP.....	15
based on interface.....	43
based on option 82.....	42
configuration guidelines.....	41
duplicate-clients-in-subnet statement	
DHCP local server.....	116
DHCP relay agent.....	116
dynamic client reconfiguration	
DHCP local server	
attempts configuration.....	60
authentication token configuration.....	62
behavior on failure configuration.....	61
configuration overview.....	58
preventing binding of nonsupporting clients.....	62
RADIUS-initiated disconnect	
configuration.....	61
requesting.....	63
Dynamic Host Control Protocol See DHCP	
dynamic profiles	
DHCP attachment.....	68
overview.....	12
interface support	
overview.....	12
dynamic-profile statement	
DHCP local server.....	117
E	
enforce-strict-scale-limit-license statement	
subscriber management.....	118
extended DHCP local server	
overview.....	4
external-authority statement	
DHCP local server pool matching.....	118
F	
failure-action statement	
liveness detection.....	119
firewall filter	
DHCP on routers using the jdncpd process.....	34
example	
DHCP on routers using the jdncpd	
process.....	79
font conventions.....	xv
forward-snooped-clients statement	
DHCP local server.....	120
G	
graceful Routing Engine switchover	
DHCP.....	33
group statement	
DHCP local server.....	121
H	
holdddown-interval statement	
liveness detection.....	123
I	
IA_NA	
DHCPv6 local server.....	25
interface delete events	
maintaining subscribers.....	24, 54

- interface groups
 - DHCP local server
 - configuration guidelines.....46
 - options.....16
 - DHCP relay
 - configuration guidelines.....46
 - interface ranges
 - DHCP configuration guidelines.....46
 - interface statement
 - DHCP local server.....124
 - interface-client-limit statement
 - DHCP local server.....126
 - interface-delete statement
 - subscriber management.....127
 - interface-name statement
 - DHCP local server.....128
 - interface-traceoptions statement
 - DHCP local server.....256
 - DHCP relay agent.....256
 - ip-address-first statement.....129
- J**
- Junos OS
 - rebooting.....198
- L**
- lease-time-threshold
 - DHCP local server.....130
 - DHCP relay agent.....130
 - lease-time-validation
 - DHCP local server.....131
 - DHCP relay agent.....131
 - license
 - subscriber scaling.....54
 - liveness detection
 - DHCP local server.....9
 - liveness-detection statement.....132
 - log files
 - collecting for Juniper Technical Support.....252
 - logical-system-name statement
 - DHCP local server.....133
 - ltv-syslog-interval statement
 - DHCP server process interval.....133
- M**
- mac-address statement
 - DHCP local server.....134
 - maintain-subscriber statement
 - subscriber management.....135
 - maintaining subscribers
 - interface delete events.....24, 54
 - verifying configuration.....184
 - manuals
 - comments on.....xvii
 - method statement
 - liveness detection.....136
 - minimum-interval statement
 - liveness detection.....137, 138
 - multi-address-embedded-option-responsestatement
 - DHCPv6 local server.....139
 - multiple address assignment
 - DHCPv6.....26
 - multiple DHCPv6 addresses
 - predefined variable.....26
 - multiplier statement
 - liveness detection.....140
- N**
- no-adaptation statement
 - liveness detection.....141
- O**
- opaque DHCP options.....28
 - option 50
 - DHCP local server.....25
 - option-60 statement
 - DHCP local server.....142
 - option-82 statement
 - DHCP local server authentication.....143
 - DHCP local server pool matching.....144
 - overrides statement
 - DHCP local server.....145
- P**
- parentheses, in syntax descriptions.....xvi
 - password statement
 - DHCP local server.....147
 - passwords
 - DHCP users.....71
 - per-interface tracing operations
 - DHCP local server.....250, 251
 - DHCP relay.....250, 251
 - pool statement
 - DHCP local server.....148
 - pool-match-order statement.....149
 - process-inform statement
 - DHCP local server.....150

R

radius-disconnect statement	
DHCP local server.....	152
RADIUS-sourced DHCP options.....	28
rapid commit	
DHCP.....	57
rapid-commit statement	
DHCP local server.....	153
rebooting router software	
requesting a system reboot.....	198
reconfigure statement	
DHCP local server.....	154
relay-agent-interface-id statement	
DHCP local server.....	155
relay-agent-remote-id statement	
DHCP local server statements.....	156
relay-agent-subscriber-id statement	
DHCP local server.....	157
request dhcp server reconfigure command.....	194
request dhcpv6 server reconfigure command.....	196
request system reboot command.....	198
requested-ip-network-match statement	
DHCP local server.....	158
route-suppression	
DHCP local server.....	159
DHCP relay agent.....	159
routing-instance-name statement	
DHCP local server.....	160

S

service-profile statement	
DHCP local server.....	161
session-mode statement	
liveness detection.....	162
show dhcp server binding command.....	203
show dhcp server statistics command.....	208
show dhcpv6 server binding command.....	211
show dhcpv6 server statistics command.....	217
show subscribers command.....	220
show subscribers summary command.....	238
strict statement	
DHCP local server.....	163
subscriber access	
subscriber information, displaying.....	220
subscriber summary information,	
displaying.....	238
subscriber management statements	
enforce-strict-scale-limit-license.....	118
interface-delete.....	127

maintain-subscriber.....	135
subscriber-management.....	164
subscriber service	
default.....	14, 45
subscriber-management statement	
subscriber management.....	164
subscribers	
displaying.....	220
displaying summary.....	238
support, technical See technical support	
syntax conventions.....	xv

T

technical support	
collecting logs for.....	252
contacting JTAC.....	xvii
third-party DHCP leases	
overriding.....	67
timeout statement	
DHCP local server.....	167
token statement	
DHCP local server.....	168
trace operations	
collecting logs for Juniper technical	
support.....	252
trace statement	
DHCP local server.....	258
traceoptions statement	
DHCP local server.....	259
DHCP relay agent.....	259
tracing operations	
DHCP local server.....	245
DHCP local server interface-specific.....	256
DHCP relay.....	245
DHCP relay interface-specific.....	256
transmit-interval statement	
liveness detection.....	165, 166, 169
trigger statement	
DHCP local server.....	170
troubleshooting subscriber access	
collecting logs for Juniper Technical	
Support.....	252

U

use-primary statement	
DHCP local server.....	171
user-prefix statement	
DHCP local server.....	172

username-include statement
 DHCP local server.....173

V

version statement
 liveness detection.....174

violation-action
 DHCP local server.....175
 DHCP relay agent.....175

VSA 26-55
 opaque DHCP options.....28
 RADIUS-sourced DHCP options.....28

