



Junos[®] OS for EX Series Ethernet Switches

System Services on EX4300 Switches

Release

14.1X53



Modified: 2016-06-13

Juniper Networks, Inc.
1133 Innovation Way
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 for EX Series Ethernet Switches System Services on EX4300 Switches
Release 14.1X53
Copyright © 2016, 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	xvii
	Documentation and Release Notes	xvii
	Supported Platforms	xvii
	Using the Examples in This Manual	xvii
	Merging a Full Example	xviii
	Merging a Snippet	xviii
	Documentation Conventions	xix
	Documentation Feedback	xxi
	Requesting Technical Support	xxi
	Self-Help Online Tools and Resources	xxi
	Opening a Case with JTAC	xxii
Part 1	Overview	
Chapter 1	Software Overview	3
	Understanding Software Infrastructure and Processes	3
	Routing Engine and Packet Forwarding Engine	3
	Junos OS Processes	4
Chapter 2	DHCP Local Server	7
	Extended DHCP Local Server Overview	8
	Interaction Among the DHCP Client, Extended DHCP Local Server, and Address-Assignment Pools	10
	Providing DHCP Client Configuration Information	10
	Minimal Configuration for Clients	12
	DHCP Local Server and Address-Assignment Pools	12
	DHCPv6 Local Server Overview	13
	DHCP Local Server Handling of Client Information Request Messages	15
	Configuring Group-Specific DHCP Local Server Options	16
	Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients	16
	Default Client/Server Interaction	16
	Dynamic Client/Server Interaction for DHCPv4	17
	Dynamic Client/Server Interaction for DHCPv6	17
	Manually Forcing the Local Server to Initiate the Reconfiguration Process	18
	Action Taken for Events That Occur During a Reconfiguration	18
	DHCP Snooping Support	19
	DHCP Auto Logout Overview	20
	Auto Logout Overview	20
	How DHCP Identifies and Releases Clients	21

	Option 60 and Option 82 Requirements	22
	Address-Assignment Pools Overview	22
	Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option	23
	Multiple Address Assignment for DHCPv6 Clients	23
	Multiple Address Assignment Using Local Address Pools or RADIUS	24
	Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment	24
	Centrally Configured Opaque DHCP Options	25
	Data Flow for RADIUS-Sourced DHCP Options	27
	Multiple VSA 26-55 Instances Configuration	28
	DHCP Options That Cannot Be Centrally Configured	28
	Port Number Requirements for DHCP Firewall Filters	29
Chapter 3	DHCP Relay Agent	31
	Extended DHCP Relay Agent Overview	32
	Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers	33
	DHCP Liveness Detection	34
	DHCP Relay Proxy Overview	35
	Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers	35
	DHCPv6 Relay Agent Overview	37
	Configuring Group-Specific DHCP Relay Options	38
	DHCP Snooping Support	39
	DHCP Auto Logout Overview	40
	Auto Logout Overview	40
	How DHCP Identifies and Releases Clients	40
	Option 60 and Option 82 Requirements	41
	Suppressing DHCP Access, Access-Internal, and Destination Routes	42
Chapter 4	Public Key Cryptography Overview	43
	Understanding Public Key Cryptography on Switches	43
	Public Key Infrastructure (PKI) and Digital Certificates	44
Chapter 5	Self-Signed Certificates Overview	45
	Understanding Self-Signed Certificates on EX Series Switches	45
Part 2	Configuration	
Chapter 6	DHCP Local Server Examples	49
	Example: Minimum Extended DHCP Local Server Configuration	49
	Example: Extended DHCP Local Server Configuration with Optional Pool Matching	50
	Example: Configuring Group Liveness Detection for DHCP Local Server Clients	50
Chapter 7	DHCP Relay Agent Examples	55
	Example: Minimum DHCP Relay Agent Configuration	55
	Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings	56
	Example: Configuring DHCP Snooping Support for DHCP Relay Agent	60

Chapter 8	Configuration Tasks	63
	Configuring DHCP Services (J-Web Procedure)	63
	Configuring DHCP Services (J-Web Procedure) on EX Series Switches	63
	Configuring DHCP Services on EX4300 Switches (J-Web Procedure)	66
	Configuring a DHCP SIP Server (CLI Procedure)	71
	Configuring a DHCP Client (CLI Procedure)	71
	Configuring a Switch as a DHCP Server (CLI Procedure)	72
	Configuring the Switch as a Local DHCP Server	73
	Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)	75
	Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)	76
	Manually Generating Self-Signed Certificates on Switches (CLI Procedure)	77
	Generating a Public-Private Key Pair on Switches	77
	Generating Self-Signed Certificates on Switches	78
	Deleting Self-Signed Certificates (CLI Procedure)	78
	Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default	79
Chapter 9	Configuration Tasks for DHCP Local Server	81
	Using External AAA Authentication Services with DHCP	82
	Grouping Interfaces with Common DHCP Configurations	83
	Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces	84
	Overriding Default DHCP Local Server Configuration Settings	85
	Specifying the Maximum Number of DHCP Clients Per Interface	86
	Automatically Logging Out DHCP Clients	88
	Enabling Processing of Client Information Requests	89
	Specifying the Delegated Address Pool for IPv6 Prefix Assignment	90
	Enabling DHCPv6 Rapid Commit Support	90
	Deleting DHCP Local Server and DHCP Relay Override Settings	91
	Configuring Dynamic Client Reconfiguration of Extended Local Server Clients	92
	Configuring Dynamic Reconfiguration Attempts for DHCP Clients	94
	Configuring Deletion of the Client When Dynamic Reconfiguration Fails	95
	Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect	95
	Configuring a Token for DHCP Local Server Authentication	96
	Preventing Binding of Clients That Do Not Support Reconfigure Messages	96
	Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings	97
	Configuring Detection of DHCP Local Server Client Connectivity	98
	Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server	100
	Configuring Passwords for Usernames	101
	Creating Unique Usernames for DHCP Clients	101
	Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use	104

Chapter 10	Configuration Tasks for DHCP Relay Agent	107
	Using External AAA Authentication Services with DHCP	108
	Grouping Interfaces with Common DHCP Configurations	109
	Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces	110
	Overriding the Default DHCP Relay Configuration Settings	111
	Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent	113
	Replacing the DHCP Relay Request and Release Packet Source Address	113
	Overriding Option 82 Information	114
	Using Layer 2 Unicast Transmission for DHCP Packets	114
	Trusting Option 82 Information	115
	Specifying the Maximum Number of DHCP Clients Per Interface	115
	Automatically Logging Out DHCP Clients	116
	How DHCP Relay Agent Uses Option 82 for Auto Logout	117
	Configuring DHCP Snooping for DHCP Relay Agent	119
	Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent	119
	Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent	124
	Sending Release Messages When Clients Are Deleted	126
	Disabling Automatic Binding of Stray DHCP Requests	127
	Using DHCP Relay Agent Option 82 Information	128
	Configuring Option 82 Information	129
	Including a Prefix in DHCP Options	131
	Including a Textual Description in DHCP Options	133
	Configuring Server Groups	135
	Configuring Active Server Groups	135
	Enabling DHCP Relay Proxy Mode	136
	Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets	136
	DHCP Liveness Detection Overview	137
	Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity	139
	Disabling DHCP Relay	140
Chapter 11	DHCP Local Server Configuration Statements	143
	allow-no-end-option (DHCP Local Server)	145
	attempts (DHCP Local Server)	146
	authentication (DHCP Local Server)	147
	bfd	148
	circuit-type (DHCP Local Server)	149
	clear-on-abort (DHCP Local Server)	150
	client-discover-match (DHCP Local Server)	151
	client-id (DHCP Local Server)	152
	delegated-pool (DHCP Local Server)	153
	delimiter (DHCP Local Server)	154
	detection-time	155
	dhcp (DHCP Client)	156
	dhcp-local-server	157
	dhcpv6 (DHCP Local Server)	162

domain-name (DHCP Local Server)	165
dynamic-profile (DHCP Local Server)	166
external-authority	167
failure-action	168
forward-snooped-clients (DHCP Local Server)	169
group (DHCP Local Server)	170
holddown-interval	172
interface (DHCP Local Server)	173
interface-client-limit (DHCP Local Server)	175
interface-delete (Subscriber Management or DHCP Client Management)	176
interface-name (DHCP Local Server)	177
ip-address-first	178
liveness-detection	179
mac-address (DHCP Local Server)	180
method	181
minimum-interval	182
minimum-receive-interval	183
multiplier	184
no-adaptation	185
option-60 (DHCP Local Server)	186
option-82 (DHCP Local Server Authentication)	187
option-82 (DHCP Local Server Pool Matching)	188
overrides (DHCP Local Server)	189
password (DHCP Local Server)	191
pool (DHCP Local Server Overrides)	192
pool-match-order	193
process-inform	194
radius-disconnect (DHCP Local Server)	196
rapid-commit (DHCPv6 Local Server)	197
reconfigure (DHCP Local Server)	198
relay-agent-interface-id (DHCP Local Server)	199
relay-agent-remote-id (DHCP Local Server)	200
routing-instance-name (DHCP Local Server)	201
service-profile (DHCP Local Server)	202
session-mode	203
strict (DHCP Local Server)	204
threshold (detection-time)	205
threshold (transmit-interval)	206
timeout (DHCP Local Server)	207
token (DHCP Local Server)	208
traceoptions (DHCP Server)	209
transmit-interval	212
trigger (DHCP Local Server)	213
use-primary (DHCP Local Server)	214
user-prefix (DHCP Local Server)	215
username-include (DHCP Local Server)	216
version (bfd)	217

Chapter 12	DHCP Relay Agent Configuration Statements	219
	[edit forwarding-options dhcp-relay] Configuration Statement Hierarchy for EX Series Switches	221
	Supported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level	221
	Unsupported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level	225
	access (Dynamic Access Routes)	226
	access-internal (Dynamic Access-Internal Routes)	227
	active-server-group	228
	allow-snooped-clients	229
	always-write-giaddr	230
	always-write-option-82	231
	authentication (DHCP Relay Agent)	232
	bfd	233
	circuit-id (DHCP Relay Agent)	234
	circuit-type (DHCP Relay Agent)	236
	client-discover-match (DHCP Relay Agent)	237
	client-id (DHCP Relay Agent)	238
	delete-binding-on-renegotiation	238
	delimiter (DHCP Relay Agent)	239
	detection-time	240
	dhcp-relay	241
	dhcpcv6 (DHCP Relay Agent)	247
	disable-relay	250
	domain-name (DHCP Relay Agent)	251
	drop (DHCP Relay Agent Option)	252
	dynamic-profile (DHCP Relay Agent)	253
	failure-action	254
	forward-snooped-clients (DHCP Relay Agent)	255
	group (DHCP Relay Agent)	256
	holddown-interval	259
	interface (DHCP Relay Agent)	260
	interface-client-limit (DHCP Relay Agent)	262
	interface-delete (Subscriber Management or DHCP Client Management)	263
	interface-name (DHCP Relay Agent)	264
	layer2-unicast-replies	265
	liveness-detection	266
	local-server-group (DHCP Relay Agent Option)	267
	mac-address (DHCP Relay Agent)	268
	method	269
	minimum-interval	270
	minimum-receive-interval	271
	multiplier	272
	next-hop (Dynamic Access-Internal Routes)	273
	no-adaptation	274
	no-allow-snooped-clients	275
	no-bind-on-request (DHCP Relay Agent)	276
	option-60 (DHCP Relay Agent)	277

option-82 (DHCP Relay Agent)	278
option-number (DHCP Relay Agent Option)	279
overrides (DHCP Relay Agent)	280
password (DHCP Relay Agent)	282
preference (Subscriber Management)	283
prefix (DHCP Relay Agent)	284
proxy-mode	285
relay-agent-interface-id (DHCPv6 Relay Agent)	286
relay-agent-remote-id (DHCPv6 Relay Agent Username)	287
relay-option (DHCP Relay Agent)	288
relay-option-82	289
relay-server-group (DHCP Relay Agent Option)	290
replace-ip-source-with	291
route-suppression (DHCP Local Server and Relay Agent)	292
routing-instance-name (DHCP Relay Agent)	293
send-release-on-delete (DHCP Relay Agent)	294
server-group	295
service-profile (DHCP Relay Agent)	296
session-mode	297
threshold (detection-time)	298
threshold (transmit-interval)	299
trace (DHCP Relay Agent)	300
transmit-interval	301
trust-option-82	302
use-interface-description	303
use-primary (DHCP Relay Agent)	305
user-prefix (DHCP Relay Agent)	306
username-include (DHCP Relay Agent)	307
version (BFD)	308
Chapter 13 Other Configuration Statements	309
cache-size	311
cache-timeout-negative	312
certificates	313
certification-authority	314
connection-limit	315
crl (Encryption Interface)	316
domain-search	316
encoding	317
enrollment-retry	317
enrollment-url	318
family (for EX Series switches)	319
file	322
ftp	323
http	324
https	325
ldap-url	326
lease-time	327
load-key-file	328

	local	329
	local-certificate	330
	maximum-certificates	330
	maximum-hop-count	331
	maximum-lease-time (DHCP)	331
	minimum-wait-time	332
	name-server	332
	no-listen	333
	outbound-ssh	334
	path-length	337
	port (HTTP/HTTPS)	337
	port (SRC Server)	338
	process-inform	338
	protocol-version	339
	rate-limit	340
	reconfigure	341
	retransmission-attempt	342
	retransmission-interval	343
	server (DNS and TFTP Service)	343
	server-address	344
	server-identifier	345
	servers	346
	service-deployment	346
	services (System Services)	347
	session (Time-out)	349
	sip-server	350
	source-address (SRC Software)	350
	source-address-giaddr	351
	ssh	352
	static-binding	353
	system-generated-certificate	354
	telnet	354
	tftp	355
	traceoptions (DNS and TFTP Packet Forwarding)	356
	traceoptions	358
	update-server	360
	web-management	361
	wins-server (System)	362
Part 3	Administration	
Chapter 14	Routine Monitoring	365
	Monitoring DHCP Services	365
Chapter 15	Verifying and Managing DHCP Local Server Configurations	371
	Verifying and Managing DHCP Local Server Configuration	371
	Verifying and Managing DHCPv6 Local Server Configuration	371

Chapter 16	Verifying and Managing DHCP Relay Agent Configurations	373
	Verifying and Managing DHCP Relay Configuration	373
	Verifying and Managing DHCPv6 Relay Configuration	373
Chapter 17	DHCP Local Server Monitoring Commands	375
	clear dhcp server binding	376
	clear dhcp server statistics	379
	clear dhcpv6 server binding	381
	clear dhcpv6 server statistics	383
	request dhcp server reconfigure	384
	request dhcpv6 server reconfigure	386
	request system reboot	388
	show dhcp server binding	393
	show dhcp server statistics	398
	show dhcpv6 server binding	401
	show dhcpv6 server statistics	407
Chapter 18	DHCP Relay Agent Monitoring Commands	411
	clear dhcp relay binding	412
	clear dhcp relay statistics	414
	clear dhcpv6 relay binding	417
	clear dhcpv6 relay statistics	420
	show dhcp relay binding	422
	show dhcp relay statistics	427
	show dhcpv6 relay binding	430
	show dhcpv6 relay statistics	436
	show route extensive	439
	show route protocol	456
Chapter 19	Other Operational Commands	469
	clear security pki local-certificate	470
	clear system services dhcp binding	471
	clear system services dhcp conflict	472
	clear system services dhcp statistics	473
	request ipsec switch	474
	request security certificate (signed)	475
	request security certificate (unsigned)	477
	request security key-pair	478
	request security pki generate-key-pair	479
	request security pki local-certificate generate-self-signed	480
	show security pki local-certificate	481
	show system services dhcp binding	484
	show system services dhcp conflict	487
	show system services dhcp global	488
	show system services dhcp pool	490
	show system services dhcp statistics	492
	show system services service-deployment	495
	ssh	496
	telnet	498

List of Figures

Part 1	Overview	
Chapter 2	DHCP Local Server	7
	Figure 1: DHCP Options Data Flow	27

List of Tables

	About the Documentation	xvii
	Table 1: Notice Icons	xix
	Table 2: Text and Syntax Conventions	xix
Part 1	Overview	
Chapter 1	Software Overview	3
	Table 3: Junos OS Processes	4
Chapter 2	DHCP Local Server	7
	Table 4: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server	9
	Table 5: Information in Authentication Grant	11
	Table 6: RADIUS Attributes and VSAs for DHCPv6 Local Server	13
	Table 7: Action Taken for Events That Occur During a Reconfiguration	18
	Table 8: Unsupported Opaque DHCP Options	29
Part 2	Configuration	
Chapter 8	Configuration Tasks	63
	Table 9: DHCP Service Configuration Pages Summary	64
	Table 10: DHCP Service Configuration Pages Summary for EX4300 Switches	67
	Table 11: DHCP Client Settings	72
Chapter 9	Configuration Tasks for DHCP Local Server	81
	Table 12: Actions for DHCP Local Server Snooped Packets	100
Chapter 10	Configuration Tasks for DHCP Relay Agent	107
	Table 13: DHCP Relay Agent Option 82 Value for Auto Logout	118
	Table 14: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled	124
	Table 15: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled	125
	Table 16: Actions for Snooped BOOTREPLY Packets	125
Chapter 12	DHCP Relay Agent Configuration Statements	219
	Table 17: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches	225
Chapter 13	Other Configuration Statements	309
	Table 18: Protocol Families and Supported Interface Types	321

Part 3	Administration	
Chapter 14	Routine Monitoring	365
	Table 19: Summary of DHCP Output Fields	366
	Table 20: Summary of DHCP Output Fields for EX4300 Switches	368
	Table 21: Summary of the DHCP Statistics Information Output for EX4300 switches	369
Chapter 17	DHCP Local Server Monitoring Commands	375
	Table 22: show dhcp server binding Output Fields	394
	Table 23: show dhcp server statistics Output Fields	399
	Table 24: show dhcpv6 server binding Output Fields	402
	Table 25: show dhcpv6 server statistics Output Fields	408
Chapter 18	DHCP Relay Agent Monitoring Commands	411
	Table 26: clear dhcp relay statistics Output Fields	415
	Table 27: show dhcp relay binding Output Fields	423
	Table 28: show dhcp relay statistics Output Fields	428
	Table 29: show dhcpv6 relay binding Output Fields	431
	Table 30: show dhcpv6 relay statistics Output Fields	436
	Table 31: show route extensive Output Fields	439
Chapter 19	Other Operational Commands	469
	Table 32: show security pki local-certificate Output Fields	481
	Table 33: show system services dhcp binding Output Fields	484
	Table 34: show system services dhcp conflict Output Fields	487
	Table 35: show system services dhcp global Output Fields	488
	Table 36: show system services dhcp pool Output Fields	490
	Table 37: show system services dhcp statistics Output Fields	492
	Table 38: show system services service-deployment Output Fields	495

About the Documentation

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

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:

- EX 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 xix 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 xix 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 provide feedback by using either of the following methods:

- Online feedback rating system—On any page of the Juniper Networks TechLibrary site at <http://www.juniper.net/techpubs/index.html>, simply click the stars to rate the content, and use the pop-up form to provide us with information about your experience. Alternately, you can use the online feedback form at <http://www.juniper.net/techpubs/feedback/>.
- E-mail—Send your comments to techpubs-comments@juniper.net. Include the document or topic name, URL or page number, and software 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 Partner Support Service 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

- [Software Overview on page 3](#)
- [DHCP Local Server on page 7](#)
- [DHCP Relay Agent on page 31](#)
- [Public Key Cryptography Overview on page 43](#)
- [Self-Signed Certificates Overview on page 45](#)

CHAPTER 1

Software Overview

- [Understanding Software Infrastructure and Processes on page 3](#)

Understanding Software Infrastructure and Processes

Each switch runs the Juniper Networks Junos operating system (Junos OS) for Juniper Networks EX Series Ethernet Switches on its general-purpose processors. Junos OS includes processes for Internet Protocol (IP) routing and for managing interfaces, networks, and the chassis.

The Junos OS runs on the Routing Engine. The Routing Engine kernel coordinates communication among the Junos OS processes and provides a link to the Packet Forwarding Engine.

With the J-Web interface and the command-line interface (CLI) to the Junos OS, you configure switching features and routing protocols and set the properties of network interfaces on your switch. After activating a software configuration, use either the J-Web or CLI user interface to monitor the switch, manage operations, and diagnose protocol and network connectivity problems.

- [Routing Engine and Packet Forwarding Engine on page 3](#)
- [Junos OS Processes on page 4](#)

Routing Engine and Packet Forwarding Engine

A switch has two primary software processing components:

- **Packet Forwarding Engine**—Processes packets; applies filters, routing policies, and other features; and forwards packets to the next hop along the route to their final destination.
- **Routing Engine**—Provides three main functions:
 - Creates the packet forwarding switch fabric for the switch, providing route lookup, filtering, and switching on incoming data packets, then directing outbound packets to the appropriate interface for transmission to the network
 - Maintains the routing tables used by the switch and controls the routing protocols that run on the switch.

- Provides control and monitoring functions for the switch, including controlling power and monitoring system status.

Junos OS Processes

The Junos OS running on the Routing Engine and Packet Forwarding Engine consists of multiple processes that are responsible for individual functions.

The separation of functions provides operational stability, because each process accesses its own protected memory space. In addition, because each process is a separate software package, you can selectively upgrade all or part of the Junos OS, for added flexibility.

[Table 3 on page 4](#) describes the primary Junos OS processes.

Table 3: Junos OS Processes

Process	Name	Description
Chassis process	chassisd	<p>Detects hardware on the system that is used to configure network interfaces.</p> <p>Monitors the physical status of hardware components and field-replaceable units (FRUs), detecting when environment sensors such as temperature sensors are triggered.</p> <p>Relays signals and interrupts—for example, when devices are taken offline, so that the system can close sessions and shut down gracefully.</p>
Ethernet switching process	eswd	<p>Handles Layer 2 switching functionality such as MAC address learning, Spanning Tree protocol and access port security. The process is also responsible for managing Ethernet switching interfaces, VLANs, and VLAN interfaces.</p> <p>Manages Ethernet switching interfaces, VLANs, and VLAN interfaces.</p>
Forwarding process	pfem	<p>Defines how routing protocols operate on the switch. The overall performance of the switch is largely determined by the effectiveness of the forwarding process.</p>
Interface process	dcd	<p>Configures and monitors network interfaces by defining physical characteristics such as link encapsulation, hold times, and keepalive timers.</p>
Management process	mgd	<p>Provides communication between the other processes and an interface to the configuration database.</p> <p>Populates the configuration database with configuration information and retrieves the information when queried by other processes to ensure that the system operates as configured.</p> <p>Interacts with the other processes when commands are issued through one of the user interfaces on the switch.</p> <p>If a process terminates or fails to start when called, the management process attempts to restart it a limited number of times to prevent thrashing and logs any failure information for further investigation.</p>
Routing protocol process	rpd	<p>Defines how routing protocols such as RIP, OSPF, and BGP operate on the device, including selecting routes and maintaining forwarding tables.</p>

- Related Documentation**
- For more information about processes, see *Junos OS Network Operations Guide*
 - For more information about basic system parameters, supported protocols, and software processes, see *Junos OS System Basics Configuration Guide*

CHAPTER 2

DHCP Local Server

- [Extended DHCP Local Server Overview on page 8](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [DHCP Local Server Handling of Client Information Request Messages on page 15](#)
- [Configuring Group-Specific DHCP Local Server Options on page 16](#)
- [Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients on page 16](#)
- [DHCP Snooping Support on page 19](#)
- [DHCP Auto Logout Overview on page 20](#)
- [Address-Assignment Pools Overview on page 22](#)
- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 23](#)
- [Multiple Address Assignment for DHCPv6 Clients on page 23](#)
- [Centrally Configured Opaque DHCP Options on page 25](#)
- [Port Number Requirements for DHCP Firewall Filters on page 29](#)

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 4 on page 9](#) 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 4: 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 10](#)
- [Providing DHCP Client Configuration Information on page 10](#)
- [Minimal Configuration for Clients on page 12](#)
- [DHCP Local Server and Address-Assignment Pools on page 12](#)

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 5 on page 11](#) 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 5: 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
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.

Related Documentation

- [Address-Assignment Pools Overview on page 22](#)

- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 104](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)
- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 23](#)
- [Graceful Routing Engine Switchover for DHCP](#)
- [High Availability Using Unified ISSU in the PPP Access Network](#)
- [Tracing Extended DHCP Operations](#)
- [Verifying and Managing DHCP Local Server Configuration on page 371](#)
- [Example: Minimum Extended DHCP Local Server Configuration on page 49](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 50](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine](#)

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 6 on page 13](#) to configure the client:

Table 6: 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

Table 6: RADIUS Attributes and VSAs for DHCPv6 Local Server (*continued*)

Attribute Number	Attribute Name	Description
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* 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 8](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)
- [Grouping Interfaces with Common DHCP Configurations on page 83](#)
- [Configuring Group-Specific DHCP Local Server Options on page 16](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 85](#)
- [Configuring Passwords for Usernames on page 101](#)
- [Creating Unique Usernames for DHCP Clients on page 101](#)

- [Assign a Specific IP Address to a Client Using DHCP Option 50 and DHCPv6 IA_NA Option on page 23](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 371](#)
- *Example: Extended DHCPv6 Local Server Configuration*

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.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients 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.



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 85](#)
- [Enabling Processing of Client Information Requests on page 89](#)

Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the `[edit system services dhcp-local-server group group-name]` hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the `[edit system services dhcp-local-server group group-name]` hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the `[edit system services dhcp-local-server]` hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the `dynamic-profile` statement.

- **authentication**—Configure the parameters the router sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **overrides**—Override the default configuration settings for the extended DHCP local server. For information, see “[Overriding Default DHCP Local Server Configuration Settings](#)” on page 85.

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 83](#)

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.

Manually Forcing the Local Server to Initiate the Reconfiguration Process

You can force the local server to initiate the reconfiguration process for clients by issuing the **request dhcp server reconfigure** command for DHCPv4 clients, and the **request dhcpv6 server reconfigure** command for DHCPv6 clients. Command options determine whether reconfiguration is then attempted for all clients or specified clients.

Action Taken for Events That Occur During a Reconfiguration

Events that take place while a reconfiguration is in process take precedence over the reconfiguration. [Table 7 on page 18](#) lists the actions taken in response to several different events.

Table 7: 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.

Table 7: Action Taken for Events That Occur During a Reconfiguration (*continued*)

Event	Action
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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)

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. The router discards snooped packets by default. To enable normal processing of snooped packets, you must explicitly configure the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

You can configure DHCP snooping support for 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 Snooped Packets Forwarding Support for DHCP Local Server on page 100](#)
- [Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 119](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 124](#)
- [Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 60](#)
- [Example: Enabling DHCP Snooping Support for DHCPv6 Relay Agent](#)

DHCP Auto Logout Overview

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

- [Auto Logout Overview on page 20](#)
- [How DHCP Identifies and Releases Clients on page 21](#)
- [Option 60 and Option 82 Requirements on page 22](#)

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the address pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method—DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.



NOTE: The incoming interface method differs from the `overrides interface-client-limit 1` statement, which retains the existing binding and rejects the newly connected client.

- Option 60 and option 82 method—DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client's existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.



NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, 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 [“How DHCP Relay Agent Uses Option 82 for Auto Logout” on page 117](#).

Related Documentation

- [Automatically Logging Out DHCP Clients on page 88](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 117](#)
- *Allowing Only One DHCP Client Per Interface*
- *Clearing DHCP Bindings for Subscriber Access*

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](#)
 - [Address-Assignment Pools Licensing Requirements](#)
 - [Example: Configuring an Address-Assignment Pool](#)

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

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

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



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

- Related Documentation**
- [Extended DHCP Local Server Overview on page 8](#)
 - [DHCPv6 Local Server Overview on page 13](#)

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 24](#)
- [Junos OS Predefined Variable for Multiple DHCPv6 Address Assignment on page 24](#)

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 90](#)
- [Junos OS Predefined Variables](#)

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).



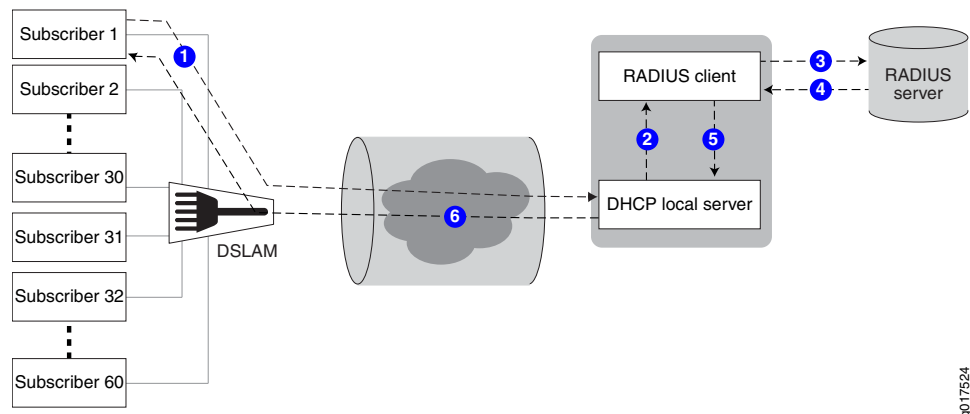
NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

- [Data Flow for RADIUS-Sourced DHCP Options on page 27](#)
- [Multiple VSA 26-55 Instances Configuration on page 28](#)
- [DHCP Options That Cannot Be Centrally Configured on page 28](#)

Data Flow for RADIUS-Sourced DHCP Options

Figure 1 on page 27 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 8 on page 29 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 8: 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*

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*
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- *Understanding Dynamic Firewall Filters*

CHAPTER 3

DHCP Relay Agent

- [Extended DHCP Relay Agent Overview on page 32](#)
- [DHCP Relay Proxy Overview on page 35](#)
- [DHCPv6 Relay Agent Overview on page 37](#)
- [Configuring Group-Specific DHCP Relay Options on page 38](#)
- [DHCP Snooping Support on page 39](#)
- [DHCP Auto Logout Overview on page 40](#)
- [Suppressing DHCP Access, Access-Internal, and Destination Routes on page 42](#)

Extended DHCP Relay Agent Overview

You can configure extended DHCP relay options on the router or on the switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.



NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCP relay agents.

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers. For information about how to use the DHCP relay agent in a video/IPTV application, see *Broadband Subscriber Management Edge Router Overview*.

On the switches, you can use DHCP relay to obtain configuration parameters including an IP address for DHCP clients.



NOTE: The extended DHCP relay agent options configured with the `dhcp-relay` statement are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.

For information about the DHCP/BOOTP relay agent, see *Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents*.

You can also configure the extended DHCP relay agent to support IPv6 clients. See [“DHCPv6 Relay Agent Overview” on page 37](#) for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level. See the [\[edit forwarding-options dhcp-relay\] Hierarchy Level](#) for the complete DHCP relay agent syntax.

You can also include the `dhcp-relay` statement at the following hierarchy levels:

- `[edit logical-systems logical-system-name forwarding-options]`
- `[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options]`
- `[edit routing-instances routing-instance-name forwarding-options]`

This overview covers:

- [Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers on page 33](#)
- [DHCP Liveness Detection on page 34](#)

Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers

The pattern of interaction among the DHCP Relay agent, DHCP client, and DHCP servers is the same regardless of whether the software installation is on a router or a switch. However, there are some difference in the details of usage.

On routers—In a typical carrier edge network configuration, the DHCP client is on the subscriber's computer, and the DHCP relay agent is configured on the router between the DHCP client and one or more DHCP servers.

On switches—In a typical network configuration, the DHCP client is on an access device such as a personal computer and the DHCP relay agent is configured on the switch between the DHCP client and one or more DHCP servers.

The following steps describe, at a high level, how the DHCP client, DHCP relay agent, and DHCP server interact in a configuration that includes two DHCP servers.

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

agent “snoops” on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as *lease shadowing* or *passive snooping*.

DHCP Liveness Detection

Liveness detection for DHCP subscriber or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients are expected to respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.



NOTE: DHCP liveness detection either globally or per DHCP group.

Related Documentation

- [DHCPv6 Relay Agent Overview on page 37](#)
- [Access and Access-Internal Routes for Subscriber Management](#)
- [Dynamic Profile Attachment to DHCP Subscriber Interfaces Overview](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)
- [DHCP Relay Proxy Overview on page 35](#)
- [Graceful Routing Engine Switchover for DHCP](#)
- [High Availability Using Unified ISSU in the PPP Access Network](#)
- [Verifying and Managing DHCP Relay Configuration on page 373](#)
- [Tracing Extended DHCP Operations](#)
- [Example: Minimum DHCP Relay Agent Configuration on page 55](#)
- [Example: DHCP Relay Agent Configuration with Multiple Clients and Servers](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 56](#)
- [Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing](#)
- [Example: Configuring a DHCP Firewall Filter to Protect the Routing Engine](#)

DHCP Relay Proxy Overview

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.
- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.



NOTE: You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:
 - a. Selects the first offer received as the offer to sent to the client
 - b. Replaces the DHCP server address with the address of the DHCP relay proxy
 - c. Forwards the offer to the DHCP client.
4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 32](#)
- [Enabling DHCP Relay Proxy Mode on page 136](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139](#)

DHCPv6 Relay Agent Overview

The DHCPv6 relay agent enhances the extended DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agent supports an IPv4 network.

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.



NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

The DHCPv6 relay agent 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.

To configure the DHCPv6 relay agent on the router (or switch), you include the **dhcpv6** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

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

- **[edit logical-systems *logical-system-name* forwarding-options dhcp-relay]**
- **[edit logical-systems *logical-system-name* routing-instances *routing-instance-name* forwarding-options dhcp-relay]**
- **[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay]**

Related Documentation

- [Using External AAA Authentication Services with DHCP on page 82](#)
- [Grouping Interfaces with Common DHCP Configurations on page 83](#)
- [Configuring Group-Specific DHCP Relay Options on page 38](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 111](#)
- [Configuring Passwords for Usernames on page 101](#)
- [Creating Unique Usernames for DHCP Clients on page 101](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 371](#)
- [Example: Extended DHCPv6 Local Server Configuration](#)

Configuring Group-Specific DHCP Relay Options

You can include the following statements at the **[edit forwarding-options dhcp-relay group group-name]** hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the **[edit forwarding-options dhcp-relay dhcpv6 group group-name]** hierarchy level to configure group-specific options for DHCPv6 relay agent.

- **active-server-group**—Configure an active server group to apply a common DHCP relay agent configuration to a named group of DHCP server addresses. For information, see [“Configuring Active Server Groups” on page 135](#).
- **authentication**—Configure the parameters the router (or switch) sends to the external AAA server.
- **dynamic-profile**—Specify the dynamic profile that is attached to a group of interfaces.
- **interface**—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- **liveness-detection**—Configure bidirectional failure detection timers and authentication criteria for static routes. For more information, see [“DHCP Liveness Detection Overview” on page 137](#).
- **overrides**—Override the default configuration settings for the extended DHCP relay agent. For information, see [“Overriding the Default DHCP Relay Configuration Settings” on page 111](#).
- **relay-agent-interface-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.
- **relay-agent-remote-id**—(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.
- **relay-option**—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see *Using DHCP Option Information to Selectively Process DHCP Client Traffic*.
- **relay-option-82**—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see [“Using DHCP Relay Agent Option 82 Information” on page 128](#).
- **service-profile**—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see *Default Subscriber Service Overview*.

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 83](#)

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. The router discards snooped packets by default. To enable normal processing of snooped packets, you must explicitly configure the **allow-snooped-clients** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level.

You can configure DHCP snooping support for 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 Snooped Packets Forwarding Support for DHCP Local Server on page 100](#)
- [Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 119](#)

- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 124](#)
- [Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 60](#)
- [Example: Enabling DHCP Snooping Support for DHCPv6 Relay Agent](#)

DHCP Auto Logout Overview

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

- [Auto Logout Overview on page 40](#)
- [How DHCP Identifies and Releases Clients on page 40](#)
- [Option 60 and Option 82 Requirements on page 41](#)

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the address pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address—the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful—the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method—DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.



NOTE: The incoming interface method differs from the `overrides interface-client-limit 1` statement, which retains the existing binding and rejects the newly connected client.

- Option 60 and option 82 method—DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client's existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.



NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, 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 [“How DHCP Relay Agent Uses Option 82 for Auto Logout” on page 117](#).

- Related Documentation**
- [Automatically Logging Out DHCP Clients on page 88](#)
 - [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 117](#)
 - [Allowing Only One DHCP Client Per Interface](#)
 - [Clearing DHCP Bindings for Subscriber Access](#)

Suppressing DHCP Access, Access-Internal, and Destination Routes

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds 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.

- Related Documentation**
- [Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 79](#)
 - [Extended DHCP Local Server Overview on page 8](#)
 - [DHCPv6 Local Server Overview on page 13](#)
 - [Extended DHCP Relay Agent Overview on page 32](#)
 - [DHCPv6 Relay Agent Overview on page 37](#)

CHAPTER 4

Public Key Cryptography Overview

- [Understanding Public Key Cryptography on Switches on page 43](#)

Understanding Public Key Cryptography on Switches

Cryptography describes the techniques related to the following aspects of information security:

- Privacy or confidentiality
- Integrity of data
- Authentication
- Nonrepudiation or nonrepudiation of origin—Nonrepudiation of origin means that signers cannot claim that they did not sign a message while claiming that their private key remains secret. In some nonrepudiation schemes used in digital signatures, a timestamp is attached to the digital signature, so that even if the private key is exposed, the signature remains valid. Public and private keys are described in the following text.

In practice, cryptographic methods protect the data transferred from one system to another over public networks by encrypting the data using an encryption key. Public key cryptography (PKC), which is used on Juniper Networks EX Series Ethernet Switches, uses a pair of encryption keys: a public key and a private key. The public and private keys are created simultaneously using the same encryption algorithm. The private key is held by a user secretly and the public key is published. Data encrypted with a public key can be decrypted only with the corresponding private key and vice versa. When you generate a public/private key pair, the switch automatically saves the key pair in a file in the certificate store, from which it is subsequently used in certificate request commands. The generated key pair is saved as *certificate-id.priv*.



NOTE: The default RSA and DSA key size is 1024 bits. If you are using the Simple Certificate Enrollment Protocol (SCEP), Juniper Networks Junos operating system (Junos OS) supports RSA only.

This topic describes:

- [Public Key Infrastructure \(PKI\) and Digital Certificates on page 44](#)

Public Key Infrastructure (PKI) and Digital Certificates

Public key infrastructure (PKI) allows the distribution and use of the public keys in public key cryptography with security and integrity. PKI manages the public keys by using digital certificates. A digital certificate provides an electronic means of verifying the identity of an individual, an organization, or a directory service that can store digital certificates.

A PKI typically consists of a Registration Authority (RA) that verifies the identities of entities, authorizes their certificate requests, and generates unique asymmetric key pairs (unless the users' certificate requests already contain public keys); and a Certificate Authority (CA) that issues corresponding digital certificates for the requesting entities. Optionally, you can use a Certificate Repository that stores and distributes certificates and a certificate revocation list (CRL) identifying the certificates that are no longer valid. Each entity possessing the authentic public key of a CA can verify the certificates issued by that CA.

Digital signatures exploit the public key cryptographic system as follows:

1. A sender digitally signs data by applying a cryptographic operation, involving its private key, on a digest of the data.
2. The resulting signature is attached to the data and sent to the receiver.
3. The receiver obtains the digital certificate of the sender, which provides the sender's public key and confirmation of the link between its identity and the public key. The sender's certificate is often attached to the signed data.
4. The receiver either trusts this certificate or attempts to verify it. The receiver verifies the signature on the data by using the public key contained in the certificate. This verification ensures the authenticity and integrity of the received data.

As an alternative to using a PKI, an entity can distribute its public key directly to all potential signature verifiers, so long as the key's integrity is protected. The switch does it by using a self-signed certificate as a container for the public key and the corresponding entity's identity.

Related Documentation

- [Understanding Self-Signed Certificates on EX Series Switches on page 45](#)

Self-Signed Certificates Overview

- [Understanding Self-Signed Certificates on EX Series Switches on page 45](#)

Understanding Self-Signed Certificates on EX Series Switches

When you initialize a Juniper Networks EX Series Ethernet Switch with the factory default configuration, the switch generates a self-signed certificate, allowing secure access to the switch through the Secure Sockets Layer (SSL) protocol. Hypertext Transfer Protocol over Secure Sockets Layer (HTTPS) and XML Network Management over Secure Sockets Layer (XNM-SSL) are the two services that can make use of the self-signed certificates.



NOTE: Self-signed certificates do not provide additional security as do those generated by Certificate Authorities (CAs). This is because a client cannot verify that the server he or she has connected to is the one advertised in the certificate.

The switches provide two methods for generating a self-signed certificate:

- Automatic generation

In this case, the creator of the certificate is the switch. An automatically generated (also called “system-generated”) self-signed certificate is configured on the switch by default.

After the switch is initialized, it checks for the presence of an automatically generated self-signed certificate. If it does not find one, the switch generates one and saves it in the file system.

A self-signed certificate that is automatically generated by the switch is similar to an SSH host key. It is stored in the file system, not as part of the configuration. It persists when the switch is rebooted, and it is preserved when a **request system snapshot** command is issued.

The switch uses the following distinguished name for the automatically generated certificate:

“CN=<device serial number>, CN=system generated, CN=self-signed”

If you delete the system-generated self-signed certificate on the switch, the switch generates a self-signed certificate automatically.

- Manual generation

In this case, you create the self-signed certificate for the switch. At any time, you can use the CLI to generate a self-signed certificate. Manually generated self-signed certificates are stored in the file system, not as part of the configuration.

Self-signed certificates are valid for five years from the time they are generated. When the validity of an automatically generated self-signed certificate expires, you can delete it from the switch so that the switch generates a new self-signed certificate.

System-generated self-signed certificates and manually generated self-signed certificates can coexist on the switch.

**Related
Documentation**

- [Understanding Public Key Cryptography on Switches on page 43](#)
- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 77](#)

PART 2

Configuration

- [DHCP Local Server Examples on page 49](#)
- [DHCP Relay Agent Examples on page 55](#)
- [Configuration Tasks on page 63](#)
- [Configuration Tasks for DHCP Local Server on page 81](#)
- [Configuration Tasks for DHCP Relay Agent on page 107](#)
- [DHCP Local Server Configuration Statements on page 143](#)
- [DHCP Relay Agent Configuration Statements on page 219](#)
- [Other Configuration Statements on page 309](#)

CHAPTER 6

DHCP Local Server Examples

- [Example: Minimum Extended DHCP Local Server Configuration on page 49](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 50](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50](#)

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 8](#)

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 8](#)
 - [Address-Assignment Pools Overview on page 22](#)

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 50](#)
- [Overview on page 51](#)
- [Configuration on page 51](#)

Requirements

- Juniper Networks MX Series routers

- Juniper Networks EX Series switches
- Configure DHCP local server. See [“Extended DHCP Local Server Overview”](#) on page 8.

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-servergroup local_group_1 liveness-detection method  
bfd]  
user@host# set minimum-interval 45000
```

8. Configure the minimum receive interval (in milliseconds).



NOTE: You do not need to configure the BFD minimum receive interval if you configure the BFD minimum transmit and receive interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection  
method bfd]  
user@host# set minimum-receive-interval 60000
```

9. Configure a multiplier value for the detection time.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection  
method bfd]  
user@host# set multiplier 100
```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection  
method bfd]  
user@host# set no-adaptation
```

11. Configure the BFD session mode.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection  
method bfd]  
user@host# set session-mode automatic
```

12. Configure the threshold and minimum interval for the BFD transmit interval.



NOTE: You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection  
method bfd]
```

```
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

13. Configure the BFD protocol version you want to detect.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection
method bfd]
user@host# set version automatic
```

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit failure-action action
```

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

```
[edit]
user@host# show system
services {
  dhcp-local-server {
    group local_group_1 {
      liveness-detection {
        failure-action clear-binding-if-interface-up;
        method {
          bfd {
            version automatic;
            minimum-interval 45000;
            minimum-receive-interval 60000;
            multiplier 100;
            no-adaptation;
            transmit-interval {
              minimum-interval 45000;
              threshold 60000;
            }
            detection-time {
              threshold 30000;
            }
            session-mode automatic;
            holddown-interval 50;
          }
        }
      }
    }
  }
}
```

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

- Related Documentation**
- [Extended DHCP Local Server Overview on page 8](#)
 - [DHCP Liveness Detection Overview on page 137](#)
 - [Configuring Detection of DHCP Local Server Client Connectivity on page 98](#)

CHAPTER 7

DHCP Relay Agent Examples

- [Example: Minimum DHCP Relay Agent Configuration on page 55](#)
- [Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings on page 56](#)
- [Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 60](#)

Example: Minimum DHCP Relay Agent Configuration

This example shows the minimum configuration you need to use the extended DHCP relay agent on the router or switch:

```
[edit forwarding-options]
dhcp-relay {
  server-group {
    test 10.0.2.1;
  }
  active-server-group test;
  group all {
    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 a server group and an active server group named **test** with IP address 10.0.2.1. The DHCP relay agent configuration is applied to a group named **all**. Within this group, the DHCP relay agent is enabled on interface fe-0/0/2.0.

Related Documentation

- [Extended DHCP Relay Agent Overview on page 32](#)

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

This example shows how to configure DHCP relay agent to use DHCP option strings to selectively identify, filter, and process client traffic.

- [Requirements on page 56](#)
- [Overview on page 56](#)
- [Configuration on page 57](#)
- [Verification on page 58](#)

Requirements

This example uses the following hardware and software components:

- MX Series 3D Universal Edge Routers or EX Series Switches

Before you configure DHCP relay agent selective processing support, be sure you:

- Configure DHCP relay agent.

See [“Extended DHCP Relay Agent Overview” on page 32](#).

- (Optional) Configure a named DHCP local server group if you want to forward client traffic to a server group.

See [“Grouping Interfaces with Common DHCP Configurations” on page 83](#).

Overview

In this example, you configure DHCP relay agent to use DHCP option strings in client packets to selectively identify, filter, and process client traffic. To configure selective processing, you perform the following procedures:

1. Identify the client traffic—Specify the DHCP option that DHCP relay agent uses to identify the client traffic you want to process. The option you specify matches the option in the client traffic.
2. Configure a default action—Specify the default processing action, which DHCP relay uses for identified client traffic that does not satisfy any configured match criteria.
3. Create match filters and associate an action with each filter—Specify match criteria that filter the client traffic. The criteria can be an exact match or a partial match with the option string in the client traffic. Associate a processing action with each match criterion.

Configuration

To configure DHCP relay agent selective processing based on DHCP option information, perform these tasks:

- [Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings on page 57](#)
- [Results on page 58](#)

CLI Quick Configuration

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

```
set forwarding-options dhcp-relay relay-option option-number 60
set forwarding-options dhcp-relay relay-option equals ascii video-gold forward-only
set forwarding-options dhcp-relay relay-option equals ascii video-bronze local-server-group
servergroup-15
set forwarding-options dhcp-relay relay-option starts-with hexadecimal ffff
local-server-group servergroup-east
set forwarding-options dhcp-relay relay-option default-action drop
```

Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings

Step-by-Step Procedure

To configure DHCP relay selective processing:

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

```
[edit forwarding-options]
user@host# edit dhcp-relay
```
2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option option-number 60
```
3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```
4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```
5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-bronze local-server-group
servergroup-15
```

6. Configure a partial match criteria and associated action that DHCP relay uses to process client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option starts-with hexadecimal ffff local-server-group
servergroup-east
```

Results

From configuration mode, confirm the results of your configuration by issuing the **show** statement at the **[edit forwarding-options]** hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host# show
dhcp-relay {
  relay-option {
    option-number 60;
    equals {
      ascii video-gold {
        forward-only;
      }
    }
    equals {
      ascii video-bronze {
        local-server-group servergroup-15;
      }
    }
    default-action {
      drop;
    }
    starts-with {
      hexadecimal ffff {
        local-server-group servergroup-east;
      }
    }
  }
}
```

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

Verification

To verify the status of DHCP relay agent selective traffic processing, perform this task:

- [Verifying the Status of DHCP Relay Agent Selective Traffic Processing on page 58](#)

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose Verify the DHCP relay agent selective traffic processing status.

Action Display statistics for DHCP relay agent.

```

user@host> show dhcp relay statistics
Packets dropped:
    Total                  30
    Bad hardware address   1
    Bad opcode             1
    Bad options            3
    Invalid server address 5
    No available addresses 1
    No interface match     2
    No routing instance match 9
    No valid local address 4
    Packet too short       2
    Read error             1
    Send error             1
    Option 60              1
    Option 82              2

Messages received:
    BOOTREQUEST           116
    DHCPDECLINE           0
    DHCPDISCOVER          11
    DHCPINFORM            0
    DHCPRELEASE           0
    DHCPREQUEST           105

Messages sent:
    BOOTREPLY             0
    DHCPOFFER             2
    DHCPACK               1
    DHCPNAK               0
    DHCPFORCERENEW        0

Packets forwarded:
    Total                 4
    BOOTREQUEST           2
    BOOTREPLY             2

```

Meaning The **Packets forwarded** field in the **show dhcp relay statistics** command output displays the number of client packets that have been forwarded as a result of the selective traffic processing configuration. In this example, the output indicates the total number of packets that DHCP relay agent has forwarded, as well as a breakdown for the number of **BOOTREQUEST** and **BOOTREPLY** packets forwarded.

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - *DHCP Options and Selective Traffic Processing Overview*
 - *Using DHCP Option Information to Selectively Process DHCP Client Traffic*
 - *Displaying a Count of DHCP Packets That Are Dropped or Forwarded During Selective Processing That Is Based on DHCP Option Strings*
 - *Example: Configuring DHCP and DHCPv6 Relay Agent Group-Level Selective Traffic Processing*

Example: Configuring DHCP Snooping Support for DHCP Relay Agent

This example shows how to configure DHCP snooping support for DHCP relay agent.

- [Requirements on page 60](#)
- [Overview on page 60](#)
- [Configuration on page 60](#)

Requirements

- Configure DHCP relay agent. See “[Extended DHCP Relay Agent Overview](#)” on page 32.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

- Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group **frankfurt**.
- Configure DHCP relay agent to forward snooped packets to only configured interfaces.



NOTE: By default, DHCP snooping is disabled globally.

Configuration

Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.
`[edit]`
`user@host# edit forwarding-options dhcp-relay`
2. Specify the named group of interfaces on which DHCP snooping is supported.
`[edit forwarding-options dhcp-relay]`
`user@host# edit group frankfurt`
3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.
`[edit forwarding-options dhcp-relay group frankfurt]`
`user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9`
4. Specify that you want to override the default configuration for the group.
`[edit forwarding-options dhcp-relay group frankfurt]`
`user@host# edit overrides`
5. Enable DHCP snooping support for the group.
`[edit forwarding-options dhcp-relay group frankfurt overrides]`
`user@host# set allow-snooped-clients`

6. Return to the **[edit forwarding-options dhcp-relay]** hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

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

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group **frankfurt**).

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```

Results From configuration mode, confirm your configuration by entering the **show forwarding-options** command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group **frankfurt**.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
  forward-snooped-clients configured-interfaces;
  group frankfurt {
    overrides {
      allow-snooped-clients;
    }
    interface fe-1/0/1.3 {
      upto fe-1/0/1.9;
    }
  }
}
```

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

- Related Documentation**
- [DHCP Snooping Support on page 19](#)
 - [Configuring DHCP Snooping for DHCP Relay Agent on page 119](#)

CHAPTER 8

Configuration Tasks

- [Configuring DHCP Services \(J-Web Procedure\) on page 63](#)
- [Configuring a DHCP SIP Server \(CLI Procedure\) on page 71](#)
- [Configuring a DHCP Client \(CLI Procedure\) on page 71](#)
- [Configuring a Switch as a DHCP Server \(CLI Procedure\) on page 72](#)
- [Configuring an Extended DHCP Relay Server on EX Series Switches \(CLI Procedure\) on page 75](#)
- [Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates \(CLI Procedure\) on page 76](#)
- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 77](#)
- [Deleting Self-Signed Certificates \(CLI Procedure\) on page 78](#)
- [Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 79](#)

Configuring DHCP Services (J-Web Procedure)

- [Configuring DHCP Services \(J-Web Procedure\) on EX Series Switches on page 63](#)
- [Configuring DHCP Services on EX4300 Switches \(J-Web Procedure\) on page 66](#)

Configuring DHCP Services (J-Web Procedure) on EX Series Switches



NOTE: This topic applies only to the J-Web Application package.

Use the J-Web DHCP Configuration pages to configure DHCP pools for subnets and static bindings for DHCP clients on an ACX Series Universal Access Gateway router or an EX Series Ethernet Switch. If DHCP pools or static bindings are already configured, use the Configure Global DHCP Parameters Configuration page to add settings for these pools and static bindings. Settings that have been previously configured for DHCP pools or static bindings are not overridden when you use the Configure Global DHCP Parameters Configuration page.

To configure the DHCP server:

1. Select **Configure > Services > DHCP**
2. Access a DHCP Configuration page:
 - To configure a DHCP pool for a subnet, click **Add** in the DHCP Pools box.
 - To configure a static binding for a DHCP client, click **Add** in the DHCP Static Binding box.
 - To globally configure settings for existing DHCP pools and static bindings, click **Configure Global DHCP Parameters**.
3. Enter information into the DHCP Service Configuration pages as described in [Table 9 on page 64](#)
4. To apply the configuration, click **Apply**.



NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

Table 9: DHCP Service Configuration Pages Summary

Field	Function	Your Action
DHCP Pool Information		
DHCP Subnet (required)	Specifies the subnet on which DHCP is configured.	Type an IP address prefix.
Address Range (Low) (required)	Specifies the lowest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet field.
Address Range (High) (required)	Specifies the highest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet. This address must be greater than the address specified in the Address Range (Low) field.
Exclude Addresses	Specifies addresses to exclude from the IP address pool.	<ul style="list-style-type: none"> • To add an excluded address, type the address next to the Add button, and click Add. • To delete an excluded address, select the address in the Exclude Addresses box, and click Delete.
Lease Time		
Maximum Lease Time (Seconds)	Specifies the maximum length of time a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)	Type a number from 60 through 4,294,967,295 (seconds). You can also type infinite to specify a lease that never expires.

Table 9: DHCP Service Configuration Pages Summary (*continued*)

Field	Function	Your Action
Default Lease Time (Seconds)	Specifies the length of time a client can hold a lease for clients that do not request a specific lease length.	Type a number from 60 through 2,147,483,647 (seconds). You can also type infinite to specify a lease that never expires.
Server Information		
Server Identifier	Specifies the IP address of the DHCP server reported to a client.	Type the IP address of the server. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.
Domain Name	Specifies the domain name that clients must use to resolve hostnames.	Type the name of the domain.
Domain Search	Specifies the order—from top to bottom—in which clients must append domain names when resolving hostnames using DNS.	<ul style="list-style-type: none"> To add a domain name, type the name next to the Add button, and click Add. To delete a domain name, select the name in the Domain Search box, and click Delete.
DNS Name Servers	Defines a list of DNS servers that the client can use, in the specified order—from top to bottom.	<ul style="list-style-type: none"> To add a DNS server, type an IP address next to the Add button, and click Add. To remove a DNS server, select the IP address in the DNS Name Servers box, and click Delete.
Gateway Routers	Defines a list of relay agents on the subnet, in the specified order—from top to bottom.	<ul style="list-style-type: none"> To add a relay agent, type an IP address next to the Add button, and click Add. To remove a relay agent, select the IP address in the Gateway Routers box, and click Delete.
WINS Servers	Defines a list of NetBIOS name servers, in the specified order—from top to bottom.	<ul style="list-style-type: none"> To add a NetBIOS name server, type an IP address next to the Add button, and click Add. To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click Delete.
Boot Options		
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Type a path and filename.
Boot Server	Specifies the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	Type the IP address or hostname of the TFTP server.
DHCP Static Binding Information		
DHCP MAC Address (required)	Specifies the MAC address of the client to be permanently assigned a static IP address.	Type the hexadecimal MAC address of the client.

Table 9: DHCP Service Configuration Pages Summary (*continued*)

Field	Function	Your Action
Fixed IP Addresses (required)	Defines a list of IP addresses permanently assigned to the client. A static binding must have at least one fixed address assigned to it, but multiple addresses are also allowed.	<ul style="list-style-type: none"> To add an IP address, type it next to the Add button, and click Add. To remove an IP address, select it in the Fixed IP Addresses box, and click Delete.
Host Name	Specifies the name of the client used in DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides.	Type a client hostname.
Client Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in string form.
Hexadecimal Client Identifier	Specifies the name of the client, in hexadecimal form, used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	Type a client identifier in hexadecimal form.

Configuring DHCP Services on EX4300 Switches (J-Web Procedure)

On EX4300 switches, use the DHCP Configuration page to create DHCP pools and set the DHCP parameters for them and to configure DHCP settings for existing DHCP pools and static bindings.

To configure the DHCP services on EX4300 switches:

1. Select **Configure > Services > DHCP**
2. Access a DHCP Configuration page:
 - To configure a DHCP pool for a subnet, click **Add** in the DHCP Pools box.
 - To configure DHCP groups, click **Add** in the DHCP Groups box.
 - To globally configure settings for existing DHCP pools and static bindings, click **Configure Global DHCP Parameters**.
3. Enter information into the DHCP Service Configuration pages as described in [Table 10 on page 67](#)
4. To apply the configuration, click **OK**.



NOTE: After you make changes to the configuration on this page, you must commit the changes for them to take effect. To commit all changes to the active configuration, select **Commit Options > Commit**. See [Using the Commit Options to Commit Configuration Changes](#) for details about all commit options.

Table 10: DHCP Service Configuration Pages Summary for EX4300 Switches

Field	Function	Your Action
DHCP Groups		
Group Name	Specifies the name of the group.	Enter the name of the group.
Interfaces	Family inet interface is listed , only if it is already configured with family inet.	Select the interface for the specific group.
DHCP Pool Information		
Pool Name	Specifies the name of an address-assignment pool.	Type the pool name.
Link Pool	Specifies the pool name to which it is linked.	Select the option from the list.
Network Address		
IP Address	Specifies the IP address pool range.	Type an IP address that is part of the subnet specified in the DHCP Subnet field.
Subnet mask	Specifies the subnet specified in DHCP Subnet.	Type a subnet mask that is specified in the DHCP Subnet field.
DHCP Pool Attributes		
Pool Name	Displays the name of an address-assignment pool.	The pool name is displayed.
Server Identifier	Specifies the IP address of the DHCP server reported to a client.	Type the IP address of the server. If you do not specify a server identifier, the primary address of the interface on which the DHCP exchange occurs is used.
TFTP Server	Specifies the Trivial File Transfer Protocol (TFTP) server that the client uses to obtain the client configuration file.	Enter the IP address of the TFTP server.
Maximum Lease Time (Seconds)	Specifies the maximum length of time a client can hold a lease. (Dynamic BOOTP lease lengths can exceed this maximum time.)	Type a number.
Boot File	Specifies the path and filename of the initial boot file to be used by the client.	Type a path and filename.
Boot Server	Specifies the TFTP server that provides the initial boot file to the client.	Type the IP address or hostname of the TFTP server.
Grace Period	Specifies the grace period for which a client can hold a lease.	Type the grace period in seconds.

Table 10: DHCP Service Configuration Pages Summary for EX4300 Switches (*continued*)

Field	Function	Your Action
DNS Name Servers	Defines a list of DNS servers the client can use.	<ul style="list-style-type: none"> To add a DNS server, click Add. Type an IP address in the Add IP Address pop-up window. Click OK. To remove a DNS server, select the IP address in the DNS Name Servers box, and click Remove.
WINS Servers	Defines a list of NetBIOS name servers.	<ul style="list-style-type: none"> To add a NetBIOS name server, click Add. Type an IP address in the Add IP Address pop-up window. Click OK. To remove a NetBIOS name server, select the IP address in the WINS Servers box, and click Remove.
Domain Name	Specifies the domain name that clients must use to resolve hostnames.	Type the name of the domain.
NetBIOS Node Type	Specifies the NetBOIS node that provides the initial node file to the client.	Select the type from the list.
Gateway Routers	Defines a list of relay agents on the subnet, in the specified order—from top to bottom.	<ul style="list-style-type: none"> To add a relay agent, click Add. Type an IP address in the Add IP Address pop-up window. Click OK. To remove a relay agent, select the IP address in the Gateway Routers box, and click Remove.
Option	Specifies the DHCP options.	<ul style="list-style-type: none"> To add a DHCP option, click Add. The Add DHCP Option pop-up window is displayed. Enter the following: <ul style="list-style-type: none"> Enter the DHCP Code in the Code box. Select the DHCP type from the Type list. Select the DHCP subtype from the Sub Type list. Enter the DHCP value in the Value box. Click OK. To remove a DHCP option, select the option in the Option box, and click Remove.
Option-82		
Circuit Identifier	Identifies the circuit (interface or VLAN or both) on the switch on which the request was received.	Type the circuit identifier.
Ranges	Specifies the circuit identifier range.	Type the range for the circuit identifier.

Table 10: DHCP Service Configuration Pages Summary for EX4300 Switches (*continued*)

Field	Function	Your Action
Remote Identifier	By default, the remote ID is the MAC address of the switch	Type the remote identifier.
Ranges	Specifies the remote identifier range.	Type the range for the remote identifier.
Address Range		
Range Name	Specifies the name of the range.	Click Add . The Add Address Range pop-up window is displayed: <ul style="list-style-type: none"> Type the range name in the Range Name box.
Address Range		
Address Range (Low)	Specifies the lowest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet
Address Range (High)	Specifies the highest address in the IP address pool range.	Type an IP address that is part of the subnet specified in DHCP Subnet. This address must be greater than the address specified in Address Range (Low).
Static Bindings		
Host Name	Specifies the name of the client used in DHCP messages exchanged between the server and the client. The name must be unique to the client within the subnet on which the client resides.	Type a client hostname.
MAC Address	Specifies the MAC address of the client to be permanently assigned a static IP address.	Type the hexadecimal MAC address of the client.
Fixed IP Address	Specifies the IP address of the client.	Type the IP address.
Global Settings		
General		
Duplicate clients on interface	Specifies the DHCP local server to include the client subinterface when distinguishing between duplicate DHCP clients (clients with the same MAC address or client ID) in the same subnet.	To enable this option, select the check box.
Pool Match Order	Specifies 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.	Select the pool match order.
Authentication		

Table 10: DHCP Service Configuration Pages Summary for EX4300 Switches (*continued*)

Field	Function	Your Action
Password	Specifies the password that is sent to the external AAA authentication server for subscriber authentication.	Type the password.
Username-include		
Circuit Type	Specifies the circuit type that is linked with the username.	To enable this option, select the check box.
Interface Name	Name of the interface.	To enable this option, select the check box.
Mac Address	Specifies the MAC address of the client PDU that is linked with the username during the subscriber authentication process.	To enable this option, select the check box.
Logical System Name	Specifies that the logical system name that is linked with the username during the subscriber authentication process.	To enable this option, select the check box.
Option-60	Specifies the payload of Option 60 (Vendor Class Identifier) from the client PDU be linked with the username during the subscriber authentication process.	To enable this option, select the check box.
Routing Instance Name	Specifies the routing instance name that is linked with the username during the subscriber authentication process.	To enable this option, select the check box.
Option-82		
Circuit Identifier	Specifies the name of the client used by the DHCP server to index its database of address bindings. The name must be unique to the client within the subnet on which the client resides.	To enable this option, select the check box.
Remote Identifier	Specifies the remote ID option in the client.	To enable this option, select the check box.
Domain Name	Specifies the domain name that clients must use to resolve hostnames.	Type the domain name.
User Prefix	Specifies the prefix to the username as defined by the user.	Type the prefix.
Delimiter	Specifies a character that separates components that make up the username.	Type the delimiter.

Related Documentation

- [Understanding DHCP Services for Switches](#)
- [Monitoring DHCP Services on page 365](#)

Configuring a DHCP SIP Server (CLI Procedure)

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

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

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

For example, to configure one address:

```
[edit system services dhcp]
user@switch set sip-server 172.168.0.11
```

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

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

For example, to configure a name:

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

- Related Documentation**
- [Configuring a DHCP Client \(CLI Procedure\) on page 71](#)
 - *Understanding DHCP Services for Switches*

Configuring a DHCP Client (CLI Procedure)

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

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see *Configuring a DHCP Server on Switches (CLI Procedure)* or [“Configuring a DHCP Server on Switches \(CLI Procedure\)” on page 72](#).

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

[edit]

```
user@switch# set interfaces interface-name unit number family inet dhcp
configuration-statement
```

The options that you can configure are listed in [Table 11 on page 72](#). Replace the variable *configuration-statement* with one or more of the statements listed in this table. If you do not explicitly configure these options, the switch uses default values for them.

Table 11: DHCP Client Settings

Configuration Statement	Description
client-identifier	Unique client ID—By default this consists of the hardware type (01 for Ethernet) and the MAC address (a.b.c.d). For this example, the value would be 01abcd.
lease-time	Time in seconds that a client holds the lease for an IP address assigned by a DHCP server. If a client does not request a specific lease time, then the server sends the default lease time. The default lease time on a Junos OS DHCP server is 1 day.
retransmission-attempt	Number of times the client attempts to retransmit a DHCP packet.
retransmission-interval	Time between transmission attempts.
server-address	IP address of the server that the client queries for an IP address.
update-server	TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch are propagated.
vendor-option	Vendor class ID (CPU's manufacturer ID string) for the DHCP client.

- Related Documentation**
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)
 - [Understanding DHCP Services for Switches](#)

Configuring a Switch as a DHCP Server (CLI Procedure)



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

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

A DHCP configuration consists of two components—an optional reconfiguration of default settings on DHCP clients and the configuration of a DHCP server. This topic covers

configuration of the switch as a local DHCP server using DHCP for IPv4 (DHCPv4). For information about DHCPv6 local server, see [“DHCPv6 Local Server Overview” on page 13](#).

This topic describes the following task:

1. [Configuring the Switch as a Local DHCP Server on page 73](#)

Configuring the Switch as a Local DHCP Server

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

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

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

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

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

For example:

```
[edit]
user@switch# set interfaces ge-0/0/1 unit 0 family inet address 40.1.1.2/24
user@switch# set vlans server vlan-id 301
user@switch# set vlans server l3-interface irb.301
user@switch# set interfaces irb.301 family inet address 50.1.1.2/24
```

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

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

For example:

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

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

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

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet network
20.1.1.0/24
```

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

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

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet range range1 low
20.1.1.101
user@switch# set access address-assignment pool pool1 family inet range range1 high
20.1.1.110
```

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

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

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
router 20.1.1.254
```

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

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

For example:

```
[edit]
user@switch# set access address-assignment pool pool1 family inet dhcp-attributes
server-identifier 20.1.1.254
```


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

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

For example:

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

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

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

For example:

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

Related Documentation

- [Configuring a DHCP Client \(CLI Procedure\) on page 71](#)
- [Configuring a DHCP SIP Server \(CLI Procedure\) on page 71](#)

Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure)

You can configure an EX Series switch to act as an extended DHCP relay agent. This means that a locally attached host can issue a DHCP request as a broadcast message and the switch configured for DHCP relay relays the message to a specified DHCP server. Configure a switch to be a DHCP relay agent if you have locally attached hosts and a remote DHCP server.

Before you begin:

- Ensure that the switch can connect to the DHCP server.

To configure a switch to act as an extended DHCP relay agent server:

1. Create at least one DHCP server group, which is a group of 1 through 5 DHCP server IP addresses:

```
[edit forwarding-options dhcp-relay]
user@switch# set server-group server-group-name ip-address
```

2. Set the global active DHCP server group. The DHCP relay server relays DHCP client requests to the DHCP servers defined in the active server group:

```
[edit forwarding-options dhcp-relay]
user@switch# set active-server-group server-group-name
```

3. Create a DHCP relay group that includes at least one interface. DHCP relay runs on the interfaces defined in DHCP groups:

```
[edit forwarding-options dhcp-relay]
user@switch# set group group-name interface interface-name
```

4. (Optional) Configure overrides of default DHCP relay behaviors, at the global level. See the override options in the [overrides](#) statement.

```
[edit forwarding-options dhcp-relay]
user@switch# set overrides
```

5. (Optional) Configure DHCP relay to use the DHCP vendor class identifier option (option 60) in DHCP client packets, at the global level:

```
[edit forwarding-options dhcp-relay]
user@switch# set relay-option option-number 60
```

6. (Optional) Configure settings for a DHCP relay group that override the settings at the global level, using these statements:

```
[edit forwarding-options dhcp-relay group group-name]
user@switch# set active-server-group server-group-name
user@switch# set overrides
user@switch# set relay-option option-number 60
```

7. (Optional) Configure settings for a DHCP relay group interface that override the settings at the global and **group** levels, using these statements:

```
[edit forwarding-options dhcp-relay group group-name interface interface-name]
user@switch# exclude
user@switch# set overrides
user@switch# set trace
user@switch# set upto upto-interface-name
```

- Related Documentation**
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)
 - [Configuring a DHCP Client \(CLI Procedure\) on page 71](#)
 - [Understanding the Extended DHCP Relay Agent for EX Series Switches](#)

Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure)

You can use the system-generated self-signed certificate or a manually generated self-signed certificate to enable Web management HTTPS and XNM-SSL services.

- To enable HTTPS services using the automatically generated self-signed certificate:

```
[edit]
user@switch# set system services web-management https system-generated-certificate
```

- To enable HTTPS services using a manually generated self-signed certificate:

```
[edit]
user@switch# set system services web-management https pki-local-certificate
certificate-id-name
```



NOTE: The value of the *certificate-id-name* must match the name you specified when you generated the self-signed certificate manually.

- To enable XNM-SSL services using a manually generated self-signed certificate:

```
[edit]
```

```
user@switch# set system services xnm-ssl local-certificate certificate-id-name
```



NOTE: The value of the *certificate-id-name* must match the name you specified when you generated the self-signed certificate manually.

Related Documentation

- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 77](#)
- [Understanding Self-Signed Certificates on EX Series Switches on page 45](#)

Manually Generating Self-Signed Certificates on Switches (CLI Procedure)

EX Series switches allow you to generate custom self-signed certificates and store them in the file system. The certificate you generate manually can coexist with the automatically generated self-signed certificate on the switch. To enable secure access to the switch over SSL, you can use either the system-generated self-signed certificate or a certificate you have generated manually.

To generate self-signed certificates manually, you must complete the following tasks:

- [Generating a Public-Private Key Pair on Switches on page 77](#)
- [Generating Self-Signed Certificates on Switches on page 78](#)

Generating a Public-Private Key Pair on Switches

A digital certificate has an associated cryptographic key pair that is used to sign the certificate digitally. The cryptographic key pair comprises a public key and a private key. When you generate a self-signed certificate, you must provide a public-private key pair that can be used to sign the self-signed certificate. Therefore, you must generate a public-private key pair before you can generate a self-signed certificate.

To generate a public-private key pair:

```
user@switch> request security pki generate-key-pair certificate-id certificate-id-name
```



NOTE: Optionally, you can specify the encryption algorithm and the size of the encryption key. If you do not specify the encryption algorithm and encryption key size, default values are used. The default encryption algorithm is RSA, and the default encryption key size is 1024 bits.

After the public-private key pair is generated, the switch displays the following:

```
generated key pair certificate-id-name, key size 1024 bits
```

Generating Self-Signed Certificates on Switches

To generate the self-signed certificate manually, include the certificate ID name, the subject of the distinguished name (DN), the domain name, the IP address of the switch, and the e-mail address of the certificate holder:

```
user@switch> request security pki local-certificate generate-self-signed certificate-id  
certificate-id-name domain-name domain-name email email-address ip-address switch-ip-address  
subject subject-of-distinguished-name
```

The certificate you have generated is stored in the switch's file system. The certificate ID you have specified while generating the certificate is a unique identifier that you can use to enable the HTTPS or XNM-SSL services.

To verify that the certificate was generated and loaded properly, enter the **show security pki local-certificate** operational command.

Related Documentation

- [Enabling HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates \(CLI Procedure\) on page 76](#)
- [Understanding Self-Signed Certificates on EX Series Switches on page 45](#)

Deleting Self-Signed Certificates (CLI Procedure)

You can delete a self-signed certificate that is automatically or manually generated from the EX Series switch. When you delete the automatically generated self-signed certificate, the switch generates a new self-signed certificate and stores it in the file system.

- To delete the automatically generated certificate and its associated key pair from the switch:

```
user@switch> clear security pki local-certificate system-generated
```

- To delete a manually generated certificate and its associated key pair from the switch:

```
user@switch> clear security pki local-certificate certificate-id certificate-id-name
```

- To delete all manually generated certificates and their associated key pairs from the switch:

```
user@switch> clear security pki local-certificate all
```

Related Documentation

- [Manually Generating Self-Signed Certificates on Switches \(CLI Procedure\) on page 77](#)
- [Understanding Self-Signed Certificates on EX Series Switches on page 45](#)

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: 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 (DHCP Local Server and Relay Agent) access-internal
```

- For DHCP relay (for example, a group-specific configuration):

```
[edit forwarding-options dhcp-relay group southeast]
user@host# set route-suppression (DHCP Local Server and Relay Agent) 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 (DHCP Local Server and Relay Agent) access
access-internal
```

- For DHCPv6 relay (for example, a global configuration):

```
[edit forwarding-options dhcp-relay]
user@host# set dhcpv6 route-suppression (DHCP Local Server and Relay Agent) access
```

Related Documentation

- [Suppressing DHCP Access, Access-Internal, and Destination Routes on page 42](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [DHCPv6 Relay Agent Overview on page 37](#)

CHAPTER 9

Configuration Tasks for DHCP Local Server

- [Using External AAA Authentication Services with DHCP on page 82](#)
- [Grouping Interfaces with Common DHCP Configurations on page 83](#)
- [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 84](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 85](#)
- [Specifying the Maximum Number of DHCP Clients Per Interface on page 86](#)
- [Automatically Logging Out DHCP Clients on page 88](#)
- [Enabling Processing of Client Information Requests on page 89](#)
- [Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 90](#)
- [Enabling DHCPv6 Rapid Commit Support on page 90](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 94](#)
- [Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 95](#)
- [Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 95](#)
- [Configuring a Token for DHCP Local Server Authentication on page 96](#)
- [Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 96](#)
- [Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings on page 97](#)
- [Configuring Detection of DHCP Local Server Client Connectivity on page 98](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 100](#)
- [Configuring Passwords for Usernames on page 101](#)
- [Creating Unique Usernames for DHCP Clients on page 101](#)
- [Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use on page 104](#)

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 101](#).

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

See [“Creating Unique Usernames for DHCP Clients” on page 101](#).

Related Documentation

- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [DHCPv6 Relay Agent Overview on page 37](#)

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

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

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

2. Create the group and assign a name.

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

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface interface-name` statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the `upto` option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

- Related Documentation**
- [Extended DHCP Local Server Overview on page 8](#)
 - [Extended DHCP Relay Agent Overview on page 32](#)
 - [DHCPv6 Local Server Overview on page 13](#)
 - [DHCPv6 Relay Agent Overview on page 37](#)
 - [Configuring Group-Specific DHCP Local Server Options on page 16](#)
 - [Configuring Group-Specific DHCP Relay Options on page 38](#)
 - [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 84](#)

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```

- The start subunit, **interface** *interface-name*, serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit .0 subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, **interface** *ge-2/2/2* is treated as **interface** *ge-2/2/2.0*.
- Ranged entries contain the **upto** option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a 0 (zero) subunit acts as a wildcard.
- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because **ge-1/0/0.10** is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface **ge-1/0/0.26** is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface **ge-1/0/0.20** takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 83](#)

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 86](#).
3. (Optional) Configure DHCP client auto logout.
See [“Automatically Logging Out DHCP Clients” on page 88](#).
4. (Optional) Enable processing of information requests from clients.
See [“Enabling Processing of Client Information Requests” on page 89](#).
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 90](#).
6. (Optional, DHCPv6 only) Enable DHCPv6 rapid commit support.
See [“Enabling DHCPv6 Rapid Commit Support” on page 90](#).
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.
8. (Optional) Delete DHCP override settings.
See [“Deleting DHCP Local Server and DHCP Relay Override Settings” on page 91](#).

**Related
Documentation**

- [Configuring Group-Specific DHCP Local Server Options on page 16](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)

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 85](#)
- [Allowing Only One DHCP Client Per Interface](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)

- [Extended DHCP Relay Agent Overview on page 32](#)

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 20](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 117](#)
- [Allowing Only One DHCP Client Per Interface](#)

- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

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 Applied When Clients Obtain an Address* 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 85](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

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 85](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

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-method exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

You can configure the DHCPv6 local server to support the Rapid Commit option globally, for a specific group, or for a specific interface. By default, rapid commit support is disabled on the DHCPv6 local server.

To configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option:

1. Specify that you want to configure the **overrides** options.

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

2. Enable rapid commit support.

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

Related Documentation

- [Overriding Default DHCP Local Server Configuration Settings on page 85](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)

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 85](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

Configuring Dynamic Client Reconfiguration of Extended Local Server Clients

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

You can 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.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

For DHCPv4:

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

For DHCPv6:

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

2. (Optional) Enable dynamic reconfiguration for only the DHCP clients serviced by a group of interfaces.

For DHCPv4:

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

For DHCPv6:

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

3. (Optional) Configure an authentication token. The DHCP local server then includes this token inside the authentication option when it sends forcereboot 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.

- a. For all clients:

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
```

```
user@host# set token token-value
```

For DHCPv6:

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

- b. For only the DHCP clients serviced by a group of interfaces:

For DHCPv4:

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

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set token token-value
```

4. 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.

For all DHCPv6 clients:

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

For only the DHCPv6 clients serviced by a group of interfaces:

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

5. (Optional) Configure how the server attempts reconfiguration.

See [“Configuring Dynamic Reconfiguration Attempts for DHCP Clients” on page 94](#).

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

See [“Configuring Deletion of the Client When Dynamic Reconfiguration Fails” on page 95](#).

7. (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 95](#).

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

See [“Configuring a Token for DHCP Local Server Authentication” on page 96](#).

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

See [“Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings” on page 97](#).

10. (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 96](#).

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending `forcerenew` or `reconfigure` messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

For DHCPv4:

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

For DHCPv6:

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

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

Related Documentation

- [Configuring Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [clear-on-abort on page 150](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [radius-disconnect on page 196](#)
- [trigger on page 213](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [token on page 208](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [strict on page 204](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
- [request dhcp server reconfigure on page 384](#)

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: 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 50](#) 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 137](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50](#)
- [Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients](#)

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 12 on page 100 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 12: 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 19](#)

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 myPasswordD1234

```

Related Documentation

- [Extended DHCP Local Server Overview on page 8](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)
- [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 8](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)

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 22](#)
- [Configuring Address-Assignment Pools](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Example: Extended DHCP Local Server Configuration with Optional Pool Matching on page 50](#)

CHAPTER 10

Configuration Tasks for DHCP Relay Agent

- [Using External AAA Authentication Services with DHCP on page 108](#)
- [Grouping Interfaces with Common DHCP Configurations on page 109](#)
- [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 110](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 111](#)
- [Changing the Gateway IP Address \(giaddr\) Field to the giaddr of the DHCP Relay Agent on page 113](#)
- [Replacing the DHCP Relay Request and Release Packet Source Address on page 113](#)
- [Overriding Option 82 Information on page 114](#)
- [Using Layer 2 Unicast Transmission for DHCP Packets on page 114](#)
- [Trusting Option 82 Information on page 115](#)
- [Specifying the Maximum Number of DHCP Clients Per Interface on page 115](#)
- [Automatically Logging Out DHCP Clients on page 116](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 117](#)
- [Configuring DHCP Snooping for DHCP Relay Agent on page 119](#)
- [Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 119](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 124](#)
- [Sending Release Messages When Clients Are Deleted on page 126](#)
- [Disabling Automatic Binding of Stray DHCP Requests on page 127](#)
- [Using DHCP Relay Agent Option 82 Information on page 128](#)
- [Configuring Server Groups on page 135](#)
- [Configuring Active Server Groups on page 135](#)
- [Enabling DHCP Relay Proxy Mode on page 136](#)
- [Inserting DHCPv6 Interface-ID Option \(Option 18\) In DHCPv6 Packets on page 136](#)
- [DHCP Liveness Detection Overview on page 137](#)
- [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139](#)
- [Disabling DHCP Relay on page 140](#)

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 101.

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

See [“Creating Unique Usernames for DHCP Clients”](#) on page 101.

Related Documentation

- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [DHCPv6 Relay Agent Overview on page 37](#)

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

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

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

2. Create the group and assign a name.

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

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the **interface interface-name** statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the **upto** option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the **exclude** option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

- Related Documentation**
- [Extended DHCP Local Server Overview on page 8](#)
 - [Extended DHCP Relay Agent Overview on page 32](#)
 - [DHCPv6 Local Server Overview on page 13](#)
 - [DHCPv6 Relay Agent Overview on page 37](#)
 - [Configuring Group-Specific DHCP Local Server Options on page 16](#)
 - [Configuring Group-Specific DHCP Relay Options on page 38](#)
 - [Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces on page 84](#)

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following configuration statement:

```
user@host# set interface interface-name upto upto-interface-name
```

- The start subunit, **interface** *interface-name* , serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit .0 subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, **interface ge-2/2/2** is treated as **interface ge-2/2/2.0**.
- Ranged entries contain the **upto** option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a 0 (zero) subunit acts as a wildcard.
- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because **ge-1/0/0.10** is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface **ge-1/0/0.26** is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface **ge-1/0/0.20** takes precedence and enforces an interface client limit of 5.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

Related Documentation

- [Grouping Interfaces with Common DHCP Configurations on page 83](#)

Overriding the Default DHCP Relay Configuration Settings

You can override the default DHCP and DHCPv6 relay agent configuration settings at the global level, for a named group of interfaces, or for a specific interface within a named group.

- To override global default DHCP relay agent configuration options, include the **overrides** statement and its subordinate statements at the **[edit forwarding-options dhcp-relay]** hierarchy level.
- To override DHCP relay configuration options for a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group group-name]** hierarchy level.
- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the **[edit forwarding-options dhcp-relay group group-name interface]** hierarchy level.
- To configure overrides for DHCPv6 relay, use the supported statements at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

To override default DHCP relay agent configuration settings:

1. Specify that you want to configure override options.

Global override:

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

Group-level override:

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

Per-interface override:

```
[edit forwarding-options dhcp-relay]
user@host# edit group boston interface fe-1/0/1.2 overrides
```

2. (DHCPv4 only) Enable DHCP relay proxy mode.
See [“Enabling DHCP Relay Proxy Mode” on page 136](#).
3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.
See [“Changing the Gateway IP Address \(giaddr\) Field to the giaddr of the DHCP Relay Agent” on page 113](#).
4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
See [“Replacing the DHCP Relay Request and Release Packet Source Address” on page 113](#).
5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.
See [“Overriding Option 82 Information” on page 114](#).
6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.
See [“Using Layer 2 Unicast Transmission for DHCP Packets” on page 114](#).
7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.
See [“Trusting Option 82 Information” on page 115](#).
8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.
See [“Specifying the Maximum Number of DHCP Clients Per Interface” on page 86](#).
9. (DHCPv4 only) Configure client auto logout.
See [“DHCP Auto Logout Overview” on page 20](#).
10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.
See [“Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 119](#).
11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.
See the *delay-authentication* statement.
12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.
See [“Sending Release Messages When Clients Are Deleted” on page 126](#).

13. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.
See [“Disabling DHCP Relay” on page 140](#).
14. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.
See [“Disabling Automatic Binding of Stray DHCP Requests” on page 127](#).

- Related Documentation**
- [Configuring Group-Specific DHCP Relay Options on page 38](#)
 - [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)

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

You can configure the DHCP relay agent to change the gateway IP address (giaddr) field in packets that it forwards between a DHCP client and a DHCP server.

To overwrite the giaddr of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```
2. Specify that the giaddr of DHCP packets is overwritten.

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

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Replacing the DHCP Relay Request and Release Packet Source Address

You can configure the DHCP relay agent to replace request and release packets with the gateway IP address (giaddr) before forwarding the packet to the DHCP server.

To replace the source address with giaddr:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```
2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

```
[edit forwarding-options dhcp-relay overrides]
user@host# set replace-ip-source-with giaddr
```

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Overriding Option 82 Information

You can configure the DHCP relay agent to add or remove the DHCP relay agent information option (option 82) in DHCP packets.

This feature causes the DHCP relay agent to perform one of the following actions, depending on the configuration:

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

To override the default option 82 information in DHCP packets destined for a DHCP server:

1. Specify that you want to configure override options.

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

2. Specify that the option 82 information in DHCP packets is overwritten.

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

Related Documentation

- [Extended DHCP Relay Agent Overview on page 32](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Using Layer 2 Unicast Transmission for DHCP Packets

You can configure the DHCP relay agent to override the setting of the broadcast bit in DHCP request packets. DHCP relay agent then instead uses the Layer 2 unicast transmission method to send DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.

To override the default setting of the broadcast bit in DHCP request packets:

1. Specify that you want to configure override options.

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

2. Specify that the DHCP relay agent uses the Layer 2 unicast transmission method.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set layer2-unicast-replies
```


- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Trusting Option 82 Information

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

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

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

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

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

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 85](#)
- [Allowing Only One DHCP Client Per Interface](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

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 20](#)
- [How DHCP Relay Agent Uses Option 82 for Auto Logout on page 117](#)
- [Allowing Only One DHCP Client Per Interface](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Extended DHCP Local Server Overview on page 8](#)
- [Extended DHCP Relay Agent Overview on page 32](#)

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 13 on page 118 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the right column.

Table 13: DHCP Relay Agent Option 82 Value for Auto Logout

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-option-82"		
No	No	—	—	—	No secondary search performed
No	Yes	Yes	—	—	Use option 82 from packet
No	Yes	No	—	Zero	Drop packet
No	Yes	No	—	Non-zero	Use option 82 from packet
Yes	No	—	—	—	Use configured option 82
Yes	Yes	No	—	Zero	Drop packet
Yes	Yes	No	No	Non-zero	Use option 82 from packet
Yes	Yes	No	Yes	Non-zero	Overwrite the configured option 82
Yes	Yes	Yes	No	—	Use option 82 from packet
Yes	Yes	Yes	Yes	—	Overwrite the configured option 82

Related Documentation

- [DHCP Auto Logout Overview on page 20](#)
- [Automatically Logging Out DHCP Clients on page 88](#)

Configuring DHCP Snooping for DHCP Relay Agent

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. First, you enable or disable snooping support for DHCP relay agent and, optionally, override the default snooping configuration. Then you configure the forwarding action for snooped clients, which specifies whether DHCP relay agent forwards or drops snooped traffic.

To configure DHCP snooping for DHCP relay agent:

1. (DHCPv4 and DHCPv6) Enable or disable DHCP snooping. You can configure DHCP snooping globally, for a named group of interfaces, or for a specific interface.
See [“Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent” on page 119](#).
2. (DHCPv4 only) Configure snooped packets forwarding support.
See [“Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 124](#).

Related Documentation

- [DHCP Snooping Support on page 19](#)
- [Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 119](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 124](#)

Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent

DHCP relay agent uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes the first procedure, in which you enable or disable snooping support for DHCP relay agent and, optionally, override the default snooping configuration.

The second procedure, which applies only to DHCPv4 relay agent, is described in [“Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent” on page 124](#), and configures the forwarding action for snooped clients, which specifies whether DHCP relay agent forwards or drops snooped traffic.

You can enable or disable DHCP globally for DHCP relay, for a group of interfaces, or for a specific interface in a group.

By default, DHCP snooping is disabled for DHCP relay. To enable or disable DHCP snooping support globally:

1. Specify that you want to configure DHCP relay agent.
 - For DHCP relay agent:
[edit]

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

- For DHCPv6 relay agent:

```
[edit]
```

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

2. Specify that you want to override the default configuration.

- 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
```

3. Enable or disable DHCP snooping support.

- To enable DHCP snooping:

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay overrides]
```

```
user@host# set allow-snooped-clients
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
```

```
user@host# set allow-snooped-clients
```

- To disable DHCP snooping:

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay overrides]
```

```
user@host# set no-allow-snooped-clients
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
```

```
user@host# set no-allow-snooped-clients
```

For example, to enable global DHCP snooping support :

```
forwarding-options {  
  dhcp-relay {  
    overrides {  
      allow-snooped-clients;  
    }  
  }  
}
```

To enable or disable DHCP snooping support for a group of interfaces:

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

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

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

2. Specify the named group.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

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

3. Specify that you want to override the default configuration.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name]
user@host# edit overrides
```

4. Enable or disable DHCP snooping support.

- To enable DHCP snooping:

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay group group-name overrides]
user@host# set allow-snooped-clients
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides]
user@host# set allow-snooped-clients
```

- To disable DHCP snooping:

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay group group-name overrides]
user@host# set no-allow-snooped-clients
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides]
user@host# set no-allow-snooped-clients
```

For example, to enable DHCP snooping support on all interfaces in group **boston**:

```
forwarding-options {  
  dhcp-relay {  
    group boston {  
      overrides {  
        allow-snooped-clients;  
      }  
    }  
  }  
}
```

To enable or disable DHCP snooping support on a specific interface:

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

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

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

2. Specify the named group containing the interface.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

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

3. Specify the interface for which you want to configure DHCP snooping.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name]  
user@host# edit interface interface-name
```

4. Specify that you want to override the default configuration on the interface.

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay group group-name interface interface-name]  
user@host# edit overrides
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface  
interface-name]  
user@host# edit overrides
```

5. Enable or disable DHCP snooping support.

- To enable DHCP snooping:
 - For DHCP relay agent:


```
[edit forwarding-options dhcp-relay group group-name interface interface-name
overrides]
user@host# set allow-snooped-clients
```
 - For DHCPv6 relay agent:


```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface
interface-name overrides]
user@host# set allow-snooped-clients
```
- To disable DHCP snooping:
 - For DHCP relay agent:


```
[edit forwarding-options dhcp-relay group group-name interface interface-name
overrides]
user@host# set no-allow-snooped-clients
```
 - For DHCPv6 relay agent:


```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface
interface-name overrides]
user@host# set no-allow-snooped-clients
```

For example, to disable DHCP snooping support on interface **ge-2/1/8.0** in group **boston**:

```
forwarding-options {
  dhcp-relay {
    group boston {
      interface ge-2/1/8.0 {
        overrides {
          no-allow-snooped-clients;
        }
      }
    }
  }
}
```

To enable DHCPv6 snooping support on interface **ge-3/2/1.1** in group **sunnyvale**:

```
forwarding-options {
  dhcp-relay {
    dhcpv6 {
      group sunnyvale {
        interface ge-3/2/1.1 {
          overrides {
            allow-snooped-clients;
          }
        }
      }
    }
  }
}
```

Related Documentation

- [DHCP Snooping Support on page 19](#)
- [Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent on page 124](#)
- [Example: Configuring DHCP Snooping Support for DHCP Relay Agent on page 60](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

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

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the **forward-snooped-clients** statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, which is described in “[Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent](#)” on page 119, you enable or disable the DHCP relay snooping feature.

[Table 14 on page 124](#) shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the **allow-snooped-clients** statement.

[Table 15 on page 125](#) shows the action the router (or switch) takes on snooped packets when DHCP snooping is disabled by the **no-allow-snooped-clients** statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets. [Table 16 on page 125](#) shows the action the router (or switch) takes for the snooped BOOTREPLY packets.



NOTE: Configured interfaces have been configured with the **group** statement in the **[edit forwarding-options dhcp-relay]** hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the **group** statement.

Table 14: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
forward-snooped-clients not configured	snooped packets result in subscriber (DHCP client) creation	dropped
all-interfaces	forwarded	forwarded
configured-interfaces	forwarded	dropped

Table 14: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Enabled (*continued*)

forward-snooped-clients Configuration	Action on Configured Interfaces	Action on Non-Configured Interfaces
non-configured-interfaces	snooped packets result in subscriber (DHCP client) creation	forwarded

Table 15: Actions for DHCP Relay Agent Snooped Packets When DHCP Snooping Is Disabled

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

Table 16: Actions for Snooped BOOTREPLY Packets

forward-snooped-clients Configuration	Action
forward-snooped-clients not configured	snooped BOOTREPLY packets dropped if client is not found
forward-snooped-clients all configurations	snooped BOOTREPLY packets forwarded if client is not found

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

- Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```
- Enable DHCP snooped packet forwarding.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```
- Specify the interfaces that are supported for snooped packet forwarding.

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
  dhcp-relay {
    forward-snooped-clients configured-interfaces;
  }
}
```

- Related Documentation**
- [DHCP Snooping Support on page 19](#)
 - [Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent on page 119](#)

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.



NOTE: You must include the **send-release-on-delete** statement to configure DHCP relay and relay proxy to send the release message when the **client-discover-match** statement is included.

You can use the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.

- For DHCP relay agent:

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

- For DHCPv6 relay agent:

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

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set send-release-on-delete
```

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Disabling Automatic Binding of Stray DHCP Requests

DHCP requests that are received but have no entry in the database are known as stray requests. By default, DHCP relay, DHCP relay proxy, and DHCPv6 relay agent attempt to bind the requesting client by creating a database entry and forwarding the request to the DHCP server. If the server responds with an ACK, the client is bound and the ACK is forwarded to the client. If the server responds with a NAK, the database entry is deleted and the NAK is forwarded to the client. This behavior occurs regardless of whether authentication is configured.

You can override the default configuration at the global level, for a named group of interfaces, or for a specific interface within a named group. Overriding the default causes DHCP relay, DHCP relay proxy, and DHCPv6 relay agent to drop all stray requests instead of attempting to bind the clients.



NOTE: Automatic binding of stray requests is enabled by default.

- To disable automatic binding behavior, include the **no-bind-on-request** statement when you configure DHCP overrides at the global, group, or interface level.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set no-bind-on-request
```

- To override the default behavior for DHCPv6 relay agent, configure the override at the **[edit forwarding-options dhcp-relay dhcpv6]** hierarchy level.

```
[edit forwarding-options dhcp-relay dhcpv6 overrides]
user@host# set no-bind-on-request
```

The following two examples show a configuration that disables automatic binding of stray requests for a group of interfaces and a configuration that disables automatic binding on a specific interface.

To disable automatic binding of stray requests on a group of interfaces:

- Specify the named group.

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

- Specify that you want to configure overrides.

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

- Disable automatic binding for the group.

```
[edit forwarding-options dhcp-relay group boston overrides]
user@host# set no-bind-on-request
```

To disable automatic binding of stray requests on a specific interface:

- Specify the named group of which the interface is a member.

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

2. Specify the interface on which you want to disable automatic binding.

```
[edit forwarding-options dhcp-relay group boston]
user@host# edit interface fe-1/0/1.2
```

3. Specify that you want to configure overrides.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2]
user@host# edit overrides
```

4. Disable automatic binding on the interface.

```
[edit forwarding-options dhcp-relay group boston interface fe-1/0/1.2 overrides]
user@host# set no-bind-on-request
```

**Related
Documentation**

- [Extended DHCP Relay Agent Overview on page 32](#)
- [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Using DHCP Relay Agent Option 82 Information

Subscriber management enables you to configure the DHCP relay agent to include additional option 82 information in the DHCP packets that the relay agent receives from clients and forwards to a DHCP server. The DHCP server uses the additional information to determine the IP address to assign to the client. The server might also use the information for other purposes—for example, to determine which services to grant the client, or to provide additional security against threats such as address spoofing. The DHCP server sends its reply back to the DHCP relay agent, and the agent removes the option 82 information from the message and forwards the packet to the client.

To configure support for the DHCP relay agent information option 82, you use the **relay-option-82** statement. You can configure the DHCP relay agent to include the following suboptions in the packet the relay agent sends to the DHCP server:

- Agent Circuit ID (suboption 1)—An ASCII string that identifies the interface on which the client DHCP packet is received.
- Agent Remote ID (suboption 2)—An ASCII string assigned by the DHCP relay agent that securely identifies the client.

You can configure the option 82 support globally or for a named group of interfaces.

To restore the default behavior, in which option 82 information is not inserted into DHCP packets, you use the **delete relay-option-82** statement.



NOTE: The DHCPv6 relay agent provides similar Agent Circuit ID and Agent Remote ID support for DHCPv6 clients. For DHCPv6, subscriber management uses DHCPv6 option 18 to include the circuit ID in the packets that the relay agent sends to a DHCPv6 server, and option 37 to include the remote ID in the packets. See *DHCPv6 Relay Agent Options*.

The following sections describe the option 82 operations you can configure:

- [Configuring Option 82 Information on page 129](#)
- [Including a Prefix in DHCP Options on page 131](#)
- [Including a Textual Description in DHCP Options on page 133](#)

Configuring Option 82 Information

You use the **relay-option-82** statement to configure the DHCP relay agent to insert option 82 information in DHCP packets that the relay agent receives from clients and forwards to a DHCP server. When you configure option 82, you can include one of the suboption statements to specify the type of information you want to include in the DHCP packets. If you configure option 82 without including one of the suboption statements, the Agent Circuit ID option is included by default. Use the **circuit-id** statement to include the Agent Circuit ID (suboption 1) in the packets, or the **remote-id** statement to include the Agent Remote ID (suboption 2).

You can optionally configure DHCP relay agent to include a prefix or the interface description as part of the suboption information. If you specify the **circuit-id** or **remote-id** statement without including any of the optional **prefix**, **use-interface-description**, **use-vlan-id**, **include-irb-and-l2**, or **no-vlan-interface-name** statements, the format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet (fe), Gigabit Ethernet (ge), and integrated routing and bridging (irb) interfaces is one of the following, depending on your network configuration:



NOTE: Integrated routing and bridging (IRB) provides simultaneous support for Layer 2 bridging and Layer 3 IP routing on the same interface. IRB enables you to route local packets to another routed interface or to another bridging domain that has a Layer 3 protocol configured.

The interface to bridge domain relationship might be implicit (the interface is mapped to the bridge domain by the system based on the VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

- For Fast Ethernet or Gigabit Ethernet interfaces that do not use VLANs, stacked VLANs (S-VLANs), or bridge domains:

(fe | ge)-fpc/pic/port.subunit



NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

- For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-id

- For Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs:

(fe | ge)-fpc/pic/port:svlan-id-vlan-id

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port.subunit:bridge-domain-name

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port.subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

irb.subunit

To enable insertion of option 82 information:

- Specify that you want to configure option 82 support.

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

- Configure the DHCP relay agent to insert the Agent Circuit ID suboption, the Agent Remote ID suboption, or both.

- To insert the Agent Circuit ID:

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

- To insert the Agent Remote ID:

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


- To insert both, configure both set commands.
3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.
See [“Including a Prefix in DHCP Options” on page 131](#).
 4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.
See [“Including a Textual Description in DHCP Options” on page 133](#).

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the **host-name**, **logical-system-name**, and **routing-instance-name** options. The DHCP relay agent obtains the values for the **host-name**, **logical-system-name**, and **routing-instance-name** as follows:

- If you include the **host-name** option, the DHCP relay agent uses the hostname of the device configured with the **host-name** statement at the **[edit system]** hierarchy level.
- If you include the **logical-system-name** option, the DHCP relay agent uses the logical system name configured with the **logical-system** statement at the **[edit logical-system]** hierarchy level.
- If you include the **routing-instance-name** option, the DHCP relay agent uses the routing instance name configured with the **routing-instance** statement at the **[edit routing-instances]** hierarchy level or at the **[edit logical-system logical-system-name routing-instances]** hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the DHCP option information when you specify the **prefix** statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
hostname:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

host-name/logical-system-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

host-name/logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the *vlan-id* value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

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

2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.

- To configure the Agent Circuit ID:

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

- To configure the Agent Remote ID:

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

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.

- To include the prefix with the Agent Circuit ID:

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

- To include the prefix with the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82 remote-id]
user@host# set prefix host-name logical-system-name
```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

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

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

- To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

- To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the **description** statement at the **[edit interfaces interface-name]** hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.



NOTE: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

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

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

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

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

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

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

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

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

- To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

- To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

- To include the textual description in option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description device
```

- To include the textual description in option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description device
```

Configuring Server Groups

You can configure a named group of DHCP servers for use by the extended DHCP relay agent on the router or switch.

You specify the name of the DHCP server group and the IP addresses of one or more DHCP servers that belong to this group. You can configure a maximum of five IP addresses per named server group.

To configure a named server group:

1. Specify the name of the server group.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group myServerGroup
```

2. Add the IP addresses of the DHCP servers belonging to the group.

```
[edit forwarding-options dhcp-relay server-group myServerGroup]
user@host# set 192.168.100.50
user@host# set 192.168.100.75
```

Related Documentation

- [Extended DHCP Relay Agent Overview on page 32](#)

Configuring Active Server Groups

You can configure an active server group. Using an active server group enables you to apply a common DHCP relay agent configuration to a named group of DHCP server addresses.

Use the statement at the **[edit ... dhcpv6]** hierarchy levels to configure DHCPv6 support.

To configure an active server group:

- Specify the name of the active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group myServerGroup
```

To create an active server group as a global DHCP relay agent configuration option, include the **active-server-group** statement at the **[edit forwarding-options dhcp-relay]**

hierarchy level. To have the group apply only to a named group of interfaces, include the **active-server-group** statement at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level.

Including the **active-server-group** statement at the **[edit forwarding-options dhcp-relay group *group-name*]** hierarchy level (as a group-specific option) overrides the effect of including the **active-server-group** statement at the **[edit forwarding-options dhcp-relay]** hierarchy level as a global option.

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Grouping Interfaces with Common DHCP Configurations on page 83](#)

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

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

2. Enable DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set proxy-mode
```

- Related Documentation**
- [DHCP Relay Proxy Overview on page 35](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

- **Prefix**—Specify the **prefix** option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- **Interface description**—Specify the **use-interface-description** option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- **Option 82 Agent Circuit ID suboption (suboption 1)**—Specify the **use-option-82** option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router

checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.



NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the **logical** interface description or the **device** interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-option-82
```

Related Documentation

- *DHCPv6 Relay Agent Options*
- *Configuring DHCPv6 Relay Agent Options*
- [Including a Prefix in DHCP Options on page 131](#)
- [Including a Textual Description in DHCP Options on page 133](#)

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: Only BFD for DHCPv4 and DHCPv6 liveness detection is supported.

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 98](#)
 - [Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139](#)

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity

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.

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.

- For DHCP global configuration:

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

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name]
user@host# edit liveness-detection
```



NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the **liveness-detection** statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay group group-name]
user@host# set overrides proxy-mode
```

3. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:

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

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit method
```

4. Specify the liveness detection method that you want DHCP to use.



NOTE: The only method supported for liveness detection is Bidirectional Forwarding Detection (BFD).

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit bfd
```

5. Configure the liveness detection method as desired.

See *Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients* for an example of how to globally configure DHCP relay liveness detection.

6. Configure the action the router takes when a liveness detection failure occurs.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit failure-action action
```

Related Documentation

- [Extended DHCP Relay Agent Overview on page 32](#)
- [DHCP Liveness Detection Overview on page 137](#)
- [Configuring Detection of DHCP Local Server Client Connectivity on page 98](#)
- [Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50](#)
- [Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients](#)

Disabling DHCP Relay

You can disable DHCP relay on all interfaces or a group of interfaces.

To disable DHCP relay agent:

1. Specify that you want to configure override options.

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

2. Disable the DHCP relay agent.

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

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)

CHAPTER 11

DHCP Local Server Configuration Statements

- [allow-no-end-option \(DHCP Local Server\) on page 145](#)
- [attempts \(DHCP Local Server\) on page 146](#)
- [authentication \(DHCP Local Server\) on page 147](#)
- [bfd on page 148](#)
- [circuit-type \(DHCP Local Server\) on page 149](#)
- [clear-on-abort \(DHCP Local Server\) on page 150](#)
- [client-discover-match \(DHCP Local Server\) on page 151](#)
- [client-id \(DHCP Local Server\) on page 152](#)
- [delegated-pool \(DHCP Local Server\) on page 153](#)
- [delimiter \(DHCP Local Server\) on page 154](#)
- [detection-time on page 155](#)
- [dhcp \(DHCP Client\) on page 156](#)
- [dhcp-local-server on page 157](#)
- [dhcpv6 \(DHCP Local Server\) on page 162](#)
- [domain-name \(DHCP Local Server\) on page 165](#)
- [dynamic-profile \(DHCP Local Server\) on page 166](#)
- [external-authority on page 167](#)
- [failure-action on page 168](#)
- [forward-snooped-clients \(DHCP Local Server\) on page 169](#)
- [group \(DHCP Local Server\) on page 170](#)
- [holddown-interval on page 172](#)
- [interface \(DHCP Local Server\) on page 173](#)
- [interface-client-limit \(DHCP Local Server\) on page 175](#)
- [interface-delete \(Subscriber Management or DHCP Client Management\) on page 176](#)
- [interface-name \(DHCP Local Server\) on page 177](#)
- [ip-address-first on page 178](#)

- [liveness-detection](#) on page 179
- [mac-address \(DHCP Local Server\)](#) on page 180
- [method](#) on page 181
- [minimum-interval](#) on page 182
- [minimum-receive-interval](#) on page 183
- [multiplier](#) on page 184
- [no-adaptation](#) on page 185
- [option-60 \(DHCP Local Server\)](#) on page 186
- [option-82 \(DHCP Local Server Authentication\)](#) on page 187
- [option-82 \(DHCP Local Server Pool Matching\)](#) on page 188
- [overrides \(DHCP Local Server\)](#) on page 189
- [password \(DHCP Local Server\)](#) on page 191
- [pool \(DHCP Local Server Overrides\)](#) on page 192
- [pool-match-order](#) on page 193
- [process-inform](#) on page 194
- [radius-disconnect \(DHCP Local Server\)](#) on page 196
- [rapid-commit \(DHCPv6 Local Server\)](#) on page 197
- [reconfigure \(DHCP Local Server\)](#) on page 198
- [relay-agent-interface-id \(DHCP Local Server\)](#) on page 199
- [relay-agent-remote-id \(DHCP Local Server\)](#) on page 200
- [routing-instance-name \(DHCP Local Server\)](#) on page 201
- [service-profile \(DHCP Local Server\)](#) on page 202
- [session-mode](#) on page 203
- [strict \(DHCP Local Server\)](#) on page 204
- [threshold \(detection-time\)](#) on page 205
- [threshold \(transmit-interval\)](#) on page 206
- [timeout \(DHCP Local Server\)](#) on page 207
- [token \(DHCP Local Server\)](#) on page 208
- [traceoptions \(DHCP Server\)](#) on page 209
- [transmit-interval](#) on page 212
- [trigger \(DHCP Local Server\)](#) on page 213
- [use-primary \(DHCP Local Server\)](#) on page 214
- [user-prefix \(DHCP Local Server\)](#) on page 215
- [username-include \(DHCP Local Server\)](#) on page 216
- [version \(BFD\)](#) on page 217

allow-no-end-option (DHCP Local Server)

Syntax	allow-no-end-option;
Hierarchy Level	[edit system services dhcp-local-server overrides], [edit system services dhcp-local-server dhcpv6 group group-name overrides], [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
Release Information	Statement introduced in Junos OS Release 14.1X53-D15 for EX Series switches.
Description	Override the configuration on a DHCP local server in order to enable the server to process DHCP packets that are sent from the client without Option 255 (End-of-options). Option 255 is used to mark the end of the vendor option field. The default behavior in Junos OS is to drop packets that do not include option 255.
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 8 • Overriding Default DHCP Local Server Configuration Settings on page 85 • Deleting DHCP Local Server and DHCP Relay Override Settings on page 91 • Configuring a DHCP Server on Switches (CLI Procedure)

attempts (DHCP Local Server)

Syntax	<code>attempts <i>attempt-count</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 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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 94

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 group-name], [edit system services dhcp-local-server group group-name], [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 82

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 50 • 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 82

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 • Configuring Deletion of the Client When Dynamic Reconfiguration Fails on page 95

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 8 • Overriding Default DHCP Local Server Configuration Settings on page 85 • DHCP Auto Logout Overview on page 20 • Allowing Only One DHCP Client Per Interface

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 101

delegated-pool (DHCP Local Server)

Syntax	<code>delegated-pool <i>pool-name</i>;</code>
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 <i>interface-name overrides</i>],</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	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
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	<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"> • Specifying the Delegated Address Pool for IPv6 Prefix Assignment on page 90 • Overriding Default DHCP Local Server Configuration Settings on page 85

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 82](#)

detection-time

Syntax	<pre>detection-time { threshold 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>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	<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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

dhcp (DHCP Client)

Syntax	<pre>dhcp { client-identifier (ascii <i>ascii</i> hexadecimal <i>hexadecimal</i>); lease-time (<i>seconds</i> infinite); retransmission-attempt <i>number</i>; retransmission-interval <i>seconds</i>; server-address <i>ip-address</i>; update-server; vendor-id <i>vendor-id</i>; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>Configure a DHCP client for an IPv4 interface.</p> <p>The remaining statements are described separately.</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">• Configuring a DHCP Client (CLI Procedure) on page 71

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);
    include-option-82 {
        forcerenew;
        nak;
    }
    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);
    include-option-82 {
        forcerenew;
        nak;
    }
    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);
    include-option-82 {
        forcerenew;
        nak;
    }
    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.
 Statement introduced in Junos OS Release 13.2X51 for the QFX Series.
 Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

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 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 **dhcpx6** 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 8](#)
- [DHCPv6 Local Server Overview on page 13](#)
- [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 {
        include-option-82;
        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;
    include-option-82;
    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;
    include-option-82;
    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 <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 9.6. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	<p>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.</p> <p>The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.</p> <p>The remaining statements are explained separately.</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">• DHCPv6 Local Server Overview on page 13

domain-name (DHCP Local Server)

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<pre> [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include], [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], [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], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server authentication username-include], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include], [edit logical-systems <i>logical-system-name</i> 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 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include], [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], [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], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server authentication username-include], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group group-name authentication username-include], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server group group-name authentication username-include], [edit system services dhcp], [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] </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	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 82](#)

dynamic-profile (DHCP Local Server)

Syntax	dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); use-primary <i>primary-profile-name</i> ; }
Hierarchy Level	[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 ...]
Release Information	Statement introduced in Junos OS Release 9.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Options aggregate-clients and use-primary introduced in Junos OS Release 9.3. Support at the [edit ... interface] hierarchy levels introduced in Junos OS Release 11.2.
Description	Specify the dynamic profile that is attached to all interfaces, a named group of interfaces, or a specific interface.
Options	profile-name —Name of the dynamic profile. 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"> • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces • Configuring a Default Subscriber Service

external-authority

Syntax	external-authority;
Hierarchy Level	<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 logical-systems <i>logical-system-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 10.0.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.</p> <p>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.</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 104 • Extended DHCP Local Server Overview on page 8 • Address-Assignment Pools Overview on page 22

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	clear-binding —The client session is cleared when a liveness detection failure occurs. 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. log-only —A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.
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 137• Configuring Detection of DHCP Local Server Client Connectivity on page 98• Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50• 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 19 • Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server on page 100

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	[edit system services dhcp-local-server], [edit system services dhcp-local-server dhcpv6], [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 9.0. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Configure a group of interfaces that have a common configuration, such as authentication parameters. A group must contain at least one interface.
Options	group-name —Name of the group. 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 8](#)
 - [Grouping Interfaces with Common DHCP Configurations on page 83](#)
 - [Using External AAA Authentication Services with DHCP on page 82](#)
 - *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
 - *Configuring a DHCP Server on Switches (CLI Procedure)*

holddown-interval

Syntax	<code>holddown-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 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 50• <i>Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients</i>

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

Related Documentation	<ul style="list-style-type: none">• Extended DHCP Local Server Overview on page 8• Grouping Interfaces with Common DHCP Configurations on page 83• Using External AAA Authentication Services with DHCP on page 82
------------------------------	--

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 86](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 85](#)

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](#)

interface-name (DHCP Local Server)

Syntax	interface-name;
Hierarchy Level	<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> <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 11.4.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
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	<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"> • Creating Unique Usernames for DHCP Clients on page 101

ip-address-first

Syntax	ip-address-first;
Hierarchy Level	[edit logical-systems <i>logical-system-name</i> system services dhcp-local-server pool-match-order], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-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 12.1 for EX Series switches.
Description	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.
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 104• Extended DHCP Local Server Overview on page 8• Address-Assignment Pools Overview on page 22• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

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 <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], [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 <i>group-name</i>], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</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 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 137 • Configuring Detection of DHCP Local Server Client Connectivity on page 98 • Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139 • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50

- *Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients*

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 82

method

Syntax	<pre> 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	<p>[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]</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 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 50 • 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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

minimum-receive-interval

Syntax	<code>minimum-receive-interval <i>milliseconds</i>;</code>
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	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	<p><i>milliseconds</i> — Specify the minimum receive interval value. Range: 1 through 255,000</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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

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 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 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	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —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 50• 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 50 • <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 82

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 82

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 104• Extended DHCP Local Server Overview on page 8• Address-Assignment Pools Overview on page 22

overrides (DHCP Local Server)

Syntax	<pre> overrides { allow-no-end-option; client-discover-match (option60-and-option82 incoming-interface); delegated-pool; interface-client-limit number; multi-address-embedded-option-response; process-inform { pool pool-name; } 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 group-name], [edit system services dhcp-local-server dhcpv6 group group-name interface interface-name], [edit system services dhcp-local-server group group-name], [edit system services dhcp-local-server group group-name interface interface-name], [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 ...] </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> <p>Support for the allow-no-end-option option introduced in Junos OS Release 14.1X53-D15 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 group-name] 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 group-name interface interface-name] 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

- [Extended DHCP Local Server Overview on page 8](#)
- [Overriding Default DHCP Local Server Configuration Settings on page 85](#)
- [Deleting DHCP Local Server and DHCP Relay Override Settings on page 91](#)
- [Configuring a DHCP Server on Switches \(CLI Procedure\)](#)

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 82

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 89 • Overriding Default DHCP Local Server Configuration Settings on page 85

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 104 • Extended DHCP Local Server Overview on page 8 • 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 89• Overriding Default DHCP Local Server Configuration Settings on page 85• <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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 95

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	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.
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 90 • Overriding Default DHCP Local Server Configuration Settings on page 85

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)
 - [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 101

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 101

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 82](#)

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 8 • Default Subscriber Service Overview • Configuring a Default Subscriber Service


session-mode

Syntax	<code>session-mode (automatic multihop singlehop);</code>
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], [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.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Configure the session mode.
Options	<p>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.</p> <p>multihop—Configure multihop BFD sessions.</p> <p>single-hop—Configure single hop BFD sessions.</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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients


strict (DHCP Local Server)

Syntax	strict;
Hierarchy Level	<pre>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure], [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], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 reconfigure], [edit logical-systems <i>logical-system-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 reconfigure], [edit routing-instances <i>routing-instance-name</i> system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure], [edit system services dhcp-local-server dhcpv6 reconfigure], [edit system services dhcp-local-server dhcpv6 group <i>group-name</i> reconfigure]</pre>
Release Information	Statement introduced in Junos OS Release 10.4. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
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	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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92• Preventing Binding of Clients That Do Not Support Reconfigure Messages on page 96

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],</p> <p>[edit system services dhcp-local-server dhcpv6 liveness-detection method bfd detection-time],</p> <p>[edit forwarding-options dhcp-relay liveness-detection method bfd detection-time],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method bfd detection-time],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> liveness-detection method bfd detection-time],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method bfd detection-time],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method bfd detection-time],</p> <p>[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 50 • 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], [edit system services dhcp-local-server dhcpv6 liveness-detection method bfd transmit-interval], [edit forwarding-options dhcp-relay liveness-detection method bfd transmit-interval], [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 transmit-interval], [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 transmit-interval], [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 50 • 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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 • Configuring Dynamic Reconfiguration Attempts for DHCP Clients on page 94

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 • Configuring a Token for DHCP Local Server Authentication on page 96

traceoptions (DHCP Server)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; } </pre>
Hierarchy Level	[edit system services dhcp]
Release Information	<p>Statement for tracing J Series Services Router DHCP processes introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Define tracing operations for DHCP processes for J Series Services Routers and EX Series switches.
Options	<p>file <i>filename</i>—Name of the file that receives the output of the tracing operation. Enclose the name in quotation marks. All files are placed in the directory <i>/var/log</i>.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named <i>trace-file</i> reaches its maximum size, it is renamed <i>trace-file.0</i>, then <i>trace-file.1</i>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</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. You can include the following flags:</p> <ul style="list-style-type: none"> • all—All tracing operations • binding—Trace binding operations • config—Log reading of configuration • conflict—Trace user-detected conflicts for IP addresses • event—Trace important events • ifdb—Trace interface database operations • io— Trace I/O operations • lease—Trace lease operations • main—Trace main loop operations • misc— Trace miscellaneous operations • packet—Trace DHCP packets

- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

match *regex*—(Optional) Refine the output to include lines that contain the regular expression.

- **all**—All tracing operations
- **binding**—Trace binding operations
- **config**—Log reading of configuration
- **conflict**—Trace user-detected conflicts for IP addresses
- **event**—Trace important events
- **ifdb**—Trace interface database operations
- **io**—Trace I/O operations
- **lease**—Trace lease operations
- **main**—Trace main loop operations
- **match *regex***—Refine the output to include lines that contain the regular expression.
- **misc**—Trace miscellaneous operations
- **packet**—Trace DHCP packets
- **options**—Trace DHCP options
- **pool**—Trace address pool operations
- **protocol**—Trace protocol operations
- **rtsock**—Trace routing socket operations
- **scope**—Trace scope operations
- **signal**—Trace DHCP signal operations
- **trace**—All tracing operations
- **ui**—Trace user interface operations

no-world-readable—(Optional) Disable unrestricted file access.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB

Range: 10 KB through 1 GB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

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

Related Documentation	• <i>Configuring Tracing Operations for DHCP Processes</i>
	• <i>System Management Configuration Statements</i>

transmit-interval

Syntax	<pre>transmit-interval { threshold milliseconds; minimum-interval 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	Configure the Bidirectional Forwarding Detection (BFD) transmit interval. The remaining statements are explained separately.
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 50• 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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92 • Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect on page 95 • radius-disconnect on page 196

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"> • <i>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</i>

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 82](#)

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	<pre>[edit system services dhcp-local-server authentication], [edit system services dhcp-local-server dhcpv6 authentication], [edit system services dhcp-local-server dhcpv6 group group-name authentication], [edit system services dhcp-local-server group group-name authentication], [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 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 82 • Creating Unique Usernames for DHCP Clients on page 101

version (BFD)

Syntax	version (0 1 automatic);
Hierarchy Level	<p>[edit logical-systems <i>logical-system-name</i> protocols ldp oam bfd-liveness-detection],</p> <p>[edit logical-systems <i>logical-system-name</i> protocols ldp oam fec <i>address</i> bfd-liveness-detection],</p> <p>[edit system services dhcp-local-server liveness-detection method <i>bfd</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 liveness-detection method <i>bfd</i>],</p> <p>[edit forwarding-options dhcp-relay liveness-detection method <i>bfd</i>],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method <i>bfd</i>],</p> <p>[edit system services dhcp-local-server group <i>group-name</i> liveness-detection method <i>bfd</i>],</p> <p>[edit system services dhcp-local-server dhcpv6 group <i>group-name</i> liveness-detection method <i>bfd</i>],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> liveness-detection method <i>bfd</i>],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> liveness-detection method <i>bfd</i>],</p> <p>[edit protocols ldp oam bfd-liveness-detection],</p> <p>[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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients • Configuring BFD for LDP LSPs

CHAPTER 12

DHCP Relay Agent Configuration Statements

- [\[edit forwarding-options dhcp-relay\] Configuration Statement Hierarchy for EX Series Switches on page 221](#)
- [access \(Dynamic Access Routes\) on page 226](#)
- [access-internal \(Dynamic Access-Internal Routes\) on page 227](#)
- [active-server-group on page 228](#)
- [allow-snooped-clients on page 229](#)
- [always-write-giaddr on page 230](#)
- [always-write-option-82 on page 231](#)
- [authentication \(DHCP Relay Agent\) on page 232](#)
- [bfd on page 233](#)
- [circuit-id \(DHCP Relay Agent\) on page 234](#)
- [circuit-type \(DHCP Relay Agent\) on page 236](#)
- [client-discover-match \(DHCP Relay Agent\) on page 237](#)
- [client-id \(DHCP Relay Agent\) on page 238](#)
- [delete-binding-on-renegotiation on page 238](#)
- [delimiter \(DHCP Relay Agent\) on page 239](#)
- [detection-time on page 240](#)
- [dhcp-relay on page 241](#)
- [dhcpv6 \(DHCP Relay Agent\) on page 247](#)
- [disable-relay on page 250](#)
- [domain-name \(DHCP Relay Agent\) on page 251](#)
- [drop \(DHCP Relay Agent Option\) on page 252](#)
- [dynamic-profile \(DHCP Relay Agent\) on page 253](#)
- [failure-action on page 254](#)
- [forward-snooped-clients \(DHCP Relay Agent\) on page 255](#)
- [group \(DHCP Relay Agent\) on page 256](#)
- [holddown-interval on page 259](#)

- [interface \(DHCP Relay Agent\) on page 260](#)
- [interface-client-limit \(DHCP Relay Agent\) on page 262](#)
- [interface-delete \(Subscriber Management or DHCP Client Management\) on page 263](#)
- [interface-name \(DHCP Relay Agent\) on page 264](#)
- [layer2-unicast-replies on page 265](#)
- [liveness-detection on page 266](#)
- [local-server-group \(DHCP Relay Agent Option\) on page 267](#)
- [mac-address \(DHCP Relay Agent\) on page 268](#)
- [method on page 269](#)
- [minimum-interval on page 270](#)
- [minimum-receive-interval on page 271](#)
- [multiplier on page 272](#)
- [next-hop \(Dynamic Access-Internal Routes\) on page 273](#)
- [no-adaptation on page 274](#)
- [no-allow-snooped-clients on page 275](#)
- [no-bind-on-request \(DHCP Relay Agent\) on page 276](#)
- [option-60 \(DHCP Relay Agent\) on page 277](#)
- [option-82 \(DHCP Relay Agent\) on page 278](#)
- [option-number \(DHCP Relay Agent Option\) on page 279](#)
- [overrides \(DHCP Relay Agent\) on page 280](#)
- [password \(DHCP Relay Agent\) on page 282](#)
- [preference \(Subscriber Management\) on page 283](#)
- [prefix \(DHCP Relay Agent\) on page 284](#)
- [proxy-mode on page 285](#)
- [relay-agent-interface-id \(DHCPv6 Relay Agent\) on page 286](#)
- [relay-agent-remote-id \(DHCPv6 Relay Agent Username\) on page 287](#)
- [relay-option \(DHCP Relay Agent\) on page 288](#)
- [relay-option-82 on page 289](#)
- [relay-server-group \(DHCP Relay Agent Option\) on page 290](#)
- [replace-ip-source-with on page 291](#)
- [route-suppression \(DHCP Local Server and Relay Agent\) on page 292](#)
- [routing-instance-name \(DHCP Relay Agent\) on page 293](#)
- [send-release-on-delete \(DHCP Relay Agent\) on page 294](#)
- [server-group on page 295](#)
- [service-profile \(DHCP Relay Agent\) on page 296](#)
- [session-mode on page 297](#)
- [threshold \(detection-time\) on page 298](#)

- [threshold \(transmit-interval\)](#) on page 299
- [trace \(DHCP Relay Agent\)](#) on page 300
- [transmit-interval](#) on page 301
- [trust-option-82](#) on page 302
- [use-interface-description](#) on page 303
- [use-primary \(DHCP Relay Agent\)](#) on page 305
- [user-prefix \(DHCP Relay Agent\)](#) on page 306
- [username-include \(DHCP Relay Agent\)](#) on page 307
- [version \(BFD\)](#) on page 308

[edit forwarding-options dhcp-relay] Configuration Statement Hierarchy for EX Series Switches

This topic lists supported and unsupported configuration statements in the **[edit forwarding-options dhcp-relay]** hierarchy level on EX Series switches.

- *Supported* statements are those that you can use to configure some aspect of a software feature on the switch.
- *Unsupported* statements are those that appear in the command-line interface (CLI) on the switch, but that have no effect on switch operation if you configure them.
- Not all features are supported on all switch platforms. For detailed information about feature support on specific EX Series switch platforms, see [Feature Explorer](#).

This topic lists:

- [Supported Statements in the \[edit forwarding-options dhcp-relay\] Hierarchy Level](#) on page 221
- [Unsupported Statements in the \[edit forwarding-options dhcp-relay\] Hierarchy Level](#) on page 225

Supported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level

The following hierarchy shows the **[edit forwarding-options dhcp-relay]** configuration statements supported on EX Series switches:

```
forwarding-options {
  dhcp-relay {
    active-server-group server-group-name;
    arp-inspection;
    authentication {
      ...
    }
  }
  authentication {
    password password-string;
  }
  username-include {
    circuit-type;
```

```
    client-id;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-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;
}
dhcpv6 {
    active-server-group server-group-name;
    authentication {
        ...
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    group group-name {
        ...
    }
}
liveness-detection {
    failure-action (clear-binding | clear-binding-if-interface-up | log-only);
    method {
        ...
    }
    overrides {
        ...
    }
    relay-agent-interface-id;
    relay-option {
        ...
    }
    server-group {
        server-group-name {
            server-ip-address;
        }
    }
    service-profile dynamic-profile-name;
    duplicate-clients-on-interface;
    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 {
```

```

active-server-group server-group-name;
authentication {
    ...
}
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
interface interface-name {
    exclude;
    liveness-detection {
        ...
    }
    overrides {
        ...
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    client-discover-match <option60-and-option82>;
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
    }
}

```

```

        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
}
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 {
    allow-snooped-clients;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
}
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}

```

```

    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
service-profile dynamic-profile-name;
}
}
```

Unsupported Statements in the [edit forwarding-options dhcp-relay] Hierarchy Level


All statements in the [edit forwarding-options dhcp-relay] hierarchy level that are displayed in the command-line interface (CLI) on the switch are supported on the switch and operate as documented with the following exceptions:

Table 17: Unsupported [edit forwarding-options] Configuration Statements on EX Series Switches

Statement	Hierarchy Level
NOTE: Variables, such as <i>filename</i> , are not shown in the statements or hierarchies.	
logical-system-name	[edit forwarding-options dhcp-relay authentication]

- Related Documentation
- *Notational Conventions Used in Junos OS Configuration Hierarchies*
 - *[edit forwarding-options] Configuration Statement Hierarchy on EX Series Switches*

access (Dynamic Access Routes)

Syntax	<pre>access { route <i>prefix</i> { <i>next-hop</i> <i>next-hop</i>; metric <i>route-cost</i>; <i>preference</i> <i>route-distance</i>; tag <i>route-tag</i>; } }</pre>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-options]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options] and [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i>] hierarchy levels introduced in Junos OS Release 10.1.</p>
Description	Dynamically configure access routes.
<div style="display: flex; align-items: center;">  <div style="margin-left: 10px;"> <p>BEST PRACTICE: We recommend that you always include the <code>access-internal</code> stanza in the dynamic-profile when the <code>access</code> stanza is present for framed-route support.</p> </div> </div>	
Options	The remaining statements are explained separately.
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"> <i>Configuring Dynamic Access Routes for Subscriber Management</i>

access-internal (Dynamic Access-Internal Routes)

Syntax	<pre>access-internal { route <i>subscriber-ip-address</i> { qualified-next-hop <i>underlying-interface</i> { mac-address <i>address</i>; } } }</pre>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i>],</p> <p>[edit dynamic-profiles routing-options]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options] and [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i>] hierarchy levels introduced in Junos OS Release 10.1.</p>
Description	<p>Dynamically configure access-internal routes. Access-internal routes are optional, but are used instead of access routes if the next-hop address is not specified in the Framed-Route Attribute [22] for IPv4 or the Framed-IPv6-Route attribute [99] for IPv6.</p>



BEST PRACTICE: We recommend that you always include the `access-internal` stanza in the dynamic-profile when the `access` stanza is present for framed-route support.


The remaining statements are explained separately.

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"> • <i>Configuring Dynamic Access-Internal Routes for DHCP Subscriber Management</i> • <i>Configuring Dynamic Access-Internal Routes for PPP Subscriber Management</i>

active-server-group

Syntax	<code>active-server-group <i>server-group-name</i>;</code>
Hierarchy Level	<pre> [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 group <i>group-name</i> dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options group <i>group-name</i> dhcpv6], [edit logical-systems <i>logical-system-name</i> 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> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay] [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Apply a DHCP relay agent configuration to the named group of DHCP server addresses. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>A group-specific configuration overrides a global option.</p>
Options	<i>server-group-name</i> —Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.
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"> • Extended DHCP Relay Agent Overview on page 32 • Configuring Active Server Groups on page 135 • Configuring Group-Specific DHCP Relay Options on page 38 • dhcp-relay on page 241

allow-snooped-clients

Syntax	allow-snooped-clients;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.2.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.</p>
Description	<p>Explicitly enable DHCP snooping support on the router.</p> <p>Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly enable snooping support on the router for DHCPv6 relay agent.</p>
<div>  NOTE: DHCP snooping is <i>disabled</i> by default. </div>	
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"> • Extended DHCP Relay Agent Overview on page 32 • Overriding the Default DHCP Relay Configuration Settings on page 111 • DHCP Snooping Support on page 19

always-write-giaddr

Syntax	<code>always-write-giaddr;</code>
Hierarchy Level	<code>[edit forwarding-options dhcp-relay <i>overrides</i>],</code> <code>[edit forwarding-options dhcp-relay group <i>group-name overrides</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay <i>overrides</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name overrides</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i></code> <code>forwarding-options dhcp-relay <i>overrides</i>],</code> <code>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i></code> <code>forwarding-options dhcp-relay group <i>group-name overrides</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>overrides</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group</code> <code><i>group-name overrides</i>],</code> <code>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group</code> <code><i>group-name</i> interface <i>interface-name overrides</i>]</code>
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	Overwrite the gateway IP address (giaddr) of every DHCP packet with the giaddr of the DHCP relay agent before forwarding the packet to the DHCP server.
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">• Extended DHCP Relay Agent Overview on page 32• dhcp-relay on page 241

always-write-option-82

Syntax	<code>always-write-option-82;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. The use of this option causes the DHCP relay agent to perform one of the following actions, depending on how it is configured:</p> <ul style="list-style-type: none"> • If the DHCP relay agent is configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the DHCP packets and inserts the new values before forwarding the packets to the DHCP server. • If the DHCP relay agent is not configured to add option 82 information to DHCP packets, it clears the existing option 82 values from the packets, but does not add any new values before forwarding the packets to the DHCP server.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • Extended DHCP Relay Agent Overview on page 32

authentication (DHCP Relay Agent)

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 forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [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 ...]</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> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	<p>Configure the parameters the router sends to the external AAA server. A group configuration takes precedence over a global DHCP relay configuration. Use the statement at the [edit...dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>The remaining statements are explained separately.</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-relay on page 241 Using External AAA Authentication Services with DHCP on page 82

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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

circuit-id (DHCP Relay Agent)

Syntax	<pre> circuit-id { include-irb-and-l2; no-vlan-interface-name; prefix <i>prefix</i>; use-interface-description (logical device); use-vlan-id; } </pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay relay-option-82], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay relay-option-82], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay relay-option-82], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> relay-option-82] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>include-irb-and-l2 , no-vlan-interface-name, and use-vlan-id options added in Junos OS Release 14.1.</p>
Description	<p>Specify the Agent Circuit ID suboption (suboption 1) of the DHCP relay agent information option (option 82) to include in DHCP packets destined for a DHCP server. Optionally specify that the suboption includes a prefix, textual description, or VLAN tag.</p>



NOTE: For Layer 3 interfaces, when you configure **relay-option-82** only, the Agent Circuit ID is the default. If no VLAN tags are configured, then the default is the logical interface device (IFL) name. For integrated routing and bridging (IRB) interfaces, the default is the Layer 2 IFL name and bridge domain name.

The interface to bridge domain relationship may be implicit (the interface is mapped to the bridge domain by the system based on VLAN tag) or explicit (the interface is mapped to the bridge domain by configuring it in the bridge domain definition). For the explicit case, tagging might not be relevant for the mapping.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that do not use virtual LANs (VLANs), stacked VLANs (S-VLANs), or bridge domains is as follows:

```
(fe | ge)-fpc/pic/port.subunit
```




NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface for remote systems.

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use VLANs is as follows:

(fe | ge)-fpc/pic/port:vlan-id

The format of the Agent Circuit ID information for Fast Ethernet or Gigabit Ethernet interfaces that use S-VLANs is as follows:

(fe | ge)-fpc/pic/port:svlan-id-vlan-id

In the case of an IRB interface, the format displays the Layer 2 interface instead of the IRB interface along with the bridge domain name. For IRB interfaces (or other pseudo devices) the default format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port.subunit:bridge-domain-name

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port.subunit:vlan-name

To include the IRB interface name with the Layer 2 interface name, configure the **include-irb-and-l2** statement. The format is as follows:

- IRB interfaces that use bridge domains but do not use VLANs or S-VLANs:

(fe | ge)-fpc/pic/port:bridge-domain-name+irb.subunit

- IRB interfaces that use VLANs:

(fe | ge)-fpc/pic/port:vlan-name+irb.subunit

To include only the IRB interface name without the Layer 2 interface and bridge domain or VLAN, configure the **no-vlan-interface-name** statement. The format is as follows:

irb.subunit


The remaining statements are explained separately.

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"> • Using DHCP Relay Agent Option 82 Information on page 128 • Configuring Option 82 Information on page 129

circuit-type (DHCP Relay Agent)

Syntax	circuit-type;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [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 ...]
Release Information	Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.
Description	Specify that the circuit type is concatenated with the username during the subscriber authentication or 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">• Using External AAA Authentication Services with DHCP on page 82• Creating Unique Usernames for DHCP Clients on page 101

client-discover-match (DHCP Relay Agent)

Syntax	client-discover-match (option60-and-option82 incoming-interface);
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ... overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group ... 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 relay 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 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>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"> • Extended DHCP Relay Agent Overview on page 32 • Overriding the Default DHCP Relay Configuration Settings on page 111 • DHCP Auto Logout Overview on page 20 • Allowing Only One DHCP Client Per Interface

client-id (DHCP Relay Agent)

Syntax	client-id;
Hierarchy Level	[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 ...]
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 client ID is concatenated with the username during the subscriber authentication or client authentication process.
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">• Using External AAA Authentication Services with DHCP on page 82• Creating Unique Usernames for DHCP Clients on page 101

delete-binding-on-renegotiation

Syntax	delete-binding-on-renegotiation;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides]
Release Information	Statement introduced in Junos OS Release 13.2 for EX Series switches.
Description	Configure the DHCP relay agent to delete binding information for a specific client when a DHCP DISCOVER packet is received from the client while the client already has a binding on the relay that is in BOUND state. A DHCP client sends discover messages to renegotiate the lease for an IP address.
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">• Extended DHCP Relay Agent Overview on page 32

delimiter (DHCP Relay Agent)

Syntax	<code>delimiter <i>delimiter-character</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the character used as the delimiter between the concatenated components of the username. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
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>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"> • Using External AAA Authentication Services with DHCP on page 82 • Creating Unique Usernames for DHCP Clients on page 101

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 50• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

dhcp-relay

```
Syntax  dhcp-relay {
    active-server-group server-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>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    dhcpv6 {
        active-server-group server-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;
            }
        }
        dynamic-profile profile-name {
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        group group-name {
            active-server-group server-group-name;
            authentication {
                ...
            }
            dynamic-profile 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 {
    ...
}
relay-option {
    ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
route-suppression:
service-profile dynamic-profile-name;
overrides {
    ...
}
relay-agent-interface-id {
    ...
}
relay-agent-remote-id {
    ...
}
relay-option {
    ...
}
route-suppression;
server-response-time seconds;
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 {
    allow-snooped-clients;
    delay-authentication;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
server-group {
    server-group-name {
        server-ip-address;
    }
}
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 {
    active-server-group server-group-name;
    authentication {
        ...
    }
    dynamic-profile 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 {
    ...
}
service-profile dynamic-profile-name;
trace;
upto upto-interface-name;
}
overrides {
    ...
}
relay-option {
    ...
}
relay-option-82 {
    ...
}
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 {

```

```

allow-snooped-clients;
always-write-giaddr;
always-write-option-82;
client-discover-match (option60-and-option82 | incoming-interface);
delay-authentication;
disable-relay;
interface-client-limit number;
layer2-unicast-replies;
no-allow-snooped-clients;
no-bind-on-request;
proxy-mode;
replace-ip-source-with;
send-release-on-delete;
trust-option-82;
}
relay-option {
  option-number option-number;
  default-action {
    drop;
    forward-only;
    relay-server-group group-name;
  }
  equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
  starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    local-server-group local-server-group;
    relay-server-group relay-server-group;
  }
}
}
relay-option-82 {
  circuit-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
  remote-id {
    prefix prefix;
    use-interface-description (logical | device);
  }
}
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
}
route-suppression:
server-response-time seconds;
service-profile dynamic-profile-name;
}

```

Hierarchy Level	[edit forwarding-options], [edit logical-systems <i>logical-system-name</i> forwarding-options], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options], [edit routing-instances <i>routing-instance-name</i> forwarding-options]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches. Statement introduced in Junos OS Release 13.2X51 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<p>Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch and enable the router (or switch) to function as a DHCP relay agent. A DHCP relay agent forwards DHCP request and reply packets between a DHCP client and a DHCP server.</p> <p>DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication or client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.</p> <p>The extended DHCP and DHCPv6 relay agent options configured with the dhcp-relay and dhcpv6 statements are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, the extended DHCP or DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot both be enabled on the router (or switch) at the same time.</p> <p>The remaining statements are explained separately.</p>
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">• Extended DHCP Relay Agent Overview on page 32• DHCPv6 Relay Agent Overview on page 37• DHCP Relay Proxy Overview on page 35• Using External AAA Authentication Services with DHCP on page 82

dhcpx6 (DHCP Relay Agent)

```
Syntax  dhcpx6 {
    active-server-group server-group-name;
    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;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    group group-name {
        active-server-group server-group-name;
        authentication {
            ...
        }
        dynamic-profile 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 {
        ...
    }
    service-profile dynamic-profile-name;
    trace;
    upto upto-interface-name;
}
}
overrides {
    ...
}
relay-agent-interface-id {
    ...
}
relay-agent-remote-id {
    ...
}
relay-option {
    ...
}
route-suppression;
service-profile dynamic-profile-name;
}
liveness-detection {
    ...
}
overrides {
    allow-snooped-clients;
    delay-authentication;
    interface-client-limit number;
    no-allow-snooped-clients;
    no-bind-on-request;
    send-release-on-delete;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        relay-server-group relay-server-group;
    }
}
equals (ascii ascii-string | hexadecimal hexadecimal-string) {
    drop;
    forward-only;
    relay-server-group relay-server-group;
}
starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
```

```

    drop;
    forward-only;
    relay-server-group relay-server-group;
  }
}
server-group {
  server-group-name {
    server-ip-address;
  }
}
route-suppression;
server-response-time seconds;
service-profile dynamic-profile-name;
}

```

Hierarchy Level	[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]
Release Information	Statement introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.3 for EX Series switches.
Description	<p>Configure DHCPv6 relay options on the router or switch and enable the router or switch to function as a DHCPv6 relay agent. A DHCPv6 relay agent forwards DHCPv6 request and reply packets between a DHCPv6 client and a DHCPv6 server.</p> <p>The DHCPv6 relay agent server is fully compatible with the extended DHCP local server and DHCP relay agent. However, the options configured with the dhcpv6 statement are incompatible with the DHCP/BOOTP relay agent options configured with the bootp statement. As a result, the DHCPv6 relay agent and the DHCP/BOOTP relay agent cannot be enabled on the router or switch at the same time.</p> <p>The remaining statements are explained separately.</p>
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"> • dhcp-relay on page 241 • DHCPv6 Relay Agent Overview on page 37 • Using External AAA Authentication Services with DHCP on page 82

disable-relay

Syntax	disable-relay;
Hierarchy Level	[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]
Release Information	Statement introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Disable DHCP relay on specific interfaces in a group.
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">• Extended DHCP Relay Agent Overview on page 32

domain-name (DHCP Relay Agent)

Syntax	<code>domain-name <i>domain-name-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include] [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the domain name that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>domain-name-string</i> —Domain name formatted string.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-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 82 • Creating Unique Usernames for DHCP Clients on page 101

drop (DHCP Relay Agent Option)

Syntax	drop;
Hierarchy Level	[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option (default-action equals starts-with)], [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 ...]
Release Information	Statement introduced in Junos OS Release 12.3.
Description	Drop (discard) specified DHCP client packets when you use DHCP relay agent selective processing. You can configure the drop operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.
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">• <i>Using DHCP Option Information to Selectively Process DHCP Client Traffic</i>

dynamic-profile (DHCP Relay Agent)

Syntax	<pre>dynamic-profile <i>profile-name</i> { aggregate-clients (merge replace); use-primary <i>primary-profile-name</i>; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [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 ...]</pre>
Release Information	<p>Statement introduced in Junos OS Release 9.2.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
Options	<p><i>profile-name</i>—Name of the dynamic profile.</p> <p>The remaining statements are explained separately.</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-relay on page 241 • <i>Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces</i> • Grouping Interfaces with Common DHCP Configurations on page 83 • <i>Configuring a Default Subscriber Service</i>

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	clear-binding —The client session is cleared when a liveness detection failure occurs. 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. log-only —A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure.
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 137• Configuring Detection of DHCP Local Server Client Connectivity on page 98• Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139• Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

forward-snooped-clients (DHCP Relay Agent)

Syntax	forward-snooped-clients (all-interfaces configured-interfaces non-configured-interfaces);
Hierarchy Level	<p>[edit forwarding-options dhcp-relay],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay]</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	<p>Configure how DHCP relay agent handles DHCP snooped packets on specific interfaces. The router or switch determines the DHCP snooping action to perform based on a combination of the forward-snooped-clients configuration and the configuration of either the allow-snooped-clients statement or the no-allow-snooped-clients statement.</p> <p>The router (or switch) also uses this statement to determine how to handle snooped BOOTREPLY packets received on nonconfigured interfaces.</p>
Options	<p>all-interfaces—Perform the action on all interfaces.</p> <p>configured-interfaces—Perform the action only on configured interfaces.</p> <p>non-configured-interfaces—Perform the action only on nonconfigured interfaces.</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 Snooping Support on page 19 • Configuring DHCP Snooping for DHCP Relay Agent on page 119

group (DHCP Relay Agent)

```
Syntax  group group-name {
        active-server-group server-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;
            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 {
            ...
        }
        service-profile dynamic-profile-name;
        trace;
```

```

    upto upto-interface-name;
}
overrides {
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    client-discover-match (option60-and-option82 | incoming-interface);
    disable-relay;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
    no-bind-on-request;
    proxy-mode;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
relay-agent-interface-id {
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82;
}
relay-agent-remote-id {
    prefix prefix;
    use-interface-description (logical | device);
}
relay-option {
    option-number option-number;
    default-action {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    equals (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
    starts-with (ascii ascii-string | hexadecimal hexadecimal-string) {
        drop;
        forward-only;
        local-server-group local-server-group;
        relay-server-group relay-server-group;
    }
}
relay-option-82 {
    circuit-id {
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82;
    }
    remote-id {
        prefix prefix;
        use-interface-description (logical | device);
    }
}

```

```
    }  
  }  
  route-suppression;  
  service-profile dynamic-profile-name;  
}
```

Hierarchy Level [edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay **dhcpv6**],
[edit logical-systems *logical-system-name* forwarding-options **dhcp-relay** ...],
[edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
forwarding-options **dhcp-relay** ...],
[edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information Statement introduced in Junos OS Release 8.3.
Support at the [edit ... **dhcpv6**] hierarchy levels introduced in Junos OS Release 11.4.
Statement introduced in Junos OS Release 12.1 for EX Series switches.

Description Specify the name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration. A group must contain at least one interface. Use the statement at the [edit ... **dhcpv6**] hierarchy levels to configure DHCPv6 support.

Options *group-name*—Name of a group of interfaces that have a common DHCP or DHCPv6 relay agent configuration.

The remaining statements are explained separately.

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

Related Documentation

- [dhcp-relay on page 241](#)
- [Extended DHCP Relay Agent Overview on page 32](#)
- [Configuring Group-Specific DHCP Relay Options on page 38](#)
- [Grouping Interfaces with Common DHCP Configurations on page 83](#)
- [Using External AAA Authentication Services with DHCP on page 82](#)
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces](#)

holddown-interval

Syntax	<code>holddown-interval <i>milliseconds</i>;</code>
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	Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.
Options	<p><i>milliseconds</i>—Interval specifying how long a BFD session must remain up before a state change notification is sent.</p> <p>Range: 0 through 255,000</p> <p>Default: 0</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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

interface (DHCP Relay Agent)

Syntax	<pre> interface <i>interface-name</i> { exclude; overrides { allow-snooped-clients; always-write-giaddr; always-write-option-82; client-discover-match (option60-and-option82 incoming-interface); disable-relay; interface-client-limit <i>number</i>; layer2-unicast-replies; no-allow-snooped-clients; proxy-mode; replace-ip-source-with; send-release-on-delete; trust-option-82; } service-profile <i>dynamic-profile-name</i>; trace; upto <i>upto-interface-name</i>; } </pre>
Hierarchy Level	<pre> [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i>], [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 ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Options upto and exclude introduced in Junos OS Release 9.1.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify one or more interfaces, or a range of interfaces, that are within a specified group on which the DHCP or DHCPv6 relay agent 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 local server. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>EX Series switches do not support DHCPv6.</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 *Configuring Integrated Routing and Bridging for Bridge Domains*.

- Options**
- exclude**—Exclude an interface or a range of interfaces from the group. This option and the **overrides** option are mutually exclusive.
 - interface-name**—Name of the interface. You can repeat this option multiple times.
 - overrides**—Override the specified default configuration settings for the interface. The **overrides** statement is described separately.
 - upto-interface-name**—Upper end of the range of interfaces; the lower end of the range is the interface-name entry. The interface device name of the **upto-interface-name** must be the same as the device name of the **interface-name**.

The remaining statements are explained separately.

Required Privilege Level

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

- Related Documentation**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [dhcp-relay on page 241](#)
 - *dhcp-relay (EX Series Switches only)*
 - *Understanding the Extended DHCP Relay Agent for EX Series Switches*
 - [Configuring an Extended DHCP Relay Server on EX Series Switches \(CLI Procedure\) on page 75](#)
 - [Grouping Interfaces with Common DHCP Configurations on page 83](#)
 - [Using External AAA Authentication Services with DHCP on page 82](#)

interface-client-limit (DHCP Relay Agent)

Syntax	<code>interface-client-limit <i>number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Set the maximum number of DHCP (or DHCPv6) subscribers or 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. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
Default	No limit
Options	<p><i>number</i>—Maximum number of clients allowed.</p> <p>Range: 1 through 500,000</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**
- [dhcp-relay on page 241](#)
 - [Extended DHCP Relay Agent Overview on page 32](#)
 - [Configuring Group-Specific DHCP Relay Options on page 38](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)

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	<p>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.</p> <p>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.</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"> • <i>Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events</i>

interface-name (DHCP Relay Agent)

Syntax	interface-name;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [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 ...]
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 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 101

layer2-unicast-replies

Syntax	layer2-unicast-replies;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	Override the setting of the broadcast bit in DHCP request packets and instead use the Layer 2 unicast transmission method to transmit DHCP Offer reply packets and DHCP ACK reply packets from the DHCP server to DHCP clients during the discovery process.
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"> • Extended DHCP Relay Agent Overview on page 32 • dhcp-relay on page 241

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 <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], [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 137 • Configuring Detection of DHCP Local Server Client Connectivity on page 98 • Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity on page 139 • Example: Configuring Group Liveness Detection for DHCP Local Server Clients on page 50

- *Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients*

local-server-group (DHCP Relay Agent Option)

Syntax	<code>local-server-group <i>local-server-group</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with)], [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with)], [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 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3. Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Forward DHCP client packets to the specified group of DHCP local servers when you use the DHCP relay selective processing feature. You can configure the forwarding operation globally or for a group of interfaces.</p> <p>The local-server-group option is not supported for DHCPv6 relay agent.</p>
Options	local-server-group —Name of DHCP local server group.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • <i>Using DHCP Option Information to Selectively Process DHCP Client Traffic</i>

mac-address (DHCP Relay Agent)

Syntax	mac-address;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1. 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 client authentication process.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-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 82

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 50 • 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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

minimum-receive-interval

Syntax	<code>minimum-receive-interval <i>milliseconds</i>;</code>
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	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	<p><i>milliseconds</i> — Specify the minimum receive interval value. Range: 1 through 255,000</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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

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 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 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	<code>routing</code> —To view this statement in the configuration. <code>routing-control</code> —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 50• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients


next-hop (Dynamic Access-Internal Routes)

Syntax	<code>next-hop <i>next-hop</i>;</code>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options access route <i>prefix</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i> access route <i>prefix</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-options access route <i>prefix</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at the [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options access route <i>prefix</i>] and [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i> access route <i>prefix</i>] hierarchy levels introduced in Junos OS Release 10.1.</p>
Description	Dynamically configure the next-hop address for an access route. Access routes are typically unnumbered interfaces.
Options	<p><i>next-hop</i>—Either the specific next-hop address you want to assign to the access route or one of the following next-hop address predefined variables.</p> <ul style="list-style-type: none"> For IPv4 access routes, use the variable, \$junos-framed-route-nexthop. The route prefix variable is dynamically replaced with the value in Framed-Route RADIUS attribute [22]. For IPv6 access routes, use the variable, \$junos-framed-route-ipv6-nexthop. The variable is dynamically replaced with the value in Framed-IPv6-Route RADIUS attribute [99].
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"> <i>Configuring Dynamic Access Routes for Subscriber Management</i>


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 50• <i>Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients</i>

no-allow-snooped-clients

Syntax	no-allow-snooped-clients;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.2.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 12.1.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Explicitly disable DHCP snooping support on the router or switch.</p> <p>Use the statement at the [edit ... dhcpv6] hierarchy levels to explicitly disable snooping support on the router or switch for DHCPv6 relay agent.</p>
<div>  <p>NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is <i>enabled</i> by default. In Release 10.1 and later, DHCP snooping is <i>disabled</i> by default.</p> </div>	
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"> • Extended DHCP Relay Agent Overview on page 32 • Overriding the Default DHCP Relay Configuration Settings on page 111 • DHCP Snooping Support on page 19

no-bind-on-request (DHCP Relay Agent)


Syntax	no-bind-on-request;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (<i>stray</i> requests). Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p>
<div>  <p>NOTE: Beginning with Junos OS Release 10.4, automatic binding of stray requests is enabled by default. In Junos OS Release 10.3 and earlier releases, automatic binding of stray requests is disabled by default.</p> </div>	
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**
- [Extended DHCP Relay Agent Overview on page 32](#)
 - [Overriding the Default DHCP Relay Configuration Settings on page 111](#)
 - [Disabling Automatic Binding of Stray DHCP Requests on page 127](#)


option-60 (DHCP Relay Agent)

Syntax	option-60;
Hierarchy Level	[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include]
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 payload of the Option 60 (Vendor Class Identifier) from the client PDU is concatenated with the username during the subscriber authentication or client authentication process.
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"> • Using External AAA Authentication Services with DHCP on page 82

option-82 (DHCP Relay Agent)

Syntax	<code>option-82 <circuit-id> <remote-id>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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 the option 82 that is concatenated with the username during the subscriber authentication or client authentication process. You can specify either, both, or neither the Agent Circuit ID and the 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 neither suboption is supplied, the raw payload of option 82 is concatenated to the username.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: The option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.</p> </div> </div>	
Options	<p>circuit-id—(Optional) The string for the Agent Circuit ID suboption (suboption 1).</p> <p>remote-id—(Optional) The string for the Agent Remote ID suboption (suboption 2).</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"> • Using External AAA Authentication Services with DHCP on page 82

option-number (DHCP Relay Agent Option)

Syntax	<code>option-number <i>option-number</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 relay-option],</p> <p>[edit forwarding-options dhcp-relay group group-name relay-option],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Specify the DHCP option DHCP relay agent uses for selective processing of client traffic. You can configure support globally or for a named group of interfaces. You can also configure support for the extended DHCP relay agent on a per logical system and per routing instance basis.</p> <p>Use the [edit forwarding-options dhcp-relay dhcpv6] hierarchy level to configure the DHCPv6 relay agent support.</p>
Options	<i>option-number</i> —The DHCP or DHCPv6 option in the incoming traffic.
<div>  NOTE: EX Series switches do not support the User Class Options. </div>	
<ul style="list-style-type: none"> • 15 (DHCPv6 only)—Use DHCPv6 option 15 (User Class Option) in packets • 16 (DHCPv6 only)—(MX Series routers and EX Series switches only) Use DHCPv6 option 16 (Vendor Class Option) in packets • 60 (DHCPv4 only)—(MX Series routers and EX Series switches only) Use DHCP option 60 (Vendor Class Identifier) in DHCP packets • 77 (DHCPv4 only)—Use DHCP option 77 (User Class Identifier) in packets 	
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"> • Using DHCP Option Information to Selectively Process DHCP Client Traffic • Configuring an Extended DHCP Relay Server on EX Series Switches (CLI Procedure) on page 75

overrides (DHCP Relay Agent)

Syntax	<pre> overrides { allow-snooped-clients; allow-no-end-options; always-write-giaddr; always-write-option-82; client-discover-match (option60-and-option82 incoming-interface); delay-authentication; delete-binding-on-renegotiation; disable-relay; interface-client-limit <i>number</i>; layer2-unicast-replies; no-allow-snooped-clients; no-bind-on-request; proxy-mode; replace-ip-source-with; send-release-on-delete; trust-option-82; } </pre>
Hierarchy Level	<pre> [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 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [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 ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Support for the delete-binding-on-renegotiation statement introduced in Junos OS Release 13.2 for EX Series switches.</p> <p>Support for the allow-no-end-options statement introduced in Junos OS Release 14.1X53 for EX Series switches.</p>
Description	<p>Override the default configuration settings for the extended DHCP relay agent. Specifying the overrides statement with no subordinate statements removes all DHCP relay agent overrides at that hierarchy level. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</p> <p>The following statements are supported at both the [edit ... dhcp-relay] and [edit ... dhcpv6] hierarchy levels. All other statements are supported at the dhcp-relay hierarchy levels only.</p> <ul style="list-style-type: none"> • allow-snooped-clients

- `interface-client-limit`
- `no-allow-snooped-clients`
- `no-bind-on-request`
- `send-release-on-delete`

The remaining statements are explained separately.

Required Privilege Level	<code>interface</code> —To view this statement in the configuration. <code>interface-control</code> —To add this statement to the configuration.
---------------------------------	---

Related Documentation	<ul style="list-style-type: none">• Extended DHCP Relay Agent Overview on page 32• Overriding the Default DHCP Relay Configuration Settings on page 111• Deleting DHCP Local Server and DHCP Relay Override Settings on page 91• dhcp-relay on page 241
------------------------------	--

password (DHCP Relay Agent)

Syntax	<code>password password-string;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication], [edit forwarding-options dhcp-relay dhcpv6 authentication], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.1. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Configure the password that is sent to the external AAA authentication server for subscriber authentication or client authentication. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>password-string</i> —Authentication password.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-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 82 • Configuring Passwords for Usernames on page 101

preference (Subscriber Management)

Syntax	<code>preference route-distance</code>
Hierarchy Level	<p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options access route <i>prefix</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i> access route <i>prefix</i>],</p> <p>[edit dynamic-profiles <i>profile-name</i> routing-options access route <i>prefix</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Support at [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options access route <i>prefix</i>] and [edit dynamic-profiles <i>profile-name</i> routing-instances \$junos-routing-instance routing-options rib <i>routing-table-name</i> access route <i>prefix</i>] hierarchy levels introduced in Junos OS Release 10.1.</p>
Description	Dynamically configure the distance for an access route.
Options	<p>route-distance—Either the specific distance you want to assign to the access route or either of the following distance variables:</p> <ul style="list-style-type: none"> • \$junos-framed-route-distance—Distance of an IPv4 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-Route attribute [22]. • \$junos-framed-route-ipv6-distance—Distance of an IPv6 access route; the variable is dynamically replaced with the preference value (Subattribute 5) from the RADIUS Framed-IPv6-Route attribute [99].
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"> • <i>Configuring Dynamic Access Routes for Subscriber Management</i>

prefix (DHCP Relay Agent)

Syntax	<code>prefix <i>prefix</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.</p>
Description	<p>Add a prefix to the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or to the DHCPv6 option 18 (Relay Agent Interface-ID) or option 37 (Relay Agent Remote-ID) information in DHCP packets that DHCP relay agent sends to a DHCP server. The prefix can consist of any combination of the hostname, logical system name, and routing instance name.</p>
Options	<p><i>prefix</i>—Any of the following:</p> <ul style="list-style-type: none"> host-name—Prepend the hostname of the router configured with the host-name statement at the [edit system] hierarchy level to the DHCP option information. logical-system-name—Prepend the name of the logical system to the option information. routing-instance-name—Prepend the name of the routing instance to the option information.
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"> Including a Prefix in DHCP Options on page 131 Using DHCP Relay Agent Option 82 Information on page 128 Configuring DHCPv6 Relay Agent Options

proxy-mode

Syntax	proxy-mode;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.5.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	<p>Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.</p> <p>You cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.</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 Relay Proxy Overview on page 35 • Extended DHCP Relay Agent Overview on page 32 • Enabling DHCP Relay Proxy Mode on page 136

relay-agent-interface-id (DHCPv6 Relay Agent)

Syntax	<pre>relay-agent-interface-id { <i>prefix prefix</i>; <i>use-interface-description</i> (logical device); use-option-82; }</pre>
Hierarchy Level	<pre>[edit forwarding-options dhcp-relay <i>dhcpv6</i>], [edit forwarding-options dhcp-relay <i>dhcpv6 group group-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options <i>dhcp-relay dhcpv6 ...</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>dhcpv6 ...</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay <i>dhcpv6 ...</i>]</pre>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.</p> <p>The remaining statements are explained separately.</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-relay on page 241• Extended DHCP Relay Agent Overview on page 32• DHCPv6 Relay Agent Overview on page 37• Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets on page 136

relay-agent-remote-id (DHCPv6 Relay Agent Username)

Syntax	relay-agent-remote-id;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.4.</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 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>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"> • DHCPv6 Relay Agent Overview on page 37 • Creating Unique Usernames for DHCP Clients on page 101

relay-option (DHCP Relay Agent)

Syntax	<pre> relay-option { option-number option-number; default-action { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } equals (ascii <i>ascii-string</i> hexadecimal <i>hexadecimal-string</i>) { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } starts-with (ascii <i>ascii-string</i> hexadecimal <i>hexadecimal-string</i>) { drop; forward-only; local-server-group local-server-group; relay-server-group relay-server-group; } } </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 forwarding-options dhcp-relay ...], [edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay ...], [edit routing-instances routing-instance-name forwarding-options dhcp-relay ...] </pre>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Configure the extended DHCP relay agent selective processing that is based on DHCP options in DHCP client packets and specify the action to perform on client traffic. You can configure support globally or for a named group of interfaces, and for either DHCP or DHCPv6 relay agent.</p> <p>The remaining statements are explained separately.</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"> Using DHCP Option Information to Selectively Process DHCP Client Traffic

relay-option-82

```
Syntax  relay-option-82 {
        circuit-id {
            include-irb-and-l2;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-vlan-id;
        }
        remote-id {
            include-irb-and-l2;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-vlan-id;
        }
    }
```

Hierarchy Level [edit forwarding-options dhcp-relay],
 [edit forwarding-options dhcp-relay **group** *group-name*],
 [edit logical-systems *logical-system-name* forwarding-options **dhcp-relay**],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay **group** *group-name*],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay **group** *group-name*],
 [edit routing-instances *routing-instance-name* forwarding-options **dhcp-relay**],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay **group**
group-name]

Release Information Statement introduced in Junos OS Release 8.3.
 Statement introduced in Junos OS Release 12.3 for EX Series switches.

Description Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

When you configure **relay-option-82** without configuring the **circuit-id** or **remote-id** option, the Agent Circuit ID is added by default.

You can use the **relay-option-82** statement and its subordinate statements at the [edit forwarding-options dhcp-relay] hierarchy level to control insertion of option 82 information globally, or at the [edit forwarding-options dhcp-relay **group** *group-name*] hierarchy level to control insertion of option 82 information for a named group of interfaces.

To restore the default behavior (option 82 information is not inserted into DHCP packets), use the **delete relay-option-82** statement.

The remaining statements are explained separately.

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

- Related Documentation**
- [Using DHCP Relay Agent Option 82 Information on page 128](#)
 - [dhcp-relay on page 241](#)


relay-server-group (DHCP Relay Agent Option)

Syntax	<code>relay-server-group <i>relay-server-group</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay dhcpv6 relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay group <i>group-name</i> relay-option (default-action equals starts-with), [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> relay-option (default-action equals starts-with), [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 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 12.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Relay DHCP client packets to the specified group of DHCP servers when you use the DHCP relay selective processing feature. You can configure the relay operation globally or for a group of interfaces, and for either DHCP or DHCPv6 relay agent.
Options	<i>relay-server-group</i> —Name of DHCP server group.
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">• Using DHCP Option Information to Selectively Process DHCP Client Traffic

replace-ip-source-with

Syntax	replace-ip-source-with giaddr;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</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	Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).
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"> • Extended DHCP Relay Agent Overview on page 32 • Replacing the DHCP Relay Request and Release Packet Source Address on page 113

route-suppression (DHCP Local Server and Relay Agent)

Syntax	route-suppression (access access-internal destination);
Hierarchy Level	<p>[edit forwarding-options dhcp-relay],</p> <p>[edit forwarding-options dhcp-relay dhcpv6],</p> <p>[edit forwarding-options dhcp-relay group group-name],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group group-name],</p> <p>[edit logical-systems <i>logical-system-name</i> ...],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i>...],</p> <p>[edit routing-instances <i>routing-instance-name</i> ...],</p> <p>[edit system services dhcp-local-server],</p> <p>[edit system services dhcp-local-server dhcpv6],</p> <p>[edit system services dhcp-local-server group group-name],</p> <p>[edit system services dhcp-local-server dhcpv6 group group-name]</p>
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	<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"> • Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default on page 79

routing-instance-name (DHCP Relay Agent)

Syntax	routing-instance-name;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify that the routing instance name is concatenated with the username during the subscriber authentication or client authentication process. No routing instance name is concatenated if the configuration is in the default routing instance. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
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"> • Using External AAA Authentication Services with DHCP on page 82 • Creating Unique Usernames for DHCP Clients on page 101

send-release-on-delete (DHCP Relay Agent)

Syntax	send-release-on-delete;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 overrides], [edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.2.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p>
Description	<p>Send a release message to the DHCP (or DHCPv6) server whenever DHCP relay or relay proxy deletes a client. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>M120 and M320 routers do not support DHCPv6.</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"> • Extended DHCP Relay Agent Overview on page 32 • Overriding the Default DHCP Relay Configuration Settings on page 111 • Sending Release Messages When Clients Are Deleted on page 126

server-group

Syntax	<pre>server-group { server-group-name { server-ip-address; } }</pre>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay], [edit forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6], [edit logical-systems <i>logical-system-name</i> 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> forwarding-options dhcp-relay dhcpv6], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3. Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4. Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p>
Options	<p><i>server-group-name</i>—Name of the group of DHCP or DHCPv6 server addresses.</p> <p><i>server-ip-address</i>—IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. You can configure a maximum of five IP addresses in each named server group.</p>
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 241 • Extended DHCP Relay Agent Overview on page 32 • Configuring Server Groups on page 135


service-profile (DHCP Relay Agent)

Syntax	<code>service-profile <i>dynamic-profile-name</i>;</code>
Hierarchy Level	<p>[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 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [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 ...]</p>
Release Information	<p>Statement introduced in Junos OS Release 11.2. Statement introduced in Junos OS Release 12.3R2 for EX Series switches. Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	<p>Specify the default subscriber service (or the default 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 relay agent clients, include the service-profile statement at the [edit forwarding-options dhcp relay] hierarchy level. • To specify the default service for a named group of interfaces, include the service-profile statement at the [edit forwarding-options dhcp relay 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 forwarding-options dhcp relay group <i>group-name</i> interface <i>interface-name</i>] hierarchy level.
Options	<i>dynamic-profile-name</i> —Name of the dynamic profile.
Required Privilege Level	<p>interface—To view this statement in the configuration. interface-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> • dhcp-relay on page 241 • Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces • Grouping Interfaces with Common DHCP Configurations on page 83 • Default Subscriber Service Overview • Configuring a Default Subscriber Service


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 50 • <i>Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients</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. 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>  <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>	
Options	<p><i>milliseconds</i>— Value for the detection time adaptation threshold. Range: 1 through 255,000</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 50 • 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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

trace (DHCP Relay Agent)

Syntax	trace;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay 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> forwarding-options dhcp-relay dhcpv6 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> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> interface <i>interface-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i>]</p>
Release Information	<p>Statement introduced in Junos OS Release 10.4.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels 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 trace operations for a group of interfaces or for a specific interface within a group. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</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">• <i>Tracing Extended DHCP Operations</i>• <i>Tracing Extended DHCP Operations for Specific Interfaces</i>

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 50 • Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients

trust-option-82

Syntax	trust-option-82;
Hierarchy Level	<p>[edit forwarding-options dhcp-relay overrides], [edit forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> overrides], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> interface <i>interface-name</i> overrides]</p>
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 12.3R2 for EX Series switches.</p>
Description	Enable processing of DHCP client packets that have a gateway IP address (giaddr) of 0 (zero) and contain option 82 information. By default, the DHCP relay agent treats such packets as if they originated at an untrusted source, and drops them without further processing.
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">• Trusting Option 82 Information on page 115• Overriding the Default DHCP Relay Configuration Settings on page 111

use-interface-description

Syntax	<code>use-interface-description (logical device);</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit forwarding-options dhcp-relay relay-option-82 (circuit-id remote-id)],</p> <p>[edit forwarding-options dhcp-relay group <i>group-name</i> relay-option-82 (circuit-id remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit logical-systems <i>logical-system-name</i> ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id relay-agent-remote-id)],</p> <p>[edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay ... relay-option-82 (circuit-id remote-id)],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-18],</p> <p>[edit vlans <i>vlan-name</i> forwarding-options dhcp-security dhcpv6-options option-37]</p>
Release Information	<p>Statement introduced in Junos OS Release 9.6.</p> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.3 for EX Series switches.</p> <p>Support at the [edit ... relay-agent-remote-id] and [edit ... remote-id] hierarchy levels introduced in Junos OS Release 14.1.</p> <p>Support at the [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-18] and [edit vlans <i>vlan-name</i> dhcp-security dhcpv6-options option-37] hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.</p>
Description	Use the textual interface description instead of the interface identifier in the DHCP base option 82 Agent Circuit ID (suboption 1) or Agent Remote ID (suboption 2) information, or in the DHCPv6 option 18 (Relay Agent Interface ID) or option 37 (Relay Agent Remote ID) information in DHCP packets that the DHCP relay agent sends to a DHCP server.



NOTE: For integrated routing and bridging (IRB) interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID. You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

The textual description is configured using the **description** statement at the [edit **interfaces interface-name**] hierarchy level. If you specify that the textual description be used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name. When you use the interface description rather than the interface name,

the interface description has to be specified under interface unit ("set interfaces ge-0/0/0 unit 0 description "client"). If you do not do this, then the interface name is used.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used. To include the IRB interface description instead of the Layer 2 interface description, configure the **use-interface-description** and the **no-vlan-interface-name** statements. If no description is configured for the IRB interface, DHCP relay defaults to using the IRB interface name.



NOTE: The **use-interface-description** statement is mutually exclusive with the **use-vlan-id** statement.

If you specify the textual interface description, rather than accepting the default syntax, the identification is for packets returned from the server, and only for instances where that identification would be required by the DHCP relay, such as a stateless pass-through.



NOTE: By default, DHCP relay accepts a maximum of 253 ASCII characters. If the textual interface description exceeds 253 characters, DHCP relay drops the packet, which results in the DHCP client failing to bind.

Options **logical**—Use the textual description that is configured for the logical interface.
device—Use the textual description that is configured for the device interface.

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

Related Documentation

- [Including a Textual Description in DHCP Options on page 133](#)
- [Using DHCP Relay Agent Option 82 Information on page 128](#)
- [Configuring DHCPv6 Relay Agent Options](#)

use-primary (DHCP Relay Agent)

Syntax	<code>use-primary <i>primary-profile-name</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> dynamic-profile <i>profile-name</i>], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p> <p>Statement introduced in Junos OS Release 12.1 for EX Series switches.</p>
Description	<p>Specify the dynamic profile to configure as the primary dynamic profile. The primary dynamic profile 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.</p> <p>Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.</p> <p>EX Series switches do not support DHCPv6.</p>
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**
- [Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces](#)

user-prefix (DHCP Relay Agent)

Syntax	<code>user-prefix <i>user-prefix-string</i>;</code>
Hierarchy Level	<p>[edit forwarding-options dhcp-relay authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit logical-systems <i>logical-system-name</i> routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay dhcpv6 group <i>group-name</i> authentication username-include], [edit routing-instances <i>routing-instance-name</i> forwarding-options dhcp-relay 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> <p>Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.</p>
Description	Specify the user prefix that is concatenated with the username during the subscriber authentication or client authentication process. Use the statement at the [edit ... dhcpv6] hierarchy levels to configure DHCPv6 support.
Options	<i>user-prefix-string</i> —User prefix string.
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"> • Using External AAA Authentication Services with DHCP on page 82

username-include (DHCP Relay Agent)

Syntax `username-include {
 circuit-type;
 client-id;
 delimiter delimiter-character;
 domain-name domain-name-string;
 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 user-prefix-string;
 }`

Hierarchy Level [edit forwarding-options dhcp-relay [authentication](#)],
 [edit forwarding-options dhcp-relay dhcpv6 [authentication](#)],
 [edit forwarding-options dhcp-relay dhcpv6 group *group-name* [authentication](#)],
 [edit forwarding-options dhcp-relay group *group-name* [authentication](#)],
 [edit logical-systems *logical-system-name* forwarding-options dhcp-relay ...],
 [edit logical-systems *logical-system-name* routing-instances *routing-instance-name*
 forwarding-options dhcp-relay ...],
 [edit routing-instances *routing-instance-name* forwarding-options dhcp-relay ...]

Release Information Statement introduced in Junos OS Release 9.1.
 Statement introduced in Junos OS Release 12.3R2 for EX Series switches.
 Support at the [edit ... [dhcpv6](#)] hierarchy levels introduced in Junos OS Release 11.4.

Description 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. Use the statement at the [edit...[dhcpv6](#)] hierarchy levels to configure DHCPv6 support.

The following statements are not supported in the DHCPv6 hierarchy levels:

- `mac-address`
- `option-60`
- `option-82`

The following statements are supported in the DHCPv6 hierarchy levels only:

- `relay-agent-interface-id`
- `relay-agent-remote-id`
- `relay-agent-subscriber-id`

The remaining statements are explained separately.

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 101• Using External AAA Authentication Services with DHCP on page 82

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 address bfd-liveness-detection], [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], [edit protocols ldp oam bfd-liveness-detection], [edit protocols ldp oam fec address bfd-liveness-detection]</p>
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 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	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 50• Example: Configuring Global Liveness Detection for DHCP Relay Agent Clients• Configuring BFD for LDP LSPs

Other Configuration Statements

- [cache-size](#) on page 311
- [cache-timeout-negative](#) on page 312
- [certificates](#) on page 313
- [certification-authority](#) on page 314
- [connection-limit](#) on page 315
- [crl](#) (Encryption Interface) on page 316
- [domain-search](#) on page 316
- [encoding](#) on page 317
- [enrollment-retry](#) on page 317
- [enrollment-url](#) on page 318
- [family](#) (for EX Series switches) on page 319
- [file](#) on page 322
- [ftp](#) on page 323
- [http](#) on page 324
- [https](#) on page 325
- [ldap-url](#) on page 326
- [lease-time](#) on page 327
- [load-key-file](#) on page 328
- [local](#) on page 329
- [local-certificate](#) on page 330
- [maximum-certificates](#) on page 330
- [maximum-hop-count](#) on page 331
- [maximum-lease-time](#) (DHCP) on page 331
- [minimum-wait-time](#) on page 332
- [name-server](#) on page 332
- [no-listen](#) on page 333
- [outbound-ssh](#) on page 334
- [path-length](#) on page 337

- [port \(HTTP/HTTPS\) on page 337](#)
- [port \(SRC Server\) on page 338](#)
- [process-inform on page 338](#)
- [protocol-version on page 339](#)
- [rate-limit on page 340](#)
- [reconfigure on page 341](#)
- [retransmission-attempt on page 342](#)
- [retransmission-interval on page 343](#)
- [server \(DNS and TFTP Service\) on page 343](#)
- [server-address on page 344](#)
- [server-identifier on page 345](#)
- [servers on page 346](#)
- [service-deployment on page 346](#)
- [services \(System Services\) on page 347](#)
- [session \(Time-out\) on page 349](#)
- [sip-server on page 350](#)
- [source-address \(SRC Software\) on page 350](#)
- [source-address-giaddr on page 351](#)
- [ssh on page 352](#)
- [static-binding on page 353](#)
- [system-generated-certificate on page 354](#)
- [telnet on page 354](#)
- [tftp on page 355](#)
- [traceoptions \(DNS and TFTP Packet Forwarding\) on page 356](#)
- [traceoptions on page 358](#)
- [update-server on page 360](#)
- [web-management on page 361](#)
- [wins-server \(System\) on page 362](#)

cache-size

Syntax	cache-size <i>bytes</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the cache size for digital certificates.
Options	bytes —Cache size for digital certificates. Range: 64 through 4,294,967,295 Default: 2 megabytes (MB)



NOTE: We recommend that you limit your cache size to 4 MB.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Digital Certificates for an ES PIC</i>

cache-timeout-negative

Syntax	cache-timeout-negative <i>seconds</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure a negative cache for digital certificates.
Options	seconds —Negative time to cache digital certificates, in seconds. Range: 10 through 4,294,967,295 Default: 20



CAUTION: Configuring a large negative cache value can lead to a denial-of-service attack.

Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Digital Certificates for an ES PIC</i>

certificates

Syntax	<pre> certificates { cache-size bytes; cache-timeout-negative seconds; certification-authority ca-profile-name { ca-name ca-identity; crt file-name; encoding (binary pem); enrollment-url url-name; file certificate-filename; ldap-url url-name; } enrollment-retry attempts; local certificate-name { certificate-key-string; load-key-file URL filename; } maximum-certificates number; path-length certificate-path-length; } </pre>
Hierarchy Level	[edit security]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure the digital certificates for IPsec.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration.</p>
Related Documentation	<ul style="list-style-type: none"> <i>Configuring Digital Certificates for an ES PIC</i>

certification-authority

Syntax	<pre>certification-authority <i>ca-profile-name</i> { ca-name <i>ca-identity</i>; <i>crl</i> <i>file-name</i>; encoding (binary pem); enrollment-url <i>url-name</i>; file <i>certificate-filename</i>; ldap-url <i>url-name</i>; }</pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>(Encryption interface on M Series and T Series routers and EX Series switches only)</p> <p>Configure a certificate authority profile name.</p> <p>The remaining statements are explained separately.</p>
Required Privilege Level	<p>admin—To view this statement in the configuration.</p> <p>admin-control—To add this statement to the configuration</p>
Related Documentation	<ul style="list-style-type: none"><i>Configuring Digital Certificates for an ES PIC</i>

connection-limit

Syntax	<code>connection-limit <i>limit</i>;</code>
Hierarchy Level	<code>[edit system services finger],</code> <code>[edit system services ftp],</code> <code>[edit system services netconf ssh],</code> <code>[edit system services ssh],</code> <code>[edit system services telnet],</code> <code>[edit system services xnm-clear-text],</code> <code>[edit system services xnm-ssl]</code>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Configure the maximum number of connections sessions for each type of system services (finger, ftp, ssh, telnet, xnm-clear-text, or xnm-ssl) per protocol (either IPv6 or IPv4).
Options	<p>limit—(Optional) Maximum number of established connections per protocol (either IPv6 or IPv4).</p> <p>Range: 1 through 250</p> <p>Default: 75</p>



NOTE: The actual number of maximum connections depends on the availability of system resources, and might be fewer than the configured `connection-limit` value if the system resources are limited.

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"> • <i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i> • <i>Configuring DTCP-over-SSH Service for the Flow-Tap Application</i> • <i>Configuring Finger Service for Remote Access to the Router</i> • <i>Configuring FTP Service for Remote Access to the Router or Switch</i> • <i>Configuring SSH Service for Remote Access to the Router or Switch</i> • <i>Configuring Telnet Service for Remote Access to a Router or Switch</i>

crl (Encryption Interface)

Syntax	<code>crl <i>file-name</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the certificate revocation list (CRL). A CRL is a time-stamped list identifying revoked certificates, which is signed by a CA and made available to the participating IPsec peers on a regular periodic basis.
Options	<i>file-name</i> —Specify the file from which to read the CRL.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Digital Certificates for an ES PIC</i>

domain-search

Syntax	<code>domain-search [<i>domain-list</i>];</code>
Hierarchy Level	[edit system], [edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure a list of domains to be searched.
Options	<i>domain-list</i> —A list of domain names to search. The list can contain up to six domain names, with a total of up to 256 characters.
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">• <i>Reaching a Domain Name System Server</i>• <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i>• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

encoding

Syntax	encoding (binary pem);
Hierarchy Level	[edit security ike policy <i>ike-peer-address</i>], [edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file format used for the local-certificate and local-key-pair statements.
Options	binary —Binary file format. pem —Privacy-enhanced mail (PEM), an ASCII base 64 encoded format. Default: binary
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Digital Certificates for an ES PIC</i> • <i>Configuring an IKE Policy for Digital Certificates for an ES PIC</i>

enrollment-retry

Syntax	enrollment-retry <i>attempts</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify how many times a router or switch can resend a digital certificate request.
Options	attempts —Number of enrollment retries. Range: 0 through 100 Default: 0
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Digital Certificates for an ES PIC</i>

enrollment-url

Syntax	<code>enrollment-url <i>url-name</i>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify where your router or switch sends Simple Certificate Enrollment Protocol-based (SCEP-based) certificate enrollment requests (certificate authority URL).
Options	<i>url-name</i> —Certificate authority URL.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Digital Certificates for an ES PIC</i>

family (for EX Series switches)

Syntax	family ccc on page 319 family ethernet-switching on page 319 family inet on page 319 family inet6 on page 320 family iso on page 320 family mpls on page 320
family ccc	family ccc;
family ethernet-switching	<pre> family ethernet-switching { filter [input output] <i>filter-name</i>; native-vlan-id <i>vlan-id</i>; port-mode <i>mode</i>; vlan (802.1Q Tagging) { members [(all <i>names</i> <i>vlan-ids</i>)]; } }</pre>
family inet	<pre> family inet { address <i>address</i> { arp <i>ip-address</i> (mac multicast-mac) <i>mac-address</i> <publish>; broadcast; preferred; primary; vrrp-group <i>group-id</i> { advertise-interval <i>milliseconds</i>; preempt no-preempt { hold-time <i>seconds</i>; } priority <i>number</i>; virtual-address [<i>addresses</i>]; virtual-link-local-address <i>ip-address</i>; } } dhcp { client-identifier (ascii <i>ascii</i> hexadecimal <i>hexadecimal</i>); lease-time (<i>seconds</i> infinite); retransmission-attempt <i>number</i>; retransmission-interval <i>seconds</i>; server-address <i>ip-address</i>; update-server; vendor-id <i>vendor-id</i>; } filter { input <i>filter-name</i>; output <i>filter-name</i>; } mtu <i>bytes</i>; no-redirects; no-neighbor-learn; primary; rpf-check; }</pre>

	<pre> targeted-broadcast; } family inet6 { address address { eui-64; nd6-stale-time seconds; ndp ip-address (mac multicast-mac) mac-address <publish>; preferred; primary; vrrp-inet6-group group-id { inet6-advertise-interval milliseconds; preempt preempt { hold-time seconds; } priority number; virtual-inet6-address [addresses]; virtual-link-local-address ipv6-address; } } (dad-disable no-dad-disable); filter { input filter-name; output filter-name; } mtu bytes; no-neighbor-learn rpf-check; } family iso { address interface-address; mtu bytes; } family mpls { mtu bytes; }</pre>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i>], [edit interfaces interface-range <i>name</i> unit <i>logical-unit-number</i>]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches, including options ethernet-switching , inet , and iso . Option inet6 introduced in Junos OS Release 9.3 for EX Series switches. Options ccc and mpls introduced in Junos OS Release 9.5 for EX Series switches.
Description	Configure protocol family information for the logical interface on the switch. You must configure a logical interface to be able to use the physical device.

Default Interfaces on EX2200, EX3200, EX3300, EX4200, and EX4500 switches are set to **family ethernet-switching** by the default factory configuration. Before you can change the family setting for an interface to another family type, you must delete this default setting or any user-configured family setting. EX6200 and EX8200 switch interfaces do not have a default family setting.

Options See [Table 18 on page 321](#) for protocol families available on the switch interfaces. Different protocol families support different subsets of the interface types on the switch. Interface types on the switch are:

- Aggregated Ethernet (**ae**)
- Gigabit Ethernet (**ge**)
- Interface-range configuration (**interface-range**)
- Loopback (**lo0**)
- Management Ethernet (**me0**)
- Routed VLAN interface (RVI) (**vlan**)
- Virtual management Ethernet (**vme**)
- 10-Gigabit Ethernet (**xe**)

If you are using an interface range, the supported protocol families are the ones supported by the interface types that compose the range.

Not all interface types support all **family** substatements. Check your switch CLI for supported substatements for a particular protocol family configuration.

Table 18: Protocol Families and Supported Interface Types

Family	Description	Supported Interface Types						
		ae	ge	lo0	me0	vlan	vme	xe
ccc	Circuit cross-connect protocol family	✓*	✓					✓
ethernet-switching	Ethernet switching protocol family	✓	✓		✓			✓
inet	IPv4 protocol family	✓	✓	✓	✓	✓	✓	✓
inet6	IPv6 protocol family	✓	✓	✓	✓	✓	✓	✓
iso	Junos OS protocol family for IS-IS traffic	✓	✓	✓	✓	✓	✓	✓
mpls	MPLS protocol family	✓	✓	✓	✓		✓	✓

*Supported on EX8200 switches only

The remaining statements are explained separately.

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">• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>• <i>Example: Configuring MPLS on EX8200 and EX4500 Switches</i>• <i>Configuring Gigabit Ethernet Interfaces (CLI Procedure)</i>• <i>Configuring Aggregated Ethernet Links (CLI Procedure)</i>• <i>Configuring Routed VLAN Interfaces (CLI Procedure)</i>

file

Syntax	<code>file certificate-<i>filename</i>;</code>
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Specify the file from which to read the digital certificate.
Options	<i>certificate-filename</i> —File from which to read the digital certificate.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring Digital Certificates for an ES PIC</i>

ftp

Syntax	<pre>ftp { connection-limit limit; rate-limit limit; }</pre>
Hierarchy Level	[edit system services]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Allow FTP requests from remote systems to the local router or switch.
Options	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">• <i>Configuring FTP Service for Remote Access to the Router or Switch</i>

http

Syntax	<pre>http { interfaces [<i>interface-names</i>]; port <i>port</i>; }</pre>
Hierarchy Level	[edit system services web-management]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port and interfaces for HTTP service, which is unencrypted.
Options	<p>interfaces [<i>interface-names</i>]—Name of one or more interfaces on which to allow the HTTP service. By default, HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.</p> <p>The remaining statement is explained separately.</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">• <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i>• <i>J-Web Interface User Guide</i>• https on page 325• port on page 337• web-management on page 361

https

Syntax	<pre>https { interfaces [<i>interface-names</i>]; local-certificate <i>name</i>; port <i>port</i>; }</pre>
Hierarchy Level	[edit system services web-management]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure the secure version of HTTP (HTTPS) service, which is encrypted.
Options	<p>interfaces [<i>interface-names</i>]—Name of one or more interfaces on which to allow the HTTPS service. By default, HTTPS access is allowed through any ingress interface, but HTTP access is allowed through built-in Fast Ethernet or Gigabit Ethernet interfaces only.</p> <p>local-certificate <i>name</i>—Name of the X.509 certificate for a Secure Sockets Layer (SSL) connection. An SSL connection is configured at the [edit security certificates local] hierarchy.</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"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 324 • port on page 337 • web-management on page 361


ldap-url

Syntax	<ldap-url <i>url-name</i> >;
Hierarchy Level	[edit security certificates certification-authority <i>ca-profile-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series,
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) (Optional) Specify the Lightweight Directory Access Protocol (LDAP) URL for digital certificates.
Options	<i>url-name</i> —Name of the LDAP URL.
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">• <i>Configuring Digital Certificates for an ES PIC</i>


lease-time

Syntax	lease-time (<i>seconds</i> infinite);
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Request a specific lease time for the IP address. The lease time is the length of time in seconds that a client holds the lease for an IP address assigned by a DHCP server.
Default	If no lease time is requested by client, then the server sends the lease time. The default lease time on a JUNOS OS DHCP server is one day.
Options	seconds —Request a lease time of a specific duration. Range: 60 through 2147483647 seconds infinite —Request that the lease never expire.
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"> • Configuring a DHCP Client (CLI Procedure) on page 71 • <i>Example: Configuring the Device as a DHCP Client</i> • <i>interfaces</i> • <i>unit</i> • family on page 319

load-key-file

Syntax	load-key-file <i>URL filename</i> ;
Hierarchy Level	[edit system root-authentication], [edit system login user <i>username</i> authentication]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	<div> NOTE: ECDSA is not supported on the QFabric system.</div> <p>Load RSA (SSH version 1 and SSH version 2) and DSA or ECDSA (SSH version 2) public keys from a previously-generated named file at a specified URL location or local path. The file contains one or more SSH keys that are copied into the configuration when the command is issued.</p>
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring the Root Password</i>• <i>Configuring the Root Password</i>• <i>Configuring Junos OS User Accounts</i>• <i>Configuring Junos OS User Accounts</i>

local

Syntax	<pre>local <i>certificate-name</i> { <i>certificate-key-string</i>; load-key-file <i>URL filename</i>; }</pre>
Hierarchy Level	[edit security certificates]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	Import a paired X.509 private key and authentication certificate, to enable Junos XML protocol client applications to establish Secure Sockets Layer (SSL) connections to the router or switch.
<div style="display: flex; align-items: center;">  <div> <p>NOTE: For FIPS mode, the digital security certificates must be compliant with the National Institute of Standards and Technology (NIST) SP 800-131A standard.</p> </div> </div>	
Options	<p><i>certificate-name</i><i>certificate-key-string</i>—String of alphanumeric characters that constitute the private key and certificate.</p> <p><i>certificate-name</i>—Name that uniquely identifies the certificate.</p> <p><i>load-key-file URL filename</i>—File that contains the private key and certificate. It can be one of two types of values:</p> <ul style="list-style-type: none"> • Pathname of a file on the local disk (assuming you have already used another method to copy the certificate file to the router's or switch's local disk) • URL to the certificate file location (for instance, on the computer where the Junos XML protocol client application runs)
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"> • <i>Importing SSL Certificates for Junos XML Protocol Support</i>

local-certificate

Syntax	local-certificate;
Hierarchy Level	[edit system services service-deployment], [edit system services web-management https], [edit system services xnm-ssl]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Import or reference an SSL certificate.
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i>• <i>Generating SSL Certificates to Be Used for Secure Web Access</i>• <i>Importing SSL Certificates for Junos XML Protocol Support</i>

maximum-certificates

Syntax	maximum-certificates <i>number</i> ;
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the maximum number of peer digital certificates to be cached.
Options	<i>number</i> —Maximum number of peer digital certificates to be cached. Range: 64 through 4,294,967,295 peer certificates Default: 1024 peer certificates
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">• <i>Configuring Digital Certificates for an ES PIC</i>

maximum-hop-count

Syntax	<code>maximum-hop-count <i>number</i>;</code>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootpinterface (<i>interface-name</i> <i>interface-group</i>)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Specify the maximum number of hops allowed.
Options	<i>number</i> —Maximum number of hops. Default: 4 hops
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"> • <i>Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents</i>

maximum-lease-time (DHCP)

Syntax	<code>maximum-lease-time <i>seconds</i>;</code>
Hierarchy Level	[edit system services dhcp],
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For J Series Services Routers and EX Series switches only. Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server. An exception is that the dynamic BOOTP lease length can exceed the maximum lease length specified.
Options	<i>seconds</i> —The maximum number of seconds the lease can be held.
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"> • <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i> • <i>default-lease-time</i>

minimum-wait-time

Syntax	<code>minimum-wait-time seconds;</code>
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	When the router is configured to act as a BOOTP server, the value set here defines how long the router should wait before forwarding requests.
Options	Range: 0 to 30,000 seconds. Default: 0 seconds
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">• <i>Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents</i>

name-server

Syntax	<code>name-server { <i>address</i>; }</code>
Hierarchy Level	[edit system], [edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure one or more Domain Name System (DNS) name servers.
Options	<i>address</i> —Address of the name server. To configure multiple name servers, include a maximum of three <i>address</i> options.
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">• <i>Reaching a Domain Name System Server</i>• <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i>• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

no-listen

Syntax	no-listen;
Hierarchy Level	[edit forwarding-options helpers bootp interface (<i>interface-name</i> <i>interface-group</i>)], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.3 for QFX Series switches.
Description	Disable recognition of DNS requests or stop packets from being forwarded on a logical interface, a group of logical interfaces, a router, or a switch.
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"> • <i>Configuring DNS and TFTP Packet Forwarding</i> • <i>Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents</i>

outbound-ssh

Syntax	<pre> [edit system services] outbound-ssh { client <i>client-id</i> { address { port <i>port-number</i>; retry <i>number</i>; timeout <i>seconds</i>; } device-id <i>device-id</i>; keep-alive { retry <i>number</i>; timeout <i>seconds</i>; } reconnect-strategy (in-order sticky); secret <i>password</i>; services netconf; } traceoptions { file filename <files <i>number</i>> <match <i>regex</i>> <size <i>size</i>> <world-readable no-world-readable>; flag <i>flag</i>; no-remote-trace; } } </pre>
Hierarchy Level	[edit system services]
Release Information	<p>Statement introduced in Junos OS Release 8.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure a router or switch running the Junos OS behind a firewall to communicate with client management applications on the other side of the firewall.
Default	To configure transmission of the router's or switch's device ID to the application, include the device-id statement at the [edit system services] hierarchy level.
Options	<p>client-id—Identifies the outbound-ssh configuration stanza on the router or switch. Each outbound-ssh stanza represents a single outbound SSH connection. This attribute is not sent to the client.</p> <p>device-id—Identifies the router or switch to the client during the initiation sequence.</p> <p>keep-alive—(Optional) When configured, specifies that the router or switch send keepalive messages to the management server. To configure the keepalive message, you must set both the timeout and retry attributes.</p> <p>reconnect-strategy—(Optional) Specify the method the router or switch uses to reestablish a disconnected outbound SSH connection. Two methods are available:</p>

- **in-order**—Specify that the router or switch first attempt to establish an outbound SSH session based on the management server address list. The router or switch attempts to establish a session with the first server on the list. If this connection is not available, the router or switch attempts to establish a session with the next server, and so on down the list until a connection is established.
- **sticky**—Specify that the router or switch first attempt to reconnect to the management server that it was last connected to. If the connection is unavailable, it attempts to establish a connection with the next client on the list and so forth until a connection is made.

retry—Number of keepalive messages the router or switch sends without receiving a response from the client before the current SSH connection is disconnected. The default is three messages.

secret—(Optional) Router's or switch's public SSH host key. If added to the **outbound-ssh** statement, during the initialization of the outbound SSH service, the router or switch passes its public key to the management server. This is the recommended method of maintaining a current copy of the router's or switch's public key.

timeout—Length of time that the Junos server waits for data before sending a keep alive signal. The default is 15 seconds.

When reconnecting to a client, the router or switch attempts to reconnect to the client based on the **retry** and **timeout** values for each client listed.

address—Hostname or the IPv4 address of the NSM application server. You can list multiple clients by adding each client's IP address or hostname along with the following connection parameters:

- **port**—Outbound SSH port for the client. The default is port 22.
- **retry**—Number of times the router or switch attempts to establish an outbound SSH connection before giving up. The default is three tries.
- **timeout**—Length of time that the router or switch attempts to establish an outbound SSH connection before giving up. The default is fifteen seconds.

filename—(Optional) By default, the filename of the log file used to record the trace options is the name of the traced process (for example, **mib2d** or **snmpd**). Use this option to override the default value.

files—(Optional) Maximum number of trace files generated. By default, the maximum number of trace files is 10. Use this option to override the default value.

When a trace file reaches its maximum size, the system archives the file and starts a new file. The system archives trace files by appending a number to the filename in sequential order from 1 to the maximum value (specified by the default value or the options value set here). Once the maximum value is reached, the numbering sequence is restarted at 1, overwriting the older file.

size—(Optional) Maximum size of the trace file in kilobytes (KB). Once the maximum file size is reached, the system archives the file. The default value is 1000 KB. Use this option to override the default value.

match—(Optional) When used, the system only adds lines to the trace file that match the regular expression specified. For example, if the match value is set to **=error**, the system only records lines to the trace file that include the string **error**.

services—Services available for the session. Currently, NETCONF is the only service available.

world-readable | no-world-readable—(Optional) Whether the files are accessible by the originator of the trace operation only or by any user. By default, log files are only accessible by the user that started the trace operation (**no-world-readable**).

all | configuration | connectivity—(Optional) Type of tracing operation to perform.

all—Log all events.

configuration—Log all events pertaining to the configuration of the router or switch.

connectivity—Log all events pertaining to the establishment of a connection between the client server and the router or switch.

no-remote-trace—(Optional) Disable remote tracing.

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">• <i>Configuring Outbound SSH Service</i>• <i>System Management Configuration Statements</i>
------------------------------	---

path-length

Syntax	<code>path-length <i>certificate-path-length</i>;</code>
Hierarchy Level	[edit security certificates]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Configure the digital certificate path length.
Options	<i>certificate-path-length</i> —Digital certificate path length. Range: 2 through 15 certificates Default: 15 certificates
Required Privilege Level	admin—To view this statement in the configuration. admin-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Configuring Digital Certificates for an ES PIC</i>

port (HTTP/HTTPS)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit system services web-management]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port on which the HTTP or HTTPS service is connected.
Options	<i>port-number</i> —The TCP port number on which the specified service listens.
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"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 324 • https on page 325 • web-management on page 361

port (SRC Server)

Syntax	<code>port <i>port-number</i>;</code>
Hierarchy Level	[edit system services service-deployment servers <i>server-address</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure the port number on which to contact the SRC server.
Options	<i>port-number</i> —(Optional) The TCP port number for the SRC server. Default: 3333
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">• <i>Configuring the Junos OS to Work with SRC Software</i>

process-inform

Syntax	<code>process-inform { pool <i>pool-name</i> network <i>address-range</i> }</code>
Hierarchy Level	[edit system services dhcp-local-server overrides]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	For extended Dynamic Host Configuration Protocol (DHCP) servers, enable the processing of DHCP information request messages sent from the client to the server to request DHCP options. The messages are also passed to the configured server list.
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">• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

protocol-version

Syntax	<code>protocol-version <i>version</i>;</code>
Hierarchy Level	[edit system services ssh]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the secure shell (SSH) protocol version.
Default	v2 —SSH protocol version 2 is the default, introduced in Junos OS Release 11.4.
Options	<i>version</i> —SSH protocol version: v1 , v2 , or both.
Required Privilege Level	admin —To view this statement in the configuration. admin-control —To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none">• <i>Configuring SSH Service for Remote Access to the Router or Switch</i>

rate-limit

Syntax	<code>rate-limit <i>limit</i>;</code>
Hierarchy Level	[edit system services finger], [edit system services ftp], [edit system services netconf ssh], [edit system services ssh], [edit system services telnet], [edit system services xnm-clear-text], [edit system services xnm-ssl]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Configure the maximum number of connections attempts per protocol (either IPv6 or IPv4) on an access service.
Default	150 connections
Options	rate-limit <i>limit</i> —(Optional) Maximum number of connection attempts allowed per minute, per IP protocol (either IPv4 or IPv6). Range: 1 through 250 Default: 150
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"><i>Configuring clear-text or SSL Service for Junos XML Protocol Client Applications</i>

reconfigure

Syntax	<pre>reconfigure { attempts <i>attempts</i>; clear-on-abort; timeout interval; token token; }</pre>
Hierarchy Level	[edit system services dhcp-local-server]
Release Information	Statement introduced in Junos OS Release 12.1 for EX Series switches.
Description	For extended Dynamic Host Configuration Protocol (DHCP) servers, enable dynamic reconfiguration triggered by the server of all DHCP clients.
Options	<p>attempts—Number of attempts made to reconfigure all DHCP clients.</p> <p>clear-on-abort—Delete all DHCP clients when reconfiguration fails; that is, when the maximum number of retry attempts have been made without success.</p> <p>timeout interval—Initial value (in seconds) between attempts to reconfigure all DHCP clients. 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.</p> <p>token—Configure a plain-text token for all DHCP clients. 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.</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"> <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

retransmission-attempt

Syntax	<code>retransmission-attempt <i>number</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the number of times the device retransmits a Dynamic Host Control Protocol (DHCP) packet if a DHCP server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.
Options	<i>number</i> —Number of retransmit attempts.. Range: 0 through 6 Default: 4
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">• Configuring a DHCP Client (CLI Procedure) on page 71• <i>Example: Configuring the Device as a DHCP Client</i>• <i>interfaces</i>• <i>unit</i>• family on page 319

retransmission-interval

Syntax	<code>retransmission-interval <i>seconds</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.
Options	<i>seconds</i> —Number of seconds between successive retransmissions. Range: 4 through 64 seconds Default: 4 seconds
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"> • Configuring a DHCP Client (CLI Procedure) on page 71

server (DNS and TFTP Service)

Syntax	<code>server <i>address</i> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>;</code>
Hierarchy Level	[edit forwarding-options helpers domain], [edit forwarding-options helpers domain interface <i>interface-name</i>], [edit forwarding-options helpers tftp], [edit forwarding-options helpers tftp interface <i>interface-name</i>]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Specify the DNS or TFTP server for forwarding DNS or TFTP requests. Only one server can be specified for each interface.
Options	<i>address</i> —Address of the server. logical-system <i>logical-system-name</i> —(Optional) Logical system of the server. routing-instance [<i>routing-instance-names</i>] —(Optional) Set the routing instance name or names that belong to the DNS server or TFTP server.
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"> • Configuring DNS and TFTP Packet Forwarding

server-address

Syntax	<code>server-address <i>ip-address</i>;</code>
Hierarchy Level	[edit interfaces <i>interface-name</i> unit <i>logical-unit-number</i> family inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Specify the address of the DHCP server that the client should accept DHCP offers from. If this option is included in the DHCP configuration, the client accepts offers only from this server and ignores all other offers.
Default	The client accepts the first offer it receives from any DHCP server.
Options	<i>ip-address</i> —DHCP server address.
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">• Configuring a DHCP Client (CLI Procedure) on page 71• <i>Example: Configuring the Device as a DHCP Client</i>• <i>interfaces</i>• <i>unit</i>• family on page 319

server-identifier

Syntax	<code>server-identifier <i>address</i>;</code>
Hierarchy Level	[edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	<p>For J Series Services Routers and EX Series switches only. Configure a server identifier. The identifier can be used to identify a DHCP server in a DHCP message. It can also be used as a destination address from clients to servers (for example, when the boot file is set, but not the boot server).</p> <p>Servers include the server identifier in DHCPOFFER messages so that clients can distinguish between multiple lease offers. Clients include the server identifier in DHCPREQUEST messages to select a lease and indicate which offer is accepted from multiple lease offers. Also, clients can use the server identifier to send unicast request messages to specific DHCP servers to renew a current lease.</p> <p>This address must be a manually assigned, static IP address. The server cannot send a request and receive an IP address from itself or another DHCP server.</p>
Default	If no server identifier is set, the DHCP server sets the server identifier based on the primary interface address used by the server to receive a client request. For example, if the client sends a DHCP request and the server receives it on fe-0/0/0 and the primary interface address is 1.1.1.1 , then the server identifier is set to 1.1.1.1 .
Options	address —IPv4 address of the server. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).
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"> <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i>

servers

Syntax	<code>servers server-address { port port-number; }</code>
Hierarchy Level	[edit system services service-deployment]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Configure an IPv4 address for the Session and Resource Control (SRC) server.
Options	server-address —The TCP port number. Default: 3333 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">• <i>Configuring the Junos OS to Work with SRC Software</i>

service-deployment

Syntax	<code>service-deployment { servers server-address { port port-number; } source-address source-address; }</code>
Hierarchy Level	[edit system services]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable Junos OS to work with the Session and Resource Control (SRC) software. 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">• <i>Configuring the Junos OS to Work with SRC Software</i>

services (System Services)

```
Syntax  services {
    dhcp { \* DHCP not supported on a DCF
        dhcp_services;
    }
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    ftp {
        connection-limit limit;
        rate-limit limit;
    }
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        connection-limit limit;
        protocol-version [v1 v2];
        rate-limit limit;
        root-login (allow | deny | deny-password);
    }
    telnet {
        connection-limit limit;
        rate-limit limit;
    }
    web-management {
        http {
            interfaces [ names ];
            port port;
        }
        https {
            interfaces [ names ];
            local-certificate name;
            port port;
        }
        session {
            idle-timeout [ minutes ];
            session-limit [ limit ];
        }
    }
    xnm-clear-text {
        connection-limit limit;
        rate-limit limit;
    }
    xnm-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
        ssl-renegotiation;
    }
}
```

```
}  
}
```

Hierarchy Level [edit system]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.

Description Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, finger, rlogin, SSH, telnet, Web management, Junos XML protocol clear-text, Junos XML protocol SSL, and network utilities or enable Junos OS to work with the Session and Resource Control (SRC) software.

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 clear-text or SSL Service for Junos XML Protocol Client Applications*
- *Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers*
- *Configuring the Junos OS to Work with SRC Software*

session (Time-out)

Syntax	<pre>session { idle-timeout <i>minutes</i>; session-limit <i>session-limit</i>; }</pre>
Hierarchy Level	[edit system services web-management]
Release Information	<p>Statement introduced in Junos OS Release 8.3.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure limits for the number of minutes a session can be idle before it times out, and configure the number of simultaneous J-Web user login sessions.
Options	<p>idle-timeout <i>minutes</i>—Configure the number of minutes a session can be idle before it times out.</p> <p>Range: 1 through 1440</p> <p>Default: 1440</p> <p>session-limit <i>session-limit</i>—Configure the maximum number of simultaneous J-Web user login sessions.</p> <p>Range: 1 through 1024</p> <p>Default: Unlimited</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"> • <i>J-Web Interface User Guide</i>

sip-server

Syntax	<code>sip-server [address name];</code>
Hierarchy Level	[edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	Configure Session Initiation Protocol (SIP) server addresses or names for DHCP servers.
Options	<p>address—IPv4 address of the SIP server. To configure multiple SIP servers, include multiple address options. This address must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).</p> <p>name—Fully qualified domain name of the SIP server. To configure multiple SIP servers, include multiple name options. This domain name must be accessible by all clients served within a specified range of addresses (based on an address pool or static binding).</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">• Configuring a DHCP SIP Server (CLI Procedure) on page 71• Configuring a DHCP Server on Switches (CLI Procedure)

source-address (SRC Software)

Syntax	<code>source-address source-address;</code>
Hierarchy Level	[edit system services service-deployment]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	Enable Junos OS to work with the Session and Resource Control (SRC) software.
Options	source-address — Local IPv4 address to be used as source address for traffic to the SRC server. The source address restricts traffic within the out-of-band network.
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 Junos OS to Work with SRC Software

source-address-giaddr

Syntax	source-address-giaddr;
Hierarchy Level	[edit forwarding-options helpers bootp], [edit forwarding-options helpers bootp interface <i>interface-name</i>]
Release Information	Statement introduced in Junos OS Release 10.1 for EX Series switches.
Description	<p>Configure the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent.</p> <p>When this statement is entered in the [edit forwarding-options helpers bootp] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting all interfaces on the switch.</p> <p>When this statement is entered in the [edit forwarding-options helpers bootp interface <i>interface-name</i>] hierarchy, the gateway IP address is configured as the source IP address of the switch for relayed DHCP packets exiting the specified interface of the switch.</p> <p>In Junos OS Release 10.1 for EX Series switches and later releases, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is used as the source IP address for relayed DHCP packets by default.</p> <p>In Junos OS Releases 9.6 and 10.0 for EX Series switches, the gateway IP address of the switch is always used as the source IP address for relayed DHCP packets when the switch is used as the DHCP relay agent.</p> <p>In Junos OS Releases 9.3 through 9.5 for EX Series switches, the IP address of the interface that the DHCP packet exits on the switch acting as a DHCP relay agent is always used as the source IP address for relayed DHCP packets.</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"> <i>DHCP/BOOTP Relay for Switches Overview</i>

ssh

Syntax `ssh {
 ciphers [cipher-1 cipher-2 cipher-3 ...];
 client-alive-count-max seconds;
 client-alive-interval seconds;
 connection-limit limit;
 hostkey-algorithm <algorithm|no-algorithm>;
 key-exchange <algorithm>;
 macs <algorithm>;
 max-sessions-per-connection <number>;
 no-passwords;
 no-tcp-forwarding;
 protocol-version [v1 v2];
 rate-limit limit;
 root-login (allow | deny | deny-password);
 }`

Hierarchy Level [edit system services]

Release Information Statement introduced before Junos OS Release 7.4.
Statement introduced in Junos OS Release 9.0 for EX Series switches.
Statement introduced in Junos OS Release 11.1 for the QFX Series.
client-alive-interval and **client-alive-max-count** statements introduced in Junos OS Release 12.2.
no-passwords statement introduced in Junos OS Release 13.3.
Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.

Description Allow SSH requests from remote systems to the local router or switch.

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 SSH Service for Remote Access to the Router or Switch*

static-binding

Syntax	<pre>static-binding <i>mac-address</i> { client-identifier (ascii <i>client-id</i> hexadecimal <i>client-id</i>); fixed-address { <i>address</i>; } host-name <i>client-hostname</i>; }</pre>
Hierarchy Level	<pre>[edit system services dhcp], [edit system services dhcp]</pre>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>For J Series Services routers and EX Series switches only. Set static bindings for DHCP clients. A static binding is a mapping between a fixed IP address and the client's MAC address or client identifier.</p>
Options	<p><i>mac-address</i>—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.</p> <p><i>fixed-address address</i>—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.</p> <p><i>host-name client-hostname</i>—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the <i>domain-name</i> statement.</p> <p><i>client-identifier (ascii client-id hexadecimal client-id)</i>—Used by the DHCP server to index the database of address bindings. The client identifier is an ASCII string or hexadecimal number and can include a type-value pair as specified in RFC 1700, <i>Assigned Numbers</i>. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.</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"> • <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i> • <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

system-generated-certificate

Syntax	system-generated-certificate;
Hierarchy Level	[edit system services web-management https]
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Configure the automatically generated self-signed certificate for enabling HTTPS services..
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 HTTPS and XNM-SSL Services on Switches Using Self-Signed Certificates (CLI Procedure) on page 76

telnet

Syntax	telnet { connection-limit limit ; rate-limit limit ; }
Hierarchy Level	[edit system services]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 11.1 for the QFX Series. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Provide Telnet connections from remote systems to the local router or switch. 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">• <i>Configuring Telnet Service for Remote Access to a Router or Switch</i>

tftp

Syntax	<pre> tftp { description <i>text-description</i>; interface <i>interface-name</i> { broadcast; description <i>text-description</i>; no-listen; server address <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>; } server address <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>; } </pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Enable TFTP request packet forwarding.</p> <p>The remaining statements are explained separately.</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"> • <i>Configuring DNS and TFTP Packet Forwarding</i>

traceoptions (DNS and TFTP Packet Forwarding)

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <match <i>regular-expression</i>> <size <i>bytes</i>> <world-readable no-world-readable>; flag <i>flag</i>; level <i>level</i>; <no-remote-trace>; } </pre>
Hierarchy Level	[edit forwarding-options helpers]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement standardized and match option introduced in Junos OS Release 8.0.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	Configure tracing operations for BOOTP, DNS and TFTP packet forwarding.
Default	If you do not include this statement, no tracing operations are performed.
Options	<p>file <i>filename</i>—Name of the file to receive the output of the tracing operation. Enclose the name in quotation marks (" "). All files are placed in a file named fud in the directory /var/log. If you include the file statement, you must specify a filename.</p> <p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file named trace-file reaches its maximum size, it is renamed trace-file.0, then trace-file.1, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you also must specify a maximum file size with the size option and a filename.</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. You can include the following flags:</p> <ul style="list-style-type: none"> • address—Trace address management events • all—Trace all events • bootp—Trace BOOTP or DHCP services events • config—Trace configuration events • domain—Trace DNS service events • ifdb—Trace interface database operations • io—Trace I/O operations • main—Trace main loop events • port—Trace arbitrary protocol events

- **rtsock**—Trace routing socket operations
- **tftp**—Trace TFTP service events
- **trace**—Trace tracing operations
- **ui**—Trace user interface operations
- **util**—Trace miscellaneous utility operations

match *regular-expression*—(Optional) Refine the output to include lines that contain the regular expression.

no-remote-trace—(Optional) Disable remote tracing globally or for a specific tracing operation.

no-world-readable—(Optional) Restrict file access to the owner.

size *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). When a trace file named **trace-file** reaches this size, it is renamed **trace-file.0**. When the **trace-file** file again reaches its maximum size, **trace-file.0** is renamed **trace-file.1** and **trace-file** is renamed **trace-file.0**. This renaming scheme continues until the maximum number of trace files is reached. Then the oldest trace file is overwritten.

If you specify a maximum file size, you also must specify a maximum number of trace files with the **files** option and filename.

Syntax: *xk* to specify KB, *xm* to specify MB, or *xg* to specify GB


Range: 0 bytes through 4,294,967,295 KB

Default: 128 KB

world-readable—(Optional) Enable unrestricted file access.

Required Privilege	interface—To view this statement in the configuration.
Level	interface-control—To add this statement to the configuration.
Related Documentation	<ul style="list-style-type: none"> • <i>Tracing BOOTP, DNS, and TFTP Forwarding Operations</i>

traceoptions

Syntax	<pre> traceoptions { file <i>filename</i> <files <i>number</i>> <size <i>size</i>>; flag all; flag certificates; flag database; flag general; flag ike; flag parse; flag policy-manager; flag routing-socket; flag timer; level no-remote-trace } </pre>
Hierarchy Level	<p>[edit security], [edit services ipsec-vpn]</p> <p>Trace options can be configured at either the [edit security] or the [edit services ipsec-vpn] hierarchy level, but not at both levels.</p>
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Statement introduced in Junos OS Release 11.1 for the QFX Series.</p> <p>Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.</p>
Description	<p>Configure security trace options.</p> <p>To specify more than one trace option, include multiple flag statements. Trace option output is recorded in the <code>/var/log/kmd</code> file.</p>
<div style="display: flex; align-items: center;">  <p>NOTE: The <code>traceoptions</code> statement is not supported on QFabric systems.</p> </div>	
Options	<p>files <i>number</i>—(Optional) Maximum number of trace files. When a trace file (for example, <code>kmd</code>) reaches its maximum size, it is renamed <code>kmd.0</code>, then <code>kmd.1</code>, and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>If you specify a maximum number of files, you must also specify a maximum file size with the size option.</p> <p>Range: 2 through 1000 files</p> <p>Default: 0 files</p> <p>size <i>size</i>—(Optional) Maximum size of each trace file, in kilobytes (KB). When a trace file (for example, <code>kmd</code>) reaches this size, it is renamed, <code>kmd.0</code>, then <code>kmd.1</code> and so on, until the maximum number of trace files is reached. Then the oldest trace file is overwritten.</p> <p>Default: 1024 KB</p>

flag *flag*—Trace operation to perform. To specify more than one trace operation, include multiple **flag** statements.

- **all**—Trace all security events.
- **certificates**—Trace certificate events.
- **database**—Trace database events.
- **general**—Trace general events.
- **ike**—Trace IKE module processing.
- **parse**—Trace configuration processing.
- **policy-manager**—Trace policy manager processing.
- **routing-socket**—Trace routing socket messages.
- **timer**—Trace internal timer events.

level *level*—(Optional) Set traceoptions level.

- **all**—match all levels.
- **error**—Match error conditions.
- **info**—Match informational messages.
- **notice**—Match conditions that should be handled specially.
- **verbose**—Match verbose messages.
- **warning**—Match warning messages.

no-remote-trace—(Optional) Disable remote tracing

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

Related Documentation	• <i>Configuring Tracing Operations for Security Services</i>
------------------------------	---

update-server

Syntax	update-server;
Hierarchy Level	[edit Interfaces <i>interface-name</i> unit <i>logical-unit-number</i> inet dhcp]
Release Information	Statement introduced in Junos OS Release 8.5 for J Series devices. Statement introduced in Junos OS Release 9.0 for EX Series switches. Statement introduced in Junos OS Release 9.2 for SRX Series devices. Statement introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Propagate TCP/IP settings learned from an external DHCP server to the DHCP server running on the switch, router, or device.
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">• Configuring a DHCP Client (CLI Procedure) on page 71• <i>Example: Configuring the Device as a DHCP Client</i>• <i>interfaces</i>• <i>unit</i>• family on page 319

web-management

Syntax	<pre>web-management { http { interfaces [<i>interface-names</i>]; port <i>port</i>; } https { interfaces [<i>interface-names</i>]; local-certificate <i>name</i>; port <i>port</i>; } }</pre>
Hierarchy Level	[edit system services]
Release Information	<p>Statement introduced before Junos OS Release 7.4.</p> <p>Statement introduced in Junos OS Release 9.0 for EX Series switches.</p>
Description	<p>Configure settings for HTTP or HTTPS access. HTTP access allows management of the router or switch using the browser-based J-Web graphical user interface. HTTPS access allows secure management of the router or switch using the J-Web interface. With HTTPS access, communication between the router or switch Web server and your browser is encrypted.</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"> • <i>Configuring Management Access for the EX Series Switch (J-Web Procedure)</i> • <i>J-Web Interface User Guide</i> • http on page 324 • https on page 325 • port on page 337

wins-server (System)

Syntax	wins-server { <i>address</i> ; }
Hierarchy Level	[edit system services dhcp], [edit system services dhcp], [edit system services dhcp pool], [edit system services dhcp static-binding]
Release Information	Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 for EX Series switches.
Description	For J Series Services Routers and EX Series switches only. Specify one or more NetBIOS Name Servers. When a DHCP client is added to the network and assigned an IP address, the NetBIOS Name Server manages the Windows Internet Name Service (WINS) database that matches IP addresses (such as 192.168.1.3) to Windows NetBIOS names (such as \\Marketing). List servers in order of preference.
Options	<i>address</i> —IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple <i>address</i> options.
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">• <i>Configuring the Router or Interface to Act as a DHCP Server on J Series Services Routers</i>• <i>Configuring a DHCP Server on Switches (CLI Procedure)</i>

PART 3

Administration

- [Routine Monitoring on page 365](#)
- [Verifying and Managing DHCP Local Server Configurations on page 371](#)
- [Verifying and Managing DHCP Relay Agent Configurations on page 373](#)
- [DHCP Local Server Monitoring Commands on page 375](#)
- [DHCP Relay Agent Monitoring Commands on page 411](#)
- [Other Operational Commands on page 469](#)

Routine Monitoring

- [Monitoring DHCP Services on page 365](#)

Monitoring DHCP Services

Purpose



NOTE: This topic applies only to the J-Web Application package.

A switch or router can operate as a DHCP server. Use the monitoring functionality to view information about dynamic and static DHCP leases, conflicts, pools, and statistics.

Action

To monitor the DHCP server in the J-Web interface, select **Monitor > Services > DHCP**.

To monitor the DHCP server in the CLI, enter the following CLI commands:

- `show system services dhcp binding`
- `show system services dhcp conflict`
- `show system services dhcp pool`
- `show system services dhcp statistics`
- `show system services dhcp relay-statistics`
- `show system services dhcp global`
- `show system services dhcp client`
- `clear system services dhcp binding`
- `clear system services dhcp conflict`
- `clear system services dhcp statistics`
- `clear dhcp relay-statistics`

On EX4300 switches, to monitor the DHCP server in the CLI, enter the following CLI commands:

- `show dhcp server binding`
- `show dhcp server statistics`

- **show dhcp relay binding**
- **show dhcp relay statistics**
- **clear dhcp server binding**
- **clear dhcp server statistics**
- **clear dhcp relay binding**
- **clear dhcp relay statistics**

Meaning Table 19 on page 366 summarizes the output fields in DHCP displays in the J-Web interface.

Table 19: Summary of DHCP Output Fields

Field	Values	Additional Information
Global tab		
Name	This column displays the following information: <ul style="list-style-type: none">• Boot lease length• Domain Name• Name servers• Server identifier• Domain search• Gateway routers• WINS server• Boot file• Boot server• Default lease time• Minimum lease time• Maximum lease time	
Value	Displays the value for each of the parameters in the Name column.	
Bindings tab		
Allocated Address	List of IP addresses the DHCP server has assigned to clients.	
MAC Address	Corresponding media access control (MAC) address of the client.	
Binding Type	Type of binding assigned to the client: dynamic or static .	DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.
Lease Expires	Date and time the lease expires, or never for leases that do not expire.	
Pools tab		
Pool Name	Subnet on which the IP address pool is defined.	

Table 19: Summary of DHCP Output Fields (*continued*)

Field	Values	Additional Information
Low Address	Lowest address in the IP address pool.	
High Address	Highest address in the IP address pool.	
Excluded Addresses	Addresses excluded from the address pool.	
Clients tab		
Interface Name	Name of the logical interface.	
Hardware Address	Vendor identification.	
Status	State of the client binding.	
Address Obtained	IP address obtained from the DHCP server.	
Update Server	Indicates whether server update is enabled.	
Lease Obtained	Date and time the lease was obtained.	
Lease Expires	Date and time the lease expires.	
Renew	Reacquires an IP address from the server for the interface. When you click this option, the command sends a discover message if the client state is INIT and a renew request message if the client state is BOUND. For all other states it performs no action.	
Release	Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.	
Conflicts tab		
Detection Time	Date and time the client detected the conflict.	
Detection Method	How the conflict was detected.	Only client-detected conflicts are displayed.
Address	IP address where the conflict occurs.	The addresses in the conflicts list remain excluded until you use the clear system services dhcp conflict command to manually clear the list.

Table 19: Summary of DHCP Output Fields (*continued*)

Field	Values	Additional Information
DHCP Statistics		
Relay Statistics tab		
Packet Counters	Displays the number of packet counters.	
Dropped Packet Counters	Graphically displays the number of dropped packet counters.	
Statistics tab		
Packets dropped	Total number of packets dropped and the number of packets dropped due to a particular condition.	
Messages received	Number of BOOTREQUEST, DHCPDECLINE, DHCPDISCOVER, DHCPINFORM, DHCPRELEASE, and DHCPREQUEST messages sent from DHCP clients and received by the DHCP server.	
Messages sent	Number of BOOTREPLY, DHCPACK, DHCPOFFER, DHCPNAK, and DHCPFORCERENEW messages sent from the DHCP server to DHCP clients.	

[Table 20 on page 368](#) summarizes the output fields in DHCP displays in EX4300 switches in the J-Web interface.

Table 20: Summary of DHCP Output Fields for EX4300 Switches

Field	Values	Additional Information
Binding Information tab		
IP Address	IP address of the DHCP client..	
Session ID	Session ID of the subscriber session.	
Hardware Address	Hardware address of the DHCP client.	
Expires	Number of seconds in which the lease expires.	

Table 20: Summary of DHCP Output Fields for EX4300 Switches (*continued*)

Field	Values	Additional Information
State	State of the address binding table on the extended DHCP local server: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • FORCERENEW—Client has received the FORCERENEW message from the server. • INIT—Initial state. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	
Interface	Interface on which the request was received.	

[Table 21 on page 369](#) summarizes the output fields in DHCP Statistics Information for EX4300 switches in the J-Web interface.

Table 21: Summary of the DHCP Statistics Information Output for EX4300 switches

Field	Values	Additional Information
Message Counters		
Message Counters	Graphically displays the number of messages sent and received.	
Dropped packet Counters		
MAC Limit	Graphically displays the number of dropped packet counters.	

- Related Documentation**
- [Configuring DHCP Services \(J-Web Procedure\) on page 63](#)
 - [Understanding DHCP Services for Switches](#)

Verifying and Managing DHCP Local Server Configurations

- [Verifying and Managing DHCP Local Server Configuration on page 371](#)
- [Verifying and Managing DHCPv6 Local Server Configuration on page 371](#)

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 DHCP Relay Agent Configurations

- [Verifying and Managing DHCP Relay Configuration on page 373](#)
- [Verifying and Managing DHCPv6 Relay Configuration on page 373](#)

Verifying and Managing DHCP Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCP relay agent clients:

Action • To display the address bindings for extended DHCP relay agent clients:

user@host> [show dhcp relay binding](#) routing-instance *customer routing instance*

• To display extended DHCP relay agent statistics:

user@host> [show dhcp relay statistics](#) routing-instance *customer routing instance*

• To clear the binding state of DHCP relay agent clients:

user@host> [clear dhcp relay binding](#) routing-instance *customer routing instance*

• To clear all extended DHCP relay agent statistics:

user@host> [clear dhcp relay statistics](#) routing-instance *customer routing instance*

Related Documentation • [CLI Explorer](#)

Verifying and Managing DHCPv6 Relay Configuration

Purpose View or clear address bindings or statistics for extended DHCPv6 relay agent clients:

Action • To display the address bindings for extended DHCPv6 relay agent clients:

user@host> [show dhcpv6 relay binding](#)

• To display extended DHCPv6 relay agent statistics:

user@host> [show dhcpv6 relay statistics](#)

• To clear the binding state of DHCPv6 relay agent clients:

user@host> [clear dhcpv6 relay binding](#)

- To clear all extended DHCPv6 relay agent statistics:

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

**Related
Documentation**

- [CLI Explorer](#)

CHAPTER 17

DHCP Local Server 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

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](#)
- [show dhcp server binding on page 393](#)

List of Sample Output

- [clear dhcp server binding <ip-address> on page 377](#)
- [clear dhcp server binding all on page 377](#)
- [clear dhcp server binding interface on page 378](#)
- [clear dhcp server binding <interfaces-vlan> on page 378](#)
- [clear dhcp server binding <interfaces-wildcard> on page 378](#)

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 379
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"> • <i>Clearing DHCP Bindings for Subscriber Access</i> • show dhcpv6 server binding on page 401
List of Sample Output	<p>clear dhcpv6 server binding all on page 382</p> <p>clear dhcpv6 server binding <ipv6-prefix> on page 382</p>

[clear dhcpv6 server binding interface on page 382](#)
[clear dhcpv6 server binding <interfaces-vlan> on page 382](#)
[clear dhcpv6 server binding <interfaces-wildcard> on page 382](#)

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 407
List of Sample Output	clear dhcpv6 server statistics on page 383
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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92](#)

List of Sample Output [request dhcp server reconfigure on page 385](#)

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 Dynamic Client Reconfiguration of Extended Local Server Clients on page 92
List of Sample Output	request dhcpv6 server reconfigure on page 387
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

List of Syntax	Syntax on page 388 Syntax (EX Series Switches) on page 388 Syntax (TX Matrix Router) on page 388 Syntax (TX Matrix Plus Router) on page 388 Syntax (MX Series Router) on page 388
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 member-id>
<message "text">
<other-routing-engine>
```

Release Information	<p>Command introduced before Junos OS Release 7.4.</p> <p>Option other-routing-engine introduced in Junos OS Release 8.0.</p> <p>Command introduced in Junos OS Release 9.0 for EX Series switches.</p> <p>Option sfc introduced for the TX Matrix Plus router in Junos OS Release 9.6.</p> <p>Option both-routing-engines introduced in Junos OS Release 12.1.</p>
Description	Reboot the software.
Options	<p>none—Reboot the software immediately.</p> <p>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.</p> <p>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.</p> <p>all-members—(EX4200 switches and MX Series routers only) (Optional) Reboot the software on all members of the Virtual Chassis configuration.</p> <p>at <i>time</i>—(Optional) Time at which to reboot the software, specified in one of the following ways:</p> <ul style="list-style-type: none"> • now—Stop or reboot the software immediately. This is the default. • +<i>minutes</i>—Number of minutes from now to reboot the software. • <i>yymmddhhmm</i>—Absolute time at which to reboot the software, specified as year, month, day, hour, and minute. • <i>hh:mm</i>—Absolute time on the current day at which to stop the software, specified in 24-hour time. <p>both-routing-engines—(Optional) Reboot both Routing Engines at the same time.</p> <p>in <i>minutes</i>—(Optional) Number of minutes from now to reboot the software. This option is an alias for the at +<i>minutes</i> option.</p> <p>lcc <i>number</i>—(TX Matrix routers and TX Matrix Plus routers only) (Optional) Line-card chassis number.</p> <p>Replace <i>number</i> with the following values depending on the LCC configuration:</p> <ul style="list-style-type: none"> • 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*
- [Routing Matrix with a TX Matrix Plus Router Solutions Page](#)

List of Sample Output

[request system reboot on page 392](#)
[request system reboot \(at 2300\) on page 392](#)
[request system reboot \(in 2 Hours\) on page 392](#)
[request system reboot \(Immediately\) on page 392](#)
[request system reboot \(at 1:20 AM\) on page 392](#)

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 `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>`

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

Description Display the address bindings in the client table on the extended Dynamic Host Configuration Protocol (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) Display DHCP binding information for a specific client identified by one of the following entries:

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

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`.

interface interface-name—(Optional) Display information about active client bindings on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

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

interfaces-wildcard—(Optional) The set of interfaces on which to show the binding state information. This option supports the use of the wildcard character (*).

logical-system logical-system-name—(Optional) Display information about active client bindings for DHCP clients on the specified logical system.

routing-instance routing-instance-name—(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege Level view

Related Documentation

- *Clearing DHCP Bindings for Subscriber Access*
- *Verifying and Managing Agent Circuit Identifier-Based Dynamic VLAN Configuration*
- [clear dhcp server binding on page 376](#)

List of Sample Output

[show dhcp server binding on page 396](#)
[show dhcp server binding detail on page 396](#)
[show dhcp server binding detail \(ACI Interface Set Configured\) on page 396](#)
[show dhcp server binding interface <vlan-id> on page 397](#)
[show dhcp server binding interface <svlan-id> on page 397](#)
[show dhcp server binding <ip-address> on page 397](#)
[show dhcp server binding <session-id> on page 397](#)
[show dhcp server binding summary on page 397](#)
[show dhcp server binding <interfaces-vlan> on page 397](#)
[show dhcp server binding <interfaces-wildcard> on page 397](#)

Output Fields Table 22 on page 394 lists the output fields for the **show dhcp server binding** command. Output fields are listed in the approximate order in which they appear.

Table 22: 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

Table 22: show dhcp server binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
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
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

```

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 379
List of Sample Output	show dhcp server statistics on page 399
Output Fields	Table 23 on page 399 lists the output fields for the show dhcp server statistics command. Output fields are listed in the approximate order in which they appear.

Table 23: 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"> • <i>Clearing DHCP Bindings for Subscriber Access</i> • clear dhcpv6 server binding on page 381

List of Sample Output

- [show dhcpv6 server binding on page 403](#)
- [show dhcpv6 server binding detail on page 403](#)
- [show dhcpv6 server binding interface on page 404](#)
- [show dhcpv6 server binding interface detail on page 404](#)
- [show dhcpv6 server binding \(IPv6 Prefix\) on page 405](#)
- [show dhcpv6 server binding \(Session ID\) on page 405](#)
- [show dhcpv6 server binding \(Interfaces VLAN\) on page 405](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 405](#)
- [show dhcpv6 server binding \(Interfaces Wildcard\) on page 405](#)
- [show dhcpv6 server binding summary on page 406](#)

Output Fields [Table 24 on page 402](#) lists the output fields for the **show dhcpv6 server binding** command. Output fields are listed in the approximate order in which they appear.

Table 24: 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 24: 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 383
List of Sample Output	show dhcpv6 server statistics on page 408
Output Fields	Table 25 on page 408 lists the output fields for the show dhcpv6 server statistics command. Output fields are listed in the approximate order in which they appear.

Table 25: 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

CHAPTER 18

DHCP Relay Agent Monitoring Commands

- `clear dhcp relay binding`
- `clear dhcp relay statistics`
- `clear dhcpv6 relay binding`
- `clear dhcpv6 relay statistics`
- `show dhcp relay binding`
- `show dhcp relay statistics`
- `show dhcpv6 relay binding`
- `show dhcpv6 relay statistics`
- `show route extensive`
- `show route protocol`

clear dhcp relay binding

Syntax	clear dhcp relay binding <address> <all> <interface <i>interface-name</i>> <interfaces-vlan> <interfaces-wildcard> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 8.3. Options all and interface added in Junos OS Release 8.4. Options interfaces-vlan and interfaces-wildcard added in Junos OS Release 12.1. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.
Options	<p>address—(Optional) Clear the binding state for the DHCP client, using one of the following entries:</p> <ul style="list-style-type: none">• ip-address—The specified IP address.• mac-address—The specified MAC address.• session-id—The specified session ID. <p>all—(Optional) Clear the binding state for all DHCP clients.</p> <p>interface <i>interface-name</i>—(Optional) Clear the binding state for DHCP 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) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).</p> <p>logical-system <i>logical-system-name</i>—(Optional) Clear the binding state for DHCP clients on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Clear the binding state for DHCP clients on the specified routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• <i>Clearing DHCP Bindings for Subscriber Access</i>• show dhcp relay binding on page 422

List of Sample Output [clear dhcp relay binding on page 413](#)
[clear dhcp relay binding all on page 413](#)
[clear dhcp relay binding interface on page 413](#)
[clear dhcp relay binding <interfaces-vlan> on page 413](#)
[clear dhcp relay binding <interfaces-wildcard> on page 413](#)

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

Sample Output

clear dhcp relay binding

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

```
user@host> show dhcp relay binding
IP address      Hardware address  Type    Lease expires at
100.20.32.1     90:00:00:01:00:01 active    2007-02-08 16:41:17 EST
192.168.14.8    90:00:01:01:02:01 active    2007-02-10 10:01:06 EST
```

```
user@host> clear dhcp relay binding 100.20.32.1
```

```
user@host> show dhcp relay binding
IP address      Hardware address  Type    Lease expires at
192.168.14.8    90:00:01:01:02:01 active    2007-02-10 10:01:06 EST
```

clear dhcp relay binding all

The following command clears all DHCP relay agent bindings:

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

clear dhcp relay binding interface

The following command clears DHCP relay agent bindings on a specific interface:

```
user@host> clear dhcp relay binding interface fe-0/0/3
```

clear dhcp relay binding <interfaces-vlan>

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

```
user@host> clear dhcp relay binding interface ae0
```

clear dhcp relay binding <interfaces-wildcard>

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

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

clear dhcp relay statistics

Syntax	<code>clear dhcp relay statistics</code> <code><logical-system <i>logical-system-name</i>></code> <code><routing-instance <i>routing-instance-name</i>></code>
Syntax	Syntax for EX Series switches: <code>show dhcp relay statistics</code> <code><routing-instance <i>routing-instance-name</i>></code>
Release Information	Command introduced in Junos OS Release 8.3. Statement introduced in Junos OS Release 12.1 for EX Series switches. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<code>logical-system <i>logical-system-name</i></code> —(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system. <code>routing-instance <i>routing-instance-name</i></code> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show dhcp relay statistics on page 427
List of Sample Output	clear dhcp relay statistics on page 415
Output Fields	Table 26 on page 415 lists the output fields for the <code>clear dhcp relay statistics</code> command.

Table 26: clear dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to 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 relay agent application. • 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 DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
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 • DHC PNACK—Number of DHCP NACK PDUs transmitted

Sample Output

clear dhcp relay statistics

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

```
user@host> show dhcp relay statistics
```

```
Packets dropped:
  Total          1
  Lease Time Violated 1

Messages received:
  BOOTREQUEST    116
  DHCPDECLINE    0
  DHCPDISCOVER   11
  DHCPINFORM     0
  DHCPRELEASE    0
  DHCPREQUEST    105

Messages sent:
  BOOTREPLY      44
  DHCPOFFER      11
  DHCPACK        11
  DHCPNAK        11
```

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

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

Syntax	<pre>clear dhcpv6 relay 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 11.4.</p> <p>Command introduced in Junos OS Release 12.3R2 for EX Series switches.</p> <p>Options <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> added in Junos OS Release 12.1.</p> <p>Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.</p>
Description	Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.
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>interfaces-vlan—(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.</p> <p>interfaces-wildcard—(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).</p> <p>interface interface-name—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.</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	view
Related Documentation	<ul style="list-style-type: none"> • <i>Clearing DHCP Bindings for Subscriber Access</i> • show dhcpv6 relay binding on page 430

- List of Sample Output**
- [clear dhcpv6 relay binding on page 418](#)
 - [clear dhcpv6 relay binding <prefix> on page 418](#)
 - [clear dhcpv6 relay binding all on page 418](#)
 - [clear dhc6p relay binding interface on page 418](#)
 - [clear dhcpv6 relay binding <interfaces-vlan> on page 419](#)
 - [clear dhcpv6 relay binding <interfaces-wildcard> on page 419](#)

Output Fields See [show dhcpv6 relay binding](#) for an explanation of output fields.

Sample Output

clear dhcpv6 relay binding

The following sample output displays the DHCPv6 bindings before and after the **clear dhcpv6 relay binding** command is issued.

```
user@host> show dhcpv6 relay binding
```

Prefix	Session Id	Expires	State	Interface	Client DUID
2001:bd8:3c4d:15::/64	1	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01					
2001:bd8:3c4d:16::/64	2	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02					
2001:bd8:3c4d:17::/64	3	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03					
2001:bd8:3c4d:18::/64	4	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04					
2001:bd8:3c4d:19::/64	5	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05					
2001:bd8:3c4d:20::/64	6	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06					

clear dhcpv6 relay binding <prefix>

```
user@host> clear dhcpv6 relay binding 2001:bd8:3c4d:15::/64
```

```
user@host> show dhcpv6 relay binding
```

Prefix	Session Id	Expires	State	Interface	Client DUID
2001:bd8:3c4d:16::/64	2	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02					
2001:bd8:3c4d:17::/64	3	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03					
2001:bd8:3c4d:18::/64	4	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04					
2001:bd8:3c4d:19::/64	5	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05					
2001:bd8:3c4d:20::/64	6	83720	BOUND	ge-1/0/0.0	
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06					

clear dhcpv6 relay binding all

The following command clears all DHCP relay agent bindings:

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

clear dhc6p relay binding interface

The following command clears DHCPv6 relay agent bindings on a specific interface:


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

clear dhcpv6 relay binding <interfaces-vlan>

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

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

clear dhcpv6 relay binding <interfaces-wildcard>

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

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

clear dhcpv6 relay statistics

Syntax	clear dhcpv6 relay statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>>
Release Information	Command introduced in Junos OS Release 11.4. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.
Description	Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.
Options	logical-system <i>logical-system-name</i> —(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are cleared for the default logical system. routing-instance <i>routing-instance-name</i> —(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are cleared for the default routing instance.
Required Privilege Level	view
List of Sample Output	clear dhcpv6 relay statistics on page 420
Output Fields	See show dhcpv6 relay statistics for an explanation of output fields.

Sample Output

clear dhcpv6 relay statistics

The following sample output displays the DHCPv6 relay statistics before and after the **clear dhcpv6 relay statistics** command is issued.

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total                0
    Lease Time Violated  1

Messages received:
    DHCPV6_DECLINE        0
    DHCPV6_SOLICIT        10
    DHCPV6_INFORMATION_REQUEST  0
    DHCPV6_RELEASE        0
    DHCPV6_REQUEST        10
    DHCPV6_CONFIRM        0
    DHCPV6_RENEW          0
    DHCPV6_REBIND         0
    DHCPV6_RELAY_REPL     0

Messages sent:
    DHCPV6_ADVERTISE      0
    DHCPV6_REPLY           0
    DHCPV6_RECONFIGURE    0
    DHCPV6_RELAY_FORW     0
```

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

```
user@host> show dhcpv6 relay statistics
```

```
DHCPv6 Packets dropped:
```

```
    Total                                0
```

```
Messages received:
```

```
    DHCPV6_DECLINE                      0
```

```
    DHCPV6_SOLICIT                      0
```

```
    DHCPV6_INFORMATION_REQUEST         0
```

```
    DHCPV6_RELEASE                      0
```

```
    DHCPV6_REQUEST                     0
```

```
    DHCPV6_CONFIRM                     0
```

```
    DHCPV6_RENEW                       0
```

```
    DHCPV6_REBIND                      0
```

```
    DHCPV6_RELAY_REPL                  0
```

```
Messages sent:
```

```
    DHCPV6_ADVERTISE                    0
```

```
    DHCPV6_REPLY                       0
```

```
    DHCPV6_RECONFIGURE                  0
```

```
    DHCPV6_RELAY_FORW                   0
```

show dhcp relay binding

Syntax **show dhcp relay binding**
 <address>
 <brief>
 <detail>
 <interface *interface-name*>
 <interfaces-vlan>
 <interfaces-wildcard>
 <ip-address | mac-address>
 <logical-system *logical-system-name*>
 <routing-instance *routing-instance-name*>
 <summary>

Release Information Command introduced in Junos OS Release 8.3.
 Options **interface** and **mac-address** added in Junos OS Release 8.4.
 Options **interfaces-vlan** and **interfaces-wildcard** added in Junos OS Release 12.1.
 Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.

Description Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options **address**—(Optional) Display DHCP binding information for a specific client identified by one of the following entries:

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

brief—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as **show dhcp relay binding**.

detail—(Optional) Display detailed client binding information.

interface *interface-name*—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and SVLAN ID.

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

interfaces-wildcard—(Optional) The set of interfaces on which to show binding state information. This option supports the use of the wildcard character (*).

logical-system *logical-system-name*—(Optional) Perform this operation on the specified logical system.

routing-instance *routing-instance-name*—(Optional) Perform this operation on the specified routing instance.

summary—(Optional) Display a summary of DHCP client information.

Required Privilege Level view

Related Documentation

- [Clearing DHCP Bindings for Subscriber Access](#)
- [clear dhcp relay binding on page 412](#)

List of Sample Output

- [show dhcp relay binding on page 424](#)
- [show dhcp relay binding detail on page 425](#)
- [show dhcp relay binding interface on page 425](#)
- [show dhcp relay binding interface vlan-id on page 425](#)
- [show dhcp relay binding interface svlan-id on page 425](#)
- [show dhcp relay binding ip-address on page 426](#)
- [show dhcp relay binding mac-address on page 426](#)
- [show dhcp relay binding session-id on page 426](#)
- [show dhcp relay binding <interfaces-vlan> on page 426](#)
- [show dhcp relay binding <interfaces-wildcard> on page 426](#)
- [show dhcp relay binding summary on page 426](#)

Output Fields Table 27 on page 423 lists the output fields for the **show dhcp relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 27: show dhcp relay 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> rebinding, <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.	briefdetail
Session Id	Session ID of the subscriber session.	briefdetail
Generated Remote ID	Remote ID generated by the Option 82 Agent Remote ID (suboption 1)	detail
Hardware address	Hardware address of the DHCP client.	briefdetail
Expires	Number of seconds in which the lease expires.	briefdetail

Table 27: show dhcp relay binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	State of the DHCP relay address binding table on the DHCP client: <ul style="list-style-type: none"> • BOUND—Client has an active IP address lease. • INIT—Initial state. • REBINDING—Client is broadcasting a request to renew the IP address lease. • RELEASE—Client is releasing the IP address lease. • RENEWING—Client is sending a request to renew the IP address lease. • REQUESTING—Client is requesting a DHCP server. • SELECTING—Client is receiving offers from DHCP servers. 	briefdetail
Interface	Incoming client interface.	brief
Lease Expires	Date and time at which the client's IP address lease expires.	detail
Lease Expires in	Number of seconds in which the 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
Incoming Client Interface	Client's incoming interface.	detail
Server IP Address	IP address of the DHCP server.	detail
Server Interface	Interface of the DHCP server.	detail
Bootp Relay Address	IP address of BOOTP relay.	detail
Type	Type of DHCP packet processing performed on the router: <ul style="list-style-type: none"> • active—Router actively processes and relays DHCP packets. • passive—Router passively snoops DHCP packets passing through the router. 	All levels
Lease expires at	Date and time at which the client's IP address lease expires.	All levels

Sample Output

show dhcp relay binding

```

user@host> show dhcp relay binding
IP address      Session Id  Hardware address  Expires   State   Interface
100.20.32.11    41         00:10:94:00:00:01 86371     BOUND   ge-1/0/0.0
100.20.32.12    42         00:10:94:00:00:02 86371     BOUND   ge-1/0/0.0

```

100.20.32.13	43	00:10:94:00:00:03	86371	BOUND	ge-1/0/0.0
100.20.32.14	44	00:10:94:00:00:04	86371	BOUND	ge-1/0/0.0
100.20.32.15	45	00:10:94:00:00:05	86371	BOUND	ge-1/0/0.0

show dhcp relay binding detail

user@host> show dhcp relay binding detail

```
Client IP Address: 100.20.32.11
  Hardware Address: 00:10:94:00:00:01
  State: BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
  Lease Expires: 2009-07-21 11:00:06 PDT
  Lease Expires in: 86361 seconds
  Lease Start: 2009-07-20 11:00:06 PDT
  Lease time violated: yes
  Last Packet Received: 2009-07-20 11:00:06 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address: 100.20.22.2
  Server Interface: none
  Bootp Relay Address: 100.20.32.2
  Session Id: 41

Client IP Address: 100.20.32.12
  Hardware Address: 00:10:94:00:00:02
  State: BOUND(DHCP_RELAY_STATE_BOUND_ON_INTF_DELETE)
  Lease Expires: 2009-07-21 11:00:06 PDT
  Lease Expires in: 86361 seconds
  Lease Start: 2009-07-20 11:00:06 PDT
  Last Packet Received: 2009-07-20 11:00:06 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Ip Address: 100.20.22.2
  Server Interface: none
  Bootp Relay Address: 100.20.32.2
  Session Id: 42
  Generated Remote ID: host:ge-1/0/0:100
```

show dhcp relay binding interface

user@host> show dhcp relay binding interface fe-0/0/2

IP address	Hardware address	Type	Lease expires at
100.20.32.1	90:00:00:01:00:01	active	2007-03-27 15:06:20 EDT

show dhcp relay binding interface vlan-id

user@host> show dhcp relay 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

show dhcp relay binding interface svlan-id

user@host> show dhcp relay 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 relay binding ip-address

```

user@host> show dhcp relay binding 100.20.32.13
IP address      Session Id  Hardware address  Expires    State      Interface
100.20.32.13    43         00:10:94:00:00:03  86293     BOUND      ge-1/0/0.0

```

show dhcp relay binding mac-address

```

user@host> show dhcp relay binding 00:10:94:00:00:05
IP address      Session Id  Hardware address  Expires    State      Interface
100.20.32.15    45         00:10:94:00:00:05  86279     BOUND      ge-1/0/0.0

```

show dhcp relay binding session-id

```

user@host> show dhcp relay binding 41
IP address      Session Id  Hardware address  Expires    State      Interface
100.20.32.11    41         00:10:94:00:00:01  86305     BOUND      ge-1/0/0.0

```

show dhcp relay binding <interfaces-vlan>

```

user@host> show dhcp relay 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 relay binding <interfaces-wildcard>

```

user@host> show dhcp relay 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 relay binding summary

```

user@host> show dhcp relay binding summary
3 clients, (2 init, 1 bound, 0 selecting, 0 requesting, 0 renewing, 0 rebinding,
0 releasing)

```


show dhcp relay statistics

Syntax	<pre>show dhcp relay statistics <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>></pre>
Syntax	<p>Syntax for EX Series switches:</p> <pre>show dhcp relay statistics <routing-instance <i>routing-instance-name</i>></pre>
Release Information	<p>Command introduced in Junos OS Release 8.3.</p> <p>Command introduced in Junos OS Release 12.1 for EX Series switches.</p> <p>Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Routers.</p>
Description	Display Dynamic Host Configuration Protocol (DHCP) relay statistics.
Options	<p>logical-system <i>logical-system-name</i>—(On routers only) (Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcp relay statistics on page 414
List of Sample Output	show dhcp relay statistics on page 429
Output Fields	<p>Table 28 on page 428 lists the output fields for the show dhcp relay statistics command. Output fields are listed in the approximate order in which they appear.</p>

Table 28: show dhcp relay statistics Output Fields

Field Name	Field Description
Packets dropped	<p>Number of packets discarded by the extended DHCP relay agent application due to 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 relay agent application. • 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 DHCP relay application could not send. • Option 60—Number of packets discarded containing DHCP option 60 vendor-specific information. • Option 82—Number of packets discarded because DHCP option 82 information could not be added.
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
External Server Response	State of the external DHCP server responsiveness.
Packets forwarded	<p>Number of packets forwarded.</p> <ul style="list-style-type: none"> • BOOTREQUEST—Number of BOOTREQUEST protocol data units (PDUs) forwarded • BOOTREPLY—Number of BOOTREPLY protocol data units (PDUs) forwarded

Table 28: show dhcp relay statistics Output Fields (*continued*)

Field Name	Field Description
External Server Response	State of the external DHCP server responsiveness.

Sample Output

show dhcp relay statistics

```

user@host> show dhcp relay statistics
Packets dropped:
    Total                34
    Bad hardware address  1
    Bad opcode            1
    Bad options           3
    Invalid server address 5
    Lease Time Violation  1
    No available addresses 1
    No interface match    2
    No routing instance match 9
    No valid local address 4
    Packet too short      2
    Read error            1
    Send error            1
    Option 60             1
    Option 82             2

Messages received:
    BOOTREQUEST          116
    DHCPDECLINE           0
    DHCPDISCOVER          11
    DHCPINFORM            0
    DHCPRELEASE           0
    DHCPREQUEST          105

Messages sent:
    BOOTREPLY            0
    DHCPOFFER            2
    DHCPACK               1
    DHCPNAK               0
    DHCPFORCERENEW       0

Packets forwarded:
    Total                4
    BOOTREQUEST          2
    BOOTREPLY            2

External Server Response:
    State                Responding

```

show dhcpv6 relay binding

Syntax	show dhcpv6 relay binding <address> <brief> <detail> <interface <i>interface-name</i>> <interfaces-vlan> <interfaces-wildcard> <logical-system <i>logical-system-name</i>> <routing-instance <i>routing-instance-name</i>> <summary>
Release Information	Command introduced in Junos OS Release 11.4. <i>interfaces-vlan</i> and <i>interfaces-wildcard</i> options introduced in Junos OS Release 12.1.
Description	Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.
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—(Optional) Display brief information about the active client bindings. This is the default, and produces the same output as show dhcpv6 relay binding.</p> <p>detail—(Optional) Display detailed client binding information.</p> <p>interface <i>interface-name</i>—(Optional) Perform this operation on the specified interface. You can optionally filter on VLAN ID and S-VLAN 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 <i>logical-system-name</i>—(Optional) Perform this operation on the specified logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance.</p> <p>summary—(Optional) Display a summary of DHCPv6 client information.</p>
Required Privilege Level	view

- Related Documentation**
- [Clearing DHCP Bindings for Subscriber Access](#)
 - [clear dhcpv6 relay binding on page 417](#)

- List of Sample Output**
- [show dhcpv6 relay binding on page 432](#)
 - [show dhcpv6 relay binding \(Address\) on page 433](#)
 - [show dhcpv6 relay binding detail \(Client ID\) on page 433](#)
 - [show dhcpv6 relay binding detail on page 433](#)
 - [show dhcpv6 relay binding detail \(Multi-Relay Topology\) on page 434](#)
 - [show dhcpv6 relay binding \(Session ID\) on page 434](#)
 - [show dhcpv6 relay binding \(Interfaces VLAN\) on page 434](#)
 - [show dhcpv6 relay binding \(Interfaces Wildcard\) on page 434](#)
 - [show dhcpv6 relay binding \(Interfaces Wildcard\) on page 435](#)
 - [show dhcpv6 relay binding summary on page 435](#)

Output Fields Table 29 on page 431 lists the output fields for the **show dhcpv6 relay binding** command. Output fields are listed in the approximate order in which they appear.

Table 29: show dhcpv6 relay binding Output Fields

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

Table 29: show dhcpv6 relay binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
Lease Expires in	Number of seconds in which the 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 the client's IPv6 prefix 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
Incoming Client Interface	Client's incoming interface.	detail
Server Address	IP address of the DHCPv6 server. Displays unknown for a DHCPv6 relay agent in a multi-relay topology that is not directly adjacent to the DHCPv6 server and does not detect the IP address of the server. In that case, the output instead displays the Next Hop Server Facing Relay field.	detail
Next Hop Server Facing Relay	Next-hop address in the direction of the DHCPv6 server.	detail
Server Interface	Interface of the DHCPv6 server.	detail
Relay Address	IP address of the relay.	detail
Client Pool Name	Address pool that granted the client lease.	detail
Client ID Length	Length of client ID.	All levels
Client Id	Client ID.	All levels
Generated Circuit ID	Circuit ID generated by the DHCPv6 Interface-ID option (option 18)	detail
Generated Remote ID Enterprise Number	The Juniper Networks IANA private enterprise number	detail
Generated Remote ID	Remote ID generated by the DHCPv6 Remote-ID option (option 37)	detail

Sample Output

show dhcpv6 relay binding

```

user@host> show dhcpv6 relay binding
Prefix          Session Id  Expires  State  Interface  Client DUID
2001:bd8:3c4d:15::/64  1          83720    BOUND  ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:bd8:3c4d:16::/64  2          83720    BOUND  ge-1/0/0.0

```

```

LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:bd8:3c4d:17::/64      3      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:bd8:3c4d:18::/64      4      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:bd8:3c4d:19::/64      5      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:bd8:3c4d:20::/64      6      83720      BOUND      ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:06

```

show dhcpv6 relay binding (Address)

```

user@host> show dhcpv6 relay binding 2001:bd8:1111:2222::/64 detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64
  Client DUID:             LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

  State:                   BOUND(RELAY_STATE_BOUND)
  Lease Expires:           2011-05-25 07:12:09 PDT
  Lease Expires in:        77115 seconds
  Preferred Lease Expires: 2012-07-24 00:18:14 UTC
  Preferred Lease Expires in: 600 seconds
  Lease Start:             2011-05-24 07:12:09 PDT
  Incoming Client Interface: ge-1/0/0.0
  Server Address:          2008:aaaa:bbbb::1
  Server Interface:        none
  Relay Address:           2001:bd8:1111:2222::
  Client Pool Name:        pool-25
  Client Id Length:        14
  Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001

```

show dhcpv6 relay binding detail (Client ID)

```

user@host> show dhcpv6 relay binding 14/0x00010001/0x4bfa26af/0x00109400/0x0001
detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64
  Client DUID:             LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

  State:                   BOUND(RELAY_STATE_BOUND)
  Lease Expires:           2011-05-25 07:12:09 PDT
  Lease Expires in:        77115 seconds
  Preferred Lease Expires: 2012-07-24 00:18:14 UTC
  Preferred Lease Expires in: 600 seconds
  Lease Start:             2011-05-24 07:12:09 PDT
  Lease time violated:     yes
  Incoming Client Interface: ge-1/0/0.0
  Server Address:          2008:aaaa:bbbb::1
  Server Interface:        none
  Relay Address:           2001:bd8:1111:2222::
  Client Pool Name:        pool-25
  Client Id Length:        14
  Client Id:
/0x00010001/0x4bfa26af/0x00109400/0x0001

```

show dhcpv6 relay binding detail

```

user@host> show dhcpv6 relay binding detail
Session Id: 1
  Client IPv6 Prefix:      2001:bd8:3c4d:15::/64

```

```

Client DUID:                               LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

State:                                     BOUND(RELAY_STATE_BOUND)
Lease Expires:                             2011-05-25 07:12:09 PDT
Lease Expires in:                           77115 seconds
Preferred Lease Expires:                     2012-07-24 00:18:14 UTC
Preferred Lease Expires in:                   600 seconds
Lease Start:                                2011-05-24 07:12:09 PDT
Lease time violated:                         yes
Incoming Client Interface:                   ge-1/0/0.0
Server Address:                              2008:aaaa:bbbb::1
Server Interface:                            none
Relay Address:                               2001:bd8:1111:2222::
Client Pool Name:                            pool-25
Client Id Length:                            14
Client Id:                                   /0x00010001/0x4bfa26af/0x00109400/0x0001
Generated Remote ID Enterprise Number:       1411
Generated Remote ID:                         host:ge-1/0/0:100

```

show dhcpv6 relay binding detail (Multi-Relay Topology)

```

user@host > show dhcpv6 relay binding detail
Session Id: 13
Client IPv6 Prefix:                         3000:0:0:8001::5/128
Client DUID:                                LL0x1-00:00:65:03:01:02
State:                                       BOUND(DHCPV6_RELAY_STATE_BOUND)
Lease Expires:                             2011-11-21 06:14:50 PST
Lease Expires in:                           293 seconds
Preferred Lease Expires:                     2012-07-24 00:18:14 UTC
Preferred Lease Expires in:                   600 seconds
Lease Start:                                2011-11-21 06:09:50 PST
Incoming Client Interface:                   ge-1/0/0.0
Server Address:                              unknown
Next Hop Server Facing Relay:                4000::2
Server Interface:                            none
Client Id Length:                            10
Client Id:                                   /0x00030001/0x00006503/0x0102

```

show dhcpv6 relay binding (Session ID)

```

user@host> show dhcpv6 relay binding 41
Prefix          Session Id Expires   State   Interface   Client DUID
2001:bd8:3c4d:15::/64  41      78837    BOUND   ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01

```

show dhcpv6 relay binding (Interfaces VLAN)

```

user@host> show dhcpv6 relay 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 relay binding (Interfaces Wildcard)

```

user@host> show dhcpv6 relay 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 relay binding (Interfaces Wildcard)

```

user@host> show dhcpv6 relay 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 relay binding summary

```

user@host> show dhcpv6 relay binding summary
5 clients, (0 init, 5 bound, 0 selecting, 0 requesting, 0 renewing, 0 releasing)

```

show dhcpv6 relay statistics

Syntax	show dhcpv6 relay statistics <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 11.4. Command introduced in Junos OS Release 12.1X48R3 for PTX Series Packet Transport Switches. Command introduced in Junos OS Release 12.3R2 for EX Series switches.
Description	Display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.
Options	<p>logical-system <i>logical-system-name</i>—(Optional) Perform this operation on the specified logical system. If you do not specify a logical system name, statistics are displayed for the default logical system.</p> <p>routing-instance <i>routing-instance-name</i>—(Optional) Perform this operation on the specified routing instance. If you do not specify a routing instance name, statistics are displayed for the default routing instance.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • clear dhcpv6 relay statistics on page 420
List of Sample Output	show dhcpv6 relay statistics on page 437
Output Fields	Table 30 on page 436 lists the output fields for the show dhcpv6 relay statistics command. Output fields are listed in the approximate order in which they appear.

Table 30: show dhcpv6 relay statistics Output Fields

Field Name	Field Description
DHCPv6 Packets dropped	<p>Number of packets discarded by the extended DHCPv6 relay agent application due to 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 DHCPv6 relay agent application. • Bad options—Number of packets discarded because invalid options were specified. • Bad send—Number of packets that the extended DHCP relay application could not send. • Bad src address—Number of packets discarded because the family type was not AF_INET6. • No client id—Number of packets discarded because they could not be matched to a client. • Lease Time Violation—Number of packets discarded because of a lease time violation • No safd—Number of packets discarded because they arrived on an unconfigured interface. • Short packet—Number of packets discarded because they were too short. • Relay hop count—Number of packets discarded because the hop count in the packet exceeded 32.

Table 30: show dhcpv6 relay statistics Output Fields (*continued*)

Field Name	Field Description
Messages received	<p>Number of DHCPv6 messages received.</p> <ul style="list-style-type: none"> DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE received DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT received DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION-REQUEST received DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE received DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST received DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM received DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW received DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND received DHCPV6_RELAY_REPL—Number of DHCPv6 PDUs of type RELAY-REPL received
Messages sent	<p>Number of DHCPv6 messages sent.</p> <ul style="list-style-type: none"> DHCPV6_ADVERTISE—Number of DHCPv6 ADVERTISE PDUs transmitted DHCP_REPLY—Number of DHCPv6 REPLY PDUs transmitted DHCP_RECONFIGURE—Number of DHCPv6 RECONFIGURE PDUs transmitted DHCP_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs transmitted
Packets forwarded	<p>Number of packets forwarded by the extended DHCPv6 relay agent application.</p> <ul style="list-style-type: none"> FWD REQUEST—Number of DHCPv6 REQUEST packets forwarded FWD REPLY—Number of DHCPv6 REPLY packets forwarded
External Server Response	<p>State of the external DHCP server responsiveness.</p>

Sample Output

show dhcpv6 relay statistics

```

user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total 1
    Lease Time Violation 1

Messages received:
    DHCPV6_DECLINE 0
    DHCPV6_SOLICIT 10
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE 0
    DHCPV6_REQUEST 10
    DHCPV6_CONFIRM 0
    DHCPV6_RENEW 0
    DHCPV6_REBIND 0
    DHCPV6_RELAY_REPL 0

Messages sent:
    DHCPV6_ADVERTISE 0
    DHCPV6_REPLY 0

```

DHCPV6_RECONFIGURE	0
DHCPV6_RELAY_FORW	0
Packets forwarded:	
Total	4
FWD REQUEST	2
FWD REPLY	2
External Server Response:	
State	Responding

show route extensive

List of Syntax	Syntax on page 439 Syntax (EX Series Switches) on page 439
Syntax	show route extensive <destination-prefix> <logical-system (all logical-system-name)>
Syntax (EX Series Switches)	show route extensive <destination-prefix>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	Display extensive information about the active entries in the routing tables.
Options	none —Display all active entries in the routing table. destination-prefix —(Optional) Display active entries for the specified address or range of addresses. logical-system (all logical-system-name) —(Optional) Perform this operation on all logical systems or on a particular logical system.
Required Privilege Level	view
List of Sample Output	show route extensive on page 446 show route extensive (Access Route) on page 452 show route extensive (BGP PIC Edge) on page 453 show route extensive (FRR and LFA) on page 453 show route extensive (Route Reflector) on page 454 show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs) on page 454 show route label detail (Multipoint LDP with Multicast-Only Fast Reroute) on page 455
Output Fields	Table 31 on page 439 describes the output fields for the show route extensive command. Output fields are listed in the approximate order in which they appear.

Table 31: show route extensive Output Fields

Field Name	Field Description
<i>routing-table-name</i>	Name of the routing table (for example, inet.0).
<i>number destinations</i>	Number of destinations for which there are routes in the routing table.

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
<i>number routes</i>	<p>Number of routes in the routing table and total number of routes in the following states:</p> <ul style="list-style-type: none"> • active (routes that are active). • holddown (routes that are in the pending state before being declared inactive). • hidden (routes that are not used because of a routing policy).
<i>route-destination</i> (entry, announced)	<p>Route destination (for example: 10.0.0.1/24). The entry value is the number of route for this destination, and the announced value is the number of routes being announced for this destination. Sometimes the route destination is presented in another format, such as:</p> <ul style="list-style-type: none"> • MPLS-label (for example, 80001). • interface-name (for example, ge-1/0/2). • neighbor-address:control-word-status:encapsulation type:vc-id:source (Layer 2 circuit only; for example, 10.1.1.195:NoCtrlWord:1:1:Local/96). <ul style="list-style-type: none"> • neighbor-address—Address of the neighbor. • control-word-status—Whether the use of the control word has been negotiated for this virtual circuit: NoCtrlWord or CtrlWord. • encapsulation type—Type of encapsulation, represented by a number: (1) Frame Relay DLCI, (2) ATM AAL5 VCC transport, (3) ATM transparent cell transport, (4) Ethernet, (5) VLAN Ethernet, (6) HDLC, (7) PPP, (8) ATM VCC cell transport, (10) ATM VPC cell transport. • vc-id—Virtual circuit identifier. • source—Source of the advertisement: Local or Remote.
TSI	Protocol header information.
label stacking	<p>(Next-to-the-last-hop routing device for MPLS only) Depth of the MPLS label stack, where the label-popping operation is needed to remove one or more labels from the top of the stack. A pair of routes is displayed, because the pop operation is performed only when the stack depth is two or more labels.</p> <ul style="list-style-type: none"> • S=0 route indicates that a packet with an incoming label stack depth of two or more exits this router with one fewer label (the label-popping operation is performed). • If there is no S= information, the route is a normal MPLS route, which has a stack depth of 1 (the label-popping operation is not performed).
[protocol, preference]	<p>Protocol from which the route was learned and the preference value for the route.</p> <ul style="list-style-type: none"> • +—A plus sign indicates the active route, which is the route installed from the routing table into the forwarding table. • -—A hyphen indicates the last active route. • *—An asterisk indicates that the route is both the active and the last active route. An asterisk before a to line indicates the best subpath to the route. <p>In every routing metric except for the BGP LocalPref attribute, a lesser value is preferred. In order to use common comparison routines, Junos OS stores the 1's complement of the LocalPref value in the Preference2 field. For example, if the LocalPref value for Route 1 is 100, the Preference2 value is -101. If the LocalPref value for Route 2 is 155, the Preference2 value is -156. Route 2 is preferred because it has a higher LocalPref value and a lower Preference2 value.</p>

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
Level	(IS-IS only). In IS-IS, a single autonomous system (AS) can be divided into smaller groups called areas. Routing between areas is organized hierarchically, allowing a domain to be administratively divided into smaller areas. This organization is accomplished by configuring Level 1 and Level 2 intermediate systems. Level 1 systems route within an area. When the destination is outside an area, they route toward a Level 2 system. Level 2 intermediate systems route between areas and toward other ASs.
Route Distinguisher	IP subnet augmented with a 64-bit prefix.
PMSI	Provider multicast service interface (MVPN routing table).
Next-hop type	Type of next hop. For a description of possible values for this field, see the Output Field table in the <i>show route detail</i> command.
Next-hop reference count	Number of references made to the next hop.
Flood nexthop branches exceed maximum message	Indicates that the number of flood next-hop branches exceeded the system limit of 32 branches, and only a subset of the flood next-hop branches were installed in the kernel.
Source	IP address of the route source.
Next hop	Network layer address of the directly reachable neighboring system.
via	<p>Interface used to reach the next hop. If there is more than one interface available to the next hop, the name of the interface that is actually used is followed by the word Selected. This field can also contain the following information:</p> <ul style="list-style-type: none"> • Weight—Value used to distinguish primary, secondary, and fast reroute backup routes. Weight information is available when MPLS label-switched path (LSP) link protection, node-link protection, or fast reroute is enabled, or when the standby state is enabled for secondary paths. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible. • Balance—Balance coefficient indicating how traffic of unequal cost is distributed among next hops when a routing device is performing unequal-cost load balancing. This information is available when you enable BGP multipath load balancing.
Label-switched-path lsp-path-name	Name of the LSP used to reach the next hop.
Label operation	MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).
Offset	Whether the metric has been increased or decreased by an offset value.
Interface	(Local only) Local interface name.
Protocol next hop	Network layer address of the remote routing device that advertised the prefix. This address is used to recursively derive a forwarding next hop.

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
<i>label-operation</i>	MPLS label and operation occurring at this routing device. The operation can be pop (where a label is removed from the top of the stack), push (where another label is added to the label stack), or swap (where a label is replaced by another label).
Indirect next hops	<p>When present, a list of nodes that are used to resolve the path to the next-hop destination, in the order that they are resolved.</p> <p>When BGP PIC Edge is enabled, the output lines that contain Indirect next hop: weight follow next hops that the software can use to repair paths where a link failure occurs. The next-hop weight has one of the following values:</p> <ul style="list-style-type: none"> • 0x1 indicates active next hops. • 0x4000 indicates passive next hops.
State	State of the route (a route can be in more than one state). See the Output Field table in the <i>show route detail</i> command.
Session ID	The BFD session ID number that represents the protection using MPLS fast reroute (FRR) and loop-free alternate (LFA).
Weight	<p>Weight for the backup path. If the weight of an indirect next hop is larger than zero, the weight value is shown.</p> <p>For sample output, see show route table.</p>

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
Inactive reason	<p>If the route is inactive, the reason for its current state is indicated. Typical reasons include:</p> <ul style="list-style-type: none"> • Active preferred—Currently active route was selected over this route. • Always compare MED—Path with a lower multiple exit discriminator (MED) is available. • AS path—Shorter AS path is available. • Cisco Non-deterministic MED selection—Cisco nondeterministic MED is enabled and a path with a lower MED is available. • Cluster list length—Path with a shorter cluster list length is available. • Forwarding use only—Path is only available for forwarding purposes. • IGP metric—Path through the next hop with a lower IGP metric is available. • IGP metric type—Path with a lower OSPF link-state advertisement type is available. • Interior > Exterior > Exterior via Interior—Direct, static, IGP, or EBGp path is available. • Local preference—Path with a higher local preference value is available. • Next hop address—Path with a lower metric next hop is available. • No difference—Path from a neighbor with a lower IP address is available. • Not Best in its group—Occurs when multiple peers of the same external AS advertise the same prefix and are grouped together in the selection process. When this reason is displayed, an additional reason is provided (typically one of the other reasons listed). • Number of gateways—Path with a higher number of next hops is available. • Origin—Path with a lower origin code is available. • OSPF version—Path does not support the indicated OSPF version. • RIB preference—Route from a higher-numbered routing table is available. • Route distinguisher—64-bit prefix added to IP subnets to make them unique. • Route metric or MED comparison—Route with a lower metric or MED is available. • Route preference—Route with a lower preference value is available. • Router ID—Path through a neighbor with a lower ID is available. • Unusable path—Path is not usable because of one of the following conditions: the route is damped, the route is rejected by an import policy, or the route is unresolved. • Update source—Last tiebreaker is the lowest IP address value.
Local AS	Autonomous system (AS) number of the local routing device.
Age	How long the route has been known.
AIGP	Accumulated interior gateway protocol (AIGP) BGP attribute.
Metric	Cost value of the indicated route. For routes within an AS, the cost is determined by IGP and the individual protocol metrics. For external routes, destinations, or routing domains, the cost is determined by a preference value.
MED-plus-IGP	Metric value for BGP path selection to which the IGP cost to the next-hop destination has been added.
TTL-Action	<p>For MPLS LSPs, state of the TTL propagation attribute. Can be enabled or disabled for all RSVP-signaled and LDP-signaled LSPs or for specific VRF routing instances.</p> <p>For sample output, see show route table.</p>

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
Task	Name of the protocol that has added the route.
Announcement bits	List of protocols that announce this route. n-Resolve inet indicates that the route is used for route resolution for next hops found in the routing table. n is an index used by Juniper Networks customer support only.
AS path	<p>AS path through which the route was learned. The letters at the end of the AS path indicate the path origin, providing an indication of the state of the route at the point at which the AS path originated:</p> <ul style="list-style-type: none"> • I—IGP. • E—EGP. • Recorded—The AS path is recorded by the sample process (sampled). • ?—Incomplete; typically, the AS path was aggregated. <p>When AS path numbers are included in the route, the format is as follows:</p> <ul style="list-style-type: none"> • []—Brackets enclose the local AS number associated with the AS path if more than one AS number is configured on the routing device, or if AS path prepending is configured. • { }—Braces enclose AS sets, which are groups of AS numbers in which the order does not matter. A set commonly results from route aggregation. The numbers in each AS set are displayed in ascending order. • ()—Parentheses enclose a confederation. • ([])—Parentheses and brackets enclose a confederation set. <p>NOTE: In Junos OS Release 10.3 and later, the AS path field displays an unrecognized attribute and associated hexadecimal value if BGP receives attribute 128 (attribute set) and you have not configured an independent domain in any routing instance.</p>
validation-state	<p>(BGP-learned routes) Validation status of the route:</p> <ul style="list-style-type: none"> • Invalid—Indicates that the prefix is found, but either the corresponding AS received from the EBGP peer is not the AS that appears in the database, or the prefix length in the BGP update message is longer than the maximum length permitted in the database. • Unknown—Indicates that the prefix is not among the prefixes or prefix ranges in the database. • Unverified—Indicates that origin validation is not enabled for the BGP peers. • Valid—Indicates that the prefix and autonomous system pair are found in the database.
FECs bound to route	Point-to-multipoint root address, multicast source address, and multicast group address when multipoint LDP (M-LDP) inband signaling is configured.
AS path: I <Originator>	(For route reflected output only) Originator ID attribute set by the route reflector.
Primary Upstream	When multipoint LDP with multicast-only fast reroute (MoFRR) is configured, the primary upstream path. MoFRR transmits a multicast join message from a receiver toward a source on a primary path, while also transmitting a secondary multicast join message from the receiver toward the source on a backup path.
RPF Nexthops	When multipoint LDP with MoFRR is configured, the reverse-path forwarding (RPF) next-hop information. Data packets are received from both the primary path and the secondary paths. The redundant packets are discarded at topology merge points due to the RPF checks.

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
Label	Multiple MPLS labels are used to control MoFRR stream selection. Each label represents a separate route, but each references the same interface list check. Only the primary label is forwarded while all others are dropped. Multiple interfaces can receive packets using the same label.
weight	Value used to distinguish MoFRR primary and backup routes. A lower weight value is preferred. Among routes with the same weight value, load balancing is possible.
VC Label	MPLS label assigned to the Layer 2 circuit virtual connection.
MTU	Maximum transmission unit (MTU) of the Layer 2 circuit.
VLAN ID	VLAN identifier of the Layer 2 circuit.
Cluster list	(For route reflected output only) Cluster ID sent by the route reflector.
Originator ID	(For route reflected output only) Address of router that originally sent the route to the route reflector.
Prefixes bound to route	Forwarding equivalent class (FEC) bound to this route. Applicable only to routes installed by LDP.
Communities	Community path attribute for the route. See the Output Field table in the <i>show route detail</i> command for all possible values for this field.
Layer2-info: encaps	Layer 2 encapsulation (for example, VPLS).
control flags	Control flags: none or Site Down.
mtu	Maximum transmission unit (MTU) information.
Label-Base, range	First label in a block of labels and label block size. A remote PE routing device uses this first label when sending traffic toward the advertising PE routing device.
status vector	Layer 2 VPN and VPLS network layer reachability information (NLRI).
Localpref	Local preference value included in the route.
Router ID	BGP router ID as advertised by the neighbor in the open message.
Primary Routing Table	In a routing table group, the name of the primary routing table in which the route resides.
Secondary Tables	In a routing table group, the name of one or more secondary tables in which the route resides.
Originating RIB	Name of the routing table whose active route was used to determine the forwarding next-hop entry in the resolution database. For example, in the case of inet.0 resolving through inet.0 and inet.3, this field indicates which routing table, inet.0 or inet.3, provided the best path for a particular prefix.
Node path count	Number of nodes in the path.

Table 31: show route extensive Output Fields (*continued*)

Field Name	Field Description
Forwarding nexthops	Number of forwarding next hops. The forwarding next hop is the network layer address of the directly reachable neighboring system (if applicable) and the interface used to reach it.

Sample Output

show route extensive

```

user@host> show route extensive
inet.0: 22 destinations, 23 routes (21 active, 0 holddown, 1 hidden)
10.10.0.0/16 (1 entry, 1 announced)
TSI:
KRT in-kernel 10.10.0.0/16 -> {192.168.71.254}
    *Static Preference: 5
        Next-hop reference count: 29
        Next hop: 192.168.71.254 via fxp0.0, selected
        State: <Active NoReadvrt Int Ext>
        Local AS: 69
        Age: 1:34:06
        Task: RT
        Announcement bits (2): 0-KRT 3-Resolve tree 2
        AS path: I

10.31.1.0/30 (2 entries, 1 announced)
    *Direct Preference: 0
        Next hop type: Interface
        Next-hop reference count: 2
        Next hop: via so-0/3/0.0, selected
        State: <Active Int>
        Local AS: 69
        Age: 1:32:40
        Task: IF
        Announcement bits (1): 3-Resolve tree 2
        AS path: I
    OSPF Preference: 10
        Next-hop reference count: 1
        Next hop: via so-0/3/0.0, selected
        State: <Int>
        Inactive reason: Route Preference
        Local AS: 69
        Age: 1:32:40 Metric: 1
        Area: 0.0.0.0
        Task: OSPF
        AS path: I

10.31.1.1/32 (1 entry, 1 announced)
    *Local Preference: 0
        Next hop type: Local
        Next-hop reference count: 7
        Interface: so-0/3/0.0
        State: <Active NoReadvrt Int>
        Local AS: 69
        Age: 1:32:43
        Task: IF
        Announcement bits (1): 3-Resolve tree 2
        AS path: I

```

```

...

10.31.2.0/30 (1 entry, 1 announced)
TSI:
KRT in-kerne1 10.31.2.0/30 -> {10.31.1.6}
    *OSPF   Preference: 10
            Next-hop reference count: 9
            Next hop: via so-0/3/0.0
            Next hop: 10.31.1.6 via ge-3/1/0.0, selected
            State: <Active Int>
            Local AS:    69
            Age: 1:32:19   Metric: 2
            Area: 0.0.0.0
            Task: OSPF
            Announcement bits (2): 0-KRT 3-Resolve tree 2
            AS path: I

...

224.0.0.2/32 (1 entry, 1 announced)
TSI:
KRT in-kerne1 224.0.0.2/32 -> {}
    *PIM    Preference: 0
            Next-hop reference count: 18
            State: <Active NoReadvrt Int>
            Local AS:    69
            Age: 1:34:08
            Task: PIM Recv
            Announcement bits (2): 0-KRT 3-Resolve tree 2
            AS path: I

...

224.0.0.22/32 (1 entry, 1 announced)
TSI:
KRT in-kerne1 224.0.0.22/32 -> {}
    *IGMP   Preference: 0
            Next-hop reference count: 18
            State: <Active NoReadvrt Int>
            Local AS:    69
            Age: 1:34:06
            Task: IGMP
            Announcement bits (2): 0-KRT 3-Resolve tree 2
            AS path: I

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.255.70.103/32 (1 entry, 1 announced)
State: <FlashAll>
    *RSVP   Preference: 7
            Next-hop reference count: 6
            Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
            Label-switched-path green-r1-r3
            Label operation: Push 100096
            State: <Active Int>
            Local AS:    69
            Age: 1:28:12   Metric: 2
            Task: RSVP
            Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
            AS path: I

```

```

10.255.71.238/32 (1 entry, 1 announced)
  State: <FlashAll>
  *RSVP   Preference: 7
          Next-hop reference count: 6
          Next hop: via so-0/3/0.0 weight 0x1, selected
          Label-switched-path green-r1-r2
          State: <Active Int>
          Local AS: 69
          Age: 1:28:12    Metric: 1
          Task: RSVP
          Announcement bits (2): 1-Resolve tree 1 2-Resolve tree 2
          AS path: I

private1___.inet.0: 2 destinations, 3 routes (2 active, 0 holddown, 0 hidden)

...

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

47.0005.80ff.f800.0000.0108.0001.0102.5507.1052/152 (1 entry, 0 announced)
  *Direct Preference: 0
          Next hop type: Interface
          Next-hop reference count: 1
          Next hop: via lo0.0, selected
          State: <Active Int>
          Local AS: 69
          Age: 1:34:07
          Task: IF
          AS path: I

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

0 (1 entry, 1 announced)
TSI:
KRT in-kernel 0 /36 -> {}
  *MPLS   Preference: 0
          Next hop type: Receive
          Next-hop reference count: 6
          State: <Active Int>
          Local AS: 69
          Age: 1:34:08    Metric: 1
          Task: MPLS
          Announcement bits (1): 0-KRT
          AS path: I

...

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
299840 (1 entry, 1 announced)
TSI:
KRT in-kernel 299840 /52 -> {indirect(1048575)}
  *RSVP   Preference: 7/2
          Next hop type: Flood
          Address: 0x9174a30
          Next-hop reference count: 4
          Next hop type: Router, Next hop index: 798
          Address: 0x9174c28
          Next-hop reference count: 2
          Next hop: 8.0.0.2 via lt-1/2/0.9 weight 0x1
          Label-switched-path R2-to-R4-2p2mp

```

```

Label operation: Pop
Next hop type: Router, Next hop index: 1048574
Address: 0x92544f0
Next-hop reference count: 2
Next hop: 7.0.0.2 via lt-1/2/0.7 weight 0x1
Label-switched-path R2-to-R200-p2mp
Label operation: Pop
Next hop: 6.0.0.2 via lt-1/2/0.5 weight 0x8001
Label operation: Pop
State: <Active Int>
Age: 1:29      Metric: 1
Task: RSVP
Announcement bits (1): 0-KRT
AS path: I...

```

800010 (1 entry, 1 announced)

TSI:

```

KRT in-kernel 800010 /36 -> {vt-3/2/0.32769}
  *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: via vt-3/2/0.32769, selected
    Label operation: Pop
    State: <Active Int>
    Age: 1:31:53
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

```

vt-3/2/0.32769 (1 entry, 1 announced)

TSI:

```

KRT in-kernel vt-3/2/0.32769.0 /16 -> {indirect(1048574)}
  *VPLS Preference: 7
    Next-hop reference count: 2
    Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1, selected
    Label-switched-path green-r1-r3
    Label operation: Push 800012, Push 100096(top)
    Protocol next hop: 10.255.70.103
    Push 800012
    Indirect next hop: 87272e4 1048574
    State: <Active Int>
    Age: 1:31:53      Metric2: 2
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 1-Common L2 VC
    AS path: I
    Communities: target:11111:1 Layer2-info: encaps:VPLS,
    control flags:, mtu: 0
    Indirect next hops: 1
      Protocol next hop: 10.255.70.103 Metric: 2
      Push 800012
      Indirect next hop: 87272e4 1048574
      Indirect path forwarding next hops: 1
        Next hop: 10.31.1.6 via ge-3/1/0.0 weight 0x1
        10.255.70.103/32 Originating RIB: inet.3
        Metric: 2      Node path count: 1
        Forwarding nexthops: 1
        Nexthop: 10.31.1.6 via ge-3/1/0.0

```

inet6.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)

abcd::10:255:71:52/128 (1 entry, 0 announced)

```
*Direct Preference: 0
  Next hop type: Interface
  Next-hop reference count: 1
  Next hop: via lo0.0, selected
  State: <Active Int>
  Local AS: 69
  Age: 1:34:07
  Task: IF
  AS path: I

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  *Direct Preference: 0
    Next hop type: Interface
    Next-hop reference count: 1
    Next hop: via lo0.0, selected
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:07
    Task: IF
    AS path: I

ff02::2/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::2/128 -> {}
  *PIM Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::d/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::d/128 -> {}
  *PIM Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:08
    Task: PIM Recv6
    Announcement bits (1): 0-KRT
    AS path: I

ff02::16/128 (1 entry, 1 announced)
TSI:
KRT in-kernel ff02::16/128 -> {}
  *MLD Preference: 0
    Next-hop reference count: 18
    State: <Active NoReadvrt Int>
    Local AS: 69
    Age: 1:34:06
    Task: MLD
    Announcement bits (1): 0-KRT
    AS path: I

private.inet6.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

fe80::280:42ff:fe10:f179/128 (1 entry, 0 announced)
  *Direct Preference: 0
```



```

Next hop type: Interface
Next-hop reference count: 1
Next hop: via lo0.16385, selected
State: <Active NoReadvrt Int>
Age: 1:34:07
Task: IF
AS path: I

green.l2vpn.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)

10.255.70.103:1:3:1/96 (1 entry, 1 announced)
  *BGP Preference: 170/-101
    Route Distinguisher: 10.255.70.103:1
    Next-hop reference count: 7
    Source: 10.255.70.103
    Protocol next hop: 10.255.70.103
    Indirect next hop: 2 no-forward
    State: <Secondary Active Int Ext>
    Local AS: 69 Peer AS: 69
    Age: 1:28:12 Metric2: 1
    Task: BGP_69.10.255.70.103+179
    Announcement bits (1): 0-green-l2vpn
    AS path: I
    Communities: target:11111:1 Layer2-info: encaps:VPLS,
    control flags:, mtu: 0
    Label-base: 800008, range: 8
    Localpref: 100
    Router ID: 10.255.70.103
    Primary Routing Table bgp.l2vpn.0

10.255.71.52:1:1:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699540
  *L2VPN Preference: 170/-1
    Next-hop reference count: 5
    Protocol next hop: 10.255.71.52
    Indirect next hop: 0 -
    State: <Active Int Ext>
    Age: 1:34:03 Metric2: 1
    Task: green-l2vpn
    Announcement bits (1): 1-BGP.0.0.0.0+179
    AS path: I
    Communities: Layer2-info: encaps:VPLS, control flags:Site-Down,
    mtu: 0
    Label-base: 800016, range: 8, status-vector: 0x9F

10.255.71.52:1:5:1/96 (1 entry, 1 announced)
TSI:
Page 0 idx 0 Type 1 val 8699528
  *L2VPN Preference: 170/-101
    Next-hop reference count: 5
    Protocol next hop: 10.255.71.52
    Indirect next hop: 0 -
    State: <Active Int Ext>
    Age: 1:34:03 Metric2: 1
    Task: green-l2vpn
    Announcement bits (1): 1-BGP.0.0.0.0+179
    AS path: I
    Communities: Layer2-info: encaps:VPLS, control flags:, mtu: 0
    Label-base: 800008, range: 8, status-vector: 0x9F

```

```

...

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

TSI:

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
    Label operation: Push 100000[0]
    Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
    State: <Active Int>
    Local AS: 99
    Age: 10:21
    Task: l2 circuit
    Announcement bits (1): 0-LDP
    AS path: I
    VC Label 100000, MTU 1500, VLAN ID 512

55.0.0.0/24 (1 entry, 1 announced)
TSI:
KRT queued (pending) add
  55.0.0.0/24 -> {Push 300112}
    *BGP Preference: 170/-101
      Next hop type: Router
      Address: 0x925c208
      Next-hop reference count: 2
      Source: 10.0.0.9
      Next hop: 10.0.0.9 via ge-1/2/0.15, selected
      Label operation: Push 300112
      Label TTL action: prop-ttl
      State: <Active Ext>
      Local AS: 7019 Peer AS: 13979
      Age: 1w0d 23:06:56
      AIGP: 25
      Task: BGP_13979.10.0.0.9+56732
      Announcement bits (1): 0-KRT
      AS path: 13979 7018 I
      Accepted
      Route Label: 300112
      Localpref: 100
      Router ID: 10.9.9.1

```

show route extensive (Access Route)

```

user@host> show route 13.160.0.102 extensive
inet.0: 39256 destinations, 39258 routes (39255 active, 0 holddown, 1 hidden)
13.160.0.102/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.102/32 -> {13.160.0.2}
OSPF area : 0.0.0.0, LSA ID : 13.160.0.102, LSA type : Extern
  *Access Preference: 13
    Next-hop reference count: 78472
    Next hop: 13.160.0.2 via fe-0/0/0.0, selected
    State: <Active Int>
  Age: 12
    Task: RPD Unix Domain Server./var/run/rpd_serv.local
    Announcement bits (2): 0-KRT 1-OSPFv2
    AS path: I

```

show route extensive (BGP PIC Edge)

```

user@host> show route 1.1.1.6 extensive
ed.inet.0: 6 destinations, 9 routes (6 active, 0 holddown, 0 hidden)
  1.1.1.6/32 (3 entries, 2 announced)
    State: <CalcForwarding>
TSI:
KRT in-kerne1 1.1.1.6/32 -> {indirect(1048574), indirect(1048577)}
Page 0 idx 0 Type 1 val 9219e30
  Nexthop: Self
  AS path: [2] 3 I
  Communities: target:2:1
  Path 1.1.1.6 from 1.1.1.4 Vector len 4. Val: 0
..
    #Multipath Preference: 255
      Next hop type: Indirect
      Address: 0x93f4010
      Next-hop reference count: 2
..
      Protocol next hop: 1.1.1.4
      Push 299824
      Indirect next hop: 944c000 1048574 INH Session ID: 0x3
      Indirect next hop: weight 0x1
      Protocol next hop: 1.1.1.5
      Push 299824
      Indirect next hop: 944c1d8 1048577 INH Session ID: 0x4
      Indirect next hop: weight 0x4000
      State: <ForwardingOnly Int Ext>
      Inactive reason: Forwarding use only
      Age: 25      Metric2: 15
      Validation State: unverified
      Task: RT
      Announcement bits (1): 0-KRT
      AS path: 3 I
      Communities: target:2:1

```

show route extensive (FRR and LFA)

```

user@host> show route 20.31.2.0 extensive
inet.0: 46 destinations, 49 routes (45 active, 0 holddown, 1 hidden)
  20.31.2.0/24 (2 entries, 1 announced)
    State: FlashAll
TSI:
KRT in-kerne1 20.31.2.0/24 -> {Push 299776, Push 299792}
  *RSVP Preference: 7/1
    Next hop type: Router, Next hop index: 1048574
    Address: 0xbbbc010
    Next-hop reference count: 5
    Next hop: 10.31.1.2 via ge-2/1/8.0 weight 0x1, selected
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299776
    Label TTL action: prop-ttl
    Session Id: 0x201
    Next hop: 10.31.2.2 via ge-2/1/4.0 weight 0x4001
    Label-switched-path europa-d-to-europa-e
    Label operation: Push 299792
    Label TTL action: prop-ttl
    Session Id: 0x202
    State: Active Int
    Local AS: 100
    Age: 5:31 Metric: 2

```

```

Task: RSVP
Announcement bits (1): 0-KRT
AS path: I
OSPF Preference: 10
Next hop type: Router, Next hop index: 615
Address: 0xb9d78c4
Next-hop reference count: 7
Next hop: 10.31.1.2 via ge-2/1/8.0, selected
Session Id: 0x201
State: Int
Inactive reason: Route Preference
Local AS: 100
Age: 5:35 Metric: 3
Area: 0.0.0.0
Task: OSPF
AS path: I

```

show route extensive (Route Reflector)

```

user@host> show route extensive
1.0.0.0/8 (1 entry, 1 announced)

TSI:
KRT in-kernel 1.0.0.0/8 -> {indirect(40)}
*BGP Preference: 170/-101
Source: 192.168.4.214
Protocol next hop: 207.17.136.192 Indirect next hop: 84ac908 40
State: <Active Int Ext>
Local AS: 10458 Peer AS: 10458
Age: 3:09 Metric: 0 Metric2: 0
Task: BGP_10458.192.168.4.214+1033
Announcement bits (2): 0-KRT 4-Resolve inet.0
AS path: 3944 7777 I <Originator>
Cluster list: 1.1.1.1
Originator ID: 10.255.245.88
Communities: 7777:7777
Localpref: 100
Router ID: 4.4.4.4
Indirect next hops: 1
    Protocol next hop: 207.17.136.192 Metric: 0
    Indirect next hop: 84ac908 40
    Indirect path forwarding next hops: 0
    Next hop type: Discard

```

show route label detail (Multipoint LDP Inband Signaling for Point-to-Multipoint LSPs)

```

user@host> show route label 299872 detail
mpls.0: 13 destinations, 13 routes (13 active, 0 holddown, 0 hidden)
299872 (1 entry, 1 announced)
*LDP Preference: 9
Next hop type: Flood
Next-hop reference count: 3
Address: 0x9097d90
Next hop: via vt-0/1/0.1
Next-hop index: 661
Label operation: Pop
Address: 0x9172130
Next hop: via so-0/0/3.0
Next-hop index: 654
Label operation: Swap 299872
State: **Active Int>

```

```

Local AS: 1001
Age: 8:20      Metric: 1
Task: LDP
Announcement bits (1): 0-KRT
AS path: I
FECs bound to route: P2MP root-addr 10.255.72.166, grp 232.1.1.1,
src 192.168.142.2

```

show route label detail (Multipoint LDP with Multicast-Only Fast Reroute)

```
user@host> show route label 301568 detail
```

```

mpls.0: 18 destinations, 18 routes (18 active, 0 holddown, 0 hidden)
301568 (1 entry, 1 announced)
  *LDP    Preference: 9
          Next hop type: Flood
          Address: 0x2735208
          Next-hop reference count: 3
          Next hop type: Router, Next hop index: 1397
          Address: 0x2735d2c
          Next-hop reference count: 3
          Next hop: 1.3.8.2 via ge-1/2/22.0
          Label operation: Pop
          Load balance label: None;
          Next hop type: Router, Next hop index: 1395
          Address: 0x2736290
          Next-hop reference count: 3
          Next hop: 1.3.4.2 via ge-1/2/18.0
          Label operation: Pop
          Load balance label: None;
          State: <Active Int AckRequest MulticastRPF>
          Local AS: 10
          Age: 54:05      Metric: 1
          Validation State: unverified
          Task: LDP
          Announcement bits (1): 0-KRT
          AS path: I
          FECs bound to route: P2MP root-addr 1.1.1.1, grp: 232.1.1.1, src:
192.168.219.11
          Primary Upstream : 1.1.1.3:0--1.1.1.2:0
            RPF Nexthops :
              ge-1/2/15.0, 1.2.94.1, Label: 301568, weight: 0x1
              ge-1/2/14.0, 1.2.3.1, Label: 301568, weight: 0x1
          Backup Upstream : 1.1.1.3:0--1.1.1.6:0
            RPF Nexthops :
              ge-1/2/20.0, 1.2.96.1, Label: 301584, weight: 0xffffe
              ge-1/2/19.0, 1.3.6.1, Label: 301584, weight: 0xffffe

```

show route protocol

List of Syntax	Syntax on page 456 Syntax (EX Series Switches) on page 456
Syntax	<code>show route protocol <i>protocol</i></code> <code><brief detail extensive terse></code> <code><logical-system (all <i>logical-system-name</i>)></code>
Syntax (EX Series Switches)	<code>show route protocol <i>protocol</i></code> <code><brief detail extensive terse></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. ospf2 and ospf3 options introduced in Junos OS Release 9.2. ospf2 and ospf3 options introduced in Junos OS Release 9.2 for EX Series switches. flow option introduced in Junos OS Release 10.0. flow option introduced in Junos OS Release 10.0 for EX Series switches.
Description	Display the route entries in the routing table that were learned from a particular protocol.
Options	brief detail extensive terse —(Optional) Display the specified level of output. If you do not specify a level of output, the system defaults to brief . logical-system (all <i>logical-system-name</i>) —(Optional) Perform this operation on all logical systems or on a particular logical system. <i>protocol</i> —Protocol from which the route was learned: <ul style="list-style-type: none">• access—Access route for use by DHCP application• access-internal—Access-internal route for use by DHCP application• aggregate—Locally generated aggregate route• arp—Route learned through the Address Resolution Protocol• atmvpn—Asynchronous Transfer Mode virtual private network• bgp—Border Gateway Protocol• ccc—Circuit cross-connect• direct—Directly connected route• dvmrp—Distance Vector Multicast Routing Protocol• esis—End System-to-Intermediate System• flow—Locally defined flow-specification route• frr—Precomputed protection route or backup route used when a link goes down• isis—Intermediate System-to-Intermediate System• ldp—Label Distribution Protocol• l2circuit—Layer 2 circuit

- **l2vpn**—Layer 2 virtual private network
- **local**—Local address
- **mpls**—Multiprotocol Label Switching
- **msdp**—Multicast Source Discovery Protocol
- **ospf**—Open Shortest Path First versions 2 and 3
- **ospf2**—Open Shortest Path First versions 2 only
- **ospf3**—Open Shortest Path First version 3 only
- **pim**—Protocol Independent Multicast
- **rip**—Routing Information Protocol
- **ripng**—Routing Information Protocol next generation
- **rsvp**—Resource Reservation Protocol
- **rtarget**—Local route target virtual private network
- **static**—Statically defined route
- **tunnel**—Dynamic tunnel
- **vpn**—Virtual private network



NOTE: EX Series switches run a subset of these protocols. See the switch CLI for details.

Required Privilege Level view

Related Documentation • *MPLS Feature Support on QFX Series and EX4600 Switches*

List of Sample Output

- [show route protocol access on page 458](#)
- [show route protocol access-internal extensive on page 458](#)
- [show route protocol arp on page 458](#)
- [show route protocol bgp on page 459](#)
- [show route protocol bgp detail on page 459](#)
- [show route protocol bgp extensive on page 459](#)
- [show route protocol bgp terse on page 460](#)
- [show route protocol direct on page 460](#)
- [show route protocol frr on page 461](#)
- [show route protocol l2circuit detail on page 461](#)
- [show route protocol l2vpn extensive on page 462](#)
- [show route protocol ldp on page 463](#)
- [show route protocol ldp extensive on page 463](#)
- [show route protocol ospf \(Layer 3 VPN\) on page 464](#)
- [show route protocol ospf detail on page 465](#)

[show route protocol rip on page 465](#)

[show route protocol rip detail on page 465](#)

[show route protocol ripng table inet6 on page 466](#)

[show route protocol static detail on page 466](#)

Output Fields For information about output fields, see the output field tables for the *show route* command, the *show route detail* command, the [show route extensive](#) command, or the *show route terse* command.

Sample Output

show route protocol access

```
user@host> show route protocol access
inet.0: 30380 destinations, 30382 routes (30379 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

13.160.0.3/32      *[Access/13] 00:00:09
                   > to 13.160.0.2 via fe-0/0/0.0
13.160.0.4/32      *[Access/13] 00:00:09
                   > to 13.160.0.2 via fe-0/0/0.0
13.160.0.5/32      *[Access/13] 00:00:09
                   > to 13.160.0.2 via fe-0/0/0.0
```

show route protocol access-internal extensive

```
user@host> show route protocol access-internal 13.160.0.19 extensive
inet.0: 100020 destinations, 100022 routes (100019 active, 0 holddown, 1 hidden)
13.160.0.19/32 (1 entry, 1 announced)
TSI:
KRT in-kernel 13.160.0.19/32 -> {13.160.0.2}
    *Access-internal Preference: 12
        Next-hop reference count: 200000
        Next hop: 13.160.0.2 via fe-0/0/0.0, selected
        State: <Active Int>
    Age: 36
        Task: RPD Unix Domain Server./var/run/rpd_serv.local
        Announcement bits (1): 0-KRT
        AS path: I
```

show route protocol arp

```
user@host> show route protocol arp
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32      [ARP/4294967293] 00:04:35, from 20.20.1.1
                   Unusable
20.20.1.4/32      [ARP/4294967293] 00:04:35, from 20.20.1.1
                   Unusable
20.20.1.5/32      [ARP/4294967293] 00:04:32, from 20.20.1.1
                   Unusable
20.20.1.6/32      [ARP/4294967293] 00:04:34, from 20.20.1.1
                   Unusable
20.20.1.7/32      [ARP/4294967293] 00:04:35, from 20.20.1.1
                   Unusable
```



```

20.20.1.8/32      [ARP/4294967293] 00:04:35, from 20.20.1.1
                  Unusable
20.20.1.9/32      [ARP/4294967293] 00:04:35, from 20.20.1.1
                  Unusable
20.20.1.10/32     [ARP/4294967293] 00:04:35, from 20.20.1.1
                  Unusable
20.20.1.11/32     [ARP/4294967293] 00:04:33, from 20.20.1.1
                  Unusable
20.20.1.12/32     [ARP/4294967293] 00:04:33, from 20.20.1.1
                  Unusable
20.20.1.13/32     [ARP/4294967293] 00:04:33, from 20.20.1.1
                  Unusable
...

```

show route protocol bgp

```

user@host> show route protocol bgp 192.168.64.0/21
inet.0: 335832 destinations, 335833 routes (335383 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.64.0/21    *[BGP/170] 6d 10:41:16, localpref 100, from 192.168.69.71
                  AS path: 10458 14203 2914 4788 4788 I
                  > to 192.168.167.254 via fxp0.0

```

show route protocol bgp detail

```

user@host> show route protocol bgp 66.117.63.0/24 detail
inet.0: 335805 destinations, 335806 routes (335356 active, 0 holddown, 450 hidden)
66.117.63.0/24    (1 entry, 1 announced)
   *BGP           Preference: 170/-101
                   Next hop type: Indirect
                   Next-hop reference count: 1006436
                   Source: 192.168.69.71
                   Next hop type: Router, Next hop index: 324
                   Next hop: 192.168.167.254 via fxp0.0, selected
                   Protocol next hop: 192.168.69.71
                   Indirect next hop: 8e166c0 342
                   State: <Active Ext>
                   Local AS: 69 Peer AS: 10458
                   Age: 6d 10:42:42 Metric2: 0
                   Task: BGP_10458.192.168.69.71+179
                   Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree

1

   AS path: 10458 14203 2914 4788 4788 I
   Communities: 2914:410 2914:2403 2914:3400
   Accepted
   Localpref: 100
   Router ID: 207.17.136.192

```

show route protocol bgp extensive

```

user@host> show route protocol bgp 192.168.64.0/21 extensive

inet.0: 335827 destinations, 335828 routes (335378 active, 0 holddown, 450 hidden)
192.168.64.0/21 (1 entry, 1 announced)
TSI:
KRT in-kernel 1.9.0.0/16 -> {indirect(342)}
Page 0 idx 1 Type 1 val db31a80
  Nexthop: Self
    AS path: [69] 10458 14203 2914 4788 4788 I
    Communities: 2914:410 2914:2403 2914:3400
  Path 1.9.0.0 from 192.168.69.71 Vector len 4. Val: 1

```

```

*BGP      Preference: 170/-101
          Next hop type: Indirect
          Next-hop reference count: 1006502
          Source: 192.168.69.71
          Next hop type: Router, Next hop index: 324
          Next hop: 192.168.167.254 via fxp0.0, selected
          Protocol next hop: 192.168.69.71
          Indirect next hop: 8e166c0 342
          State: <Active Ext>
          Local AS: 69 Peer AS: 10458
          Age: 6d 10:44:45 Metric2: 0
          Task: BGP_10458.192.168.69.71+179
          Announcement bits (3): 0-KRT 2-BGP RT Background 3-Resolve tree

1
  AS path: 10458 14203 2914 4788 4788 I
  Communities: 2914:410 2914:2403 2914:3400
  Accepted
  Localpref: 100
  Router ID: 207.17.136.192
  Indirect next hops: 1
    Protocol next hop: 192.168.69.71
    Indirect next hop: 8e166c0 342
    Indirect path forwarding next hops: 1
      Next hop type: Router
      Next hop: 192.168.167.254 via fxp0.0
    192.168.0.0/16 Originating RIB: inet.0
    Node path count: 1
    Forwarding nexthops: 1
      Nexthop: 192.168.167.254 via fxp0.0

```

show route protocol bgp terse

```

user@host> show route protocol bgp 192.168.64.0/21 terse

inet.0: 24 destinations, 32 routes (23 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

A Destination      P Prf  Metric 1  Metric 2  Next hop      AS path
192.168.64.0/21   B 170      100          >100.1.3.2    10023 21 I

```

show route protocol direct

```

user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

8.8.8.0/24        *[Direct/0] 17w0d 10:31:49
> via fe-1/3/1.0
10.255.165.1/32   *[Direct/0] 25w4d 04:13:18
> via lo0.0
30.30.30.0/24     *[Direct/0] 17w0d 23:06:26
> via fe-1/3/2.0
192.168.164.0/22  *[Direct/0] 25w4d 04:13:20
> via fxp0.0

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

47.0005.80ff.f800.0000.0108.0001.0102.5516.5001/152
*[Direct/0] 25w4d 04:13:21

```

```

> via lo0.0

inet6.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

abcd::10:255:165:1/128
    *[Direct/0] 25w4d 04:13:21
    > via lo0.0
fe80::2a0:a5ff:fe12:ad7/128
    *[Direct/0] 25w4d 04:13:21
    > via lo0.0

```

show route protocol frr

```

user@host> show route protocol frr
inet.0: 43 destinations, 43 routes (42 active, 0 holddown, 1 hidden)

inet.3: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)

cust1.inet.0: 1033 destinations, 2043 routes (1033 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

20.20.1.3/32      *[FRR/200] 00:05:38, from 20.20.1.1
                  > to 20.20.1.3 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.4/32      *[FRR/200] 00:05:38, from 20.20.1.1
                  > to 20.20.1.4 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.5/32      *[FRR/200] 00:05:35, from 20.20.1.1
                  > to 20.20.1.5 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.6/32      *[FRR/200] 00:05:37, from 20.20.1.1
                  > to 20.20.1.6 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.7/32      *[FRR/200] 00:05:38, from 20.20.1.1
                  > to 20.20.1.7 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.8/32      *[FRR/200] 00:05:38, from 20.20.1.1
                  > to 20.20.1.8 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.9/32      *[FRR/200] 00:05:38, from 20.20.1.1
                  > to 20.20.1.9 via ge-4/1/0.0
                  to 10.10.15.1 via ge-0/2/4.0, Push 16, Push 299792(top)
20.20.1.10/32     *[FRR/200] 00:05:38, from 20.20.1.1
...

```

show route protocol l2circuit detail

```

user@host> show route protocol l2circuit detail

mpls.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
100000 (1 entry, 1 announced)
    *L2CKT Preference: 7
        Next hop: via ge-2/0/0.0, selected
        Label operation: Pop      Offset: 4
        State: <Active Int>
        Local AS: 99
        Age: 9:52
        Task: Common L2 VC
        Announcement bits (1): 0-KRT
        AS path: I

```

```

ge-2/0/0.0 (1 entry, 1 announced)
  *L2CKT Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
    Label operation: Push 100000, Push 100000(top)[0] Offset: -4
    Protocol next hop: 10.245.255.63
    Push 100000 Offset: -4
    Indirect next hop: 86af0c0 298
    State: <Active Int>
    Local AS: 99
    Age: 9:52
    Task: Common L2 VC
    Announcement bits (2): 0-KRT 1-Common L2 VC
    AS path: I

l2circuit.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

10.245.255.63:CtrlWord:4:3:Local/96 (1 entry, 1 announced)
  *L2CKT Preference: 7
    Next hop: via so-1/1/2.0 weight 1, selected
    Label-switched-path my-lsp
    Label operation: Push 100000[0]
    Protocol next hop: 10.245.255.63 Indirect next hop: 86af000 296
    State: <Active Int>
    Local AS: 99
    Age: 10:21
    Task: l2 circuit
    Announcement bits (1): 0-LDP
    AS path: I
    VC Label 100000, MTU 1500, VLAN ID 512

```

show route protocol l2vpn extensive

```

user@host> show route protocol l2vpn extensive

inet.0: 14 destinations, 15 routes (13 active, 0 holddown, 1 hidden)

inet.3: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

iso.0: 1 destinations, 1 routes (1 active, 0 holddown, 0 hidden)

mpls.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
800001 (1 entry, 1 announced)
TSI:
KRT in-kernel 800001 /36 -> {so-0/0/0.0}
  *L2VPN Preference: 7
    Next hop: via so-0/0/0.0 weight 49087 balance 97%, selected
    Label operation: Pop Offset: 4
    State: <Active Int>
    Local AS: 69
    Age: 7:48
    Task: Common L2 VC
    Announcement bits (1): 0-KRT
    AS path: I

so-0/0/0.0 (1 entry, 1 announced)
TSI:
KRT in-kernel so-0/0/0.0 /16 -> {indirect(288)}
  *L2VPN Preference: 7
    Next hop: via so-0/0/1.0, selected

```

```

Label operation: Push 800000 Offset: -4
Protocol next hop: 10.255.14.220
Push 800000 Offset: -4
  Indirect next hop: 85142a0 288
State: <Active Int>
Local AS: 69
Age: 7:48
Task: Common L2 VC
Announcement bits (2): 0-KRT 1-Common L2 VC
AS path: I
Communities: target:69:1 Layer2-info: encaps:PPP,
control flags:2, mtu: 0

```

show route protocol ldp

```

user@host> show route protocol ldp
inet.0: 12 destinations, 13 routes (12 active, 0 holddown, 0 hidden)

inet.3: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

192.168.16.1/32    *[LDP/9] 1d 23:03:35, metric 1
                  > via t1-4/0/0.0, Push 100000
192.168.17.1/32    *[LDP/9] 1d 23:03:35, metric 1
                  > via t1-4/0/0.0

private1___.inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

100064            *[LDP/9] 1d 23:03:35, metric 1
                  > via t1-4/0/0.0, Pop
100064(S=0)        *[LDP/9] 1d 23:03:35, metric 1
                  > via t1-4/0/0.0, Pop
100080            *[LDP/9] 1d 23:03:35, metric 1
                  > via t1-4/0/0.0, Swap 100000

```

show route protocol ldp extensive

```

user@host> show route protocol ldp extensive
192.168.16.1/32 (1 entry, 1 announced)
  State: <FlashAll>
  *LDP    Preference: 9
          Next-hop reference count: 3
          Next hop: via t1-4/0/0.0, selected
          Label operation: Push 100000
          State: <Active Int>
          Local AS: 65500
          Age: 1d 23:03:58      Metric: 1
          Task: LDP
          Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
          AS path: I

192.168.17.1/32 (1 entry, 1 announced)
  State: <FlashAll>
  *LDP    Preference: 9
          Next-hop reference count: 3
          Next hop: via t1-4/0/0.0, selected
          State: <Active Int>
          Local AS: 65500

```

```

Age: 1d 23:03:58      Metric: 1
Task: LDP
Announcement bits (2): 0-Resolve tree 1 2-Resolve tree 2
AS path: I

private1__inet.0: 2 destinations, 2 routes (2 active, 0 holddown, 0 hidden)

mpls.0: 6 destinations, 6 routes (6 active, 0 holddown, 0 hidden)

100064 (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /36 -> {t1-4/0/0.0}
    *LDP      Preference: 9
              Next-hop reference count: 2
              Next hop: via t1-4/0/0.0, selected
              State: <Active Int>
              Local AS: 65500
              Age: 1d 23:03:58      Metric: 1
              Task: LDP
              Announcement bits (1): 0-KRT
              AS path: I
              Prefixes bound to route: 192.168.17.1/32

100064(S=0) (1 entry, 1 announced)
TSI:
KRT in-kernel 100064 /40 -> {t1-4/0/0.0}
    *LDP      Preference: 9
              Next-hop reference count: 2
              Next hop: via t1-4/0/0.0, selected
              Label operation: Pop
              State: <Active Int>
              Local AS: 65500
              Age: 1d 23:03:58      Metric: 1
              Task: LDP
              Announcement bits (1): 0-KRT
              AS path: I

100080 (1 entry, 1 announced)
TSI:
KRT in-kernel 100080 /36 -> {t1-4/0/0.0}
    *LDP      Preference: 9
              Next-hop reference count: 2
              Next hop: via t1-4/0/0.0, selected
              Label operation: Swap 100000
              State: <Active Int>
              Local AS: 65500
              Age: 1d 23:03:58      Metric: 1
              Task: LDP
              Announcement bits (1): 0-KRT
              AS path: I
              Prefixes bound to route: 192.168.16.1/32

```

show route protocol ospf (Layer 3 VPN)

```

user@host> show route protocol ospf
inet.0: 40 destinations, 40 routes (39 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.4/30      * [OSPF/10] 00:05:18, metric 4
                  > via t3-3/2/0.0
10.39.1.8/30      [OSPF/10] 00:05:18, metric 2

```

```

> via t3-3/2/0.0
10.255.14.171/32  *[OSPF/10] 00:05:18, metric 4
> via t3-3/2/0.0
10.255.14.179/32  *[OSPF/10] 00:05:18, metric 2
> via t3-3/2/0.0
224.0.0.5/32     *[OSPF/10] 20:25:55, metric 1

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30    [OSPF/10] 00:05:43, metric 1
> via so-0/2/2.0
10.255.14.173/32 *[OSPF/10] 00:05:43, metric 1
> via so-0/2/2.0
224.0.0.5/32    *[OSPF/10] 20:26:20, metric 1

```

show route protocol ospf detail

```

user@host> show route protocol ospf detail
VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

10.39.1.16/30 (2 entries, 0 announced)
  OSPF   Preference: 10
        Nexthop: via so-0/2/2.0, selected
        State: <Int>
        Inactive reason: Route Preference
        Age: 6:25      Metric: 1
        Area: 0.0.0.0
        Task: VPN-AB-OSPF
        AS path: I
        Communities: Route-Type:0.0.0.0:1:0

...

```

show route protocol rip

```

user@host> show route protocol rip
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32  *[RIP/100] 20:24:34, metric 2
> to 10.39.1.22 via t3-0/2/2.0
224.0.0.9/32     *[RIP/100] 00:03:59, metric 1

```

show route protocol rip detail

```

user@host> show route protocol rip detail
inet.0: 26 destinations, 27 routes (25 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

VPN-AB.inet.0: 5 destinations, 5 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both
10.255.14.177/32 (1 entry, 1 announced)
  *RIP   Preference: 100
        Nexthop: 10.39.1.22 via t3-0/2/2.0, selected
        State: <Active Int>
        Age: 20:25:02  Metric: 2
        Task: VPN-AB-RIPv2
        Announcement bits (2): 0-KRT 2-BGP.0.0.0.0+179

```

```
AS path: I
Route learned from 10.39.1.22 expires in 96 seconds
```

show route protocol ripng table inet6

```
user@host> show route protocol ripng table inet6
inet6.0: 4215 destinations, 4215 routes (4214 active, 0 holddown, 1 hidden)
+ = Active Route, - = Last Active, * = Both

1111::1/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::2/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::3/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::4/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::5/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
1111::6/128      *[RIPng/100] 02:13:33, metric 2
                  > to fe80::2a0:a5ff:fe3d:56 via t3-0/2/0.0
```

show route protocol static detail

```
user@host> show route protocol static detail
inet.0: 3 destinations, 3 routes (3 active, 0 holddown, 0 hidden)
10.5.0.0/16 (1 entry, 1 announced)
    *Static Preference: 5
        Next hop type: Router, Next hop index: 324
        Address: 0x9274010
        Next-hop reference count: 27
        Next hop: 192.168.187.126 via fxp0.0, selected
        Session Id: 0x0
        State: <Active NoReadvrt Int Ext>
        Age: 7w3d 21:24:25
        Validation State: unverified
        Task: RT
        Announcement bits (1): 0-KRT
        AS path: I

10.10.0.0/16 (1 entry, 1 announced)
    *Static Preference: 5
        Next hop type: Router, Next hop index: 324
        Address: 0x9274010
        Next-hop reference count: 27
        Next hop: 192.168.187.126 via fxp0.0, selected
        Session Id: 0x0
        State: <Active NoReadvrt Int Ext>
        Age: 7w3d 21:24:25
        Validation State: unverified
        Task: RT
        Announcement bits (1): 0-KRT
        AS path: I

10.13.10.0/23 (1 entry, 1 announced)
    *Static Preference: 5
        Next hop type: Router, Next hop index: 324
        Address: 0x9274010
        Next-hop reference count: 27
        Next hop: 192.168.187.126 via fxp0.0, selected
        Session Id: 0x0
```



State: <Active NoReadvrt Int Ext>
Age: 7w3d 21:24:25
Validation State: unverified
Task: RT
Announcement bits (1): 0-KRT
AS path: I

CHAPTER 19

Other Operational Commands

- clear security pki local-certificate
- clear system services dhcp binding
- clear system services dhcp conflict
- clear system services dhcp statistics
- request ipsec switch
- request security certificate (signed)
- request security certificate (unsigned)
- request security key-pair
- request security pki generate-key-pair
- request security pki local-certificate generate-self-signed
- show security pki local-certificate
- show system services dhcp binding
- show system services dhcp conflict
- show system services dhcp global
- show system services dhcp pool
- show system services dhcp statistics
- show system services service-deployment
- ssh
- telnet

clear security pki local-certificate

Syntax	clear security pki local-certificate <all certificate-id <i>certificate-id-name</i> system-generated>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Delete local digital certificates, certificate requests, and the corresponding public/private key pairs from the switch.
Options	all —(Optional) Delete all local digital certificates, certificate requests, and the corresponding public and private key pairs from the router.
<div> NOTE: This option does not delete the automatically generated self-signed certificate or its public/private key pair.</div>	
certificate-id <i>certificate-id-name</i> —(Optional) Delete the specified local digital certificate and corresponding public and private key pair.	
system-generated —(Optional) Delete the automatically generated self-signed certificate.	
Required Privilege Level	clear
Related Documentation	<ul style="list-style-type: none">• Deleting Self-Signed Certificates (CLI Procedure) on page 78
List of Sample Output	clear security pki local-certificate all on page 470
Output Fields	This command produces no output.

Sample Output

clear security pki local-certificate all

```
user@switch> clear security pki local-certificate all
```

clear system services dhcp binding

Syntax	clear system services dhcp binding <address>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Remove obsolete IP address bindings on a Dynamic Host Configuration Protocol (DHCP) server and return them to the IP address pool.
Options	address —(Optional) Remove a specific IP address binding and return it to the address pool.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none">• show system services dhcp binding on page 484
List of Sample Output	clear system services dhcp binding on page 471
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp binding

```
user@host> clear system services dhcp binding
```

clear system services dhcp conflict

Syntax	clear system services dhcp conflict <address>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Remove IP addresses from the Dynamic Host Configuration Protocol (DHCP) server conflict list and return them to the IP address pool.
Options	address —(Optional) Remove a specific IP address from the conflict list and return it to the address pool.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none">• show system services dhcp conflict on page 487
List of Sample Output	clear system services dhcp conflict on page 472
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp conflict

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

clear system services dhcp statistics

Syntax	clear system services dhcp statistics
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Clear Dynamic Host Configuration Protocol (DHCP) server statistics.
Options	This command has no options.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none">• show system services dhcp statistics on page 492
List of Sample Output	clear system services dhcp statistics on page 473
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

clear system services dhcp statistics

```
user@host> clear system services dhcp statistics
```

request ipsec switch

Syntax	<code>request ipsec switch (interface <es-fpc/pic/port> security-associations <sa-name>)</code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series, PTX Series, and T Series routers and EX Series switches only) Manually switch from the primary to the backup encryption services interface, or switch from the primary to the backup IP Security (IPsec) tunnel.
Options	<code>interface <es-fpc/pic/port></code> —Switch to the backup encryption interface. <code>security-associations <sa-name></code> —Switch to the backup tunnel.
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none">• show ipsec redundancy
List of Sample Output	request ipsec switch on page 474
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request ipsec switch

```
user@host> request ipsec switch security-associations sa-private
```


request security certificate (signed)

Syntax	<code>request security certificate enroll filename <i>filename</i> subject <i>subject</i> alternative-subject <i>alternative-subject</i> certification-authority <i>certification-authority</i> encoding (binary pem) key-file <i>key-file</i> domain-name <i>domain-name</i></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a signed certificate from a certificate authority (CA). The signed certificate validates the CA and the owner of the certificate. The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
Options	<p>filename <i>filename</i>—File that stores the certificate.</p> <p>subject <i>subject</i>—Distinguished name (dn), which consists of a set of components—for example, an organization (o), an organization unit (ou), a country (c), and a locality (l).</p> <p>alternative-subject <i>alternative-subject</i>—Tunnel source address.</p> <p>certification-authority <i>certification-authority</i>—Name of the certificate authority profile in the configuration.</p> <p>encoding (binary pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default format is binary.</p> <p>key-file <i>key-file</i>—File containing a local private key.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name.</p>
Required Privilege Level	maintenance
List of Sample Output	request security certificate (signed) on page 475
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate (signed)

```

user@host> request security certificate enroll filename host.crt subject c=uk,o=london
alternative-subject 10.50.1.4 certification-authority verisign key-file host-1.prv domain-name
host.juniper.net
CA name: juniper.net CA file: ca_verisign
local pub/private key pair: host.prv
subject: c=uk,o=london domain name: host.juniper.net
alternative subject: 10.50.1.4
Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
the key management process (kmd) log file at /var/log/kmd. <-----

```


request security certificate (unsigned)

Syntax	<code>request security certificate enroll filename <i>filename</i> ca-file <i>ca-file</i> ca-name <i>ca-name</i> encoding (binary perm) url <i>url</i></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Obtain a certificate from a certificate authority (CA). The results are saved in a specified file to the <code>/var/etc/ikecert</code> directory.
Options	<p>filename <i>filename</i>—File that stores the public key certificate.</p> <p>ca-file <i>ca-file</i>—Name of the certificate authority profile in the configuration.</p> <p>ca-name <i>ca-name</i>—Name of the certificate authority.</p> <p>encoding (binary pem)—File format used for the certificate. The format can be a binary file or privacy-enhanced mail (PEM), an ASCII base64-encoded format. The default value is binary.</p> <p>url <i>url</i>—Certificate authority URL.</p>
Required Privilege Level	maintenance
List of Sample Output	request security certificate (unsigned) on page 477
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security certificate (unsigned)

```
user@host> request security certificate enroll filename ca_verisign ca-file verisign ca-name
juniper.net urlxyzcompany URL
http://<verisign ca-name xyzcompany url>/cgi-bin/pkiclient.exe CA name: juniper.net
CA file: verisign Encoding: binary
Certificate enrollment has started. To view the status of your enrollment, check
the key management process (kmd) log file at /var/log/kmd. <-----
```

request security key-pair

Syntax	<code>request security key-pair <i>filename</i></code> <code><size <i>key-size</i>></code> <code><type (rsa dsa)></code>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(Encryption interface on M Series and T Series routers and EX Series switches only) Generate a public and private key pair for a digital certificate.
Options	<p><i>filename</i>—Name of a file in which to store the key pair.</p> <p><i>size key-size</i>—(Optional) Key size, in bits. The key size can be 512, 1024, or 2048. The default value is 1024.</p> <p><i>type</i>—(Optional) Algorithm used to encrypt the key:</p> <ul style="list-style-type: none">• rsa—RSA algorithm. This is the default.• dsa—Digital signature algorithm with Secure Hash Algorithm (SHA).
Required Privilege Level	maintenance
List of Sample Output	request security key-pair on page 478
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security key-pair

```
user@host> request security key-pair security-key-file
```

request security pki generate-key-pair

Syntax	<code>request security pki generate-key-pair certificate-id <i>certificate-id-name</i></code> <code><size (512 1024 2048)></code> <code><type (dsa rsa)></code>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Generate a public key infrastructure (PKI) public/private key pair for a local digital certificate.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>size—(Optional) Key pair size. The key pair size can be 512, 1024, or 2048 bits. If a key pair size is not specified, the default value, 1024 bits, is applied.</p> <p>type—(Optional) The algorithm to be used for encrypting the public/private key pair. The encryption algorithm can be dsa or rsa. If an encryption algorithm is not specified, the default value, rsa, is applied.</p>
Required Privilege Level	maintenance
Related Documentation	<ul style="list-style-type: none"> • Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 77
List of Sample Output	request security pki generate-key-pair on page 479
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki generate-key-pair

```
user@switch> request security pki generate-key-pair certificate-id billy size 2048
Generated key pair billy, key size 2048 bits
```

request security pki local-certificate generate-self-signed

Syntax	<code>request security pki local-certificate generate-self-signed certificate-id <i>certificate-id-name</i> domain-name <i>domain-name</i> ip-address <i>ip-address</i> email <i>email-address</i> subject <i>subject-distinguished-name</i></code>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Manually generate a self-signed certificate for the given distinguished name.
Options	<p>certificate-id <i>certificate-id-name</i>—Name of the local digital certificate and the public/private key pair.</p> <p>domain-name <i>domain-name</i>—Fully qualified domain name (FQDN). The FQDN provides the identity of the certificate owner for Internet Key Exchange (IKE) negotiations and provides an alternative to the subject name.</p> <p>email <i>email-address</i>—E-mail address of the certificate holder.</p> <p>ip-address <i>ip-address</i>—IP address of the switch.</p> <p>subject <i>subject-distinguished-name</i>—Distinguished name format that contains the common name, department, company name, state, and country:</p> <ul style="list-style-type: none">• CN—Common name• OU—Organizational unit name• O—Organization name• ST—State• C—Country
Required Privilege Level	<code>maintenance</code> <code>security</code>
Related Documentation	<ul style="list-style-type: none">• Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 77
List of Sample Output	request security pki local-certificate generate-self-signed on page 480
Output Fields	When you enter this command, you are provided feedback on the status of your request.

Sample Output

request security pki local-certificate generate-self-signed

```
user@switch> request security pki local-certificate generate-self-signed certificate-id self-cert  
subject cn=abc domain-name abc.net email jdoe@abc.net  
Self-signed certificate generated and loaded successfully
```

show security pki local-certificate

Syntax	show security pki local-certificate <brief detail> <certificate-id <i>certificate-id-name</i> > <system-generated>
Release Information	Command introduced in Junos OS Release 11.1 for EX Series switches.
Description	Display information about the local digital certificates and the corresponding public keys installed in the switch.
Options	<p>none—(Same as brief) Display information about all local digital certificates and corresponding public keys.</p> <p>brief detail—(Optional) Display information about local digital certificates and corresponding public keys for the specified level of output.</p> <p>certificate-id <i>certificate-id-name</i>—(Optional) Display information about only the specified the local digital certificate and corresponding public keys.</p> <p>system-generated—(Optional) Display information about the automatically generated self-signed certificate.</p>
Required Privilege Level	view
Related Documentation	<ul style="list-style-type: none"> • Manually Generating Self-Signed Certificates on Switches (CLI Procedure) on page 77
List of Sample Output	show security pki local-certificate on page 482 show security pki local-certificate detail on page 483
Output Fields	Table 32 on page 481 lists the output fields for the show security pki local-certificate command. Output fields are listed in the approximate order in which they appear.

Table 32: show security pki local-certificate Output Fields

Field Name	Field Description	Level of Output
Certificate identifier	Name of the digital certificate.	All levels
Certificate version	Revision number of the digital certificate.	detail
Serial number	Unique serial number of the digital certificate.	detail
Issued by	Authority that issued the digital certificate.	none brief
Issued to	Device that was issued the digital certificate.	none brief

Table 32: show security pki local-certificate Output Fields (*continued*)

Field Name	Field Description	Level of Output
Issuer	Authority that issued the digital certificate, including details of the authority organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Subject	Details of the digital certificate holder organized using the distinguished name format. Possible subfields are: <ul style="list-style-type: none"> • Common name—Name of the authority. • Organization—Organization of origin. • Organizational unit—Department within an organization. • State—State of origin. • Country—Country of origin. 	detail
Alternate subject	Domain name or IP address of the device related to the digital certificate.	detail
Validity	Time period when the digital certificate is valid. Values are: <ul style="list-style-type: none"> • Not before—Start time when the digital certificate becomes valid. • Not after—End time when the digital certificate becomes invalid. 	All levels
Public key algorithm	Encryption algorithm used with the private key, such as rsaEncryption (1024 bits) .	All levels
Public key verification status	Public key verification status: Failed or Passed . The detail output also provides the verification hash.	All levels
Signature algorithm	Encryption algorithm that the CA used to sign the digital certificate, such as sha1WithRSAEncryption .	detail
Fingerprint	Secure Hash Algorithm (SHA1) and Message Digest 5 (MD5) hashes used to identify the digital certificate.	detail
Distribution CRL	Distinguished name information and URL for the certificate revocation list (CRL) server.	detail
Use for key	Use of the public key, such as Certificate signing , CRL signing , Digital signature , or Key encipherment .	detail

Sample Output

show security pki local-certificate

```

user@switch> show security pki local-certificate
Certificate identifier: local-entrust2
Issued to: router2.juniper.net, Issued by: juniper

```



```

Validity:
  Not before: 2005 Nov 21st, 23:28:22 GMT
  Not after: 2008 Nov 21st, 23:58:22 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed

```

show security pki local-certificate detail

```

user@switch> show security pki local-certificate detail
Certificate identifier: local-entrust3
Certificate version: 3
Serial number: 4355 94f9
Issuer:
  Organization: juniper, Country: us
Subject:
  Organization: juniper, Country: us, Common name: switch1.juniper.net
Alternate subject: switch1.juniper.net
Validity:
  Not before: 2005 Nov 21st, 23:33:58 GMT
  Not after: 2008 Nov 22nd, 00:03:58 GMT
Public key algorithm: rsaEncryption(1024 bits)
Public key verification status: Passed
fb:79:df:d4:a9:03:0f:d3:69:7e:c1:e4:27:35:9c:d9:b1:a2:47:78
d2:6d:f3:e5:f4:68:4f:b3:04:45:88:57:99:82:39:a6:51:9e:5f:42
23:3f:d7:6e:3d:a5:54:a9:b1:2d:6e:90:dd:12:8a:bf:ef:2b:20:50
ba:f0:da:d9:0c:ad:5e:d6:c6:98:3a:ae:3f:90:dd:94:78:c1:ea:2e
7c:f0:2d:d4:79:d4:cd:f0:52:df:5e:72:f2:e7:ae:66:f7:61:f4:bc
72:57:3e:6c:6d:d3:24:58:8b:f4:ef:da:2a:6a:fa:eb:98:f8:34:84
79:54:da:4f:d3:6f:52:1f
Signature algorithm: sha1WithRSAEncryption
Fingerprint:
  61:3a:d0:b4:7a:16:9b:39:ba:81:3f:9d:ab:34:e5:c8:be:3b:a1:6d (sha1)
  60:a0:ff:58:05:4a:65:73:9d:74:3a:e1:83:6f:1b:c8 (md5)
Distribution CRL:
  C=us, O=juniper, CN=CRL1
  http://CA-1/CRL/juniper_us_crlfile.crl
Use for key: Digital signature

```

show system services dhcp binding

Syntax	show system services dhcp binding <detail> <address>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.
Options	<p>none—Display brief information about all active client bindings.</p> <p>detail—(Optional) Display detailed information about all active client bindings.</p> <p>address—(Optional) Display detailed client binding information for the specified IP address only.</p>
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> • clear system services dhcp binding on page 471
List of Sample Output	show system services dhcp binding on page 485 show system services dhcp binding address on page 485 show system services dhcp binding address detail on page 485
Output Fields	Table 33 on page 484 describes the output fields for the show system services dhcp binding command. Output fields are listed in the approximate order in which they appear.

Table 33: show system services dhcp binding Output Fields

Field Name	Field Description	Level of Output
Allocated address	List of IP addresses the DHCP server has assigned to clients.	All levels
MAC address	Corresponding media access control (MAC) hardware address of the client.	All levels
Client identifier	(address option only) Client's unique identifier (represented by an ASCII string or hexadecimal digits). This identifier is used by the DHCP server to index its database of address bindings.	All levels
Binding Type	Type of binding assigned to the client. DHCP servers can assign a dynamic binding from a pool of IP addresses or a static binding to one or more specific IP addresses.	All levels
Lease Expires at	Time the lease expires or never for leases that do not expire.	All levels
Lease Obtained at	(address option only) Time the client obtained the lease from the DHCP server.	detail

Table 33: show system services dhcp binding Output Fields (*continued*)

Field Name	Field Description	Level of Output
State	Status of the binding. Bindings can be active or expired.	detail
Pool	Address pool that contains the IP address assigned to the client.	detail
Request received on	Interface on which the DHCP message exchange occurs. The IP address pool is configured based on the interface's IP address. If a relay agent is used, its IP address is also displayed.	detail
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	detail

Sample Output

show system services dhcp binding

```
user@host> show system services dhcp binding

Allocated address  MAC address      Binding Type  Lease expires at
192.168.1.2        00:a0:12:00:12:ab  static       never
192.168.1.3        00:a0:12:00:13:02  dynamic      2004-05-03 13:01:42 PDT
```

show system services dhcp binding address

```
user@host> show system services dhcp binding 192.168.1.3

DHCP binding information:
Allocated address: 192.168.1.3
Mac address: 00:a0:12:00:12:ab
Client identifier
61 63 65 64 2d 30 30 3a 61 30 3a 31 32 3a 30 30aced-00:a0:12:00
3a 31 33 3a 30 32:13:02

Lease information:
  Binding Type dynamic
  Obtained at 2004-05-02 13:01:42 PDT
  Expires at 2004-05-03 13:01:42 PDT
```

show system services dhcp binding address detail

```
user@host> show system services dhcp binding 192.168.1.3 detail

DHCP binding information:
Allocated address      192.168.1.3
MAC address 00:a0:12:00:12:ab
Pool                  192.168.1.0/24
Request received on fe-0/0/0, relayed by 192.168.4.254

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

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
```

Name: domain-name, Value: mydomain.tld
Code: 19, Type: flag, Value: off
Code: 40, Type: string, Value: domain.tld
Code: 32, Type: ip-address, Value: 3.3.3.33

show system services dhcp conflict

Syntax	show system services dhcp conflict
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers only and EX Series switches) Display Dynamic Host Configuration Protocol (DHCP) client-detected conflicts for IP addresses. When a conflict is detected, the DHCP server removes the address from the address pool.
Options	This command has no options.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> clear system services dhcp conflict on page 472
List of Sample Output	show system services dhcp conflict on page 487
Output Fields	Table 34 on page 487 describes the output fields for the show system services dhcp conflict command. Output fields are listed in the approximate order in which they appear.

Table 34: show system services dhcp conflict Output Fields

Field Name	Field Description
Detection time	Date and time the client detected the conflict.
Detection method	How the conflict was detected.
Address	IP address where the conflict occurs. The addresses in the conflicts list remain excluded from the pool until you use a clear system services dhcp conflict command to manually clear the list.

Sample Output

show system services dhcp conflict

```
user@host> show system services dhcp conflict
```

```

Detection time      Detection method  Address
2004-08-03 19:04:00 PDT  ARP              3.3.3.5
2004-08-04 04:23:12 PDT  Ping             4.4.4.8
2004-08-05 21:06:44 PDT  Client           3.3.3.10
```

show system services dhcp global

Syntax	show system services dhcp global
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) global configuration options. Global options apply to all scopes and clients served by the DHCP server. Global options are overridden if specified otherwise in scope or client options. Scope options apply to specific subnets or ranges of addresses. Client options apply to specific clients.
Options	This command has no options.
Required Privilege Level	view and system
List of Sample Output	show system services dhcp global on page 489
Output Fields	Table 35 on page 488 describes the output fields for the show system services dhcp global command. Output fields are listed in the approximate order in which they appear.

Table 35: show system services dhcp global Output Fields

Field Name	Field Description
BOOTP lease length	Length of lease time assigned to BOOTP clients.
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client retains an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.

Sample Output

show system services dhcp global

```
user@host> show system services dhcp global

Global settings:
  BOOTP lease length      infinite

DHCP lease times:
  Default lease time      1 hour
  Minimum lease time      2 hours
  Maximum lease time      infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.33
```

show system services dhcp pool

Syntax	show system services dhcp pool <detail> <subnet-address>
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server IP address pools.
Options	none —Display brief information about all IP address pools. detail —(Optional) Display detailed information. subnet-address —(Optional) Display information for the specified subnet address.
Required Privilege Level	view and system
List of Sample Output	show system services dhcp pool on page 491 show system services dhcp pool subnet-address on page 491 show system services dhcp pool subnet-address detail on page 491
Output Fields	Table 36 on page 490 describes the output fields for the show system services dhcp pool command. Output fields are listed in the approximate order in which they appear.

Table 36: show system services dhcp pool Output Fields

Field Name	Field Description	Level of Output
Pool name	Subnet on which the IP address pool is defined.	None specified
Low address	Lowest address in the IP address pool.	None specified
High address	Highest address in the IP address pool.	None specified
Excluded addresses	Addresses excluded from the address pool.	None specified
Subnet	(<i>subnet-address</i> option only) Subnet to which the specified address pool belongs.	None specified
Address range	(<i>subnet-address</i> option only) Range of IP addresses in the address pool.	None specified
Addresses assigned	Number of IP addresses in the pool that are assigned to DHCP clients and the total number of IP addresses in the pool.	detail
Active	Number of assigned IP addresses in the pool that are active.	detail
Excluded	Number of assigned IP addresses in the pool that are excluded.	detail
Default lease time	Lease time assigned to clients that do not request a specific lease time.	detail

Table 36: show system services dhcp pool Output Fields (*continued*)

Field Name	Field Description	Level of Output
Minimum lease time	Minimum time a client can retain an IP address lease on the server.	detail
Maximum lease time	Maximum time a client can retain an IP address lease on the server.	detail
DHCP options	User-defined options created for the DHCP server. If no options have been defined, this field is blank.	detail

Sample Output

show system services dhcp pool

```
user@host> show system services dhcp pool

Pool name      Low address    High address    Excluded addresses
3.3.3.0/24     3.3.3.2       3.3.3.254     3.3.3.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 3.3.3.0/24

Pool information:
  Subnet                3.3.3.0/24
  Address range         3.3.3.2 - 3.3.3.254
  Addresses assigned    2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 3.3.3.0/24 detail

Pool information:
  Subnet                3.3.3.0/24
  Address range         3.3.3.2 - 3.3.3.254
  Addresses assigned    2/253
  Active: 1, Excluded: 1

DHCP lease times:
  Default lease time    1 hour
  Minimum lease time    2 hours
  Maximum lease time    infinite

DHCP options:
  Name: name-server, Value: { 6.6.6.6, 6.6.6.7 }
  Name: domain-name, Value: mydomain.tld
  Name: router, Value: { 3.3.3.1 }
  Name: server-identifier, Value: 3.3.3.1
  Code: 19, Type: flag, Value: off
  Code: 40, Type: string, Value: domain.tld
  Code: 32, Type: ip-address, Value: 3.3.3.333.3.3.254 3.3.3.1
```

show system services dhcp statistics

Syntax	show system services dhcp statistics
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches.
Description	(J Series routers and EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server statistics.
Options	This command has no options.
Required Privilege Level	view and system
Related Documentation	<ul style="list-style-type: none"> • clear system services dhcp statistics on page 473
List of Sample Output	show system services dhcp statistics on page 493
Output Fields	Table 37 on page 492 describes the output fields for the show system services dhcp statistics command. Output fields are listed in the approximate order in which they appear.

Table 37: show system services dhcp statistics Output Fields

Field Name	Field Description
Default lease time	Lease time assigned to clients that do not request a specific lease time.
Minimum lease time	Minimum time a client can retain an IP address lease on the server.
Maximum lease time	Maximum time a client can retain an IP address lease on the server.
Packets dropped	Total number of packets dropped and number of packets dropped because of: <ul style="list-style-type: none"> • Invalid hardware address • Invalid opcode • Invalid server address • No available address • No interface match • No routing instance match • No valid local addresses • Packet too short • Read error • Send error

Table 37: show system services dhcp statistics Output Fields (*continued*)

Field Name	Field Description
Messages received	<p>Number of the following message types sent from DHCP clients and received by the DHCP server:</p> <ul style="list-style-type: none"> • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST
Messages sent	<p>Number of the following message types sent from the DHCP server to DHCP clients:</p> <ul style="list-style-type: none"> • BOOTREPLY • DHCPACK • DHCPOFFER • DHCPNAK

Sample Output

show system services dhcp statistics

```
user@host> show system services dhcp statistics
```

```
DHCP lease times:
  Default lease time      1 hour
  Minimum lease time      2 hours
  Maximum lease time      infinite
```

```
Packets dropped:
  Total                    0
  Bad hardware address     0
  Bad opcode               0
  Invalid server address   0
  No available addresses   0
  No interface match       0
  No routing instance match 0
  No valid local address   0
  Packet too short         0
  Read error               0
  Send error               0
```

```
Messages received:
  BOOTREQUEST              0
  DHCPDECLINE              0
  DHCPDISCOVER             0
  DHCPINFORM               0
  DHCPRELEASE              0
  DHCPREQUEST              0
```

```
Messages sent:
  BOOTREPLY                0
  DHCPACK                  0
  DHCPOFFER                0
  DHCPNAK                  0
```


show system services service-deployment

Syntax	show system services service-deployment
Release Information	Command introduced before Junos OS Release 7.4. Command introduced in Junos OS Release 9.0 for EX Series switches. Command introduced in Junos OS Release 11.1 for the QFX Series. Command introduced in Junos OS Release 14.1X53-D20 for the OCX Series.
Description	Display information about a Session and Resource Control (SRC) client.
Options	This command has no options.
Required Privilege Level	system view
List of Sample Output	show system services service-deployment on page 495
Output Fields	Table 38 on page 495 lists the output fields for the show system services service-deployment command. Output fields are listed in the approximate order in which they appear.

Table 38: show system services service-deployment Output Fields

Field Name	Field Description
PDT Keepalive settings	Configured PDT keepalive interval, in seconds.
Keepalives sent	Number of keepalives sent.
Notifications sent	Number of notifications sent.
Last update from peer	Time at which the last update from a peer was received.

Sample Output

show system services service-deployment

```
user@host> show system services service-deployment
Connected to 192.4.4.4 port 10288 since 2004-05-03 11:04:34 PDT Keepalive settings:
Interval 15 seconds Keepalives sent: 750 Notifications sent: 0 Last update from
peer: 00:00:06 ago
```

ssh

List of Syntax [Syntax on page 496](#)
 [Syntax \(EX Series Switch and the QFX Series\) on page 496](#)

Syntax `ssh host`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<logical-system logical-system-name>`
 `<routing-instance routing-instance-name>`
 `<source address>`
 `<v1 | v2>`

Syntax (EX Series Switch and the QFX Series) `ssh host`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<routing-instance routing-instance-name>`
 `<source address>`
 `<v1 | v2>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.
 Command introduced in Junos OS Release 11.1 for the QFX Series.
 Command introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

Description Use the SSH program to open a connection between a local router or switch and a remote system and execute commands on the remote system. You can issue the **ssh** command from the Junos OS CLI to log in to a remote system or from a remote system to log in to the local router or switch. When executing this command, you include one or more CLI commands by enclosing them in quotation marks and separating the commands with semicolons:

```
ssh address 'cli-command1 ; cli-command2 '
```

Options **host**—Name or address of the remote system.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Create an IPv4 or IPv6 connection, respectively.

interface interface-name—(Optional) Interface name for the SSH session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system logical-system-name—(Optional) Name of a particular logical system for the SSH attempt.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the SSH attempt.

source address—(Optional) Source address of the SSH connection.

v1 | v2—(Optional) Use SSH version 1 or 2, respectively, when connecting to a remote host.

Additional Information To configure an SSH (version 1) key for your user account, include the **authentication ssh-rsa** statement at the **[edit system login user *user-name*]** hierarchy level. To configure an SSH (version 2) key for your user account, include the **authentication dsa-rsa** statement at the **[edit system login user *user-name*]** hierarchy level.

You can limit the number of times a user can attempt to enter a password while logging in through SSH. To specify the number of times a user can attempt to enter a password to log in through SSH, include the **retry-options** statement at the **[edit system login]** hierarchy level. For details, see the .

Required Privilege Level network

Related Documentation • *Configuring SSH Host Keys for Secure Copying of Data*

List of Sample Output [ssh on page 497](#)

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

Sample Output

ssh

```
user@switch> ssh cree
Host key not found from the list of known hosts.
Are you sure you want to continue connecting (yes/no)? yes

Host ?cree' added to the list of known hosts.
boojun@cree's password:
Last login: Sun Jun 21 10:43:42 1998 from junos-router
% ...
```

telnet

List of Syntax [Syntax on page 498](#)
 [Syntax \(EX Series Switches\) on page 498](#)

Syntax `telnet host`
 `<8bit>`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<logical-system logical-system-name>`
 `<no-resolve>`
 `<port port-number>`
 `<routing-instance routing-instance-name>`
 `<source source-address>`

Syntax (EX Series Switches) `telnet host`
 `<8bit>`
 `<bypass-routing>`
 `<inet | inet6>`
 `<interface interface-name>`
 `<no-resolve>`
 `<port port-number>`
 `<routing-instance routing-instance-name>`
 `<source source-address>`

Release Information Command introduced before Junos OS Release 7.4.
 Command introduced in Junos OS Release 9.0 for EX Series switches.

Description Open a telnet session to a remote system. Type Ctrl+] to escape from the telnet session to the telnet command level, and then type **quit** to exit from telnet.

Options *host*—Name or address of the remote system.

8bit—(Optional) Use an 8-bit data path.

bypass-routing—(Optional) Bypass the normal routing tables and send ping requests directly to a system on an attached network. If the system is not on a directly attached network, an error is returned. Use this option to ping a local system through an interface that has no route through it.

inet | inet6—(Optional) Open an IPv4 or IPv6 session, respectively.

interface *interface-name*—(Optional) Interface name for the telnet session. (This option does not work when **default-address-selection** is configured at the **[edit system]** hierarchy level, because this configuration uses the loopback interface as the source address for all locally generated IP packets.)

logical-system *logical-system-name*—(Optional) Name of a particular logical system for the telnet attempt.

no-resolve—(Optional) Do not attempt to determine the hostname that corresponds to the IP address.

port *port-number*—(Optional) Port number or service name on the remote system.

routing-instance *routing-instance-name*—(Optional) Name of the routing instance for the telnet attempt.

source *source-address*—(Optional) Source address of the telnet connection.

Additional Information You can limit the number of times a user can attempt to enter a password while logging in through telnet. To specify the number of times a user can attempt to enter a password to log in through telnet, include the **retry-options** statement at the [edit system login] hierarchy level. For details, see the *Junos OS Administration Library for Routing Devices*.

Required Privilege Level network

List of Sample Output [telnet on page 499](#)

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

Sample Output

telnet

```
user@host> telnet 192.154.1.254
Trying 192.154.169.254...
Connected to level5.company.net.
Escape character is '^]'.
ttypa
login:
```

