JUNIPER NETWORKS | Engineering Simplicity

Junos® OS

DHCP User Guide

Published
2021-09-21

JUNOS

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

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

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

Junos® OS DHCP User Guide
Copyright © 2021 Juniper Networks, Inc. All rights reserved.

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

YEAR 2000 NOTICE

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

END USER LICENSE AGREEMENT

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

Table of Contents

About This Guide | xxiv

1 Overview

DHCP Overview | 2

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

DHCP Access Service Overview | 9

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

Legacy DHCP and Extended DHCP | 16

- Understanding Differences Between Legacy DHCP and Extended DHCP | 17
- DHCP Statement Hierarchy and Inheritance | 20
- Difference in Legacy DHCP Relay and Extended DHCP Relay | 24
- Restrictions in Using Legacy DHCP and Extended DHCP | 24

2 Address Assignment Pool

IP Address Assignment Pool | 27

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

Configuring Address-Assignment Pools | 34

Configuring an Address-Assignment Pool Name and Addresses | 35

Configuring a Named Address Range for Dynamic Address Assignment | 35

Configuring Static Address Assignments | 36

Configuring Address-Assignment Pool Linking | 37

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

DHCPv6 Address-Assignment Pools | 39

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

Requirements | 40

Overview | 40

Configuration | 40

Verification | 42

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

Configuring an Address-Assignment Pool for Router Advertisement | 44

Configuring Nontemporary Address Assignment | 44

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation | 45

Configuring Auto-Prefix Delegation | 46

Multiple Address Assignment for DHCPv6 Clients | 47

3 **DHCP Server**

DHCP Server | 49

Understanding DHCP Server Operation | 49

Graceful Routing Engine Switchover for DHCP | 50

DHCP Server Configuration | 51

DHCP Server Configuration Overview | 52

Minimum DHCP Local Server Configuration | 54

Example: Complete DHCP Server Configuration | 56

Requirements | 56

Overview | 56

Configuration | 56

Configure a Router as an Extended DHCP Local Server | 60

Configuring a Switch as a DHCP Server | 62

Configuring the Switch as a Local DHCP Server | 63

Configuring a DHCP Server on Switches | 66

Configuring an Extended DHCP Server on a Switch | 67

Example: Configuring a Security Device as a DHCP Server | 68

Requirements | 69

Overview | 69

Configuration | 69

Verification | 74

DHCP Server Options | 77

Configure DHCP Server Identifier | 77

Configure Address Pools for DHCP Dynamic Bindings | 78

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

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

Specify DHCP Lease Times for IP Address Assignments | 81

Configure a DHCP Boot File and DHCP Boot Server | 81

Configure Domain Name and Domain Search List | 82

Configure Routers Available to the DHCP Client | 83

Configure User-Defined DHCP Options | 83

Configure DHCP SIP Server | 84

Overriding the Default DHCP Local Server Configuration Settings | 85

Legacy DHCP Server Configuration Options | 87

Verifying DHCP Server Configuration | 95

Verifying DHCP Server Binding and Server Statistics | 96

Viewing DHCP Bindings (Legacy DHCP) | **97**

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

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

Monitoring the DHCP Server Configuration | 100

DHCP Processes Tracing Flags | **100**

Tracing Extended DHCP Local Server Operations | **102**

Configuring the Filename of the Extended DHCP Local Server Processes Log | **103**

Configuring the Number and Size of Extended DHCP Local Server Processes Log Files | **103**

Configuring Access to the Log File | **104**

Configuring a Regular Expression for Lines to Be Logged | **104**

Configuring Trace Option Flags | **104**

Configuring Tracing Operations for DHCP Processes | **105**

Configuring the DHCP Processes Log Filename | **106**

Configuring the Number and Size of DHCP Processes Log Files | **107**

Configuring Access to the DHCP Log File | **107**

Configuring a Regular Expression for Refining the Output of DHCP Logged Events | **107**

Configuring DHCP Trace Operation Events | **108**

DHCPv6 Server | 109

DHCPv6 Local Server Overview | **109**

DHCPv6 Server Overview | **111**

Example: Configuring DHCPv6 Server Options | **112**

Requirements | **112**

Overview | **113**

Configuration | **113**

Verification | **116**

Specifying the Address Pool for IPv6 Prefix Assignment | **117**

Specifying the Delegated Address Pool for IPv6 Prefix Assignment | **118**

Preventing Binding of Clients That Do Not Support Reconfigure Messages | **119**

Configuring DHCPv6 Rapid Commit (MX Series, EX Series) | **120**

Allow Host Inbound Traffic for DHCPv6 Traffic | **121**

Verifying and Managing DHCPv6 Local Server Configuration | **122**

Understanding Cascaded DHCPv6 Prefix Delegating | **123**

Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) | **124**

- Requirements | **125**
- Overview | **125**
- Configuration | **126**
- Verification | **147**

4 **DHCP Relay Agent**

DHCP Relay Agent | 156

Understanding DHCP Relay Agent Operation | **156**

Minimum DHCP Relay Agent Configuration | **158**

Configuring DHCP Relay Agent | **159**

- Requirements | **159**
- Overview | **160**
- Configuration | **161**
- Verification | **170**

Configuring a DHCP Relay Agent on EX Series Switches | **171**

Configuring DHCP Smart Relay (Legacy DHCP Relay) | **173**

Disabling Automatic Binding of Stray DHCP Requests | **174**

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets | **176**

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

Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address | **177**

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

Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally | **180**

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

- Requirements | **181**
- Overview | **181**

Configuration | **182**

Verification | **184**

Verifying and Managing DHCP Relay Configuration | **186**

Extended DHCP Relay Agent Overview | **187**

DHCP and BOOTP Relay Agent | 190

DHCP and BOOTP Relay Overview for Switches | **191**

Configuring DHCP and BOOTP Relay | **194**

Configuring DHCP and BOOTP Relay on QFX Series | **195**

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

Configuring DHCP Smart Relay on QFX Series | **197**

DHCP Relay Agent Information Option (Option 82) | 198

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

Configuring Option 82 Information | **200**

Overriding Option 82 Information | **203**

Including a Prefix in DHCP Options | **203**

Including a Textual Description in DHCP Options | **207**

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

Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | **211**

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

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

Example: Configure DHCP Relay in Forward Only Mode | **214**

Requirements | **214**

Overview | **215**

Configuration | **215**

Verification | **218**

DHCPv6 Relay Agent | 222

DHCPv6 Relay Agent Overview | **223**

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets | **224**

Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets | **226**

Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets | **227**

Verifying and Managing DHCPv6 Relay Configuration | **228**

DHCP Relay Proxy | 230

DHCP Relay Proxy Overview | **230**

Enabling DHCP Relay Proxy Mode | **232**

5 **DHCP Client**

DHCP Client | 234

Understanding DHCP Client Operation | **234**

Minimum DHCP Client Configuration | **235**

Configuring a DHCP Client | **235**

Example: Configuring the Device as a DHCP Client | **238**

Requirements | **238**

Overview | **239**

Configuration | **240**

Verification | **243**

Verifying and Managing DHCP Client Configuration | **245**

Example: Configuring as a DHCP Client in Chassis Cluster Mode | **246**

Requirements | **246**

Overview | **247**

Configuration | **247**

Verification | **253**

DHCPv6 Client | 255

DHCPv6 Client Overview | **256**

Understanding DHCPv6 Client and Server Identification | **257**

Minimum DHCPv6 Client Configuration on SRX Series Devices | **258**

Configuring DHCP Client-Specific Attributes | **259**

DHCPv6 Client Configuration Options | **260**

Configuring the DHCPv6 Client Rapid Commit Option | **262**

Configuring a DHCPv6 Client in Autoconfig Mode | **263**

Configuring TCP/IP Propagation on a DHCPv6 Client | **264**

6 **DHCP with External Authentication Server**

DHCP with External Authentication Server | 266

Using External AAA Authentication Services to Authenticate DHCP Clients | **266**

Steps to Configure DHCP with External Authentication Server | **267**

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | **268**

Example-Configuring DHCP with External Authentication Server | **269**

Specifying Authentication Support | **270**

Creating Unique Usernames for DHCP Clients | **271**

Grouping Interfaces with Common DHCP Configurations | **274**

Centrally Configure DHCP Options on a RADIUS Server | 277

7 **Managing DHCP Services**

Group-Specific DHCP Configurations | 283

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces | **283**

Configuring Group-Specific DHCP Local Server Options | **285**

Configuring Group-Specific DHCP Relay Options | **285**

Configuring DHCP Server Configuration with Optional Pool Matching Using Groups | **286**

DHCP Snooping | 287

DHCP Snooping Support | **288**

Example: Configuring DHCP Snooping Support for DHCP Relay Agent | **290**

Requirements | **290**

Overview | **290**

Configuration | **291**

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | **293**

DHCP Auto Logout | 296

DHCP Auto Logout Overview | **296**

Automatically Logging Out DHCP Clients | 298

Additional Configurations for DHCP Clients | 300

Specifying the Maximum Number of DHCP Clients Per Interface | 300

DHCP Local Server Handling of Client Information Request Messages | 301

Enabling Processing of Client Information Requests | 302

Sending Release Messages When Clients Are Deleted | 303

Dynamic Reconfiguration of DHCP Servers and Clients | 305

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients | 305

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview | 309

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings | 310

Configuring Dynamic Reconfiguration Attempts for DHCP Clients | 311

Configuring Deletion of the Client When Dynamic Reconfiguration Fails | 312

Configuring a Token for DHCP Local Server Authentication | 313

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | 314

DHCP Liveness Detection | 315

DHCP Liveness Detection Overview | 316

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD | 318

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 320

Requirements | 320

Overview | 321

Configuration | 321

Configuring Detection of DHCP Local Server Client Connectivity with BFD | 324

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 326

Requirements | 327

Overview | 327

Configuration | 327

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 331

How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works | 331

Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets | 336

Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets | 339

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets | 342

Secure DHCP Message Exchange | 343

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs | 344

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances | 345

Client-Side Support | 346

Server-Side Support | 347

DHCP Local Server Support | 348

DHCP Active Server Groups | 349

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups | 349

Suppressing DHCP Routes | 353

Suppressing DHCP Access, Access-Internal, and Destination Routes | 353

Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | 354

8 **Configuration Statements**

access-profile | 363

active-server-group | 365

address-assignment (Address-Assignment Pools) | 367

address-pool | 370

address-pool (Access) | 372

allow-no-end-option (DHCP Relay Agent) | 374

allow-snooped-clients | 376

always-write-giaddr | 378

always-write-option-82 | 380

always-write-option-82 | 382

apply-secondary-as-giaddr | 383

attempts (DHCP Local Server) | 385

authentication (DHCP Local Server) | 388

authentication (DHCP Relay Agent) | 390

authentication-order (Access Profile) | 392

authentication-server | 394

bfd | 396

boot-server (DHCP) | 398

circuit-id (DHCP Relay Agent) | 399

circuit-type | 403

circuit-type (DHCP Local Server) | 405

circuit-type (DHCP Relay Agent) | 407

classification-key (DHCP Local Server) | 408

classification-key (DHCP Relay Agent) | 410

clear-on-abort (DHCP Local Server) | 413

client-discover-match (DHCP Local Server) | 416

client-ia-type | 418

client-id (DHCP Local Server) | 420

client-id (DHCP Relay Agent) | 422

client-identifier (DHCP Client) | 424

client-identifier (DHCPv6 Client) | 426

client-type | 428

delegated-pool (DHCP Local Server) | 430

delimiter (DHCP Local Server) | 432

delimiter (DHCP Relay Agent) | 434

detection-time | 437

dhcp | 439

dhcp (DHCP Client) | 441

dhcp-attributes (Access IPv4 Address Pools) | 444

dhcp-attributes (Access IPv6 Address Pools) | 446

dhcp-client | 449

dhcp-local-server | 451

dhcp-local-server (System Services) | 464

dhcp-relay | 470

dhcp-service | 486

dhcpv6 (DHCP Local Server) | 489

dhcpv6 (DHCP Relay Agent) | 496

dhcpv6 (System Services) | 504

dhcpv6-client | 510

disable-relay | 512

domain (Domain Map) | 514

domain-name (DHCP) | 516

domain-name (DHCP Local Server) | 517

domain-name (DHCP Relay Agent) | 520

domain-name-server (Routing Instances and Access Profiles) | 522

domain-name-server-inet (Routing Instances and Access Profiles) | 524

domain-name-server-inet6 (Routing Instances and Access Profiles) | 526

domain-search | 528

drop (DHCP Relay Agent Option) | 529

dual-stack (DHCP Local Server Overrides) | 531

dual-stack (DHCP Relay Agent Overrides) | 533

dual-stack-group (DHCP Local Server) | 535

dual-stack-group (DHCP Relay Agent) | 537

dual-stack-interface-client-limit (DHCP Local Server and Relay Agent) | 541

dynamic-pool | 543

dynamic-profile (DHCP Local Server) | 545

dynamic-profile (DHCP Relay Agent) | 547

dynamic-server | 549

excluded-address (Address-Assignment Pools) | 551

excluded-address (Address-Assignment Pools) | 552

external-authority | 554

failure-action | 556

force-discover (DHCP Client) | 558

forward-only (DHCP Relay Agent) | 559

forward-snooped-clients (DHCP Local Server) | 562

forward-snooped-clients (DHCP Relay Agent) | 563

group (DHCP Local Server) | 566

group (DHCP Relay Agent) | 571

group (System Services DHCP) | 578

holddown-interval | 582

host-name (DHCP Relay Agent) | 584

include-irb-and-l2 | 585

interface (DHCP Local Server) | 589

interface (DHCP Relay Agent) | 592

interface (System Services DHCP) | 595

interface-client-limit (DHCP Local Server) | 597

interface-client-limit (DHCP Relay Agent) | 599

interface-delete (Subscriber Management or DHCP Client Management) | 602

interface-name (DHCP Local Server) | 604

interface-traceoptions (System Services DHCP) | 605

ip-address-first | 608

keep-incoming-circuit-id (DHCP Relay Agent) | 610

keep-incoming-remote-id (DHCP Relay Agent) | 611

layer2-liveness-detection (Send) | 613

layer2-unicast-replies | 616

lease-time | 618

lease-time (dhcp-client) | 620

liveness-detection | 621

local-server-group (DHCP Relay Agent Option) | 624

location (DHCP Relay Agent) | 626

log | 627

logical-system-name (DHCP Local Server) | 630

mac-address (DHCP Local Server) | 631

mac-address (DHCP Relay Agent) | 633

maximum-hop-count | 635

maximum-lease-time (DHCP) | 637

method | 638

minimum-interval | 640

minimum-receive-interval | 643

minimum-wait-time | 645

multiplier | 646

name-server (Access) | 648

name-server (System Services) | 650

next-server | 652

no-adaptation | 653

no-allow-snooped-clients | 655

no-bind-on-request (DHCP Relay Agent) | 657

no-listen | 659

no-vlan-interface-name | 660

on-demand-address-allocation | 663

option (DHCP server) | 665

option-60 (DHCP Local Server) | 667

option-60 (DHCP Relay Agent) | 669

option-82 (DHCP Local Server Authentication) | 672

option-82 (DHCP Local Server Pool Matching) | 674

option-82 (DHCP Relay Agent) | 675

option-number (DHCP Relay Agent Option) | 677

overrides (DHCP Local Server) | 679

overrides (DHCP Relay Agent) | 683

overrides (DHCP Relay Agent) | 686

overrides (System Services DHCP) | 688

password (DHCP Local Server) | 690

password (DHCP Relay Agent) | 693

pool (DHCP Local Server Overrides) | 695

pool (System) | 698

pool-match-order | 700

preferred-prefix-length | 702

prefix (DHCP Client) | 703

prefix (DHCP Relay Agent) | 704

process-inform | 707

profile (Access) | 709

protocol-master | 717

proxy-mode | 720

radius-disconnect (DHCP Local Server) | 722

rapid-commit (DHCPv6 Client) | 724

rapid-commit (DHCPv6 Local Server) | 725

reauthenticate (DHCP Local Server) | 727

reconfigure (DHCP Local Server) | 730

reconfigure (DHCP Local Server) | 732

relay-agent-interface-id (DHCP Local Server) | 735

relay-agent-interface-id (DHCPv6 Relay Agent) | 737

relay-agent-option-79 | 739

relay-agent-remote-id (DHCP Local Server) | 741

relay-agent-remote-id (DHCPv6 Relay Agent Username) | 743

relay-option (DHCP Relay Agent) | 745

relay-option-82 | 747

relay-server-group (DHCP Relay Agent Option) | 750

remote-id (DHCP Relay Agent) | 752

replace-ip-source-with (DHCP Relay Agent) | 755

replace-ip-source-with (DHCP Relay Agent) | 756

req-option | 758

retransmission-attempt (DHCP Client) | 760

retransmission-attempt (DHCP Client) | 762

retransmission-attempt (DHCPv6 Client) | 764

retransmission-interval (DHCP Client) | 765

retransmission-interval (DHCP Client) | 767

retransmission-interval (DHCP Client) | 769

route-suppression (DHCP Local Server and Relay Agent) | 771

routing-instance-name (DHCP Local Server) | 773

routing-instance-name (DHCP Relay Agent) | 775

send-release-on-delete (DHCP Relay Agent) | 777

server-address | 779

server-address (dhcp-client) | 781

server-group | 783

server-identifier | 785

service-profile (DHCP Local Server) | 787

service-profile (DHCP Relay Agent) | 789

services (System Services) | 791

session-mode | 799

short-cycle-protection (DHCP Local Server and Relay Agent) | 801

source-address-giaddr | 803

source-ip-change (Forwarding Options) | 805

static-binding | 806

strict (DHCP Local Server) | 808

sub-prefix-length | 810

threshold (detection-time) | 812

threshold (transmit-interval) | 814

timeout (DHCP Local Server) | 816

token (DHCP Local Server) | 818

trace (DHCP Relay Agent) | 820

traceoptions (Address-Assignment Pool) | 822

traceoptions (DHCP) | 825

traceoptions (DHCP Server) | 828

transmit-interval | 832

trigger (DHCP Local Server) | 834

trust-option-82 | 836

update-router-advertisement | 838

update-server | 839

update-server (dhcp-client) | 841

update-server (dhcpv6-client) | 842

use-interface | 843

use-interface-description | 844

use-primary (DHCP Local Server) | 847

use-primary (DHCP Relay Agent) | 849

use-vlan-id | 852

use-vlan-id (DHCP Relay Agent) | 854

user-defined-option-82 | 856

user-id | 858

user-prefix (DHCP Local Server) | 859

username-include (DHCP Local Server) | 862

username-include (DHCP Relay Agent) | 864

vendor-id | 867

vendor-option | 869

vendor-option | 871

version (BFD) | 873

wins-server (System) | 875

9

Operational Commands

clear dhcp client binding | 879

clear dhcp client statistics | 881

clear dhcp relay binding | 883

clear dhcp relay statistics | 885

clear dhcp server binding | 886

clear dhcp server statistics | 888

clear dhcpv6 client binding | 890

clear dhcpv6 client statistics | 892

clear dhcpv6 relay binding | 893

clear dhcpv6 relay statistics | 898

clear dhcpv6 server binding | 901

clear dhcpv6 server binding (Local Server) | 905

clear dhcpv6 server statistics | 907

clear dhcpv6 server statistics (Local Server) | 909

clear system services dhcp binding | 910

clear system services dhcp conflict | 912

clear system services dhcp statistics | 914

request dhcp client renew | 915

request dhcp server reconfigure | 917

request dhcpv6 server reconfigure | 919

request dhcpv6 client renew | 922

request system services dhcp | 923

restart | 925

show captive-portal firewall | 942

show dhcp client binding | 946

show dhcp client statistics | 951

show dhcp relay binding | 956

show dhcp relay statistics | 960

show dhcp server binding | 963

show dhcp server statistics | 966

show dhcpv6 client binding | 969

show dhcpv6 client statistics | 973

show dhcpv6 relay binding | 977

show dhcpv6 relay statistics | 989

show dhcpv6 server binding (View) | 997

show dhcpv6 server statistics | 1003

show dhcpv6 server statistics (View) | 1010

show route protocol | 1015

show system services dhcp binding | 1023

show system services dhcp client | 1027

show system services dhcp conflict | 1032

show system services dhcp global | 1035

show system services dhcp pool | 1037

show system services dhcp relay-statistics | 1041

show system services dhcp statistics | 1044

About This Guide

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

1
CHAPTER

Overview

DHCP Overview | 2

DHCP Access Service Overview | 9

Legacy DHCP and Extended DHCP | 16

DHCP Overview

SUMMARY

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

IN THIS SECTION

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

Benefits of DHCP

Benefits of DHCP include:

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

Introduction to DHCP

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

On Junos OS devices, DHCP provides:

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

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

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

Understand DHCP

IN THIS SECTION

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

DHCP Use Cases

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

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

DHCP Components

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

DHCP Server

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

DHCP server assigns the following configuration parameters to client device:

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

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

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

DHCP Client

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

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

DHCP Relay

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

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

DHCP Client and Server Model

DHCP IP address allocation works on a client/server model in which the server, in this case a Junos OS, assigns the client reusable IP information from an address pool. A DHCP client might receive offer

messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 1 on page 6.

Figure 1: DHCP Client/Server Model

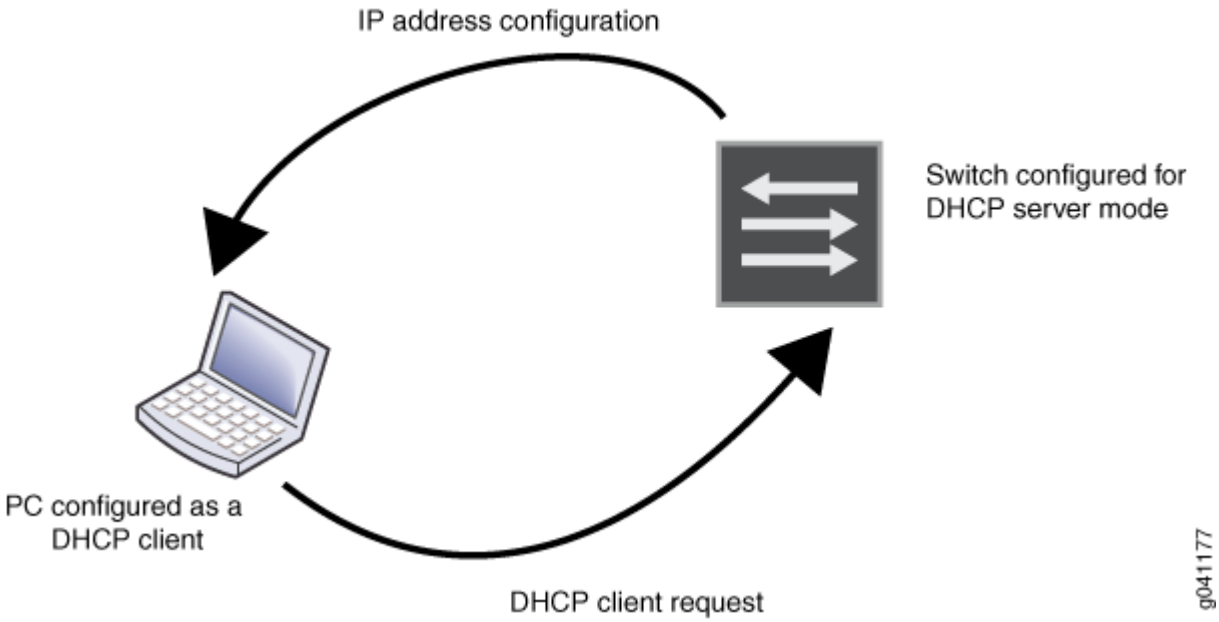
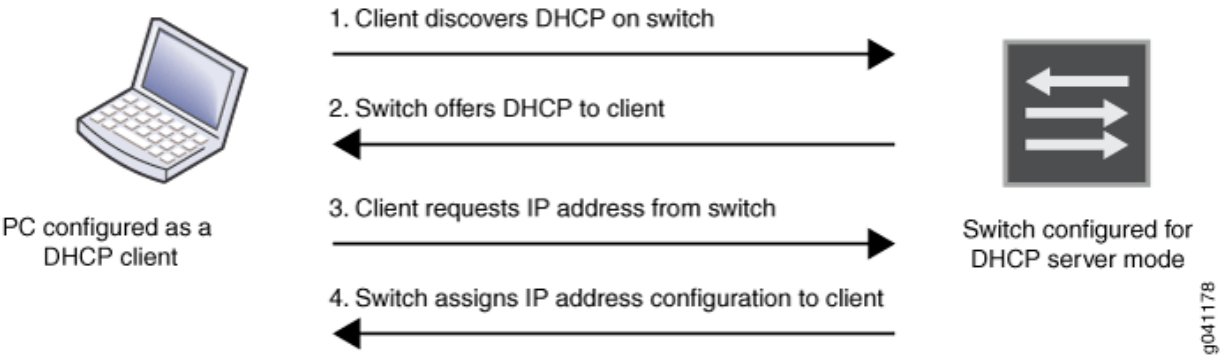


Figure 2: DHCP Four-Step Transfer



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

NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

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

DHCP Client, Server, and Relay Agent Model

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

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

11. After establishing the initial lease on the IP address, the DHCP client and the DHCP server use unicast transmission to negotiate lease renewal or release. The DHCP relay agent "snoops" on all of the packets unicast between the client and the server that pass through the router (or switch) to determine when the lease for this client has expired or been released. This process is referred to as lease shadowing or passive snooping.

DHCP Conflict Detection and Resolution

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

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

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

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

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

RELATED DOCUMENTATION

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

DHCP Access Service Overview

IN THIS SECTION

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

DHCP access service consists of two components:

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

For more information, read this topic.

IP Address Assignments

IN THIS SECTION

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

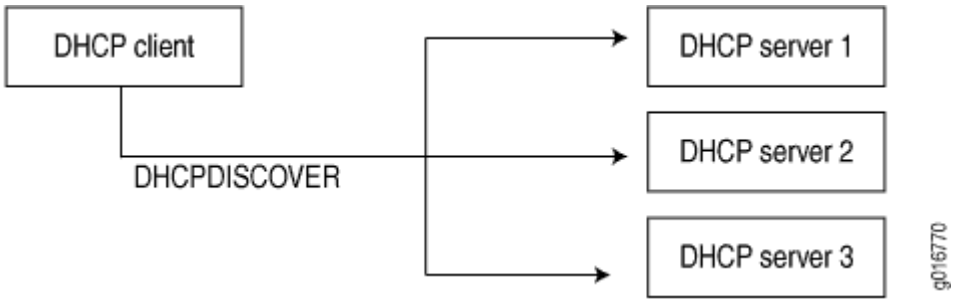
The following topics describe IP address assignment in detail:

Network Address Assignments (Allocating a New Address)

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

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

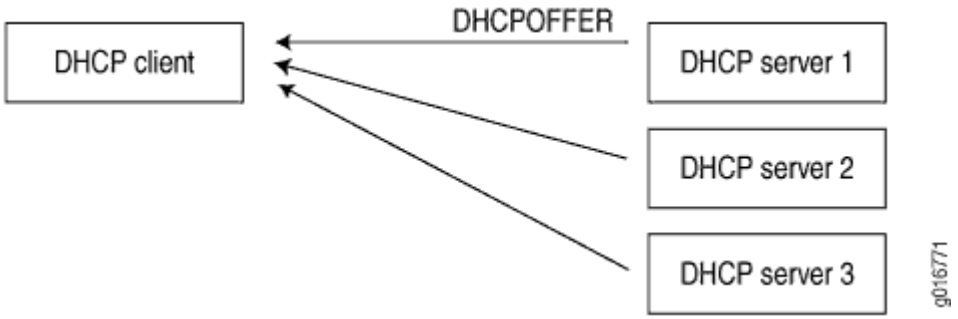
Figure 3: DHCP Discover



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

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

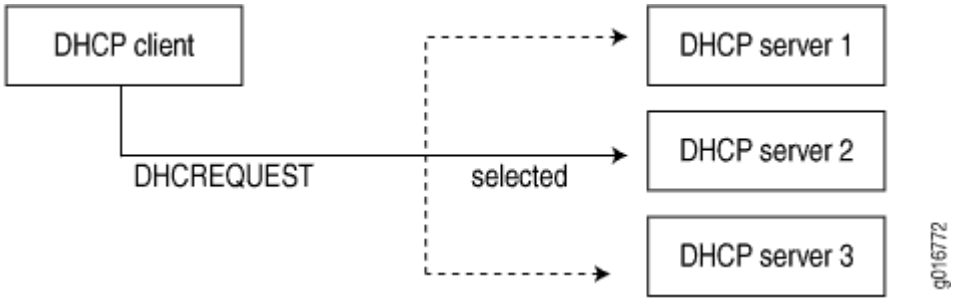
Figure 4: DHCP Offer



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

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

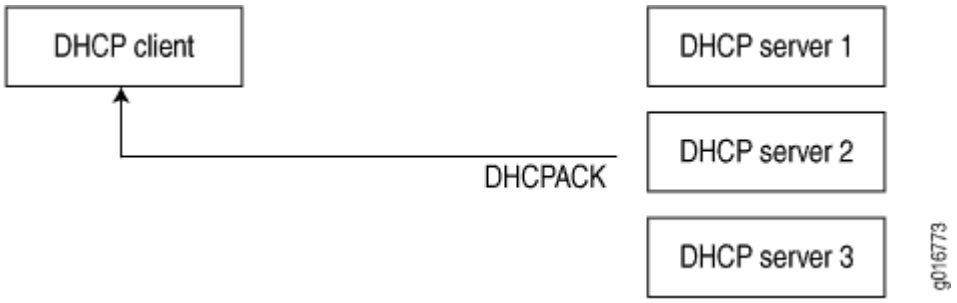
Figure 5: DHCP Request



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

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

Figure 6: DHCP ACK



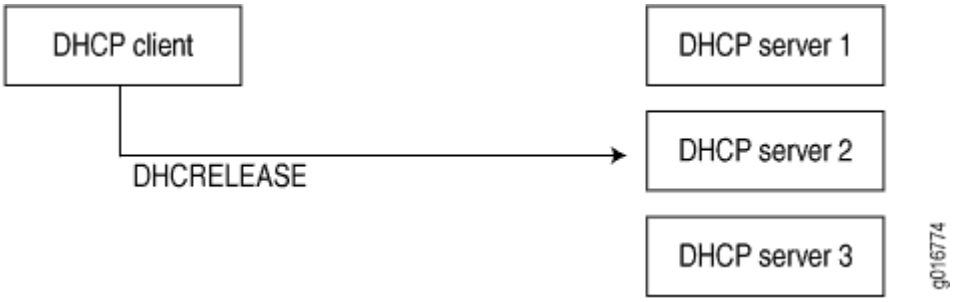
The information offered by the server is configurable.

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

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

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

Figure 7: DHCP Release



Network Address Assignments (Reusing a Previously Assigned Address)

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

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

DHCP Address Allocation Methods

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

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

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

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

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

DHCP Lease Time Management

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

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

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

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

DHCP Options

IN THIS SECTION

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

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

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

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

Table 1 on page 14 lists commonly used DHCP options.

Table 1: Commonly Used DHCP Options

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

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

Setting DHCP Options

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

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

Extended DHCP

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

Legacy DHCP

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

How DHCP Provides Minimum Network Configuration

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

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

- Domain name server—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

Legacy DHCP and Extended DHCP

IN THIS SECTION

- Understanding Differences Between Legacy DHCP and Extended DHCP | 17
- DHCP Statement Hierarchy and Inheritance | 20
- Difference in Legacy DHCP Relay and Extended DHCP Relay | 24
- Restrictions in Using Legacy DHCP and Extended DHCP | 24

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

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

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

Understanding Differences Between Legacy DHCP and Extended DHCP

IN THIS SECTION

- New Features and Enhancements in Extended DHCP | 17
- Benefits of Extended DHCP | 19
- Change in Configuring DHCP Local Server in Extended DHCP Environment | 19
- Legacy DHCP and Extended DHCP Server Hierarchy Levels Changes | 20

This topic covers the following sections:

New Features and Enhancements in Extended DHCP

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

- In extended DHCP, the address-assignment pools are external to the DHCP local server. The external address-assignment pools are managed by the **authd** process, independently of the DHCP local server, and can be shared by different client applications such as DHCP or PPPoE access. In legacy DHCP, client address pool and client configuration information reside on the DHCP server.
- Extended DHCP server interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide DHCP client authentication.
- You can configure the dynamic profile and authentication support on a global basis or for a specific group of interfaces.
- Extended DHCP local server supports IPv6 clients.
- Both DHCP local server and DHCPv6 local server support the specific address request feature, which enables you to assign a particular address to a client.
- The extended DHCP local server provides a minimal configuration to the DHCP client if the client does not have DHCP option 55 configured. The server provides the subnet mask of the address-assignment pool that is selected for the client. In addition to the subnet mask, the server provides the following values to the client if the information is configured in the selected address-assignment pool:

  - **router**—A router located on the client's subnet. This statement is the equivalent of DHCP option 3.
  - **domain name**—The name of the domain in which the client searches for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified. This is equivalent to DHCP option 15.
  - **domain name server**—A Domain Name System (DNS) name server that is available to the client to resolve hostname-to-client mappings. This is equivalent to DHCP option 6.
- You can configure the local server to use DHCP option 82 information in the client PDU to determine which named address range to use for a particular client. The client configuration information, which is configured in the address-assignment pool, includes user-defined options, such as boot server, grace period, and lease time.
- The extended DHCP server supports following features:
  - *Graceful Routing Engine switchover* (GRES), which provides mirroring support for clients.
  - Virtual routing and forwarding (VRF). The extended DHCP is also referred to as virtual router (VR) aware DHCP. See EX Series Switch Software Features Overview for a list of switches that support extended DHCP (VR-aware DHCP).

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

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

Feature	Legacy DHCP Local Server	Extended DHCP Local Server
Local address pools	X	X
External, centrally-managed address pools	–	X
Local configuration	X	X
External configuration using information from address-assignment pools or RADIUS servers	–	X
Dynamic-profile attachment	–	X

Table 2: Comparing the Extended DHCP Local Server to the Traditional DHCP Local Server *(Continued)*

Feature	Legacy DHCP Local Server	Extended DHCP Local Server
RADIUS-based subscriber authentication, and configuration using RADIUS attributes and Juniper Networks VSAs	–	X
IPv6 client support	–	X
Default minimum client configuration	X	X

Benefits of Extended DHCP

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

Change in Configuring DHCP Local Server in Extended DHCP Environment

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

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

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

Legacy DHCP and Extended DHCP Server Hierarchy Levels Changes

Legacy DHCP and extended DHCP servers can be configured at the hierarchy levels shown in Table 3 on page 20:

Table 3: Legacy DHCP and Extended DHCP Server Hierarchy Levels

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

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

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

DHCP Statement Hierarchy and Inheritance

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

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

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

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

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

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

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

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

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

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

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

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

To minimize configuration changes, include common configuration statements shown in tables above. For example, include the `domain-name` statement at the highest applicable level of the hierarchy (network or subnetwork). Configuration statements at lower levels of the hierarchy override statements inherited from a higher level. For example, if a statement appears at both the `[edit system services dhcp]` and `[edit system services dhcp pool]` hierarchy levels, the value assigned to the statement at the `[edit system services dhcp pool]` level takes priority.

Difference in Legacy DHCP Relay and Extended DHCP Relay

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

Restrictions in Using Legacy DHCP and Extended DHCP

IN THIS SECTION

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

Remember the following items while configuring extended DHCP:

- You can configure extended DHCP server and DHCP relay agent and legacy DHCP server and DHCP relay agent in the same network.
- You cannot configure extended DHCP server and DHCP relay agent and legacy DHCP server and DHCP relay agent on the same device. Because the newer extended DHCP server version has more features, we recommend that you configure the extended DHCP server if it is supported by the switch. A commit error is displayed if both legacy DHCPD and extended DHCP is configured simultaneously.

- DHCP clients on a switch are always configured at the hierarchy level `[edit interfaces interface-name family dhcp]`.
- If you delete the DHCP server configuration, DHCP server bindings might still remain. To ensure that DHCP bindings are removed, issue the `clear dhcp server binding` command before you delete the DHCP server configuration.

Features Not Supported by Extended DHCP

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

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

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information | 199

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

2

CHAPTER

Address Assignment Pool

IP Address Assignment Pool | 27

DHCPv6 Address-Assignment Pools | 39

IP Address Assignment Pool

IN THIS SECTION

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

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

Address-Assignment Pools Overview

IN THIS SECTION

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

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

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

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

Address Assignment Types

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

Named Address Ranges in Address Assignment Pool

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

Address Allocation from Linked Address Pools

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

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

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

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

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

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

Address Pool Hold-Down State

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

Address-Assignment Pool for Neighbor Discovery Router Advertisement

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

Excluding Specified Address or Address Range

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

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

Licensing Requirement

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

Benefits of Address Assignment Pools

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

Extended DHCP Local Server and Address-Assignment Pools

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

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

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

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

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

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

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

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

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

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

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

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

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

Example:

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

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

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

  Example:

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

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

Example:

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

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

  Example:

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

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

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

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

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

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

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

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

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

Configuring Address-Assignment Pools

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

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

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

Configuring an Address-Assignment Pool Name and Addresses

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

To configure an IPv4 address-assignment pool:

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

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

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

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

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

Configuring a Named Address Range for Dynamic Address Assignment

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

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

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

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

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

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

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

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

Configuring Static Address Assignments

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

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

To configure a static IPv4 address binding:

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

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

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

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

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

Configuring Address-Assignment Pool Linking

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

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

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

Configuring DHCP Client-Specific Attributes for Address-Assignment Pools

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

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

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

To configure address-assignment pool attributes for DHCP clients:

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

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

2. Configure optional DHCP client attributes.

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

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

Release History Table

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

RELATED DOCUMENTATION

DHCPv6 Address-Assignment Pools | 39

DHCP Overview | 2

Legacy DHCP and Extended DHCP | 16

DHCPv6 Address-Assignment Pools

IN THIS SECTION

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

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

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

IN THIS SECTION

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

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

Requirements

Before you begin:

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

Overview

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

Configuration

IN THIS SECTION

- Procedure | 40

Procedure

CLI Quick Configuration

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

```
set access address-assignment pool my-pool family inet6 prefix 2001:db8:3000:1::/64
set access address-assignment pool my-pool family inet6 range range1 low 2001:db8:3000:1::1/64
high 2001:db8:3000:1::100/64
set access address-assignment pool my-pool family inet6 dhcp-attributes dns-server
2001:db8:3000:1::1
set access address-assignment pool my-pool family inet6 dhcp-attributes grace-period 3600
set access address-assignment pool my-pool family inet6 dhcp-attributes maximum-lease-time 120
```

Step-by-Step Procedure

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

To configure an IPv6 address-assignment pool:

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

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

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

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

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

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

4. Configure the DHCPv6 attribute for the grace period.

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

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

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

Results

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

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

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

Verification

IN THIS SECTION

- Verifying Configuration | 42

Verifying Configuration

Purpose

Verify that the address-assignment pool has been configured.

Action

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

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

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

To configure a named address range for dynamic address assignment:

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

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

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

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

3. Configure DHCPv6 attributes for the address pool.

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

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

Configuring an Address-Assignment Pool for Router Advertisement

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

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

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

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

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

Configuring Nontemporary Address Assignment

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

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

To configure nontemporary (stateful) address assignment:

1. Specify the DHCPv6 client interface.

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

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

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

3. Specify the IA_NA assignment.

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

Configuring Identity Associations for Nontemporary Addresses and Prefix Delegation

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

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

1. Specify the DHCPv6 client interface.

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

2. Configure the client type as `statefull`.

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

3. Specify the IA_NA.

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

4. Specify the IA_PD.

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

Configuring Auto-Prefix Delegation

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

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

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

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

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

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

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

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

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

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

5. Specify the interface used to delegate prefixes.

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

Multiple Address Assignment for DHCPv6 Clients

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

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

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

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

SEE ALSO

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

RELATED DOCUMENTATION

> IP Address Assignment Pool | **27**
>
> DHCPv6 Server | **109**
>
> DHCPv6 Relay Agent | **222**
>
> DHCPv6 Client | **255**

3

CHAPTER

DHCP Server

DHCP Server | 49

DHCP Server Configuration | 51

DHCP Server Options | 77

Verifying DHCP Server Configuration | 95

Monitoring the DHCP Server Configuration | 100

DHCPv6 Server | 109

DHCP Server

IN THIS SECTION

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

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

Understanding DHCP Server Operation

IN THIS SECTION

- DHCP Options | 49
- Compatibility with Autoinstallation | 50
- Chassis Cluster Support | 50

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

This section contains the following topics:

DHCP Options

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

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

Compatibility with Autoinstallation

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

Chassis Cluster Support

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

Graceful Routing Engine Switchover for DHCP

For EX Series switches, only extended DHCP local server maintains the state of active DHCP client leases. The DHCP local server supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber authentication. You can configure dynamic profile and authentication support on a global basis or for a specific group of interfaces. The extended DHCP local server also supports the use of Junos address-assignment pools or external authorities, such as RADIUS, to provide the client address and configuration information.

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

You can enable graceful switchover support on both EX Series switches and MX Series routers. To enable graceful switchover support for the extended DHCP local server or extended DHCP relay agent on a switch, include the `graceful-switchover` statement at the `[edit chassis redundancy]` hierarchy level. To enable *graceful Routing Engine switchover* support on MX Series routers, include the `graceful-`

`switchover` statement at the `[edit chassis redundancy]` hierarchy level. You cannot disable graceful Routing Engine switchover support for the extended DHCP application when the router is configured to support graceful Routing Engine switchover.

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

SEE ALSO

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

RELATED DOCUMENTATION

- DHCP Overview | **2**
- DHCPv6 Server | **109**
- DHCP Client | **234**
- DHCPv6 Client | **255**
- DHCP with External Authentication Server | **266**
- Dynamic Reconfiguration of DHCP Servers and Clients | **305**

DHCP Server Configuration

IN THIS SECTION

- DHCP Server Configuration Overview | **52**
- Minimum DHCP Local Server Configuration | **54**
- Example: Complete DHCP Server Configuration | **56**
- Configure a Router as an Extended DHCP Local Server | **60**
- Configuring a Switch as a DHCP Server | **62**
- Configuring a DHCP Server on Switches | **66**

- Example: Configuring a Security Device as a DHCP Server | 68

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

DHCP Server Configuration Overview

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

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

In addition, the DHCP server might assign a static address to at least one client on the subnet. Table 7 on page 52 provides the settings and values for the sample DHCP server configuration.

Table 7: Sample DHCP Server Configuration Settings

Setting	Sample Value
DHCP Subnet Configuration	
Address pool subnet address	`192.168.2.0/24`
High address in the pool range	`192.168.2.254`

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

Setting	Sample Value
Low address in the pool range	`192.168.2.2`
Address pool default lease time, in seconds	`1,209,600` (14 days)
Address pool maximum lease time, in seconds	`2,419,200` (28 days)
Domain search suffixes	`mycompany.net` `mylab.net`
Address to exclude from the pool	`192.168.2.33`
DNS server address	`192.168.10.2`
Identifier code for router solicitation address option	`32`
Type choice for router solicitation address option	`Ip address`
IP address for router solicitation address option	`192.168.2.33`
DHCP MAC Address Configuration	
Static binding MAC address	`01:03:05:07:09:0B`
Fixed address	`192.168.2.50`

Minimum DHCP Local Server Configuration

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

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

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

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

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

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

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

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

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

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

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

Example: Complete DHCP Server Configuration

IN THIS SECTION

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

This topic shows a complete DHCP server configuration.

Requirements

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

Overview

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

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

Configuration

IN THIS SECTION

- Configuring [item] | 57
- Configure Legacy DHCP Server | 58

To configure the DHCP server, perform these tasks:

Configuring [item]

Step-by-Step Procedure

1. Configure DHCP server.

```
[edit access address-assignment pool P1 family inet dhcp-attributes]
range R1 {
    low 10.3.3.33;
    high 10.3.3.254;
}
dhcp-attributes {
    maximum-lease-time 7200;
    server-identifier 10.3.3.1;
    domain-name domain.tld;
    name-server {
        10.6.6.6;
        10.6.6.7;
    }
    wins-server {
        10.7.7.7;
        10.7.7.9;
    }
    router {
        198.51.100.0;
        198.51.100.1;
        10.6.6.1;
        10.7.7.1;
    }
    boot-file boot-client;
    boot-server 10.4.4.1;
    option 19 flag false;
    option 40 string domain.tld;
    option 16 ip-address 10.3.3.3;
}
host H1 {
    hardware-address 00:0d:56:f4:20:01;
    ip-address 10.4.4.4;
}
host H2 {
    hardware-address 00:0d:56:f4:01:ab;
    ip-address 10.5.5.6;
```

```
}
excluded-address 10.3.3.33;
excluded-address 192.0.2.5;
}
```

2. Configure client options.

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

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

Configure Legacy DHCP Server

Step-by-Step Procedure

1. Specify DHCP server configuration option.

```
dhcp {
    domain-name "domain.tld";
    maximum-lease-time 7200;
    default-lease-time 3600;
    name-server {
        10.6.6.6;
         10.6.6.7;
    }
```

```
    domain-search [ subnet1.domain.tld subnet2.domain.tld ];
    wins-server {
         10.7.7.7;
        10.7.7.9;
    }
    router {
        10.6.6.1;
        10.7.7.1;
    }
    option 19 flag off;       # 19: "IP Forwarding" option
    option 40 string "domain.tld"; # 40: "NIS Domain" option
    option 16 ip-address 10.3.3.33; # 16: "Swap Server" option
    pool 10.3.3.0/24 {
        address-range low 10.3.3.2 high 10.3.3.254;
        exclude-address {
            10.3.3.33;
        }
        router {
            10.3.3.1;
        }
        server-identifier 10.3.3.1;
    }
    pool 10.4.4.0/24 {
        boot-file "boot.client";
        boot-server 10.4.4.1;
    }
    static-binding 00:0d:56:f4:20:01 {
        fixed-address 10.4.4.4;
        host-name "host.domain.tld";
    }
    static-binding 00:0d:56:f4:01:ab {
        fixed-address {
            10.5.5.5;
            10.6.6.6;
        }
        host-name "another-host.domain.tld";
        client-identifier "01aa.001a.bc65.3e";
    }
}
```

2. Configure client options.

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

            address 10.3.3.1/24;
        }
}
```

Configure a Router as an Extended DHCP Local Server

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

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

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

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

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

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

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

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

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

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

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

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

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

Configuring a Switch as a DHCP Server

IN THIS SECTION

- Configuring the Switch as a Local DHCP Server | **63**

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

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

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

This topic describes the following task:

Configuring the Switch as a Local DHCP Server

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

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

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

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

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

For example:

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

```
user@switch# set vlans server l3-interface irb.301
user@switch# set interfaces irb.301 family inet address 192.0.2.2/24
```

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

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

For example:

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

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

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

For example:

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

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

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

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

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

For example:

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

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

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

For example:

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

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

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

Configuring a DHCP Server on Switches

IN THIS SECTION

- Configuring an Extended DHCP Server on a Switch | 67

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

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

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

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

This topic includes the following tasks:

Configuring an Extended DHCP Server on a Switch

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

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

1. Create an address pool for DHCP IP addresses:

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

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

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

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

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

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

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

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

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

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

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

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

Example: Configuring a Security Device as a DHCP Server

IN THIS SECTION

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

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

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

Requirements

Before you begin:

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

Overview

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

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated. and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

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

WARNING: Please see documentation for updated commands.

Configuration

IN THIS SECTION

- Procedure | 70

Procedure

CLI Quick Configuration

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

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

GUI Quick Configuration

Step-by-Step Procedure

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

1. In the J-Web interface, select **Configure** > **DHCP** > **DHCP Services**.
2. Select DHCP Pools. Click **Add**.
3. Specify the IP address that is used as the source address the DHCP server includes in IP packets when communicating with clients. The address is included in the DHCP packet in option 54.
4. Specify the subnet information for the IPv4 address-assignment pool. Type **192.168.2.0/24**.
5. In the Address Range Low, type **192.168.2.2**.
6. In the Address Range High, type **192.168.2.254**.
7. In the Exclude Addresses box, type the addresses you want excluded from a DHCP address pool. Type **192.168.2.0/24**
8. Specify the server identifier to assign to any DHCP clients in this address pool. The identifier can be used to identify a DHCP server in a DHCP message.
9. Specify the domain name to assign to any DHCP clients in this address pool.

10. Specify the next server that DHCP clients need to contact. Type **192.168.10.2**

11. Define the maximum amount of time (in seconds) that DHCP should lease an address. Type **2419200**.

12. Define DHCP option 32, the device solicitation address option. You must enter a numeric value for option code. Select the option type from the list that corresponds to the option code.

13. Click **OK**.

14. If you are done configuring the device, click **Commit** > **Commit**.

Step-by-Step Procedure

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

To configure the device as a DHCP server:

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

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

2. Configure the DHCP server.

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

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

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

4. (Optional) Specify the IP address pool range. Define a range of addresses in the address-assignment pool. The range is a subset of addresses within the pool that can be assigned to clients. If no range is

specified, then all addresses within the pool are available for assignment. Configure the name of the range and the lower and upper boundaries of the addresses in the range.

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

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

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

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

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

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

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

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

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

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

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

Results

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

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

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

```
[edit]
user@host# show system services dhcp-local-server
group g1 {
```

```
interface ge-0/0/2.0;
}
```

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

Verification

IN THIS SECTION

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

Confirm that the configuration is working properly.

Verifying the DHCP Binding Database

Purpose

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

Action

From operational mode, enter these commands:

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

These commands produce following sample output:

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

```
user@host> show dhcp server binding address detail
    IP address           192.0.2.2
    Hardware address     00:a0:12:00:13:02
```

```
    Pool                192.0.2.0/24
    Interface  fe-0/0/0, relayed by 192.0.2.200

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

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

Verifying DHCP Server Operation

Purpose

Verify that the DHCP server operation has been configured.

Action

From operational mode, enter the following command:

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

```
user@host> show dhcp server statistics
Packets dropped:
    Total                     0

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

Messages sent:
```

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

SEE ALSO

Understanding DHCP Relay Agent Operation

Release History Table

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

RELATED DOCUMENTATION

DHCP Overview | **2**

DHCP Server | **49**

DHCP Server Options | **77**

Verifying DHCP Server Configuration | **95**

Monitoring the DHCP Server Configuration | **100**

Legacy DHCP and Extended DHCP | **16**

DHCP Server Options

IN THIS SECTION

- Configure DHCP Server Identifier | 77
- Configure Address Pools for DHCP Dynamic Bindings | 78
- Configure Manual (Static) DHCP Bindings Between a Fixed IP Address and a Client MAC Address | 79
- Enabling TCP/IP Propagation on a DHCP Local Server | 80
- Specify DHCP Lease Times for IP Address Assignments | 81
- Configure a DHCP Boot File and DHCP Boot Server | 81
- Configure Domain Name and Domain Search List | 82
- Configure Routers Available to the DHCP Client | 83
- Configure User-Defined DHCP Options | 83
- Configure DHCP SIP Server | 84
- Overriding the Default DHCP Local Server Configuration Settings | 85
- Legacy DHCP Server Configuration Options | 87

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

Configure DHCP Server Identifier

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

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

Example:

```
[edit access address-assignment pool P1 family inet]
dhcp-attributes {
```

```
    server-identifier 192.0.2.0;
}
```

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

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

Configure Address Pools for DHCP Dynamic Bindings

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

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

The following is an example of a pool configuration.

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

Note the following when configuring address pools:

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

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

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

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

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

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

The following is an example of a static binding configuration:

```
[edit access address-assignment pool P1 family inet]
host H1 {
    hardware-address 2c:56:dc:72:99:f3;
    ip-address 192.0.2.0;
}
```

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

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

Enabling TCP/IP Propagation on a DHCP Local Server

Propagation of TCP/IP Settings for DHCP

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

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

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

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

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

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

```
[edit interfaces ge-0/0/1 unit 0 family inet]
dhcp {
    update-server;
}
```

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

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

```
    }
}
```

3. Configure the DHCP local server.

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

Specify DHCP Lease Times for IP Address Assignments

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

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

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

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

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

Configure a DHCP Boot File and DHCP Boot Server

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

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

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

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

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

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

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

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

Configure Domain Name and Domain Search List

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

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

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

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

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

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

Configure Routers Available to the DHCP Client

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

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

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

Example:

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

Configure User-Defined DHCP Options

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

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

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

The `option` statement specifies the following values:

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

The following example shows user-defined DHCP options:

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

Configure DHCP SIP Server

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

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

```
[edit access address-assignment pool P1 family inet]
    dhcp-attributes {
```

```
        sip-server 198.51.100.0;
    }
```

Overriding the Default DHCP Local Server Configuration Settings

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

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

To override default DHCP local server configuration settings:

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

    Global override:

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

    Group-level override:

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

Per-interface override:

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

DHCPv6 overrides.

Global override:

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

Group level override:

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

Per-interface override:

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

- (Optional) Override the maximum number of DHCP clients allowed per interface.

  See *Specifying the Maximum Number of DHCP Clients Per Interface*.

- (Optional) Configure DHCP client auto logout.

  See *Automatically Logging Out DHCP Clients*.

- (Optional) Enable processing of information requests from clients.

  See *Enabling Processing of Client Information Requests*.

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

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

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

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

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

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

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

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

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

  See *Automatically Logging Out DHCPv6 Clients*.

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

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

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

  See *Configuring DHCP Asymmetric Leasing*.

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

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

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

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

Legacy DHCP Server Configuration Options

IN THIS SECTION

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

DHCP Options | 93
DHCP SIP Server | 94

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

DHCP Server Identifier

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

You can configure DHCP server identifier in following hierarchy levels:

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

Example:

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

```
[edit system services dhcp]
pool 10.3.3.0/24 {
    address-range low 10.3.3.2 high 10.3.3.254;
    server-identifier 10.3.3.1;
}
```

Static-Binding

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

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

```
[edit system services dhcp]
static-binding mac-address {
    fixed-address {
        address;
```

```
    }
    host client-hostname;
    client-identifier (ascii client-id | hexadecimal client-id);
}
```

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

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

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

Example:

```
[edit system services dhcp]
static-binding 00:0d:56:f4:01:ab {
    fixed-address {
        10.5.5.5;
        10.6.6.6;
    }
    host-name "another-host.domain.tld";
    client-identifier hexadecimal 01001122aabbcc;
}
```

Configuring Address Pools

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

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

Example:

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

Maximum Lease Time

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

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

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

You can include these statements at the following hierarchy levels:

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

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

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

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

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

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

Boot File and Boot Server

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

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

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

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

You can include these statements at the following hierarchy levels:

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

Example:

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

Domain Name and Domain Search

```
domain-name domain;
```

You can include this statement at the following hierarchy levels:

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

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

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

You can include this statement at the following hierarchy levels:

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

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

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

Router Name

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

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

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

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

```
router {
    address;
}
```

Example:

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

You can include this statement at the following hierarchy levels:

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

DHCP Options

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

Example

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

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

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

You can include this statement at the following hierarchy levels:

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

DHCP SIP Server

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

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

For example, to configure one address:

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

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

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

For example, to configure a name:

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

RELATED DOCUMENTATION

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

Verifying DHCP Server Configuration

IN THIS SECTION

- Verifying DHCP Server Binding and Server Statistics | 96
- Viewing DHCP Bindings (Legacy DHCP) | 97
- Viewing DHCP Address Pools (Legacy DHCP) | 99
- Viewing and Clearing DHCP Conflicts (Legacy DHCP) | 99

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

Verifying DHCP Server Binding and Server Statistics

IN THIS SECTION

- Purpose | 96
- Action | 96

Purpose

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

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

Action

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

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

- To display extended DHCP local server statistics:

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

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

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

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

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

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

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

- To clear all extended DHCP local server statistics:

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

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

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

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

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

Viewing DHCP Bindings (Legacy DHCP)

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

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

```
user@host> show system services dhcp binding
IP Address       Hardware Address     Type    Lease expires at
```

```
192.168.1.2      00:a0:12:00:12:ab       static      never
192.168.1.3      00:a0:12:00:13:02       dynamic     2004-05-03 13:01:42 PDT
```

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

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

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

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

Viewing DHCP Address Pools (Legacy DHCP)

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

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

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

Viewing and Clearing DHCP Conflicts (Legacy DHCP)

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

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

```
user@host> show system services dhcp conflict
Detection time                  Detection method       Address
2004-08-03 19:04:00 PDT         client      192.168.1.5
2004-08-04 04:23:12 PDT         ping      192.168.1.8
```

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

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

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

RELATED DOCUMENTATION

DHCP Server | 49

DHCP Server Options | 77

IP Address Assignment Pool | 27

DHCP Access Service Overview | 9

Monitoring the DHCP Server Configuration

IN THIS SECTION

- DHCP Processes Tracing Flags | 100
- Tracing Extended DHCP Local Server Operations | 102
- Configuring Tracing Operations for DHCP Processes | 105

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

DHCP Processes Tracing Flags

Table 8 on page 100 describes which operation or event is recorded by each DHCP tracing flag. By default, all flags are disabled.

Table 8: DHCP Processes Tracing Flags

Flag	Operation or Event
`all`	All operations.
`binding`	Binding operations.
`config`	Logins to the configuration database.

Table 8: DHCP Processes Tracing Flags *(Continued)*

Flag	Operation or Event
`conflict`	Client-detected conflicts for IP addresses.
`event`	Important events.
`ifdb`	Interface database operations.
`io`	I/O operations.
`lease`	Lease operations.
`main`	Main loop operations.
`misc`	Miscellaneous operations.
`packet`	DHCP packets.
`options`	DHCP options.
`pool`	Address pool operations.
`protocol`	Protocol operations.
`rtsock`	Routing socket operations.
`scope`	Scope operations.
`signal`	DHCP signal operations.
`trace`	Tracing operations.

Table 8: DHCP Processes Tracing Flags *(Continued)*

Flag	Operation or Event
`ui`	User interface operations.

Tracing Extended DHCP Local Server Operations

IN THIS SECTION

- Configuring the Filename of the Extended DHCP Local Server Processes Log | **103**
- Configuring the Number and Size of Extended DHCP Local Server Processes Log Files | **103**
- Configuring Access to the Log File | **104**
- Configuring a Regular Expression for Lines to Be Logged | **104**
- Configuring Trace Option Flags | **104**

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

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

NOTE: In software releases earlier than Junos OS 11.4, you configured tracing statements at the `[edit system services dhcp-local-server]` and `[edit forwarding-options dhcp-relay]` hierarchy levels. Starting in Junos OS Release 11.4, these statements have been deprecated and hidden in

favor of a new statement at the `[edit system processes dhcp-service]` hierarchy level. The deprecated statements may be removed from a future release; we recommend that you transition to the new statement.

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

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

The following topics describe the tracing operation configuration statements:

Configuring the Filename of the Extended DHCP Local Server Processes Log

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

```
[edit system processes dhcp-servicetraceoptions]
file filename;
```

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

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

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

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

For example, set the maximum file size to 2 MB, and the maximum number of files to 20. When the file that receives the output of the tracking operation (**jdhcpd**) reaches 2 MB, **jdhcpd** is renamed **jdhcpd.0**, and a new file called **jdhcpd** is created. When the new **jdhcpd** reaches 2 MB, **jdhcpd.0** is renamed

jdhcpd.1 and ***filename*** is renamed **jdhcpd.0**. This process repeats until there are 20 trace files. Then the oldest file (**jdhcpd.19**) is overwritten by the newest file (**jdhcpd.0**).

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

Configuring Access to the Log File

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

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

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

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

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

Configuring a Regular Expression for Lines to Be Logged

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

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

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

Configuring Trace Option Flags

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

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

You can configure the following tracing flags:

- `all`—Trace all operations.
- `auth`—Trace authentication operations.
- `database`—Trace database events.
- `fwd`—Trace firewall process events.
- `general`—Trace miscellaneous events.
- `ha`—Trace high availability-related events.
- `interface`—Trace interface operations.
- `io`—Trace I/O operations.
- `packet`—Trace packet decoding operations.
- `performance`—Trace performance measurement operations.
- `profile`—Trace profile operations.
- `rpd`—Trace routing protocol process events.
- `rtsock`—Trace routing socket operations.
- `session-db`—Trace session database operations.
- `state`—Trace changes in state.
- `statistics`—Trace baseline statistics.
- `ui`—Trace user interface operations.

Configuring Tracing Operations for DHCP Processes

IN THIS SECTION

- Configuring the DHCP Processes Log Filename | **106**
- Configuring the Number and Size of DHCP Processes Log Files | **107**
- Configuring Access to the DHCP Log File | **107**

Configuring a Regular Expression for Refining the Output of DHCP Logged Events | 107
Configuring DHCP Trace Operation Events | 108

DHCP tracing operations track all DHCP operations and record them to a log file. By default, no DHCP processes are traced. If you include the `traceoptions` statement at the `[edit system services dhcp]` hierarchy level, the default tracing behavior is the following:

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

You cannot change the directory in which trace files are located. However, you can customize the other trace file settings by including the following statements at the `[edit system services dhcp traceoptions]` hierarchy level:

```
[edit system services dhcp traceoptions]
file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
flag {
    all;
}
```

Tasks for configuring DHCP tracing operations are:

Configuring the DHCP Processes Log Filename

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

```
[edit system services dhcp traceoptions]
file filename;
```

Configuring the Number and Size of DHCP Processes Log Files

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

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

```
[edit system services dhcp traceoptions]
file files number size size;
```

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

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

Configuring Access to the DHCP Log File

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

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

```
[edit system services dhcp traceoptions]
file world-readable;
```

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

```
[edit system services dhcp traceoptions]
file no-world readable;
```

Configuring a Regular Expression for Refining the Output of DHCP Logged Events

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

You can refine the output by including the match statement at the [edit system services dhcp traceoptions file *filename*] hierarchy level and specifying a regular expression (regex) to be matched:

```
[edit system services dhcp traceoptions]
file filename match regex;
```

Configuring DHCP Trace Operation Events

By default, only important events are logged. You can configure the trace operations to be logged by including the following options at the [edit system services dhcp traceoptions] hierarchy level:

```
[edit dhcp system services dhcp traceoptions]
flag {
    all;
    binding;
    config;
    conflict;
    event;
    ifdb;
    io;
    lease;
    main;
    misc;
    packet;
    options;
    pool;
    protocol;
    rtsock;
    scope;
    signal;
    trace;
    ui;
}
```

RELATED DOCUMENTATION

DHCP Server | 49

DHCP Server Options | 77

DHCP Server Configuration | 51

DHCPv6 Server

IN THIS SECTION

- DHCPv6 Local Server Overview | 109
- DHCPv6 Server Overview | 111
- Example: Configuring DHCPv6 Server Options | 112
- Specifying the Address Pool for IPv6 Prefix Assignment | 117
- Specifying the Delegated Address Pool for IPv6 Prefix Assignment | 118
- Preventing Binding of Clients That Do Not Support Reconfigure Messages | 119
- Configuring DHCPv6 Rapid Commit (MX Series, EX Series) | 120
- Allow Host Inbound Traffic for DHCPv6 Traffic | 121
- Verifying and Managing DHCPv6 Local Server Configuration | 122
- Understanding Cascaded DHCPv6 Prefix Delegating | 123
- Example - Configuring DHCPv6 Prefix Delegation (PD) over Point-to-Point Protocol over Ethernet (PPPoE) | 124

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

DHCPv6 Local Server Overview

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

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

- Configuration for a specific interface or for a group of interfaces

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

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

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

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

- Client username
- Client password

Based on the attributes that the DHCPv6 local server provides, RADIUS returns the information listed in Table 9 on page 110 to configure the client:

Table 9: RADIUS Attributes and VSAs for DHCPv6 Local Server

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

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

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

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

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

DHCPv6 Server Overview

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

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

Some features include:

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

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

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

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

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

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

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

Example: Configuring DHCPv6 Server Options

IN THIS SECTION

- Requirements | **112**
- Overview | **113**
- Configuration | **113**
- Verification | **116**

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

Requirements

Before you begin:

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

Overview

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

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

Configuration

IN THIS SECTION

- Procedure | 113

Procedure

CLI Quick Configuration

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

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

Step-by-Step Procedure

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

To configure DHCPv6 server options:

1. Configure a DHCP local server.

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

2. Set a default limit for all DHCPv6 groups.

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

3. Specify a group name and interface.

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

4. Set a range of interfaces.

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

5. Set a custom client limit for the group.

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

6. Configure an interface with an IPv6 address.

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

7. Set router advertisement for the interface.

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

Results

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

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

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

Verification

IN THIS SECTION

- Verifying DHCPv6 Local Server Configuration | **116**

Verifying DHCPv6 Local Server Configuration

Purpose

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

Action

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

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

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

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

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

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

SEE ALSO

> *Example: Configuring an Address-Assignment Pool for IPv6 Addresses*
>
> *Configuring a Named Address Range and DHCPv6 Attributes for Dynamic Address Assignment*

Specifying the Address Pool for IPv6 Prefix Assignment

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

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

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

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

To configure the address pool for DHCPv6 local server:

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

```
[edit access]
user@host# set address-assignment pool POOL family inet6 prefix 2001:db8::/32
```

2. Set range.

```
[edit access]
user@host# set address-assignment pool POOL family inet6 range RANGE1 low 2001:db8::2/32
user@host# set address-assignment pool POOL family inet6 range RANGE1 high 2001:db8::aaaa/32
```

SEE ALSO

IP Address Assignment Pool | 27

DHCPv6 Address-Assignment Pools | 39

Specifying the Delegated Address Pool for IPv6 Prefix Assignment

You can explicitly specify a delegated address pool:

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

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

To configure the delegated address pool for DHCPv6 local server:

1. Specify that you want to configure override options.

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

2. Configure the delegated address pool.

```
[edit system services dhcp-local-server dhcpv6 overrides]
user@host# set delegated-pool paris-cable-12
```

SEE ALSO

Overriding the Default DHCP Local Server Configuration Settings

Understanding Differences Between Legacy DHCP and Extended DHCP

Extended DHCP Relay Agent Overview

Preventing Binding of Clients That Do Not Support Reconfigure Messages

The DHCPv6 client and server negotiate the use of reconfigure messages. When the client can accept reconfigure messages from the server, then the client includes the Reconfigure Accept option in both solicit and request messages sent to the server.

By default, the DHCPv6 server accepts solicit messages from clients regardless of whether they support reconfiguration. You can specify that the server require clients to accept reconfigure messages. In this case, the DHCPv6 server includes the Reconfigure Accept option in both advertise and reply messages when reconfiguration is configured for the client interface. Solicit messages from nonsupporting clients are discarded and the clients are not allowed to bind.

To configure the DHCPv6 local server to bind only clients that support client-initiated reconfiguration:

- Specify strict reconfiguration.

  For all DHCPv6 clients:

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

  For only a particular group of DHCPv6 clients:

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

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

SEE ALSO

> *Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview*
>
> *Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients*

Configuring DHCPv6 Rapid Commit (MX Series, EX Series)

You can configure the DHCPv6 local server to support the DHCPv6 Rapid Commit option (DHCPv6 option 14). When rapid commit is enabled, the server recognizes the Rapid Commit option in Solicit messages sent from the DHCPv6 client. (DHCPv6 clients are configured separately to include the DHCPv6 Rapid Commit option in the Solicit messages.) The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-message exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

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

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

1. Specify that you want to configure the `overrides` options:

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

2. Enable rapid commit support:

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

SEE ALSO

> *Overriding the Default DHCP Local Server Configuration Settings*

Allow Host Inbound Traffic for DHCPv6 Traffic

For the DHCPv6 server to allow DHCPv6 requests, you must configure host inbound traffic system services to allow DCHPv6 traffic. In this example, the zone my-zone allows DHCPv6 traffic from the zone untrust, and the ge-0/0/3.0 interface is configured with the IPv6 address 2001:db8:3001::1.

To create a security zone policy to allow DHCPv6 on SRX1500, SRX5400, SRX5600, and SRX5800 devices:

1. Create the zone and add an interface to that zone.

```
[edit security zones]
user@host# edit security-zone my-zone interfaces ge-0/0/3.0
```

2. Configure host inbound traffic system services to allow DCHPv6.

```
[edit security zones security-zone my-zone interfaces ge-0/0/3.0]
user@host# set host-inbound-traffic system-services dhcpv6
```

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

SEE ALSO

Example: Configuring an Address-Assignment Pool for IPv6 Addresses

Verifying and Managing DHCPv6 Local Server Configuration

IN THIS SECTION

- Purpose | 122
- Action | 122

Purpose

View or clear information about client address bindings and statistics for the DHCPv6 local server.

Action

- To display the address bindings in the client table on the DHCPv6 local server:

```
user@host> show dhcpv6 server binding
```

- To display DHCPv6 local server statistics:

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

- To clear all DHCPv6 local server statistics:

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

- To clear all DHCPv6 local server statistics:

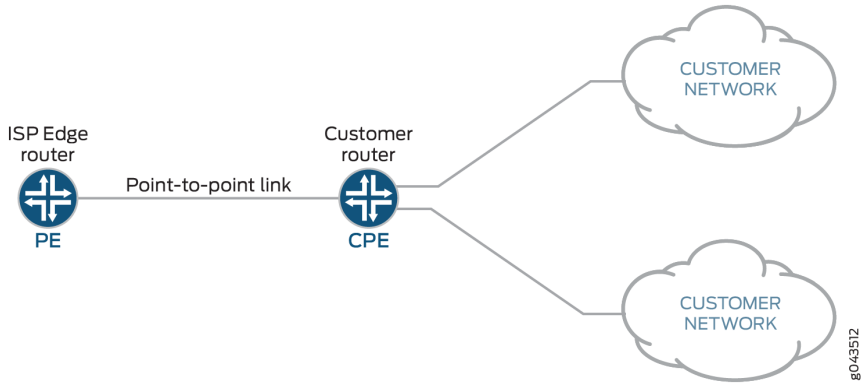
```
user@host> clear dhcpv6 server statistics
```

Understanding Cascaded DHCPv6 Prefix Delegating

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

With cascaded prefix delegation, the IPv6 address block is delegated to a DHCPv6 client that is running on the WAN interface of a customer edge device. The identity association (IA) for the client is used for the identity association for prefix delegation (IA_PD). The CE device requests, through DHCPv6, an IPv6 address with the IA type of nontemporary addresses (IA_NA). Both IA_PD and IA_NA are requesting in the same DHCPv6 exchange.

Figure 8: IPv6 Prefix Delegation

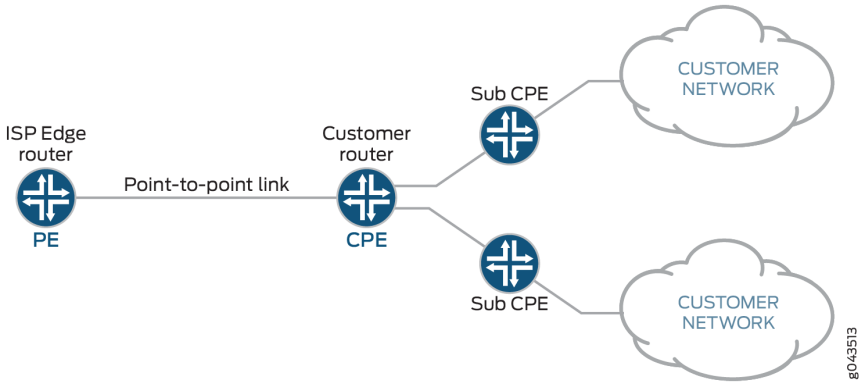


The topology in Figure 8 on page 123shows an SRX Series device acting as the CPE. The WAN interface links to the provider edge (PE) device and the LAN interfaces link to the customer networks. The service provider delegates a prefix (delegated-prefix) and an IPv6 address (cpe-wan-ipv6-address) to a DHCPv6 client. When a requesting device receives that IPv6 address through the DHCPv6 client, the device must install the IPv6 address on its WAN interface. The DHCPv6 client then divides the delegated prefix into sub-prefixes and subsequently assigns them to the connected LAN interfaces of the CPE device, making some subset of the remaining space available for sub-prefix delegation.

A CPE assigns sub-prefixes to its LAN interfaces and broadcasts the sub-prefixes through device advertisement. In this scenario, the CPE acts as a sub-PE and delegates sub-prefixes and assigns them to sub-CPEs.

NOTE: The requirements of sub-prefix delegation are the same as for the prefix delegation defined in RFC 3769.

Figure 9: Sub-prefix Delegation



There can be multi-level sub prefix delegations, see Figure 9 on page 124. The top level CPE gets a delegated prefix from the PE and delegates the sub prefixes to second level sub-CPEs, then to the third level sub-CPEs, and finally to the end levels. The end level sub-CPEs assign the IPv6 address to end hosts through SLAAC, stateless DHCPv6 or stateful DHCPv6. This is called cascaded prefix delegating.

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

IN THIS SECTION

- Requirements | 125
- Overview | 125
- Configuration | 126
- Verification | 147

This example shows how to configure DHCPv6 PD over PPPoE on SRX Series devices.

Requirements

No special configuration beyond the device initialization is required before configuring this feature.

Overview

IN THIS SECTION

- Topology | 125

The example uses SRX550M devices for configuring DHCPv6 PD over PPPoE. Before you begin, configure DHCPv6 server to permit in host-inbound traffic and receive DHCPv6 packet. Provide a host-name to establish PPPoE session. To enable IPv6, chassis reboot is required.

Configuring DHCPv6 PD over PPPoE involves the following configurations:

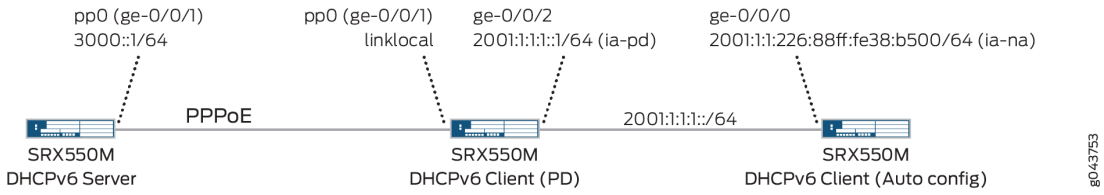
- Configuring DHCPv6 Server
- DHCPv6 Client (PD)
- DHCPv6 Client (Auto)

Topology

The following illustration describes DHCPv6 PD over PPPoE topology which provide a configuration suite using SRX Series devices.

Figure 10 on page 125 shows the topology used in this example.

Figure 10: Configuring SRX Series Devices for DHCPv6 PD over PPPoE



Configuration

IN THIS SECTION

- CLI Quick Configuration | 126
- Procedure | 129
- Procedure | 133
- Procedure | 137
- Results | 138

CLI Quick Configuration

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

Quick configuration for DHCPv6 Server:

- DHCPv6 server configuration

```
set interfaces ge-0/0/1 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 100
set system services dhcp-local-server dhcpv6 group my-group overrides interface-client-limit
200
set system services dhcp-local-server dhcpv6 group my-group overrides delegated-pool v6-pd-
pool
set system services dhcp-local-server dhcpv6 group my-group interface pp0.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap access-profile prof-ge001
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options server
set interfaces pp0 unit 0 family inet6 address 3000::1/64
```

- Router advertisement configuration

```
set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
set protocols router-advertisement interface pp0.0 managed-configuration
set protocols router-advertisement interface pp0.0 other-stateful-configuration
set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- PPPoE profile configuration

```
set access profile prof-ge001 client test_user chap-secret test
```

- PD address pool configuration

```
set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-length 48
set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-server 3000::1
```

- Security zone configuration

```
set security zones security-zone trust interface pp0.0 host-inbound-traffic system-services
dhcpv6
```

Quick configuration for DHCPv6 Client (PD):

- DHCPv6 server configuration

```
set interfaces ge-0/0/1 unit 0 family inet6
set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
```

- PPPoE configuration

```
set system host-name SRX550M
set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
set interfaces pp0 unit 0 ppp-options chap local-name test_user
set interfaces pp0 unit 0 ppp-options chap passive
set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
set interfaces pp0 unit 0 pppoe-options client
```

- DHCPv6 client configuration

```
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 other-stateful-configuration
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 max-advertisement-interval 10
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-advertisement interface
ge-0/0/2.0 min-advertisement-interval 5
set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
set protocols router-advertisement interface pp0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- DHCPv6 server propagate configuration

```
set access address-assignment pool p1 family inet6 prefix 2001::/16
set access address-assignment pool p1 family inet6 dhcp-attributes propagate-settings pp0.0
```

- Security zone configuration

```
set security zones security-zone untrust interface pp0.0 host-inbound-traffic system-services
dhcpv6
```

```
set security zones security-zone trust interface ge-0/0/2.0 host-inbound-traffic system-
services dhcpv6
```

Quick configuration for DHCPv6 Client (Auto):

- DHCPv6 client configuration

```
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-ia-type ia-na
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier duid-type duid-ll
set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

- Router advertisement configuration

```
set protocols router-advertisement interface ge-0/0/0.0
```

- Enable IPv6

```
set security forwarding-options family inet6 mode flow-based
```

- Security zone configuration

```
set security zones security-zone trust interface ge-0/0/0.0 host-inbound-traffic system-
services dhcpv6
```

Procedure

Step-by-Step Procedure

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

1. To configure DHCPv6 server on SRX550M device:

   a. Set the interface.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 family inet6
```

b. Configure a DHCP local server.

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

c. Set a default limit for all DHCPv6 groups.

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

d. Set a custom client limit for the group.

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

e. Specify delegated pool name.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group overrides delegated-pool v6-pd-pool
```

f. Create a group called my-group that contains pp0 interface.

```
[edit system services dhcp-local-server dhcpv6]
user@host# set group my-group interface pp0.0
```

2. Configuring PPPoE:

a. Set interface to encapsulate PPPoE.

```
[edit]
user@host# set interfaces ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

b. Set chap access profile value.

```
[edit system interface]
user@host# set interface pp0 unit 0 ppp-options chap access-profile prof-ge001
```

c. Set underlying interface name.

```
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

d. Set PPPoE-options server.

```
[edit system interface]
user@host# set interface pp0 unit 0 pppoe-options server
```

e. Set family name and address.

```
[edit system interface]
user@host# set interface pp0 unit 0 family inet6 address 3000::1/64
```

3. Configuring Router advertisement:

a. Set max advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 max-advertisement-interval 20
```

b. Set minimum advertisement interval limit.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 min-advertisement-interval 10
```

c. Set the configuration state to managed configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 managed-configuration
```

d. Set the configuration state to other stateful configuration.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 other-stateful-configuration
```

e. Set the prefix value.

```
[edit system protocol]
user@host# set protocols router-advertisement interface pp0.0 prefix 3000::1/64
```

4. Enable IPv6:

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring PPPoE profile:

a. Set access profile name, client name and chap secret.

```
[edit]
user@host# set access profile prof-ge001 client test_user chap-secret test
```

6. Configuring PD address pool:

a. Set address-assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 prefix 2001:1:1::/48
```

b. Set range and prefix length.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 range vp-pd prefix-
length 48
```

c. Set dhcp attributes with dns server value.

```
[edit]
user@host# set access address-assignment pool v6-pd-pool family inet6 dhcp-attributes dns-
server 3000::1
```

7. Configuring Security zone:

   a. Set the zone name, interface and host-inbound-traffic system-services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic
system-services dhcpv6
```

Procedure

Step-by-Step Procedure

1. To configure DHCPv6 client (PD) on SRX550M device:

   a. Set the interface.

```
[edit]
user@host# set interfaces ge-0/0/2 unit 0 family inet6
```

   b. Set DHCPv6 local server to override the interface client limit.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides interface-client-limit 10
```

   c. Set the process-inform pool name.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 overrides process-inform pool p1
```

   d. Set group name and interface.

```
[edit]
user@host# set system services dhcp-local-server dhcpv6 group ipv6 interface ge-0/0/2.0
```

2. Configuring PPPoE:

a. Set the interface to encapsulate ppp over ethernet.

```
[edit system interface]
user@host# set interface ge-0/0/1 unit 0 encapsulation ppp-over-ether
```

b. Set default chap secret.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap default-chap-secret test
```

c. Set chap local name.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap local-name test_user
```

d. Set PPP options chap state.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 ppp-options chap passive
```

e. Set underlying-interface.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options underlying-interface ge-0/0/1.0
```

f. Set pppoe-options.

```
[edit system interface]
user@host# set interfaces pp0 unit 0 pppoe-options client
```

3. Configuring DHCPv6 client:

a. Set the family name and dhcpv6 client type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-type statefull
```

b. Set the dhcpv6 client identity association type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-ia-type ia-pd
```

c. Set update-router-advertisement interface and other stateful-configuration.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 other-stateful-configuration
```

d. Set maximum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 max-advertisement-interval 10
```

e. Set minimum advertisement interval value.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-router-
advertisement interface ge-0/0/2.0 min-advertisement-interval 5
```

f. Set client-identifier duid type.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client client-identifier duid-
type duid-11
```

g. Set requested option for DHCPv6 client.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client req-option dns-server
```

h. Update the server.

```
[edit]
user@host# set interfaces pp0 unit 0 family inet6 dhcpv6-client update-server
```

i. Set the protocols and the interface.

```
[edit]
user@host# set protocols router-advertisement interface pp0.0
```

4. Enable IPv6

a. Set the family name and mode to enable IPv6.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

5. Configuring DHCPv6 server to propagate DNS server information to end device:

a. Set address assignment pool name, family name and prefix.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 prefix 2001::/16
```

b. Set the interface name for propagating TCP/IP settings to pool.

```
[edit]
user@host# set access address-assignment pool p1 family inet6 dhcp-attributes propagate-
settings pp0.0
```

6. Configuring security zone:

a. Set the zone name, untrust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic
system-services dhcpv6
```

b. Set the trust interface.

```
[edit]
user@host# set security zones security-zone trust interface ge-0/0/2.0 host-inbound-
traffic system-services dhcpv6
```

Procedure

Step-by-Step Procedure

1. To configure DHCPv6 client (Auto) on SRX550M device:

   a. Set the interface, unit value, family name and DHCPv6 client type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-type autoconfig
   ```

   b. Set Dhcpv6 client identity association type.

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

   c. Set client-identifier type.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client client-identifier
   duid-type duid-11
   ```

   d. Set DHCPV6 client requested option.

   ```
   [edit system interface]
   user@host# set interfaces fe-0/0/0 unit 0 family inet6 dhcpv6-client req-option dns-server
   ```

2. Configuring router advertisement:

a. Set the protocol and interface.

```
[edit]
user@host# set protocols router-advertisement interface fe-0/0/0.0
```

3. Enable IPv6.

a. Set family name and mode.

```
[edit]
user@host# set security forwarding-options family inet6 mode flow-based
```

4. Configuring security zone:

5. Set the zone name, trust interface and system services.

```
[edit]
user@host# set security zones security-zone trust interface pp0.0 host-inbound-traffic system-
services dhcpv6
```

Results

- Result for DHCPv6 Server:

From configuration mode, confirm your configuration by entering the `show system services dhcp-local-server`, `show interfaces`, `show protocols`, `show security forwarding-options`, `show access profile prof-ge001`, `show access address-assignment pool`, and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
    overrides {
        interface-client-limit 100;
    }
    group my-group {
        overrides {
            interface-client-limit 200;
            delegated-pool v6-pd-pool;
        }
```

```
        interface pp0.0set;
        interface pp0.0;
    }
    }
...
[edit]
user@host# show interfaces
ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
    }
}
ge-0/0/1 {
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
            }
        }
```

```
    }
}
...
[edit]
user@host# show protocols
interface pp0.0 {
    max-advertisement-interval 20;
    min-advertisement-interval 10;
    managed-configuration;
    other-stateful-configuration;
    prefix 3000::1/64;
}
...
[edit]
user@host# show security forwarding-options
family {
    inet6 {
        mode flow-based;
    }
}
...
[edit]
user@host#  show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
        }
    }
}
...
[edit]
user@host# show security zones
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
```

```
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
```

- Result for DHCPv6 Client (PD):

```
[edit]
user@host# show system services dhcp-local-server
dhcpv6 {
    overrides {
        interface-client-limit 10;
        process-inform {
            pool p1;
        }
    }
    group my-group {
        overrides {
            interface-client-limit 200;
            delegated-pool v6-pd-pool;
        }
        interface pp0.0;
    }
    group ipv6 {
        interface ge-0/0/2.0;
    }
}
...
[edit]
user@host# show interfaces
ge-0/0/1 {
```

```
    unit 0 {
        encapsulation ppp-over-ether;
    }
}
pt-1/0/0 {
    vdsl-options {
        vdsl-profile auto;
    }
}
pp0 {
    unit 0 {
        ppp-options {
            chap {
                default-chap-secret "$ABC123"; ## SECRET-DATA
                local-name test_user;
                passive;
            }
        }
        pppoe-options {
            underlying-interface ge-0/0/1.0;
            client;
        }
    }
}
...
[edit]
user@host# show interfaces pp0
unit 0 {
    ppp-options {
        chap {
            default-chap-secret "$ABC123"; ## SECRET-DATA
            local-name test_user;
            passive;
        }
    }
    pppoe-options {
        underlying-interface ge-0/0/1.0;
        client;
    }
    family inet6 {
        dhcpv6-client {
            client-type statefull;
            client-ia-type ia-pd;
```

```
            update-router-advertisement {
                interface ge-0/0/2.0 {
                    other-stateful-configuration;
                    max-advertisement-interval 10;
                    min-advertisement-interval 5;
                }
            }
            client-identifier duid-type duid-ll;
            req-option dns-server;
        }
    }
}
...
[edit]
user@host# show security forwarding-options
    family {
        inet6 {
            mode flow-based;
        }
    }
...
[edit]
user@host# show access address-assignment
pool v6-pd-pool {
    family inet6 {
        prefix 2001:1:1::/48;
        range vp-pd prefix-length 48;
        dhcp-attributes {
            dns-server {
                3000::1;
            }
        }
    }
}
pool p1 {
    family inet6 {
        prefix 2001::/16;
        dhcp-attributes {
            propagate-settings pp0.0;
        }
    }
}
...
```

```
[edit]
user@host# show access address-assignment
security-zone Host {
    host-inbound-traffic {
        system-services {
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
security-zone untrust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
```

- Result for DHCPv6 Client (Auto):

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

            client-type autoconfig;
            client-ia-type ia-na;
            req-option dns-server;

        }
    }
}
...
[edit]
user@host# show protocols
router-advertisement {
    interface pp0.0 {
        max-advertisement-interval 20;
        min-advertisement-interval 10;
        managed-configuration;
        other-stateful-configuration;
        prefix 3000::1/64;
    }
    interface fe-0/0/0.0;
}
...
[edit]
user@host#  show security forwarding-options
    family {
        inet6 {
            mode flow-based;
        }
    }
...
[edit]
user@host# show security zones
security-zone Host {
    host-inbound-traffic {
        system-services {
```

```
            all;
        }
    }
    interfaces {
        ge-0/0/0.0;
    }
}
security-zone trust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        ge-0/0/2.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
        fe-0/0/0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
    }
}
security-zone untrust {
    interfaces {
        pp0.0 {
            host-inbound-traffic {
                system-services {
                    dhcpv6;
                }
            }
        }
```

```
    }
}
```

Verification

IN THIS SECTION

- Verifying DHCPv6 Server Configuration | 147
- Verifying DHCPv6 Client (PD) Configuration | 148
- Verifying DHCPv6 client (Auto) Configuration | 152

Verifying DHCPv6 Server Configuration

Purpose

Verify that the DHCPv6 Server has been configured.

Action

- From operational mode, enter the `show dhcpv6 server binding` command.

  The following output shows the options for the `show dhcpv6 server binding` command.

```
[edit]
user@host>show dhcpv6 server binding detail
Session Id:  75
     Client IPv6 Prefix:                  2001:1:1::/48
     Client DUID:                         LL0x1-3c:94:d5:98:90:01
     State:                               BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Expires:                       2016-03-26 10:12:37 JST
     Lease Expires in:                    86213 seconds
     Lease Start:                         2016-03-25 10:12:37 JST
     Last Packet Received:                2016-03-25 10:12:50 JST
     Incoming Client Interface:           pp0.0
     Server Ip Address:                   0.0.0.0
     Client Prefix Pool Name:             v6-pd-pool
```

```
    Client Id Length:                    10
    Client Id:                           /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 4 destinations, 4 routes (4 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

2001:1:1::/48      *[Access/13] 00:03:45     <<<<<< Route for end device will be
automatically generated
                    > to fe80::3e94:d50f:fc98:8600 via pp0.0
3000::/64          *[Direct/0] 00:04:04
                    > via pp0.0
3000::1/128        *[Local/0] 19:53:18
                      Local via pp0.0
fe80::b2c6:9a0f:fc7d:6900/128
                   *[Local/0] 19:53:18
                      Local via pp0.0
```

- From operational mode, enter the `show interfaces pp0.0 terse` command.

  The following output shows the options for the `show interfaces pp0.0 terse` command.

```
[edit]
user@host>show interfaces pp0.0 terse
Interface               Admin Link Proto    Local                 Remote
pp0.0                   up    up   inet6    3000::1/64
                                            fe80::b2c6:9a0f:fc7d:6900/64
```

Verifying DHCPv6 Client (PD) Configuration

Purpose

Verify that the DHCPv6 Client (PD) has been configured.

Action

- From operational mode, enter the `show dhcpv6 client binding detail` command.

  The following output shows the options for the `show dhcpv6 client binding detail` command.

```
[edit]
user@host>show dhcpv6 client binding detail
Client Interface: pp0.0
     Hardware Address:             3c:94:d5:98:86:01
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND) <<<<< SRX is bound to
prefix via pp0.0
     ClientType:                   STATEFUL
     Lease Expires:                2016-03-26 10:12:50 JST
     Lease Expires in:             86232 seconds
     Lease Start:                  2016-03-25 10:12:50 JST
     Bind Type:                    IA_PD
     Client DUID:                  LL0x29-3c:94:d5:98:86:01
     Rapid Commit:                 Off
     Server Ip Address:            fe80::b2c6:9a0f:fc7d:6900
     Update Server                 Yes
     Client IP Prefix:             2001:1:1::/48
DHCP options:
    Name: server-identifier, Value: VENDOR0x00000583-0x41453530
    Name: dns-recursive-server, Value: 3000::1
```

- From operational mode, enter the `show dhcpv6 server binding detail` command.

  The following output shows the options for the `show dhcpv6 server binding detail` command.

```
[edit]
user@host>show dhcpv6 server binding detail
Session Id:  75
     Client IPv6 Prefix:                   2001:1:1::/48
     Client DUID:                          LL0x1-3c:94:d5:98:90:01
     State:                                BOUND(DHCPV6_LOCAL_SERVER_STATE_BOUND)
     Lease Expires:                        2016-03-26 10:12:37 JST
     Lease Expires in:                     86213 seconds
     Lease Start:                          2016-03-25 10:12:37 JST
     Last Packet Received:                 2016-03-25 10:12:50 JST
     Incoming Client Interface:            pp0.0
     Server Ip Address:                    0.0.0.0
```

```
    Client Prefix Pool Name:              v6-pd-pool
    Client Id Length:                     10
    Client Id:                            /0x00030001/0x3c94d598/0x9001
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 7 destinations, 7 routes (7 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[Access-internal/12] 00:03:35
                    > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
2001:1:1:1::/64    *[Direct/0] 00:03:48
                    > via ge-0/0/2.0
2001:1:1:1::1/128  *[Local/0] 00:03:48      <<<<<< IPv6 address allocated by Prefix
delegation
                      Local via ge-0/0/2.0
3000::/64          *[Access-internal/12] 00:03:35
                    > to fe80::b2c6:9a0f:fc7d:6900 via pp0.0
fe80::/64          *[Direct/0] 00:03:48
                    > via ge-0/0/2.0
fe80::3e94:d50f:fc98:8600/128
                   *[Local/0] 19:05:19
                      Local via pp0.0
fe80::3e94:d5ff:fe98:8602/128
                   *[Local/0] 00:03:48
                      Local via ge-0/0/2.0
```

- From operational mode, enter the `show interfaces pp0.0 terse` command.

  The following output shows the options for the `show interfaces pp0.0 terse` command.

```
[edit]
user@host>show interfaces pp0.0 terse
Interface               Admin Link Proto    Local                 Remote
pp0.0                   up    up   inet6    fe80::3e94:d50f:fc98:8600/64
```

- From operational mode, enter the `show interfaces ge-0/0/2.0 terse` command.

  The following output shows the options for the `show interfaces ge-0/0/2.0 terse` command.

```
[edit]
user@host>show interfaces ge-0/0/2.0 terse
Interface               Admin Link Proto    Local                 Remote
ge-0/0/2.0              up    up   inet6    2000:1:1:1::1/64
                                            fe80::3e94:d5ff:fe98:8602/64
```

- From operational mode, enter the `show ipv6 router-advertisement` command.

  The following output shows the options for the `show ipv6 router-advertisement` command.

```
[edit]
user@host>show ipv6 router-advertisement
Interface: pp0.0
  Advertisements sent: 3, last sent 00:01:56 ago
  Solicits received: 0
  Advertisements received: 10
  Advertisement from fe80::b2c6:9a0f:fc7d:6900, heard 00:00:08 ago
    Managed: 1 [0]
    Other configuration: 1 [0]
    Reachable time: 0 ms
    Default lifetime: 60 sec [1800 sec]
    Retransmit timer: 0 ms
    Current hop limit: 64
    Prefix: 3000::/64
      Valid lifetime: 2592000 sec
      Preferred lifetime: 604800 sec
      On link: 1
      Autonomous: 1
Interface: ge-0/0/2.0
  Advertisements sent: 24, last sent 00:00:03 ago
  Solicits received: 0
  Advertisements received: 0
```

Verifying DHCPv6 client (Auto) Configuration

Purpose

Verify that the DHCPv6 client (Auto) has been configured.

Action

- From operational mode, enter the `show dhcpv6 client binding detail` command.

  The following output shows the options for the `show dhcpv6 client binding detail` command.

```
[edit]
user@host>show dhcpv6 client binding detail
Client Interface: fe-0/0/0.0
     Hardware Address:             00:26:88:38:b5:00
     State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
     ClientType:                   AUTO
     Lease Expires:                2016-03-26 10:15:35 JST
     Lease Expires in:             86395 seconds
     Lease Start:                  2016-03-25 10:15:35 JST
     Bind Type:                    IA_NA
     Client DUID:                  LL0x3-00:26:88:38:b5:00
     Rapid Commit:                 Off
     Server Ip Address:            fe80::3e94:d5ff:fe98:8602
     Client IP Address:            2001:1:1:1:226:88ff:fe38:b500/128
     Client IP Prefix:             2001:1:1:1::/64

DHCP options:
    Name: server-identifier, Value: VENDOR0x00000583-0x414c3131
```

- From operational mode, enter the `show route table inet6.0` command.

  The following output shows the options for the `show route table inet6.0` command.

```
[edit]
user@host>show route table inet6.0
inet6.0: 5 destinations, 6 routes (5 active, 0 holddown, 0 hidden)
+ = Active Route, - = Last Active, * = Both

::/0               *[Access-internal/12] 00:02:36
```

```
                     > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
2001:1:1:1::/64    *[Access-internal/12] 00:02:36
                     > to fe80::3e94:d5ff:fe98:8602 via fe-0/0/0.0
2001:1:1:1:226:88ff:fe38:b500/128
                   *[Direct/0] 00:02:36
                     > via fe-0/0/0.0
                     [Local/0] 00:02:36
                       Local via fe-0/0/0.0
fe80::/64          *[Direct/0] 1w3d 15:51:19
                     > via fe-0/0/0.0
fe80::226:88ff:fe38:b500/128
                   *[Local/0] 1w3d 15:51:19
                       Local via fe-0/0/0.0
```

- From operational mode, enter the `show ipv6 router-advertisement` command.

  The following output shows the options for the `show ipv6 router-advertisement` command.

```
[edit]
user@host>show ipv6 router-advertisement
Interface: fe-0/0/0.0
  Advertisements sent: 1, last sent 00:02:45 ago
  Solicits received: 0
  Advertisements received: 8
  Advertisement from fe80::3e94:d5ff:fe98:8602, heard 00:00:02 ago
    Managed: 0
    Other configuration: 1 [0]
    Reachable time: 0 ms
    Default lifetime: 30 sec [1800 sec]
    Retransmit timer: 0 ms
    Current hop limit: 64
    Prefix: 2001:1:1:1::/64
      Valid lifetime: 86400 sec
      Preferred lifetime: 86400 sec
      On link: 1
      Autonomous: 1
```

Release History Table

Release	Description
15.1X49-D70	Starting with Junos OS Release 15.X49-D70 and Junos OS Release 17.3R1, you can add the option dynamic-server to dynamically support prefix and attributes that are updated by the WAN server.

RELATED DOCUMENTATION

DHCP Server Configuration | 51

DHCP Server Options | 77

4

CHAPTER

DHCP Relay Agent

DHCP Relay Agent | 156

DHCP and BOOTP Relay Agent | 190

DHCP Relay Agent Information Option (Option 82) | 198

DHCPv6 Relay Agent | 222

DHCP Relay Proxy | 230

DHCP Relay Agent

IN THIS SECTION

- Understanding DHCP Relay Agent Operation | 156
- Minimum DHCP Relay Agent Configuration | 158
- Configuring DHCP Relay Agent | 159
- Configuring a DHCP Relay Agent on EX Series Switches | 171
- Configuring DHCP Smart Relay (Legacy DHCP Relay) | 173
- Disabling Automatic Binding of Stray DHCP Requests | 174
- Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets | 176
- Changing the Gateway IP Address (giaddr) Field to the giaddr of the DHCP Relay Agent | 176
- Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address | 177
- Overriding the Default DHCP Relay Configuration Settings | 177
- Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally | 180
- Example: Configuring DHCP Relay Agent Selective Traffic Processing Based on DHCP Option Strings | 180
- Verifying and Managing DHCP Relay Configuration | 186
- Extended DHCP Relay Agent Overview | 187

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks. For more information, read this topic.

Understanding DHCP Relay Agent Operation

IN THIS SECTION

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers | 157

A Juniper Networks device operating as a DHCP relay agent forwards incoming requests from BOOTP and DHCP clients to a specified BOOTP or DHCP server. Client requests can pass through virtual private network (VPN) tunnels.

You cannot configure a single device interface to operate as both a DHCP client and a DHCP relay.

NOTE: The DHCP requests received on an interface are associated to a DHCP pool that is in the same subnet as the primary IP address/subnet on an interface. If an interface is associated with multiple IP addresses/subnets, the device uses the lowest numerically assigned IP address as the primary IP address/subnet for the interface. To change the IP address/subnet that is listed as the primary address on an interface, use the `set interfaces < interface name > unit 0 family inet xxx.xxx.xxx.xxx/yy primary` command and commit the change.

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*.

On all Junos OS devices, when the DHCP relay is configured with `forward-only` option, and the DHCP client is terminated on logical tunnel interface if the logical tunnel interface

- Includes multiple logical interfaces
- Use same VLAN on multiple logical interfaces of the same `lt` interface

In such cases, the DHCP relay might fail to send the *OFFER* messages.

This issue applies in Junos OS Releases 19.3R3, 19.4R2, 18.4R3, 19.4R1, 19.3R2, 18.4R3-S1, 17.4R3 releases.

Minimum DHCP Relay Agent Configuration

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 203.0.113.21;
    }
```

```
    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 203.0.113.21. 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.

Configuring DHCP Relay Agent

IN THIS SECTION

- Requirements | **159**
- Overview | **160**
- Configuration | **161**
- Verification | **170**

The DHCP relay agent operates as the interface between DHCP clients and the server. The DHCP Relay Agent relays DHCP messages between DHCP clients and DHCP servers on different IP networks.

This example describes how to configure the DHCP relay agent on the SRX Series device. SRX series device acting as DHCP relay agent is responsible for forwarding the requests and responses between the DHCP clients and the server which are part of different routing instances.

Requirements

This example uses the following hardware and software components:

- SRX Series devices with Junos OS 15.1X49-D10 or later.

Overview

IN THIS SECTION

- Topology | 160

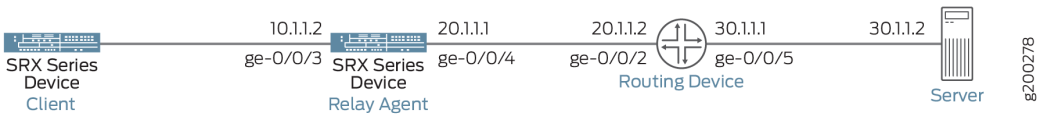
You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that is isolated from the client network.

Topology

To exchange DHCP messages between different routing instances, you must enable both the server-facing interface and the client-facing interface of the DHCP relay agent to recognize and forward DHCP packets.

The following Figure 11 on page 160 shows DHCP performance as DHCP local server, DHCP client, and DHCP relay agent

Figure 11: Understanding DHCP Services in a Routing Instance



The following list provides an overview of the tasks required to create the DHCP message exchange between the different routing instances:

- Configure the client-facing side of the DHCP relay agent.
- Configure the server-facing side of the DHCP relay agent.
- Configure the Security Zone to Allow the DHCP protocol.

  Table1: DHCP Relay Parameters:

Parameters	Client-Side-Details	Server-Side-Details
interface	ge-0/0/3.0	ge-0/0/4.0
routing interface	trust-vr	untrust-vr
ip address	10.1.1.2/24	20.1.1.1/24

NOTE: In order to make this setup work, the DHCP server connecting route and relay agent interface route must be in both routing-instances. For example, in the above topology, the server route 30.1.1.0/24 needs to be shared with the dhcp-relay VR, and the dhcp-relay interface route 10.1.1.0/24 exact needs to be shared with the default routing instance.

Also, a dummy dhcp-relay config must be added in the routing instance with the DHCP server. If this is not configured, dhcp-relay will not be able to receive packets from the DHCP server.

Configuration

IN THIS SECTION

- CLI Quick Configuration | **161**
- Procedure | **163**
- Procedure | **164**
- Procedure | **164**
- Procedure | **166**
- Results | **166**

CLI Quick Configuration

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different routing instances. To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details

necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Quick configuration for Client-Facing Support:

```
set routing-instances trust-vr instance-type virtual-router
set routing-instances trust-vr interface ge-0/0/3.0
set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

Quick configuration for Server-Facing Support:

```
set routing-instances untrust-vr instance-type virtual-router
set routing-instances untrust-vr interface ge-0/0/4.0
set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Quick configuration for DHCP Relay Support:

```
set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-config
set routing-instances untrust-vr routing-options instance-import import_relay_route_to_server_vr
set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop 20.1.1.2
set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1 30.1.1.2
set routing-instances trust-vr forwarding-options dhcp-relay active-server-group server-1
set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr interface
ge-0/0/3.0
set routing-instances trust-vr routing-options instance-import export_dhcp_server_route
set policy-options policy-statement export_dhcp_server_route term 1 from instance untrust-vr
set policy-options policy-statement export_dhcp_server_route term 1 from route-filter
30.1.1.0/24 exact
set policy-options policy-statement export_dhcp_server_route term 1 then accept
set policy-options policy-statement export_dhcp_server_route term 2 then reject
set policy-options policy-statement import_relay_route_to_server_vr term 1 from instance trust-vr
set policy-options policy-statement import_relay_route_to_server_vr term 1 from route-filter
10.1.1.0/24 exact
set policy-options policy-statement import_relay_route_to_server_vr term 1 then accept
set policy-options policy-statement import_relay_route_to_server_vr term 2 then reject
set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
```

Quick configuration for Security Zone to Allow the DHCP Protocol:

```
set security policies default-policy permit-all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic system-
services all
set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-traffic protocols all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic system-
services all
set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic protocols all
```

Procedure

Step-by-Step Procedure

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

To configure support on the client-facing side of the DHCP relay agent:

1. Set a routing instance type as virtual router.

```
[edit]
user@host# set routing-instances trust-vr instance-type virtual-router
```

2. Set an interface to the virtual router

```
[edit]
user@host# set routing-instances trust-vr interface ge-0/0/3.0
```

3. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/3 unit 0 family inet address 10.1.1.2/24
```

Procedure

Step-by-Step Procedure

To configure support on the server-facing side of the DHCP relay agent:

1. Set a virtual router.

```
[edit]
user@host# set routing-instances untrust-vr instance-type virtual-router
```

2. Set an interface to the virtual router.

```
[edit]
user@host# set routing-instances untrust-vr interface ge-0/0/4.0
```

3. Set the forward-only-replies option.

```
[edit]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay forward-only-replies
```

4. Set the IP address to the interface.

```
[edit]
user@host# set interfaces ge-0/0/4 unit 0 family inet address 20.1.1.1/24
```

Procedure

Step-by-Step Procedure

To configure the DHCP local server to support:

1. Set the configuration in dhcp-relay for untrust-vr routing instance

```
[edit ]
user@host# set routing-instances untrust-vr forwarding-options dhcp-relay server-group dummy-
config
user@host# set routing-instances untrust-vr routing-options instance-import
```

```
import_relay_route_to_server_vr
user@host# set routing-instances untrust-vr routing-options static route 30.1.1.0/24 next-hop
20.1.1.2
```

2. Set the configuration in dhcp-relay for trust-vr routing instance

```
[edit ]
user@host# set routing-instances trust-vr forwarding-options dhcp-relay server-group server-1
30.1.1.2
user@host# set routing-instances trust-vr forwarding-options dhcp-relay active-server-group
server-1
user@host# set routing-instances trust-vr forwarding-options dhcp-relay group relay-in-vr
interface ge-0/0/3.0
user@host# set routing-instances trust-vr routing-options instance-import
export_dhcp_server_route
```

3. Set the configuration to share routes between routing instances.

```
[edit ]
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from instance
untrust-vr
user@host# set policy-options policy-statement export_dhcp_server_route term 1 from route-
filter 30.1.1.0/24 exact
user@host# set policy-options policy-statement export_dhcp_server_route term 1 then accept
user@host# set policy-options policy-statement export_dhcp_server_route term 2 then reject
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from
instance trust-vr
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 from
route-filter 10.1.1.0/24 exact
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 1 then
accept
user@host# set policy-options policy-statement import_relay_route_to_server_vr term 2 then
reject
user@host# set routing-options static route 30.1.1.2/32 next-table untrust-vr.inet.0
```

NOTE: You can enable an SRX Series device to function as a DHCP local server. The DHCP local server provides an IP address and other configuration information in response to a client request.

Procedure

Step-by-Step Procedure

To configure the security zone to allow the DHCP Protocol:

1. Set the default security policy to permit all traffic.

```
[edit ]
user@host# set security policies default-policy permit-all
```

2. Set all system services and protocols on interface ge-0/0/4.0.

```
[edit ]
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic system-services all
user@host# set security zones security-zone untrust interfaces ge-0/0/4.0 host-inbound-
traffic protocols all
```

3. Set all system services and protocols on interface ge-0/0/3.0.

```
[edit ]
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
system-services all
user@host# set security zones security-zone trust interfaces ge-0/0/3.0 host-inbound-traffic
protocols all
```

Results

- Result for Client-facing Support:

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

```
[edit]
user@host# show routing-instances
trust-vr {
    instance-type virtual-router;
```

```
    interface ge-0/0/3.0;
}
```

- Result for Server-Facing Support:

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

```
[edit]
user@host# show routing-instances
untrust-vr {
    instance-type virtual-router;
    interface ge-0/0/4.0;
    forwarding-options {
        dhcp-relay {
            forward-only-replies;
        }
    }
}
```

- Result for DHCP Local Server Support:

  From configuration mode, confirm your configuration by entering the `show routing-instances`, `show policy-options` and `show routing-options` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show routing-instances
trust-vr {
    routing-options {
        instance-import export_dhcp_server_route;
    }
    forwarding-options {
        dhcp-relay {
            server-group {
                server-1 {
                    30.1.1.2;
                }
            }
            active-server-group server-1;
            group relay-in-vr {
```

```
                interface ge-0/0/3.0;
            }
        }
    }
}
untrust-vr {
    routing-options {
        static {
            route 30.1.1.0/24 next-hop 20.1.1.2;
        }
        instance-import import_relay_route_to_server_vr;
    }
    forwarding-options {
        dhcp-relay {
            server-group {
                dummy-config;
            }
        }
    }
}
[edit]
user@host# show policy-options
policy-statement export_dhcp_server_route {
    term 1 {
        from {
            instance untrust-vr;
            route-filter 30.1.1.0/24 exact;
        }
        then accept;
    }
    term 2 {
        then reject;
    }
}
policy-statement import_relay_route_to_server_vr {
    term 1 {
        from {
            instance trust-vr;
            route-filter 10.1.1.0/24 exact;
        }
        then accept;
    }
    term 2 {
```

```
        then reject;
    }
}
[edit]
user@host#  show routing-options
    static {
        route 30.1.1.2/32 next-table untrust-vr.inet.0;
    }
```

- Result for Security Zone to Allow the DHCP Protocol:

  From configuration mode, confirm your configuration by entering the `show security policies` and `show security zones` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show security policies
default-policy {
    permit-all;
}
[edit]
user@host# show security zones
    security-zone HOST {
        interfaces {
            all;
        }
    }
    security-zone untrust {
        interfaces {
            ge-0/0/4.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
    security-zone trust {
```

```
        interfaces {
            ge-0/0/3.0 {
                host-inbound-traffic {
                    system-services {
                        all;
                    }
                    protocols {
                        all;
                    }
                }
            }
        }
    }
```

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

Verification

IN THIS SECTION

- Verifying the DHCP Relay Statistics Configuration: | **170**
- Verifying DHCP client bindings in the routing instance. | **171**

Verifying the DHCP Relay Statistics Configuration:

Purpose

Verify that the DHCP Relay Statistics has been configured.

Action

- From operational mode, enter the `show dhcp relay statistics routing-instance dhcp-relay` command.

```
Packets dropped:
Total 0

Messages received:
BOOTREQUEST 1
```

```
DHCPDECLINE 0
DHCPDISCOVER 0
DHCPINFORM 0
DHCPRELEASE 0
DHCPREQUEST 1

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

Verifying DHCP client bindings in the routing instance.

Purpose

Verify that the DHCP client bindings in the routing instances has been configured.

Action

- From operational mode, enter the `show dhcp relay binding routing-instance dhcp-relay` command.

```
IP address   Session Id  Hardware address   Expires   State     Interface
10.10.10.2   14          00:0c:29:e9:6d:00  86381     BOUND     ge-0/0/1.0
```

Configuring a DHCP Relay Agent on EX Series Switches

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

Before you begin:

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

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

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

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

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

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

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

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

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
```

Configuring DHCP Smart Relay (Legacy DHCP Relay)

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See Configuring IRB Interfaces on Switches and Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface for information about this approach.
- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See Understanding Layer 3 Logical Interfaces and Configuring a Layer 3 Logical Interface for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- `set forwarding-options helpers bootp smart-relay-global`: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.
- `set forwarding-options helpers bootp interface interface-name smart-relay-agent`: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

SEE ALSO

bootp

Disabling Automatic Binding of Stray DHCP Requests

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

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

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

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

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

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

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

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

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

1. Specify the named group.

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

2. Specify that you want to configure overrides.

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

3. Disable automatic binding for the group.

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

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

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

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

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

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

3. Specify that you want to configure overrides.

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

4. Disable automatic binding on the interface.

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

Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets

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

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

1. Specify that you want to configure override options.

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

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

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

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

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

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

1. Specify that you want to configure override options.

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

2. Specify that the giaddr of DHCP packets is overwritten.

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

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

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

To replace the source address with giaddr:

1. Specify that you want to configure override options.

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

2. Specify that you want to replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

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

Overriding the Default DHCP Relay Configuration Settings

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

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

- To override DHCP relay configuration options for a specific interface within a named group of interfaces, include the statements at the `[edit forwarding-options dhcp-relay group group-name interface interface-name]` hierarchy level.
- To configure overrides for DHCPv6 relay at the global level, group level, or per-interface, use the corresponding statements at the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level.

To override default DHCP relay agent configuration settings:

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

     Global override:

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

     Group-level override:

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

     Per-interface override:

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

   - DHCPv6 overrides.

     Global override:

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

     Group-level override:

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

Per-interface override:

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

2. (DHCPv4 only) Enable DHCP relay proxy mode.

   See *Enabling DHCP Relay Proxy Mode*.

3. (DHCPv4 only) Overwrite the giaddr in DHCP packets that the DHCP relay agent forwards.

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

4. (DHCPv4 only) Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

   See *Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address*.

5. (DHCPv4 only) Override the DHCP relay agent information option (option 82) in DHCP packets.

   See *Overriding Option 82 Information*.

6. (DHCPv4 only) Override the setting of the broadcast bit in DHCP request packets and use the Layer 2 unicast transmission method.

   See *Using Layer 2 Unicast Transmission instead of Broadcast for DHCP Packets*.

7. (DHCPv4 only) Trust DHCP client packets that have a giaddr of 0 and that contain option 82 information.

   See *Enable Processing of Untrusted Packets So Option 82 Information Can Be Used*.

8. (DHCPv4 and DHCPv6) Override the maximum number of DHCP clients allowed per interface.

   See *Specifying the Maximum Number of DHCP Clients Per Interface*.

9. (DHCPv4 only) Configure client auto logout.

   See *DHCP Auto Logout Overview*.

10. (DHCPv4 and DHCPv6) Enable or disable support for DHCP snooped clients on interfaces.

    See *Enabling and Disabling DHCP Snooped Packets Support for DHCP Relay Agent*.

11. (DHCPv4 and DHCPv6) Delay authentication of subscribers until the DHCP client sends a Request packet.

    See the *delay-authentication*.

12. (DHCPv4 and DHCPv6) Send release messages to the DHCP server when clients are deleted.

    See *Sending Release Messages When Clients Are Deleted*.

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

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

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

See *Automatically Logging Out DHCPv6 Clients*.

15. (DHCPv4 only) Disable the DHCP relay agent on specific interfaces.

    See *Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally*.

16. (DHCPv4 and DHCPv6) Disable automatic binding of stray DHCP requests.

    See *Disabling Automatic Binding of Stray DHCP Requests*.

17. (DHCPv4 and DHCPv6) Assign a single-session DHCP dual-stack group to a specified group of subscribers. You must assign the group to both legs of the DHCP dual stack.

    See *Configuring Single-Session DHCP Dual-Stack Support*.

18. (Optional, DHCPv4 and DHCPv6l) Specify that a short lease be sent to the client.

    See *Configuring DHCP Asymmetric Leasing*.

Disabling DHCP Relay Agent for Interfaces, for Groups, or Globally

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

To disable DHCP relay agent:

1. Specify that you want to configure override options.

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

2. Disable the DHCP relay agent.

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

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

IN THIS SECTION

Requirements | 181

Overview | 181
Configuration | 182
Verification | 184

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

Requirements

This example uses the following hardware and software components:

- MX Series 5G Universal Routing Platforms or EX Series Switches

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

- Configure DHCP relay agent.

  See *Extended DHCP Relay Agent Overview*.

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

  See *Grouping Interfaces with Common DHCP Configurations*.

Overview

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

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

Configuration

IN THIS SECTION

- CLI Quick Configuration | **182**
- Configuring DHCP Relay Agent To Selectively Process Client Traffic Based on DHCP Option Strings | **182**
- Results | **183**

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

CLI Quick Configuration

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

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

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

Step-by-Step Procedure

To configure DHCP relay selective processing:

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

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

2. Specify the DHCP option that DHCP relay agent uses to identify incoming client traffic.

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

3. Configure a default action, which DHCP relay agent uses when the incoming client traffic does not satisfy any configured match criteria.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option default-action drop
```

4. Configure an exact match condition and associated action that DHCP relay uses to process the identified client traffic.

```
[edit forwarding-options dhcp-relay]
user@host# set relay-option equals ascii video-gold forward-only
```

5. Configure a second exact match condition and associated action that DHCP relay uses to process client traffic.

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

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

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

Results

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

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

```
    relay-option {
        option-number 60;
        equals {
            ascii video-gold {
                forward-only;
            }
        }
        equals {
            ascii video-bronze {
                local-server-group servergroup-15;
            }
        }
        default-action {
            drop;
        }
        starts-with {
            hexadecimal fffff {
                local-server-group servergroup-east;
            }
        }
    }
}
```

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

Verification

IN THIS SECTION

- Verifying the Status of DHCP Relay Agent Selective Traffic Processing | **184**

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

Verifying the Status of DHCP Relay Agent Selective Traffic Processing

Purpose

Verify the DHCP relay agent selective traffic processing status.

Action

Display statistics for DHCP relay agent.

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

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

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

Packets forwarded:
    Total                     4
    BOOTREQUEST               2
    BOOTREPLY                 2
```

Meaning

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

Verifying and Managing DHCP Relay Configuration

IN THIS SECTION

- Purpose | 186
- Action | 186

Purpose

View or clear address bindings or statistics for DHCP relay agent clients.

Action

- To display the address bindings for DHCP relay agent clients:

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

- To display DHCP relay agent statistics:

```
user@host> show dhcp relay statistics
```

- To clear the binding state of DHCP relay agent clients:

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

- To clear all DHCP relay agent statistics:

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

To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- `show dhcp relay binding routing instance <routing-instance name>`
- `show dhcp relay statistics routing instance <routing-instance name>`
- `clear dhcp relay binding routing instance <routing-instance name>`
- `clear dhcp relay statistics routing instance <routing-instance name>`

NOTE: On all SRX Series devices, DHCP relay is unable to update the binding status based on DHCP_RENEW and DHCP_RELEASE messages.

SEE ALSO

Minimum DHCP Relay Agent Configuration

Extended DHCP Relay Agent Overview

IN THIS SECTION

- Interaction Among the DHCP Relay Agent, DHCP Client, and DHCP Servers | **188**
- DHCP Liveness Detection | **190**

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

DHCP relay supports the attachment of dynamic profiles and also interacts with the local AAA Service Framework to use back-end authentication servers, such as RADIUS, to provide subscriber

authentication or DHCP client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

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

On the routers, you can use DHCP relay in carrier edge applications such as video/IPTV to obtain configuration parameters, including an IP address, for your subscribers.

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

> **NOTE**: The extended DHCP relay agent options configured with the `dhcp-relay` statement are incompatible with the DHCP/BOOTP relay agent options configured with the `bootp` statement. As a result, you cannot enable both the extended DHCP relay agent and the DHCP/BOOTP relay agent on the router at the same time.
>
> For information about the DHCP/BOOTP relay agent, see Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents.

You can also configure the extended DHCP relay agent to support IPv6 clients. See *DHCPv6 Relay Agent Overview* for information about the DHCPv6 relay agent feature.

To configure the extended DHCP relay agent on the router (or switch), include the `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level.

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

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

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

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

- DHCP Overview | 2
- Secure DHCP Message Exchange | 343
- DHCP Client | 234
- Suppressing DHCP Routes | 353

DHCP and BOOTP Relay Agent

IN THIS SECTION

- DHCP and BOOTP Relay Overview for Switches | 191
- Configuring DHCP and BOOTP Relay | 194
- Configuring DHCP and BOOTP Relay on QFX Series | 195

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay.

You can also enable BOOTP support when the switch is configured as a DHCP server. For more details, read this topic.

DHCP and BOOTP Relay Overview for Switches

IN THIS SECTION

- DHCP Client and Server Model | 191
- DHCP Client, Server, and Relay Agent Model | 193

You can configure a Juniper Networks switch to act as a Dynamic Host Configuration Protocol (DHCP) or Bootstrap Protocol (BOOTP) relay agent. This means that if the switch receives a broadcast DHCP or BOOTP request from a locally attached host (client), it relays the message to a specified DHCP or BOOTP server. You should configure the switch to be a DHCP/BOOTP relay agent if you have locally attached hosts and a distant DHCP or BOOTP server.

You can configure the switch to use the gateway IP address (giaddr) as the source IP address of the switch for relayed DHCP packets when the switch is used as the DHCP relay agent. For information on configuring this option, see the *source-address-giaddr* configuration statement.

You can also use smart DHCP relay, which enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure a Layer 3 interface, Layer 3 subinterface, or IRB interface with multiple IP addresses and configure that interface to be a relay agent.

NOTE: Because DHCP and BOOTP messages are broadcast and are not directed to a specific server, switch, or router, Juniper switches cannot function as both a DHCP server and a DHCP/BOOTP relay agent at the same time. The Junos operating system (Junos OS) generates a commit error if both options are configured at the same time, and the commit operation does not succeed until one of the options is removed.

DHCP Client and Server Model

DHCP IP address allocation works on a client/server model in which the server, in this case a Junos OS, assigns the client reusable IP information from an address pool. A DHCP client might receive offer

messages from multiple DHCP servers and can accept any one of the offers; however, the client usually accepts the first offer it receives. See Figure 12 on page 192.

Figure 12: DHCP Client/Server Model

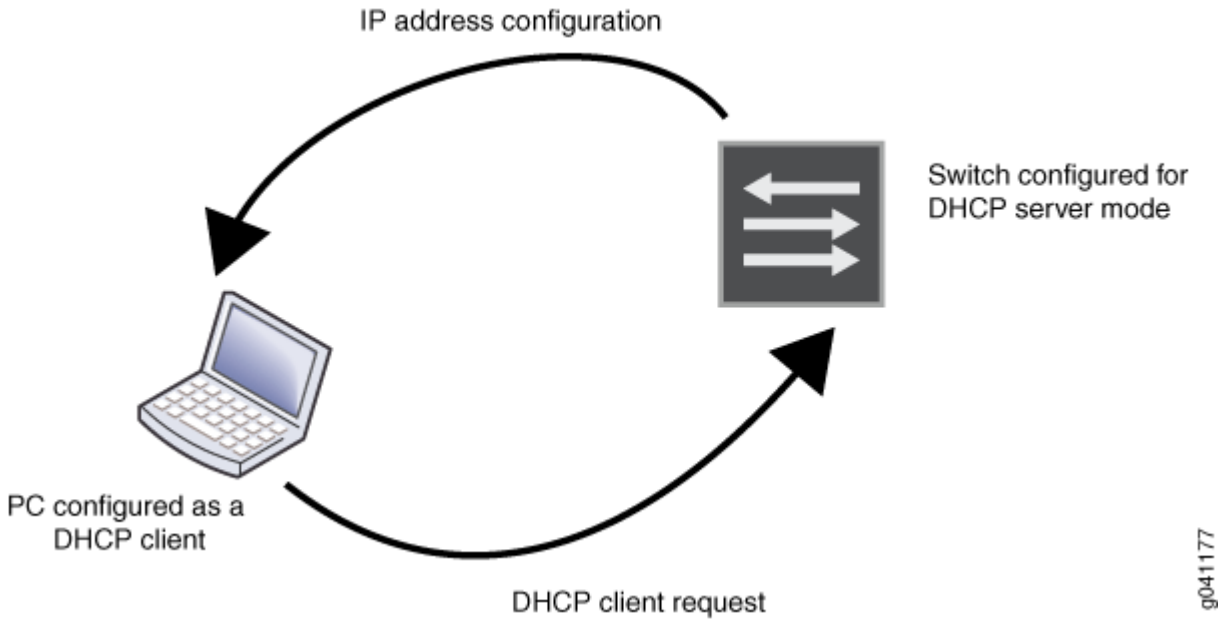
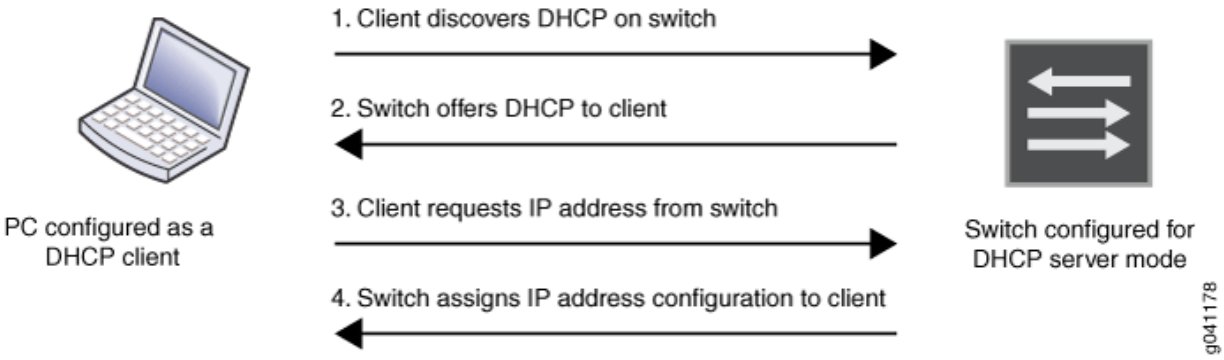


Figure 13: DHCP Four-Step Transfer



DHCP consists of a four-step transfer process beginning with a broadcast DHCP discovery message from the client. As the second step, the client receives a DHCP offer message from the server. This message includes the IP address and mask, and some other specific parameters. The client then sends a DHCP request message to accept the IP address and other parameters that it received from the server in the previous step. The DHCP server sends a DHCP response message and removes the now-allocated address from the DHCP address pool. See Figure 13 on page 192.

NOTE: Because the DHCP discovery message from the client is a broadcast message and because broadcast messages cross other segments only when they are explicitly routed, you might have to configure a DHCP relay agent on the switch interface so that all DHCP discovery messages from the clients are forwarded to one DHCP server.

DHCP Client, Server, and Relay Agent Model

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

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

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

Configuring DHCP and BOOTP Relay

You can configure a switch to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) server or DHCP relay agent. When a switch is a relay agent, if a locally attached host issues a DHCP or BOOTP request as a broadcast message, the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses the Enhanced Layer 2 Software (ELS) configuration style.If your switch runs software that does not support ELS, see *Configuring DHCP and BOOTP Relay*. For ELS details, see Using the Enhanced Layer 2 Software CLI.

To configure a switch to be a server, use the *dhcp-local-server* statement. To configure a switch to be a relay agent, use the *dhcp-relay* statement.

If you want to enable BOOTP support when the switch is configured to be a DHCP server, enter the following statement:

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

If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

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

Configuring DHCP and BOOTP Relay on QFX Series

IN THIS SECTION

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

You can configure the QFX Series to act as a Dynamic Host Configuration Protocol (DHCP) and Bootstrap Protocol (BOOTP) relay agent. This means that if a locally attached host can issue a DHCP or BOOTP request as a broadcast message and the switch relays the message to a specified DHCP or BOOTP server. You should configure a switch to be a DHCP and BOOTP relay agent if you have locally attached hosts and a remote DHCP or BOOTP server.

NOTE: This task uses a release of Junos OS that does not support the Enhanced Layer 2 Software (ELS) configuration style. If your switch runs software that supports ELS, see *Configuring DHCP and BOOTP Relay*. For ELS details, see Using the Enhanced Layer 2 Software CLI.

If you configure a switch to be a DHCP relay agent, you can also enable smart DHCP relay, which allows you to configure alternative gateway addresses for a DHCP server so that if the server fails to reply to the requests sent using the primary gateway address, the switch can resend the requests via the alternative gateway addresses. To use this feature, you must configure a routed VLAN interface or Layer 3 logical interface with multiple IP addresses and configure that interface to be a relay agent.

Configuring a DHCP and BOOTP Relay Agent on QFX Series

To configure a switch to act as a DHCP and BOOTP relay agent, include the `bootp` statement at the `[edit forwarding-options helpers]` hierarchy level:

```
[edit forwarding-options helpers]
bootp {
    apply-secondary-as-giaddr text-description;
    client-response-ttl number;
    description text-description;
    interface (interface-name | interface-group) {
        client-response-ttl number;
        description text-description;
```

```
        maximum-hop-count number;
        minimum-wait-time seconds;
        no-listen;
        server address
        apply-secondary-as-giaddr
    }
    maximum-hop-count number;
    minimum-wait-time seconds;
    relay-agent-option;
    server server-identifier
}
```

To include a description of the BOOTP service, DHCP service, or interface, use the `description` statement.

To configure a logical interface or a group of logical interfaces with a specific DHCP relay or BOOTP configuration, include the `interface` statement.

To stop packets from being forwarded, include the `no-listen` statement.

To set the maximum allowed number in the hops field of the BOOTP message, include the `maximum-hop-count` statement. BOOTP messages that have a larger number in the hops field than the maximum allowed are not forwarded. If you omit the `maximum-hop-count` statement, the default maximum number of hops is four.

To set the minimum allowed number of seconds in the `secs` field of the BOOTP message, include the `minimum-wait-time` statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the `secs` field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

To set the IP address that specify the DHCP or BOOTP server for the router, switch, or interface, include the `server` statement. You can include multiple `server` statements.

To set an IP time-to-live (TTL) value for DHCP response packets sent to a DHCP client, include the `client-response-ttl` statement.

The following example demonstrates a BOOTP relay agent configuration.

```
user@host# show forwarding-options
helpers {
    bootp {
        description "dhcp relay agent global parameters";
        server 192.168.55.44;
        server 172.16.0.3 routing-instance c3;
        maximum-hop-count 10;
```

```
        minimum-wait-time 8;
        interface {
            xe-0/0/1 {
                description "use this info for this interface";
                server 10.10.10.10;
                server 192.168.14.14;
                maximum-hop-count 11;
                minimum-wait-time 3;
            }
            xe-0/0/2 {
                no-listen;  ###ignore DHCPDISCOVER messages on this interface
            }
            all {
                description "globals apply to all other interfaces";
            }
        }
    }
}
```

SEE ALSO

bootp

Configuring DHCP Smart Relay on QFX Series

You can use DHCP smart relay to provide redundancy and resiliency to your DHCP relay configuration. Smart relay provides additional relay functionality and requires all of the configuration settings required by DHCP relay. To use DHCP smart relay, you also need an interface with multiple IP addresses assigned to it. You can achieve this by doing either of the following tasks:

- Create a routed VLAN interface and assign at least two IP addresses to it. See Configuring IRB Interfaces on Switches and Example: Configuring Routing Between VLANs on One Switch Using an IRB Interface for information about this approach.
- Create a Layer 3 logical interface (by using VLAN tagging) and assign at least two IP addresses to it. See Understanding Layer 3 Logical Interfaces and Configuring a Layer 3 Logical Interface for information about this approach.

Once you have created an interface with multiple IP addresses, complete the smart relay configuration by entering one of the following statements:

- `set forwarding-options helpers bootp smart-relay-global`: Use this statement to enable smart relay on all the interfaces that are configured as relay agents.

- `set forwarding-options helpers bootp interface` *`interface-name`* `smart-relay-agent`: Use this statement to enable smart relay on a specific interface.

When smart relay is configured for an interface, the switch initially sends DHCP request (discover) messages out of that interface using the primary address of the interface as the gateway IP address (in the giaddr field) for the DHCP message. If no DHCP offer message is received from a server in reply, the switch allows the client to send as many as three more discover messages using the same gateway IP address. If no DHCP offer message is received after three retries, the switch resends the discover message using the alternate IP address as the gateway IP address. If you configure more than two IP addresses on the relay agent interface, the switch repeats this process until a DHCP offer message is received or all of the IP addresses have been used without success.

SEE ALSO

bootp

RELATED DOCUMENTATION

DHCP Overview | 2

DHCP Client | 234

DHCP Server | 49

DHCP Relay Agent Information Option (Option 82)

IN THIS SECTION

- Using DHCP Relay Agent Option 82 Information | 199
- How DHCP Relay Agent Uses Option 82 for Auto Logout | 209
- Enable Processing of Untrusted Packets So Option 82 Information Can Be Used | 211
- Check if Your Device Support DHCP Option-82 | 211
- Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82 | 212
- Example: Configure DHCP Relay in Forward Only Mode | 214

The DHCP relay agent information option (option 82) enables you to include additional useful information in the client-originated DHCP packets that the DHCP relay forwards to a DHCP server. You can configure the option 82 support globally or for a named group of interfaces. For more information, read this topic.

Using DHCP Relay Agent Option 82 Information

IN THIS SECTION

- Configuring Option 82 Information | **200**
- Overriding Option 82 Information | **203**
- Including a Prefix in DHCP Options | **203**
- Including a Textual Description in DHCP Options | **207**

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

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

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

  NOTE: If `relay-option-82` is configured, but none of the attributes under `relay-option-82` (that is, `circuit-id` | `remote-id` | `server-id-override`) are explicitly configured, then the default behavior is for the circuit-id (that is, suboption 1) to always be included in the option-82 value. This is true whether or not the `vendor-specific` attribute under `relay-option-82` is configured.

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

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

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

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

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

Configuring Option 82 Information

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- IRB interfaces that use VLANs:

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

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

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

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

- IRB interfaces that use VLANs:

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

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

```
irb.subunit
```

To enable insertion of option 82 information:

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

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

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

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

   - To insert the Agent Remote ID:

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

   - To insert both, configure both set commands.
3. (Optional) Configure a prefix that is used in the option 82 information in the DHCP packets.

   See *Including a Prefix in DHCP Options*.
4. (Optional) Configure the DHCP relay agent to include the interface's textual description instead of the interface identifier in the option 82 information.

   See *Including a Textual Description in DHCP Options*.

Overriding Option 82 Information

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

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

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

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

1. Specify that you want to configure override options.

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

2. Specify that the option 82 information in DHCP packets is overwritten.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set always-write-option-82
```

Including a Prefix in DHCP Options

When you configure the DHCP relay agent to include DHCP options in the packets that the relay agent sends to a DHCP server, you can specify that the relay agent add a prefix to the DHCP option. You can add a prefix to the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The prefix is separated from the DHCP option information by a colon (:), and it can include any combination of the `host-name`, `logical-system-name`, and `routing-instance-name` options. The DHCP relay agent obtains the values for the `host-name`, `logical-system-name`, and `routing-instance-name` as follows:

- If you include the `host-name` option, the DHCP relay agent uses the hostname of the device configured with the `host-name` statement at the `[edit system]` hierarchy level.
- If you include the `logical-system-name` option, the DHCP relay agent uses the logical system name configured with the `logical-system` statement at the `[edit logical-system]` hierarchy level.
- If you include the `routing-instance-name` option, the DHCP relay agent uses the routing instance name configured with the `routing-instance` statement at the `[edit routing-instances]` hierarchy level or at the `[edit logical-system` *`logical-system-name`* `routing-instances]` hierarchy level.

If you include the hostname and either or both of the logical system name and the routing instance name in the prefix, the hostname is followed by a forward slash (/). If you include both the logical system name and the routing instance name in the prefix, these values are separated by a semicolon (;).

The following examples show several possible formats for the DHCP option information when you specify the `prefix` statement for Fast Ethernet (fe) or Gigabit Ethernet (ge) interfaces with S-VLANs.

- If you include only the hostname in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  `hostname``:(fe | ge)-`*`fpc/pic/port`*`:`*`svlan-id-vlan-id`*

- If you include only the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  `logical-system-name``:(fe | ge)-`*`fpc/pic/port`*`:`*`svlan-id-vlan-id`*

- If you include only the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  `routing-instance-name``:(fe | ge)-`*`fpc/pic/port`*`:`*`svlan-id-vlan-id`*

- If you include both the hostname and the logical system name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

  `host-name/logical-system-name``:(fe | ge)-`*`fpc/pic/port`*`:`*`svlan-id-vlan-id`*

- If you include both the logical system name and the routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

- If you include the hostname, logical system name, and routing instance name in the prefix for Fast Ethernet or Gigabit Ethernet interfaces with S-VLANs:

```
host-name/logical-system-name;routing-instance-name:(fe | ge)-fpc/pic/port:svlan-id-vlan-id
```

For Fast Ethernet or Gigabit Ethernet interfaces that use VLANs but not S-VLANs, only the *vlan-id* value appears in the DHCP option format.

(DHCPv4) To configure a prefix with the option 82 information:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, the Agent Remote ID, or both.
   - To configure the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

   - To configure the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit remote-id
```

3. Specify that the prefix be included in the option 82 information. In this example, the prefix includes the hostname and logical system name.
   - To include the prefix with the Agent Circuit ID:

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set prefix host-name logical-system-name
```

- To include the prefix with the Agent Remote ID:

```
[edit forwarding-options dhcp-relay relay-option-82 remote-id]
user@host# set prefix host-name logical-system-name
```

(DHCPv6) To use a prefix with the DHCPv6 option 18 or option 37 information:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

   - To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the prefix is included in the option information. In this example, the prefix includes the hostname and logical system name

   - To include the prefix with option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix host-name logical-system-name
```

   - To include the prefix with option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix host-name logical-system-name
```

Including a Textual Description in DHCP Options

By default, when DHCP relay agent inserts option information in the packets sent to a DHCP server, the options include the interface identifier. However, you can configure the DHCP relay agent to include the textual description that is configured for the interface instead of the interface identifier. You can use the textual description for either the logical interface or the device interface.

You can include the textual interface description in the following DHCP options:

- DHCPv4 option 82 Agent Circuit ID (suboption 1)
- DHCPv4 option 82 Agent Remote ID (suboption 2)
- DHCPv6 option 18 Relay Agent Interface-ID
- DHCPv6 option 37 Relay Agent Remote-ID

The textual description is configured separately, using the `description` statement at the `[edit interfaces` *`interface-name`*`]` hierarchy level. If you specify that the textual description is used and no description is configured for the interface, DHCP relay defaults to using the Layer 2 interface name.

In the case of integrated routing and bridging (IRB) interfaces, the textual description of the Layer 2 interface is used instead of the textual description of the IRB interface. If there is no description configured, the Layer 2 logical interface name is used.

> **NOTE**: For IRB interfaces, the option 82 field must be able to uniquely identify the incoming interface based on either the Agent Circuit ID or Agent Remote ID . You can modify the information in the textual interface description to match the raw IFD (physical interface without a subunit) name and configure the option 82 field to use the interface description.

You can use the textual description with the following DHCP options:

- DHCPv4 Option 82 Agent Circuit ID (suboption 1)
- DHCPv4 Option 82 Agent Remote ID (suboption 2)
- DHCPv6 Relay Agent Interface-ID (option 18)
- DHCPv6 Relay Agent Remote-ID (option 37)

(DHCPv4) To configure the DHCP relay option 82 suboption to include the textual interface description:

1. Specify that you want to configure option 82 support.

```
[edit forwarding-options dhcp-relay]
user@host# edit relay-option-82
```

2. Configure DHCP relay agent to insert the Agent Circuit ID, Agent Remote ID, or both.

```
[edit forwarding-options dhcp-relay relay-option-82]
user@host# edit circuit-id
```

3. Specify that the textual description is included in the option 82 information. In this example, the option 82 information includes the description used for the device interface.

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id]
user@host# set use-interface-description device
```

(DHCPv6) To configure the DHCPv6 option 18 or option 37 to include the textual interface description:

1. Specify that you want to configure DHCPv6 relay agent support.

```
[edit forwarding-options dhcp-relay]
user@host# edit dhcpv6
```

2. Configure DHCPv6 relay agent to insert option 18 (Relay Agent Interface-ID), option 37 (Relay Agent Remote-ID), or both.

   - To configure option 18:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

   - To configure option 37:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

3. Specify that the textual description is included in the option information. In the following example, the option information includes the description used for the device interface.

- To include the textual description in option 18:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description device
```

- To include the textual description in option 37:

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description device
```

SEE ALSO

Configuring Interface Description

How DHCP Relay Agent Uses Option 82 for Auto Logout

Table 10 on page 209 indicates how the DHCP relay agent determines the option 82 value used for the client auto logout feature. Depending on the configuration settings, DHCP relay agent takes the action indicated in the Action Taken column.

Table 10: 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

Table 10: DHCP Relay Agent Option 82 Value for Auto Logout *(Continued)*

DHCP Relay Agent Configuration Settings				giaddr in non-snooped packet	Action Taken
DHCP Relay Configured with Option 82	Discover Packet Contains Option 82	Override "trust-option-82"	Override "always-write-option-82"		
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

Enable Processing of Untrusted Packets So Option 82 Information Can Be Used

By default, the DHCP relay agent treats client packets with a giaddr of 0 (zero) and option 82 information as if the packets originated at an untrusted source, and drops them without further processing. You can override this behavior and specify that the DHCP relay agent process DHCP client packets that have a giaddr of 0 (zero) and contain option 82 information.

To configure DHCP relay agent to trust option 82 information:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Specify that the DHCP relay agent process DHCP client packets with a giaddr of 0 and that contain option 82 information.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set trust-option-82
```

Check if Your Device Support DHCP Option-82

To configure a switch with DHCP relay in forward-only mode, check whether your device supports DHCP Option 82.

Use the procedures in Table 11 on page 212 to confirm the support of Option-82 or required workaround.

Table 11: Verify support of Option-82 in DHCP Server

Problem	How to Verify ?	Solution
Verify if your switching device supports DHCP Option 82.	Use the `dhcp traceoptions` on the DHCP Relay. A message states the drop due to missing Option 82. If the DHCP Offer packet dropped because of Option-82 not included, you will receive the message like: `Feb 25 15:41:13.577519 [MSTR][NOTE] [default:default][RLY][INET][irb.6] jdhcpd_packet_handle: BOOTPREPLY could not find client table entry`	To fix the issue: • **Solution 1:** Upgrade the DHCP Server to Junos OS version that fully supports Option 82. • **Solution 2:** Change the DHCP Relay to a “stateful” mode (that is, DHCP Relay “binding” mode). • **Solution 3:** Move the DHCP Relay to a MX or to a non-ELS EX/QFX switch, so to enable the Legacy ‘helper bootp’ mode.

SEE ALSO

DHCP Relay Agent | 156

DHCP and BOOTP Relay Agent | 190

Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82

Some PXE or BOOTP servers do not support Option-82, that is, their DHCP Offer messages do not include the Option-82 value added by the DHCP Relay. As a result, the DHCP Relay will drop the DHCP Offer and the PXE/BOOTP client will not be able to complete its boot sequence.

Following are the possible solution to resolve this issue:

Solution 1: Upgrade to a PXE Server that supports Option-82

Solution 2: Host the PXE server with a DHCP Server

- Ensure that the DHCP Server (that supports Option-82) run together with the PXE server.
- Configure an Option-60 on the DHCP Server.

- Use the following CLI to configure Option-60 an a Microsoft WS DHCP Server:

```
netsh dhcp server dhcp-server-address add optiondef 60 ClientIdentifier STRING 0 PXEClient
```

- Activate the option in the user interface of the DHCP server.

This way, the PXE/BOOTP clients will receive proper DHCP Offer with Option-60 “PXEClient” and will reach the PXE server at the same IP address of the DHCP Server.

Solution 3: Include Option-60 and Option-43 DHCP Server Message

If the PXE Server is not hosted together with the DHCP Server, you need the DHCP Server to send an Option-43 also in its DHCP Offer. The Option-43 provides the IP address of the PXE server. Note that, the older PXE or BOOTP clients might ignore Option-43 and will therefore try to get the software from the DHCP Server. Enter the Option-43 in the DHCP Server configuration in a hexadecimal mode.

For is a sample option-43 message:

```
06 01 07 08 07 00 01 01 0A 0B 0C 0D 09 0B 00 01 09 53 65 72 76 65 72 50 58 45 0A 02 00 53
```

The above message indicates the following information to the PXE client:

- Disable broadcast and multicast discovery
- Accept only the PXE Server provided in this text
- PXE Server IP is 10.11.12.13 (see the bytes '0A 0B 0C 0D' in the above text)
- Boot menu on the PXE client (to present to the end user):
  - just one line, “ServerPXE”
  - Autoselect the first Boot option, prompt “S”, no timeout (that is, immediately boot unless you press F8)

DHCP packets on non-configured interfaces are dropped

Once you enable DHCP-Relay on the QFX or EX Switches, the DHCP Snooping feature gets enabled and all DHCP packets incoming through any interface (both configured and unconfigured interface) of the device are analyzed. The interfaces that are not listed under the DHCP configuration are considered ‘unconfigured’.

Depending on the configuration, DHCP packets received on unconfigured interfaces are dropped.

If the DHCP packets are dropped on ‘unconfigured’ interface, you will receive the message like:

```
May 25 18:26:31.796241 [MSTR][NOTE] [default:default][RLY][INET][irb.82] jdhcpd_packet_handle:
BOOTPREQUEST irb.82 arrived on unconfigured interface DISCOVER, flags 23, config 0x0
```

SEE ALSO

DHCP Relay Agent | 156

DHCP and BOOTP Relay Agent | 190

Example: Configure DHCP Relay in Forward Only Mode

IN THIS SECTION

- Requirements | 214
- Overview | 215
- Configuration | 215
- Verification | 218

The example shows how to configure a “stateless” (“forward-only”) DHCP Relay on Enhanced Layer 2 Software (ELS) EX Series and QFX Series switches. If your switch runs software that does not support ELS, see Configuring Interface Ranges. For ELS details, see Using the Enhanced Layer 2 Software CLI.

Requirements

This example uses the following hardware and software components:

- QFX or EX Series Switches (ELS mode).
- Junos OS Release 18.4R3.

Before you configure forward-only DHCP relay on EX Series and QFX Series switches, lets understand about Option 82 support on DHCP.

To verify whether your device supports DHCP Option-82, see "Check if Your Device Support DHCP Option-82" on page 211.

The following messages from the DHCP server include a copy of the Option 82 information on sent by the DHCP Relay in the Discover and Request messages:

- Offer
- Acknowledgement (ACK)
- Negative acknowledgment (NACK)

The DHCP relay discards any OFFER, ACK, and NACK messages that do not include a valid Option 82 information.

On how to avoid dropping of DHCP offer message when PXE or BOOTP servers do not support Option-82, see *Managing Your DHCP PXE/BOOTP Servers That Do Not Support Option-82*.

Overview

In this example, we are configuring a switching device to act as DHCP relay agent by completing the following steps:

1. Add a set of DHCP server IP addresses configured as active server groups.
2. Configure the option 82 support for a named group of interfaces.

After you configure the example, the DHCP relay agent includes option 82 information in the DHCP packets that it receives from the clients and forwards to the DHCP server.

Configuration

IN THIS SECTION

- CLI Quick Configuration | **216**
- Configure forward-only' DHCP Relay Agent | **216**
- Results | **218**

To configure a forward-only DHCP relay agent on a ELS supported EX or QFX switches, perform these tasks:

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them in a text file, remove any line breaks, change any details necessary to match your network configuration, and then copy and paste the command into the CLI at the `[edit]` hierarchy level.

```
set forwarding-options dhcp-relay server-group SV1 dhcp-server-1-address
set forwarding-options dhcp-relay server-group SV2 dhcp-server-2-address
set forwarding-options dhcp-relay active-server-group SV1
set forwarding-options dhcp-relay group DHCP-FO forward-only
set forwarding-options dhcp-relay group DHCP-FO relay-option-82 circuit-id use-interface-
description device
set forwarding-options dhcp-relay group DHCP-FO interface interface1
set forwarding-options dhcp-relay group DHCP-FO interface interface2
```

Configure forward-only' DHCP Relay Agent

Step-by-Step Procedure

To configure forward-only DHCP relay:

1. Specify the name of the server group, SV1 and SV2.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group SV1
user@host# set server-group SV2
```

2. Add the IP addresses of the DHCP servers belonging to the group.

```
[edit forwarding-options dhcp-relay]
user@host# set server-group SV1 dhcp-server-1-address
user@host# set server-group SV2 dhcp-server-2-address
```

3. (Optional) In enterprise scenario, you can use the Preboot Execution Environment (PXE) or BOOTP for a PC (or other devices) to get its Junos OS from a server.

- If you want to enable BOOTP support when the switch is configured to be a DHCP relay agent, enter the following statement:

```
[edit forwarding-options dhcp-relay]
user@host# set overrides bootp-support
```

- Add a DHCP or PXE Servers to the DHCP Servers group

```
[edit forwarding-options dhcp-relay]
user@host# server-group SV1 dhcp-server-3-address
```

4. Apply the server group as an active server group.

```
[edit forwarding-options dhcp-relay]
user@host# set active-server-group SV1
```

5. Define DHCP-FO as interface group on your switching device acting as DHCP relay. Configure:

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO forward-only
```

6. Add a list of interfaces to the interface group.

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO interface interface1
user@host# set group DHCP-FO interface interface2
```

7. Set relay option 82 to interfaces and specify Agent circuit ID. Agent Circuit ID identifies the interface on which the client DHCP packet is received. When you configure circuit ID, the include the textual interface description in the message.

```
[edit forwarding-options dhcp-relay]
user@host# set group DHCP-FO group relay-option-82 circuit-id use-interface-description device
```

Results

From configuration mode, confirm the results of your configuration by issuing the `show` statement at the `[edit forwarding-options]` hierarchy level. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit forwarding-options]
user@host> show
dhcp-relay {
    server-group {
        SV1 {
            dhcp-server-1-address;
        }
        SV2 {
            dhcp-server-2-address;
        }
    }
    active-server-group SV1;
    group DHCP-FO {
        relay-option-82 {
            circuit-id {
                use-interface-description device;
            }
        }
        forward-only;
        interface interface1;
        interface interface2;
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the Offer message with Option-82 | 219

Verify if the messages from the DHCP server includes a copy of the Option 82 information sent by the DHCP relay.

Verifying the Offer message with Option-82

Purpose

Verify the “forward-only” DHCP Relay by enabling the dhcp traceoptions on the DHCP Relay.

Action

- Receive the output of the tracing operation in the specified file.

```
user@host# set system processes dhcp-service traceoptions file dhcp_logfile size 10m
user@host# set system processes dhcp-service traceoptions level all
user@host# set system processes dhcp-service traceoptions flag all
Feb 25 15:41:11.454186 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_io_process_ip_packet: LOCAL: recv pkt; sa 10.42.6.20; da 10.42.59.251; src_port 67;
dst_port 67; len 410
Feb 25 15:41:11.454218 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
from == 10.42.6.20, port == 67 ]--
Feb 25 15:41:11.454228 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
size == 410, op == 2 ]--
Feb 25 15:41:11.454250 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
flags == 8000 ]--
Feb 25 15:41:11.454271 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
htype == 1, hlen == 6 ]--
Feb 25 15:41:11.454292 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
hops == 0, xid == e50f52a1 ]--
Feb 25 15:41:11.454313 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
secs == 0, flags == 8000 ]--
Feb 25 15:41:11.454347 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
ciaddr == 0.0.0.0 ]--
Feb 25 15:41:11.454428 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
yiaddr == 10.42.58.21 ]--
Feb 25 15:41:11.454461 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
siaddr == 10.42.6.20 ]--
Feb 25 15:41:11.454472 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
giaddr == 10.42.59.251 ]--
Feb 25 15:41:11.454486 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
chaddr == 34 48 ed 27 e2 29 00 00 00 00 00 00 00 00 00 00 ]--
Feb 25 15:41:11.454508 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
```

```
sname ==  ]--
Feb 25 15:41:11.454535 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ DHCP/BOOTP
file ==  ]--
Feb 25 15:41:11.454560 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  53,
len   1, data DHCP-OFFER ]--
Feb 25 15:41:11.454603 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   1,
len   4, data ff ff fc 00 ]--
Feb 25 15:41:11.454616 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  58,
len   4, data 00 05 46 00 ]--
Feb 25 15:41:11.454638 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  59,
len   4, data 00 09 3a 80 ]--
Feb 25 15:41:11.454675 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  51,
len   4, data 00 0a 8c 00 ]--
Feb 25 15:41:11.454701 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  54,
len   4, data 0a 2a 06 14 ]--
Feb 25 15:41:11.454724 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   3,
len   4, data 0a 2a 3b fe ]--
Feb 25 15:41:11.454748 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   4,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454778 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code   6,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454805 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  15,
len  15, data 6c 69 73 65 63 2e 69 6e 74 65 72 6e 61 6c 00 ]--
Feb 25 15:41:11.454829 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  42,
len   8, data 0a 2a 01 64 0a 2a 06 64 ]--
Feb 25 15:41:11.454858 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code 128,
len  29, data 61 74 73 65 2d 65 6d 70 69 72 75 6d 31 2e 6c 69 73 65 63 2e 69 6e 74 65 72 6e
61 6c 00 ]--
Feb 25 15:41:11.454888 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code 129,
len  29, data 61 74 73 65 2d 65 6d 70 69 72 75 6d 31 2e 6c 69 73 65 63 2e 69 6e 74 65 72 6e
61 6c 00 ]--
Feb 25 15:41:11.454902 [MSTR][DEBUG][default:default][RLY][INET][irb.56] --[ OPTION code  82,
len  19, data 01 11 49 52 42 2d 69 72 62 2e 35 36 3a 61 65 33 30 2e 30 ]--
Feb 25 15:41:11.454924 [MSTR][INFO] [default:default][RLY][INET][irb.56] --[ OPTION code 255,
len   0 ]--
Feb 25 15:41:11.454939 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_find_client_from_server_pdu: Using yiaddr from BOOTPREPLY for lookup
Feb 25 15:41:11.454962 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_platform_client_v4_app_get_l3_index:  safd is not client type
Feb 25 15:41:11.454992 [MSTR][DEBUG] client_key_compose: Composing key (0xb294380) for cid_l
0, cid NULL, mac 34 48 ed 27 e2 29, htype 1, subnet 10.42.59.251, ifindx 0, opt82_l 0, opt82
NULL
Feb 25 15:41:11.455016 [MSTR][DEBUG] client_key_compose: Successfully composed
```

```
CK_TYPE_HW_ADDR_ON_SUBNET (2) client key object.
Feb 25 15:41:11.455028 [MSTR][DEBUG] client_key_print: key_type CK_TYPE_HW_ADDR_ON_SUBNET
(2): subnet 10.42.59.251, MAC htype 1, Addr 34 48 ed 27 e2 29
Feb 25 15:41:11.455050 [MSTR][DEBUG] client_key_print: key_type CK_TYPE_HW_ADDR_ON_SUBNET (2)
other fields: subnet 10.42.59.251, ifindex 0, opt82_len 0, -
Feb 25 15:41:11.455081 [MSTR][INFO] [default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Safd irb.56 in routing context default:default - forward
only or drop processing
Feb 25 15:41:11.455114 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Removing option-82
Feb 25 15:41:11.455124 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Length of option 82 = 21 bytes
Feb 25 15:41:11.455146 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_option_strip_relay_info: Moving 2 bytes, which were after option 82 and parse again
Feb 25 15:41:11.455169 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Safd irb.56 in routing context default:default - config
supports fwd only relaying packet
Feb 25 15:41:11.455193 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_process_forward_only_or_drop: Result of forward-only: packet_consumed Yes,
packet_dropped No, message_type OFFER
Feb 25 15:41:11.455217 [MSTR][DEBUG][default:default][RLY][INET][irb.56]
jdhcpd_relay_forward_only_packet: Broadcast BOOTPREPLY OFFER for 10.42.58.21 on safd irb.56
```

- You can use the following commands to search for problems in the DHCP traceoptions log file (in this example, **‘dhcp_logfile’**).

  - To get an overview of most common problems, use:

    ```
    user@host>  show log dhcp_logfile | match "dropp|fail|unconf" | except "packet_dropped No"
    ```

  - To investigate a specific problem, use:

    ```
    user@host>  show log dhcp_logfile | find " arrived on unconfigured interface"
    ```

    The `find` command is similar to Linux `less` command. It will reach the first entry in the log and allow you to scroll up/down the message.

- (Optional) To query the traceoptions logs on a Linux sever (or from the Junos shell), you can use both the following commands:

```
user@host> egrep -i "dropp|fail|unconf" dhcp_logfile | egrep -v "packet_dropped No" | more
```

```
user@host> egrep -i -b 5 " arrived on unconfigured interface" dhcp_logfile | more
```

Meaning

The above sample confirms that the messages from the DHCP server includes a copy of the Option 82 information sent by the DHCP relay and the sample also displays the textual description of the interface.

RELATED DOCUMENTATION

Secure DHCP Message Exchange | 343

DHCP Server | 49

DHCP Server Configuration | 51

DHCP Access Service Overview | 9

Secure DHCP Message Exchange | 343

DHCP Active Server Groups | 349

DHCPv6 Server | 109

DHCP Auto Logout | 296

DHCPv6 Relay Agent

IN THIS SECTION

- DHCPv6 Relay Agent Overview | 223
- Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets | 224
- Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets | 226
- Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets | 227

Verifying and Managing DHCPv6 Relay Configuration | 228

The DHCPv6 relay agent enhances the DHCP relay agent by providing support in an IPv6 network. The DHCPv6 relay agent passes messages between the DHCPv6 client and the DHCPv6 server, similar to the way DHCP relay agent supports an IPv4 network. DHCPv6 relay agents eliminate the necessity of having a DHCPv6 server on each physical network. For more information about inserting DHCPv6 Interface-ID (Option 18), Remote-ID (Option 37) or Client MAC Address (Option 79) in DHCPv6 packets, and verifying the DHCPv6 configuration, read this topic.

DHCPv6 Relay Agent Overview

When a DHCPv6 client logs in, the DHCPv6 relay agent uses the AAA service framework to interact with the RADIUS server to provide authentication and accounting. The RADIUS server, which is configured independently of DHCP, authenticates the client and supplies the IPv6 prefix and client configuration parameters, such as session timeout and the maximum number of clients allowed per interface.

NOTE: The PTX Series Packet Transport Routers do not support authentication for DHCPv6 relay agents.

NOTE: The following DHCPv6 functionalities are not supported on ACX Series routers:

- Subscriber authentication for DHCPv6 relay agents
- DHCP snooping
- DHCPv6 client
- Liveness detection
- Dynamic profiles
- Option 37 support for remote ID insertion
- Bidirectional Forwarding Detection (BFD) for DHCPv6 relay

The DHCPv6 relay agent is compatible with the DHCP local server and the DHCP relay agent, and can be enabled on the same interface as either the DHCP local server or DHCP relay agent.

To configure the DHCPv6 relay agent on the router (or switch), you include the `dhcpv6` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can also include the `dhcpv6` statement at the following hierarchy levels:

- `[edit logical-systems` *`logical-system-name`* `forwarding-options dhcp-relay]`
- `[edit logical-systems` *`logical-system-name`* `routing-instances` *`routing-instance-name`* `forwarding-options dhcp-relay]`
- `[edit routing-instances` *`routing-instance-name`* `forwarding-options dhcp-relay]`

See *DHCPv6 Monitoring and Management* for commands specific to viewing and clearing DHCPv6 bindings and statistics.

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

You can configure DHCPv6 relay agent to insert the DHCPv6 Interface-ID (option 18) in the packets that the relay sends to a DHCPv6 server. You can configure the option 18 support at either the DHCPv6 global or group level.

When you configure option 18 support, you can optionally include the following additional information:

- Prefix—Specify the `prefix` option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the `use-interface-description` option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Circuit ID suboption (suboption 1)—Specify the `use-option-82` option to include the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 1 value and inserts it into the outgoing packets. If no DHCPv4 binding exists or if the binding does not have an option 82 suboption 1 value, the router sends the packets without adding an option 18.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Interface-ID option (option 18) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 18.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-interface-id
```

2. (Optional) Specify the prefix to include in option 18.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 18 include the textual description of the interface. You can specify either the `logical` interface description or the `device` interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 18 use the DHCPv4 Option 82 Agent Circuit ID suboption (suboption 1) value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-interface-id]
user@host# set use-option-82
```

SEE ALSO

Including a Prefix in DHCP Options

Including a Textual Description in DHCP Options

Inserting DHCPv6 Remote-ID Option (Option 37) In DHCPv6 Packets

Starting in Junos OS Release 14.1, you can configure DHCPv6 relay agent to insert DHCPv6 Remote-ID (option 37) in the packets that the relay sends to a DHCPv6 server. You can configure option 37 support at either the DHCPv6 global or group level.

When you configure option 37 support, you can optionally include the following information:

- Prefix—Specify the `prefix` option to add a prefix to the interface identifier. The prefix can be any combination of hostname, logical system name, and routing instance name.
- Interface description—Specify the `use-interface-description` option to include the textual interface description instead of the interface identifier. You can include either the device interface description or the logical interface description.
- Option 82 Agent Remote-ID suboption (suboption 2)—Specify the `use-option-82` option to use the value of the DHCPv4 option 82 Remote-ID suboption (suboption 2). This configuration is useful in a dual-stack environment, which has both DHCPv4 and DHCPv6 subscribers that reside over the same underlying logical interface. The router checks for the option 82 suboption 2 value and inserts it into the outgoing packets.

NOTE: If you specify one of the optional configurations, and the specified information does not exist (for example, there is no interface description), DHCPv6 relay ignores the optional configuration and inserts the default interface identifier in the packets.

To insert the DHCPv6 Remote-ID option (option 37) in DHCPv6 packets:

1. Configure the DHCPv6 relay to include option 37.

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit relay-agent-remote-id
```

2. (Optional) Specify the prefix to include with the option 37 information.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set prefix prefix
```

3. (Optional) Specify that option 37 include the textual description of the interface. You can specify either the `logical` interface description or the `device` interface description.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-interface-description (logical | device)
```

4. (Optional) Specify that option 37 use the DHCPv4 option 82 Remote-ID suboption (suboption 2) value.

   If no DHCPv4 binding exists, or if the binding does not include an option 82 suboption 2 value, by default the router sends the packets without adding option 37. However, you can use the optional `strict` keyword to specify that the router drop packets that do not have a suboption 2 value.

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id]
user@host# set use-option-82 strict
```

SEE ALSO

> *Extracting an Option 82 or Option 37 Substring to Create an Interface Set*

Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets

The incremental deployment of IPv6 to existing IPv4 networks can result in a dual-stack network environment in which devices act as both DHCPv4 and DHCPv6 clients. In dual-stack scenarios, operators need to be able to associate DHCPv4 and DHCPv6 messages with the same client interface, based on an identifier that is common to the interface.

You can configure a DHCPv6 relay agent to insert the DHCPv6 client MAC address in the packets that the relay sends to a DHCPv6 server. The client MAC address is used to associate DHCPv4 and DHCPv6 messages with the same client interface.

In addition to associating DHCPv4 and DHCPv6 messages from a dual-stack client, having the client MAC address in DHCPv6 packets provides additional information for event debugging and logging related to the client at the relay agent and the server.

When DHCPv6 option 79 is enabled, the DHCPv6 relay agent reads the source MAC address of DHCPv6 Solicit and DHCPv6 Request messages that it receives from a client. The relay agent encapsulates the Solicit and Request messages within a DHCPv6 Relay-Forward message, and inserts

the client MAC address as option 79 in the Relay-Forward header before relaying the message to the server.

If the DHCPv6 packet already has a Relay-Forward header, the DHCPv6 relay agent adds the client MAC address if the packet meets the following conditions: the packet has only one Relay-Forward header, the Relay-Forward header was added by an LDRA, and the Relay-Forward header does not already include option 79 information.

You can also configure DHCPv6 option 79 for a lightweight DHCPv6 relay agent (LDRA). An LDRA resides on the same IPv6 link as the DHCPv6 client and relay agent or server and acts as a layer 2 relay agent, without performing the routing function necessary to forward messages to a server or relay agent that resides on a different IPv6 link.

- To configure DHCPv6 option 79 for a DHCPv6 relay agent (layer 3):

```
[edit]
user@host# set forwarding-options dhcp-relay dhcpv6 relay-agent-option-79
```

- To configure DHCPv6 option 79 for an LDRA (layer 2):

```
[edit]
user@host# set vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-79
```

SEE ALSO

DHCPv6 Relay Agent Options

Configuring DHCPv6 Relay Agent Options

Using Lightweight DHCPv6 Relay Agent (LDRA)

Verifying and Managing DHCPv6 Relay Configuration

IN THIS SECTION

Purpose | 229

Action | 229

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
```

Release History Table

Release	Description
14.1	Starting in Junos OS Release 14.1, you can configure DHCPv6 relay agent to insert DHCPv6 Remote-ID (option 37) in the packets that the relay sends to a DHCPv6 server.

RELATED DOCUMENTATION

Centrally Configure DHCP Options on a RADIUS Server | 277

DHCP Snooping | 287

DHCP Liveness Detection | 315

DHCP Relay Agent Information Option (Option 82) | 198

DHCP Client | 234

DHCP Relay Proxy

IN THIS SECTION

- DHCP Relay Proxy Overview | 230
- Enabling DHCP Relay Proxy Mode | 232

A DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers. The DHCP relay agent is configured on the router or switch, which operates between the DHCP client and one or more DHCP servers. For more information, read this topic.

DHCP Relay Proxy Overview

IN THIS SECTION

- Benefits of Using DHCP Relay Proxy | 231
- Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers | 231

DHCP relay proxy mode is an enhancement to extended DHCP relay. DHCP relay proxy supports all DHCP relay features while providing additional features and benefits.

Normally, extended DHCP relay operates as a helper application for DHCP operations. Except for the ability to add DHCP relay agent options and the gateway address (giaddr) to DHCP packets, DHCP relay is transparent to DHCP clients and DHCP servers, and simply forwards messages between DHCP clients and servers.

When you configure DHCP relay to operate in proxy mode, the relay is no longer transparent. In proxy mode, DHCP relay conceals DHCP server details from DHCP clients, which interact with a DHCP relay

in proxy mode as though it is the DHCP server. For DHCP servers there is no change, because proxy mode has no effect on how the DHCP server interacts with the DHCP relay.

NOTE: You cannot configure both DHCP relay proxy and extended DHCP local server on the same interface.

Benefits of Using DHCP Relay Proxy

DHCP relay proxy provides the following benefits:

- DHCP server isolation and DoS protection—DHCP clients are unable to detect the DHCP servers, learn DHCP server addresses, or determine the number of servers that are providing DHCP support. Server isolation also provides denial-of-service (DoS) protection for the DHCP servers.
- Multiple lease offer selection—DHCP relay proxy receives lease offers from multiple DHCP servers and selects a single offer to send to the DHCP client, thereby reducing traffic in the network. Currently, the DHCP relay proxy selects the first offer received.
- Support for both numbered and unnumbered Ethernet interfaces—For DHCP clients connected through Ethernet interfaces, when the DHCP client obtains an address, the DHCP relay proxy adds an access internal host route specifying that interface as the outbound interface. The route is automatically removed when the lease time expires or when the client releases the address.
- Logical system support—DHCP relay proxy can be configured in a logical system, whereas a non-proxy mode DHCP relay cannot.

Interaction Among DHCP Relay Proxy, DHCP Client, and DHCP Servers

The DHCP relay agent is configured on the router (or switch), which operates between the DHCP client and one or more DHCP servers.

The following steps provide a high-level description of how DHCP relay proxy interacts with DHCP clients and DHCP servers.

1. The DHCP client sends a discover packet to locate a DHCP server in the network from which to obtain configuration parameters for the subscriber.
2. The DHCP relay proxy receives the discover packet from the DHCP client and forwards copies of the packet to each supporting DHCP server. The DHCP relay proxy then creates a client table entry to keep track of the client state.
3. In response to the discover packet, each DHCP server sends an offer packet to the client, which the DHCP relay proxy receives. The DHCP relay proxy does the following:

a. Selects the first offer received as the offer to sent to the client

b. Replaces the DHCP server address with the address of the DHCP relay proxy

c. Forwards the offer to the DHCP client.

4. The DHCP client receives the offer from the DHCP relay proxy.
5. The DHCP client sends a request packet that indicates the DHCP server from which to obtain configuration information—the request packet specifies the address of the DHCP relay proxy.
6. The DHCP relay proxy receives the request packet and forwards copies, which include the address of selected server, to all supporting DHCP servers.
7. The DHCP server requested by the client sends an acknowledgement (ACK) packet that contains the client configuration parameters.
8. The DHCP relay proxy receives the ACK packet, replaces the DHCP server address with its own address, and forwards the packet to the client.
9. The DHCP client receives the ACK packet and stores the configuration information.
10. If configured to do so, the DHCP relay proxy installs a host route and Address Resolution Protocol (ARP) entry for the DHCP client.
11. After the initial DHCP lease is established, the DHCP relay proxy receives all lease renewals and lease releases from the DHCP client and forwards them to the DHCP server.

Enabling DHCP Relay Proxy Mode

You can enable DHCP relay proxy mode on all interfaces or a group of interfaces.

To enable DHCP relay proxy mode:

1. Specify that you want to configure override options.

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable DHCP relay proxy mode.

```
[edit forwarding-options dhcp-relay overrides]
user@host# set proxy-mode
```

5
CHAPTER

DHCP Client

DHCP Client | 234

DHCPv6 Client | 255

DHCP Client

IN THIS SECTION

- Understanding DHCP Client Operation | 234
- Minimum DHCP Client Configuration | 235
- Configuring a DHCP Client | 235
- Example: Configuring the Device as a DHCP Client | 238
- Verifying and Managing DHCP Client Configuration | 245
- Example: Configuring as a DHCP Client in Chassis Cluster Mode | 246

SRX Series device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. For more information, read this topic.

Understanding DHCP Client Operation

A Juniper Networks device can act as a DHCP client, receiving its TCP/IP settings and the IP address for any physical interface in any security zone from an external DHCP server. The device can also act as a DHCP server, providing TCP/IP settings and IP addresses to clients in any zone. When the device operates as a DHCP client and a DHCP server simultaneously, it can transfer the TCP/IP settings learned through its DHCP client module to its default DHCP server module. For the device to operate as a DHCP client, you configure a *logical interface* on the device to obtain an IP address from the DHCP server in the network. You set the vendor class ID, lease time, DHCP server address, retransmission attempts, and retry interval. You can renew DHCP client releases.

DHCP client operations are supported on all SRX Series devices in chassis cluster mode.

Minimum DHCP Client Configuration

The following sample output shows the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCP client. In this output, the interface is ge-0/0/0 and the logical unit is 0.

```
[edit interfaces]
    ge-0/0/0 {
        unit 0 {
            family inet {
                dhcp-client
        }
    }
}
```

NOTE: To configure a DHCP client in a routing instance, add the interface in a routing instance using the `[edit routing-instances]` hierarchy.

Configuring a DHCP Client

A Dynamic Host Configuration Protocol (DHCP) server can provide many valuable TCP/IP network services. DHCP can dynamically allocate IP parameters, such as an IP address, to clients, and it can also deliver software upgrades to clients.

DHCP configuration consists of two components, configuration of DHCP clients and configuration of a DHCP server. Client configuration determines how clients send a message requesting an IP address, whereas a DHCP server configuration enables the server to send an IP address configuration back to the client. This topic describes configuring a DHCP client. For directions for configuring a DHCP server, see *Configuring a DHCP Server on Switches* or *Configuring a Switch as a DHCP Server*.

You can change DHCP client configurations from the switch, using client identifiers to indicate which clients you want to configure.

To configure a DHCP client, you configure an interface to belong to the DHCP family and specify additional attributes, as desired:

```
[edit]
user@switch# set interfaces interface-name unit number family  inet dhcp
 configuration-statement
```

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

The options that you can configure are listed in Table 12 on page 236. 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 12: 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.

Table 12: DHCP Client Settings *(Continued)*

Configuration Statement	Description
vendor-option	Vendor class ID (CPU's manufacturer ID string) for the DHCP client.

For the device to operate as a DHCP client, you configure a logical interface on the device to obtain an IP address from the DHCP local server in the network. You can then set the client-identifier, options no-hostname, lease time, retransmission attempts, retry interval, preferred DHCP local server address, and vendor class ID.

To configure optional DHCP client attributes on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCP client identifier prefix as the routing instance name.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

2. Configure the DHCP options no-hostname if you do not want the client to send hostname (RFC option code 12) in the packets.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Set the IPv4 address of the preferred DHCP local server.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set server-address 10.1.1.1
```

7. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

NOTE: To configure the DHCP client in a routing instance, configure the interface in the `[edit routing-instances]` hierarchy.

Example: Configuring the Device as a DHCP Client

IN THIS SECTION

- Requirements | 238
- Overview | 239
- Configuration | 240
- Verification | 243

This example shows how to configure the device as a DHCP client.

Requirements

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet. You can use the `show system services dhcp pool` CLI command to view information on DHCP address pools.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices. See the *Understanding Management Predefined Policy Applications*.
- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure the device as a DHCP client. You specify the interface as ge-0/0/2, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds.

Then you set the number of retransmission attempts to 6. The range is from 0 through 50,000, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Set the force-discover option if you want to force the DHCP client to send a DHCP discover packet after one to three failed dhcp-request attempts. The force-discover option ensures that the DHCP server will assign the same or a new IP address to the client. Finally, you set the IPv4 address of the preferred DHCP server to 10.1.1.1 and the vendor class ID to ether.

WARNING: Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported. When you upgrade to Junos OS Release 15.1X49-D60 and later releases on a device that already has the DHCPD configuration, the following warning messages are displayed:

WARNING: The DHCP configuration command used will be deprecated in future Junos releases.

WARNING: Please see documentation for updated commands.

NOTE: Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to align with other Junos platforms. There is no change in the functionality.

Configuration

IN THIS SECTION

- Procedure | 240

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

```
set interfaces ge-0/0/2 unit 0 family inet dhcp-client client-identifier prefix host-name
set interfaces ge-0/0/2 unit 0 family inet dhcp-client lease-time 86400
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces ge-0/0/2 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces ge-0/0/2 unit 0 family inet dhcp-client force-discover
set interfaces ge-0/0/2 unit 0 family inet dhcp-client server-address 192.168.2.1
set interfaces ge-0/0/2 unit 0 family inet dhcp-client vendor-id ether
set interfaces ge-0/0/2 unit 0 family inet dhcp-client options no-hostname
```

GUI Quick Configuration

Step-by-Step Procedure

To configure the device as a DHCP client:

1. In the J-Web interface, select **Configure** > **Services** > **DHCP** > **DHCP Client**.
2. Under Interfaces, add `ge-0/0/2.0`.
3. Configure the DHCP client identifier as either an ASCII or hexadecimal value.
4. From the Client identifier choice list, select `hexadecimal`.
5. In the Hexadecimal box, type the client identifier—`00:0a:12:00:12:12`.

6. Set the DHCP lease time in seconds. This is the lease time in seconds requested in a DHCP client protocol packet; the range is 60 through 2,147,483,647. Type **86400**.
7. Set the retransmission number of attempts to 6. This is the number of attempts to retransmit the DHCP client protocol packet. The range is 0 through 6.
8. Set the retransmission interval in seconds to 5. This is the number of seconds between successive transmissions. The range is 4 through 64. The default is 4 seconds.
9. Configure the force-discover option to force the DHCP client to send a DHCP discover packet after one to three failed `dhcp-request` attempts.
10. Set the IPv4 address of the preferred DHCP server. Type **192.168.2.1**.
11. Set the vendor class ID. This is the vendor class identification for the DHCP client. Type **ether**.
12. Configure options no-hostname if you do not want the client to send hostname in the packets (RFC option code 12).
13. Click **OK**.
14. If you are done configuring the device, click **Commit** >.

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the device as a DHCP client:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces ge-0/0/2 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set client-identifier prefix host
```

3. Set the DHCP lease time.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

4. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

5. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

6. Configure the force-discover option.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set force-discover.
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set server-address 192.168.2.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

9. Configure options no-hostname if you do not want the client to send the hostname in packets.

```
[edit interfaces ge-0/0/2 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

Results

From configuration mode, confirm your configuration by entering the `show interfaces ge-0/0/2 unit 0 family inet` command. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces ge-0/0/2 unit 0 family inet
dhcp-client {
    client-identifier hexadecimal 00:0a:12:00:12:12;
    options no-hostname;
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    force-discover;
    server-address 192.168.2.1;
    update-server;
    vendor-id ether;
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Client | **243**

Confirm that the configuration is working properly.

Verifying the DHCP Client

Purpose

Verify that the DHCP client information has been configured.

Action

From operational mode, enter these commands:

- `show dhcp client binding` command to display the binding state of a Dynamic Host Configuration Protocol (DHCP) client.
- `show dhcp client statistics` command to display client statistics.

These commands produce the following sample output:

```
user@host> show dhcp client binding
```

```
IP address        Hardware address   Expires     State      Interface
192.168.2.2       88:a2:5e:0a:d6:03  2419093     BOUND      ge-0/0/2.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     2
    Send error                2

Messages received:
    BOOTREPLY                 6
    DHCPOFFER                 4
    DHCPACK                   2
    DHCPNAK                   0
    DHCPFORCERENEW            0

Messages sent:
    BOOTREQUEST               39
    DHCPDECLINE               0
    DHCPDISCOVER              23
    DHCPREQUEST               16
    DHCPINFORM                0
    DHCPRELEASE               0
    DHCPRENEW                 0
    DHCPREBIND                0
```

Verifying and Managing DHCP Client Configuration

IN THIS SECTION

- Purpose | 245
- Action | 245

Purpose

View or clear information about client address bindings and statistics for the DHCP client on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

Action

- To display the address bindings in the client table on the DHCP client:

```
user@host> show dhcp client binding
```

- To display DHCP client statistics:

```
user@host> show dhcp client statistics
```

- To clear the binding state of a DHCP client from the client table on the DHCP client:

```
user@host> clear dhcp client binding
```

- To clear all DHCP client statistics:

```
user@host> clear dhcp client statistics
```

NOTE: To clear or view information about client bindings and statistics in a routing instance, run the following commands:

- show dhcp client binding routing instance *<routing-instance name>*
- show dhcp client statistics routing instance *<routing-instance name>*
- clear dhcp client binding routing instance *<routing-instance name>*
- clear dhcp client statistics routing instance *<routing-instance name>*

Example: Configuring as a DHCP Client in Chassis Cluster Mode

IN THIS SECTION

- Requirements | **246**
- Overview | **247**
- Configuration | **247**
- Verification | **253**

This example shows how to configure the device as a DHCP client in chassis cluster mode.

Requirements

This example uses the following hardware and software components:

- Two SRX Series devices as DHCP client
- One SRX Series device as DHCP server
- Junos OS Release 12.1X47-D10 or later for SRX Series Services Gateways

Before you begin:

- Determine the IP address pools and the lease durations to use for each subnet.
- Obtain the MAC addresses of the clients that require permanent IP addresses. Determine the IP addresses to use for these clients.
- List the IP addresses that are available for the servers and devices on your network; for example, DNS, NetBIOS servers, boot servers, and gateway devices.

- Determine the DHCP options required by the subnets and clients in your network.

Overview

In this example, you configure two SRX Series devices as DHCP clients and a third SRX Series device as a DHCP server. Configure the two DHCP clients in chassis cluster mode.

For DHCP clients, you specify the interface as reth1, set the logical unit as 0, and create a DHCP inet family. You then specify the DHCP client identifier as 00:0a:12:00:12:12 in hexadecimal. You use hexadecimal if the client identifier is a MAC address. You set the options no-hostname if you do not want the DHCP client to send the hostname with the packets. You set the DHCP lease time as 86,400 seconds. The range is from 60 through 2,147,483,647 seconds. You set the number of retransmission attempts to 6. The range is from 0 through 6, and the default is 4. You set the retransmission interval to 5 seconds. The range is from 4 through 64, and the default is 4 seconds. Finally, you set the IPv4 address of the preferred DHCP server to 203.0.113.1 and the vendor class ID to ether.

For the DHCP server, configure the SRX Series device as a DHCP local server with minimum DHCP local server configurations. You specify the server group as g1 and enable the DHCP local server on interface ge-0/0/2.0.

Configuration

IN THIS SECTION

- Procedure | 247

Procedure

CLI Quick Configuration

To quickly configure this example, copy the following commands, paste them into a text file, remove any line breaks, change any details necessary to match your network configuration, copy and paste the commands into the CLI at the `[edit]` hierarchy level, and then enter `commit` from configuration mode.

Configure DHCP Client 1 and Client 2:

```
set interfaces reth1 unit 0 family inet dhcp-client
set interfaces reth1 unit 0 family inet dhcp-client client-identifier user-id ascii
00:0a:12:00:12:12
set interfaces reth1 unit 0 family inet dhcp-client options no-hostname
set interfaces reth1 unit 0 family inet dhcp-client lease-time 86400
```

```
set interfaces reth1 unit 0 family inet dhcp-client retransmission-attempt 6
set interfaces reth1 unit 0 family inet dhcp-client retransmission-interval 5
set interfaces reth1 unit 0 family inet dhcp-client server-address 203.0.113.1
set interfaces reth1 unit 0 family inet dhcp-client vendor-id ether
```

Configure chassis cluster on Client 1 and Client 2:

```
set chassis cluster reth-count 2
set chassis cluster control-link-recovery
set chassis cluster heartbeat-interval 1000
set chassis cluster redundancy-group 1 node 0 priority 100
set chassis cluster redundancy-group 1 node 1 priority 1
set chassis cluster redundancy-group 0 node 0 priority 100
set chassis cluster redundancy-group 0 node 1 priority 1
set interfaces ge-0/0/1 gigether-options redundant-parent reth1
set interfaces ge-4/0/1 gigether-options redundant-parent reth1
set interfaces reth1 redundant-ether-options redundancy-group 1
```

Configure the DHCP server:

```
set system service dhcp-local-server group g1 interface ge-0/0/2.0
set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
set access address-assignment pool p1 family inet network 203.0.113.0/24
set access address-assignment pool p1 family inet range r1 low 203.0.113.5
set access address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Step-by-Step Procedure

The following example requires you to navigate various levels in the configuration hierarchy. For instructions on how to do that, see *Using the CLI Editor in Configuration Mode* in the CLI User Guide.

To configure the devices as DHCP clients:

1. Specify the DHCP client interface.

```
[edit]
user@host# edit interfaces reth1 unit 0 family inet dhcp-client
```

2. Configure the DHCP client identifier as a hexadecimal value.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set client-identifier user-id ascii 00:0a:12:00:12:12
```

3. Set the hostname if you do not want the DHCP client to send hostname in the packets (RFC option code 12).

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set options no-hostname
```

4. Set the DHCP lease time.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set lease-time 86400
```

5. Set the number of attempts allowed to retransmit a DHCP packet.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-attempt 6
```

6. Set the interval (in seconds) allowed between retransmission attempts. The range is 4 through 64. The default is 4 seconds.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set retransmission-interval 5
```

7. Set the IPv4 address of the preferred DHCP server.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set server-address 203.0.113.1
```

8. Set the vendor class ID for the DHCP client.

```
[edit interfaces reth1 unit 0 family inet dhcp-client]
user@host# set vendor-id ether
```

Step-by-Step Procedure

To configure the DHCP clients in chassis cluster mode:

1. Specify the number of redundant Ethernet interfaces for the chassis cluster.

```
{primary:node0}[edit]
user@host# set chassis cluster reth-count 2
```

2. Enable control link recovery.

```
{primary:node0}[edit]
user@host# set chassis cluster control-link-recovery
```

3. Configure heartbeat settings.

```
{primary:node0}[edit]
user@host# set chassis cluster heartbeat-interval 1000
```

4. Configure the redundancy groups.

```
{primary:node0}[edit]
user@host# set chassis cluster redundancy-group 1 node 0 priority 100
user@host# set chassis cluster redundancy-group 1 node 1 priority 1
user@host# set chassis cluster redundancy-group 0 node 0 priority 100
user@host# set chassis cluster redundancy-group 0 node 1 priority 1
```

5. Configure redundant Ethernet interfaces.

```
{primary:node0}[edit]
user@host# set interfaces ge-0/0/1 gigether-options redundant-parent reth1
user@host# set interfaces reth1 redundant-ether-options redundancy-group 1
```

Step-by-Step Procedure

To configure the device as DHCP server:

1. Configure the DHCP local server.

```
[edit system services]
user@host# set dhcp-local-server group g1 interface ge-0/0/2.0
```

2. Configure IP address of the server.

```
[edit interfaces]
user@host# set interfaces ge-0/0/2 unit 0 family inet address 203.0.113.1/24
```

3. Configure an address pool.

```
[edit access]
user@host# set address-assignment pool p1 family inet network 203.0.113.0/24
user@host# set address-assignment pool p1 family inet range r1 low 203.0.113.5
user@host# set address-assignment pool p1 family inet range r1 high 203.0.113.20
```

Results

From configuration mode, confirm your configuration by entering the `show` commands. If the output does not display the intended configuration, repeat the configuration instructions in this example to correct it.

```
[edit]
user@host# show interfaces reth1 unit 0 family inet
dhcp-client {
    client-identifier user-id ascii 00:0a:12:00:12:12;
    options no-hostname;
```

```
    lease-time 86400;
    retransmission-attempt 6;
    retransmission-interval 5;
    server-address 203.0.113.1;
    vendor-id ether;
}
```

```
[edit]
user@host# show chassis cluster
control-link-recovery;
reth-count 2;
heartbeat-interval 1000;
redundancy-group 0 {
    node 0 priority 100;
    node 1 priority 1;
}
redundancy-group 1{
    node 0 priority 100;
    node 1 priority 1;
}
```

```
[edit]
user@host# show interfaces reth1
redundant-ether-options {

    redundancy-group 1;
}
```

```
[edit]
user@host# show access address-assignment
pool p1 {
    family inet {
        network 203.0.113.0/24;
        range r1 {
            low 203.0.113.5;
            high 203.0.113.20;
        }
```

```
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Verification

IN THIS SECTION

- Verifying the DHCP Client in Chassis Cluster Mode | 253

Verifying the DHCP Client in Chassis Cluster Mode

Purpose

Verify that the DHCP client is working in chassis cluster mode.

Action

From operational mode, enter the `show dhcp client binding`, `show dhcp client statistics` and `show dhcp client binding interface reth1 detail` commands.

```
user@host> show dhcp client binding
```

```
IP address     Hardware address   Expires     State      Interface
 203.0.113.14      00:1f:12:e3:34:01  84587       BOUND      reth1.0
```

```
user@host> show dhcp client statistics
```

```
Packets dropped:
    Total                     4
    Send error                4

Messages received:
    BOOTREPLY                 3
```

```
    DHCPOFFER                   1
    DHCPACK                     2
    DHCPNAK                     0
    DHCPFORCERENEW              0

Messages sent:
    BOOTREQUEST                 0
    DHCPDECLINE                 0
    DHCPDISCOVER                5
    DHCPREQUEST                 8
    DHCPINFORM                  0
    DHCPRELEASE                 1
    DHCPRENEW                   0
    DHCPREBIND                  0
```

```
user@host> show dhcp client binding interface reth1 detail
```

```
Client Interface: reth1.0
     Hardware Address:             00:10:db:ff:10:01
     State:                        BOUND(LOCAL_CLIENT_STATE_BOUND)
     Lease Expires:                2013-12-18 10:15:36 CST
     Lease Expires in:             30 seconds
     Lease Start:                  2013-12-17 10:15:36 CST
     Server Identifier:            203.0.113.1
     Client IP Address:            10.1.1.14
     Update Server                 No

DHCP options:
    Name: dhcp-lease-time, Value: 1 day
    Name: server-identifier, Value: 10.1.1.1
    Name: subnet-mask, Value: 255.255.255.0
```

Meaning

The sample output shows that DHCP clients configured in the example work in a chassis cluster.

Release History Table

Release	Description
17.3R1	Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option dhcp-client at [edit interfaces interface-name unit logical-unit-number family inet] hierarchy is changed to dhcp to align with other Junos platforms.
15.1X49-D60	Starting with Junos OS Release 15.1X49-D60 and Junos OS Release 17.3R1, the legacy DHCPD (DHCP daemon) configuration on all SRX Series devices is being deprecated and only the new JDHCP CLI is supported.

RELATED DOCUMENTATION

- DHCP Server | 49
- DHCP Relay Agent | 156
- Suppressing DHCP Routes | 353
- DHCP Overview | 2
- DHCP Access Service Overview | 9
- Legacy DHCP and Extended DHCP | 16

DHCPv6 Client

IN THIS SECTION

- DHCPv6 Client Overview | 256
- Understanding DHCPv6 Client and Server Identification | 257
- Minimum DHCPv6 Client Configuration on SRX Series Devices | 258
- Configuring DHCP Client-Specific Attributes | 259
- DHCPv6 Client Configuration Options | 260
- Configuring the DHCPv6 Client Rapid Commit Option | 262
- Configuring a DHCPv6 Client in Autoconfig Mode | 263
- Configuring TCP/IP Propagation on a DHCPv6 Client | 264

SRX Series device can act as a DHCPv6 client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. To enable a device to operate as a DHCPv6 client, you must configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. For more information, read this topic.

DHCPv6 Client Overview

A Juniper Networks device can act as a Dynamic Host Configuration Protocol version 6 (DHCPv6) client, receiving its TCP/IP settings and the IPv6 address for any physical interface in any security zone from an external DHCPv6 server. When the device operates as a DHCPv6 client and a DHCPv6 server simultaneously, it can transfer the TCP/IP settings learned through its DHCPv6 client module to its default DHCPv6 server module. For the device to operate as a DHCPv6 client, you configure a *logical interface* on the device to obtain an IPv6 address from the DHCPv6 server in the network.

DHCPv6 client support for Juniper Networks devices includes the following features:

- Identity association for nontemporary addresses (IA_NA)
- Identity association for prefix delegation (IA_PD)
- Rapid commit
- TCP/IP propagation
- Auto-prefix delegation
- Autoconfig mode (stateful and stateless)

To configure the DHCPv6 client on the device, include the `dhcpv6-client` statement at the [`edit interfaces`] hierarchy level.

NOTE: To configure a DHCPv6 client in a routing instance, add the interface in a routing instance using the [`edit routing-instances`] hierarchy.

NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Understanding DHCPv6 Client and Server Identification

Each DHCPv6 client and server is identified by a DHCP unique identifier (DUID). The DUID is unique across all DHCPv6 clients and servers, and it is stable for any specific client or server. DHCPv6 clients use DUIDs to identify a server in messages where a server needs to be identified. DHCPv6 servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

The DUID is a 2-octet type code represented in network byte order, followed by a variable number of octets that make up the actual identifier; for example, 00:02:00:01:02:03:04:05:07:a0. A DUID can be up to 128 octets in length (excluding the type code). The following types are currently defined for the DUID parameter:

- Type 1—Link Layer address plus time (duid-llt)
- Type 2—Vendor-assigned unique ID based on enterprise number (vendor)
- Type 3—Link Llayer address (duid-ll)

The duid-llt DUID consists of a 2-octet type field that contains the value 1, a 2-octet hardware type code, 4 octets that signify a time value, followed by the Link Layer address of any one network interface that is connected to the DHCP device at the time that the DUID is generated.

The vendor DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the identity association for nontemporary addresses (IA_NA) assignment, followed by a unique identifier assigned by the vendor.

The duid-ll DUID contains a 2-octet type field that stores the value 3, and a 2-octet network hardware type code, followed by the Link Layer address of any one network interface that is permanently connected to the client or server device.

SEE ALSO

> *DHCPv6 Client Overview*

Minimum DHCPv6 Client Configuration on SRX Series Devices

This topic describes the minimum configuration you must use to configure an SRX300, SRX320, SRX340, SRX345, SRX550M, or SRX1500 device as a DHCPv6 client.

To configure the device as a DHCPv6 client:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the DHCPv6 client type. The client type can be autoconfig or statefull.

   - To enable DHCPv6 auto configuration mode, configure the client type as `autoconfig`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

   - For stateful address assignment, configure the client type as `statefull`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type statefull
```

3. Specify the identity association type.

- To configure identity association for nontemporary address (IA_NA) assignment, specify the `client-ia type` as `ia-na`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

- To configure identity association for prefix delegation (IA_PD), specify the `client-ia-type` as `ia-pd`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-pd
```

4. Configure the DHCPv6 client identifier by specifying the DHCP unique identifier (DUID) type. The following DUID types are supported:

   - Link Layer address (duid-ll)
   - Link Layer address plus time (duid-llt)
   - Vendor-assigned unique ID based on enterprise number (vendor)

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-identifier duid-type duid-ll
```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [`edit routing-instances`] hierarchy.

Configuring DHCP Client-Specific Attributes

You use the address-assignment pool feature to include application-specific attributes when clients obtain an address. A client application, such as DHCPv6, uses the attributes to determine how addresses are assigned and to provide optional application-specific characteristics to the client. For example, the DHCPv6 application might specify that a client that matches certain prerequisite information is dynamically assigned an address from a particular named range. Based on which named range is used, DHCPv6 specifies additional DHCPv6 attributes such as the DNS server or the maximum lease time for clients.

You use the `dhcp-attributes` statement to configure DHCPv6 client-specific attributes for address-assignment pools at the `[edit access address-assignment pool` *`pool-name`* `family inet6] hierarchy`.

Table 13 on page 260 describes the DHCPv6 client attributes for configuring IPv6 address-assignment pools.

Table 13: DHCPv6 Attributes

Attribute	Description	DHCPv6 Option
`dns-server`	IPv6 address of DNS server to which clients can send DNS queries	23
`grace-period`	Grace period offered with the lease	–
`maximum-lease-time`	Maximum lease time allowed by the DHCPv6 server	–
`option`	User-defined options	–
`sip-server-address`	IPv6 address of SIP outbound proxy server	22
`sip-server-domain-name`	Domain name of the SIP outbound proxy server	21

DHCPv6 Client Configuration Options

To enable a device to operate as a DHCPv6 client, you configure a logical interface on the device to obtain an IPv6 address from the DHCPv6 local server in the network. You can then specify the retransmission attempts, client requested configuration options, interface used to delegate prefixes, rapid commit, and update server options.

To configure optional DHCPv6 client attributes:

1. Specify one of the following DHCPv6 client requested configuration options:
   - dns-server
   - domain
   - ntp-server

- sip-domain
- sip-server

For example, to specify the DHCPv6 client requested option as `dns-server`:

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set req-option dns-server
```

2. Set the number of attempts allowed to retransmit a DHCPv6 client protocol packet.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set retransmission-attempt 6
```

3. Configure the `update-server` option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

4. Specify the interface used to delegate prefixes.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-router-advertisement interface ge-0/0/0
```

5. Configure the two-message (rapid commit) exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```

NOTE: To configure a DHCPv6 client in a routing instance, add the interface to a routing instance using the [`edit routing-instances`] hierarchy.

NOTE: On all SRX Series devices, DHCPv6 client authentication is not supported.

NOTE: On SRX300, SRX320, SRX340, and SRX345, and SRX550M devices, DHCPv6 client does not support:

- Temporary addresses
- Reconfigure messages
- Multiple identity association for nontemporary addresses (IA_NA)
- Multiple prefixes in a single identity association for prefix delegation (IA_PD)
- Multiple prefixes in a single router advertisement

Configuring the DHCPv6 Client Rapid Commit Option

The DHCPv6 client can obtain configuration parameters from a DHCPv6 server through a rapid two-message exchange (solicit and reply). When the rapid commit option is enabled by both the DHCPv6 client and the DHCPv6 server, the two-message exchange is used, rather than the default four-method exchange (solicit, advertise, request, and reply). The two-message exchange provides faster client configuration and is beneficial in environments in which networks are under a heavy load.

To configure the DHCPv6 client to support the DHCPv6 rapid commit option on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Specify the DHCPv6 client interface.

```
[edit]
user@host# set interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client
```

2. Configure the two-message exchange option for address assignment.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set rapid-commit
```

Configuring a DHCPv6 Client in Autoconfig Mode

A DHCPv6 client configured in autoconfig mode acts as a stateful client, a stateless client (DHCPv6 server is required for TCP/IP configuration), and stateless–no DHCP client, based on the managed (M) and other configuration (O) bits in the received router advertisement messages.

If the managed bit is 1 and the other configuration bit is 0, the DHCPv6 client acts as a stateful client. In stateful mode, the client receives IPv6 addresses from the DHCPv6 server, based on the identity association for nontemporary addresses (IA_NA) assignment.

If the managed bit is 0 and the other configuration bit is 1, the DHCPv6 client acts as a stateless client. In stateless mode, the addresses are automatically configured, based on the prefixes in the router advertisement messages received from the router. The stateless client receives configuration parameters from the DHCPv6 server.

If the managed bit is 0 and the other configuration bit is also 0, the DHCPv6 client acts as a stateless–no DHCP client. In the stateless–no DHCP mode, the client receives IPv6 addresses from the router advertisement messages.

To configure DHCPv6 client in autoconfig mode on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices:

1. Configure the DHCPv6 client type as `autoconfig`.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-type autoconfig
```

2. Specify the identity association type as `ia-na` for nontemporary addresses.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set client-ia-type ia-na
```

3. Specify the interface on which to configure router advertisement.

```
[edit protocols router-advertisement]
user@host# set interface ge-0/0/0
```

Configuring TCP/IP Propagation on a DHCPv6 Client

You can enable or disable the propagation of TCP/IP settings received on the device acting as a DHCPv6 client. The settings can be propagated to the server pool running on the device. This topic describes how to configure TCP/IP settings on a DHCPv6 client, where both the DHCPv6 client and DHCPv6 server are on the same device.

NOTE: This feature is supported on SRX300, SRX320, SRX340, SRX550M, and SRX1500 devices.

To configure TCP/IP setting propagation on a DHCPv6 client:

1. Configure the `update-server` option on the DHCPv6 client.

```
[edit interfaces ge-0/0/0 unit 0 family inet6 dhcpv6-client]
user@host# set update-server
```

2. Configure the address pool to specify the interface (where `update-server` is configured) from which TCP/IP settings can be propagated.

```
[edit access]
user@host# set address-assignment pool 2 family inet6 dhcp-attributes propagate-settings
ge-0/0/0
```

RELATED DOCUMENTATION

DHCP Client | 234

DHCPv6 Client | 255

Understanding DHCPv6 Client and Server Identification | 257

CHAPTER 6

DHCP with External Authentication Server

DHCP with External Authentication Server | 266

Centrally Configure DHCP Options on a RADIUS Server | 277

DHCP with External Authentication Server

IN THIS SECTION

- Using External AAA Authentication Services to Authenticate DHCP Clients | 266
- Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client | 268
- Example-Configuring DHCP with External Authentication Server | 269
- Specifying Authentication Support | 270
- Creating Unique Usernames for DHCP Clients | 271
- Grouping Interfaces with Common DHCP Configurations | 274

Extended DHCP local server and the extended DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. For more information, read this topic.

This topic uses the term extended DHCP application to refer to both the extended DHCP local server and the extended DHCP relay agent.

Using External AAA Authentication Services to Authenticate DHCP Clients

IN THIS SECTION

- Steps to Configure DHCP with External Authentication Server | 267

The authentication, authorization, and accounting (AAA) Service Framework provides a single point of contact for all the authentication, authorization, accounting, address assignment, and dynamic request services that the router supports for network access.

In extended DHCP applications, both DHCP server and the DHCP relay agent support the use of external AAA authentication services, such as RADIUS, to authenticate DHCP clients. The support id available for DHCPv6 local server and DHCPv6 relay agent.

Junos OS devices use the AAA infrastructure for authenticating (the DHCP client for DHCP service with the assigned DHCP server. The following high-level steps are involved in DHCP client authentication:

- DHCP local server or relay agent receives a discover PDU from a client
- DHCP service contacts the AAA server to authenticate the DHCP client.
- DHCP service can obtain client addresses and DHCP configuration options from the external AAA authentication server.

The external authentication feature also supports AAA directed logout. If the external AAA service supports a user logout directive, the extended DHCP application honors the logout and views it as if it was requested by a CLI management command.

All of the client state information and allocated resources are deleted at logout. The extended DHCP application supports directed logout using the list of configured authentication servers you specify with the `authentication-server` statement at the `[edit access profile` *`profile-name`*`]` hierarchy level.

Steps to Configure DHCP with External Authentication Server

To configure DHCP local server and DHCP relay agent for authentication support:

1. Specify that you want to configure authentication by including authentication keyword at respective hierarchy levels.
2. (Optional) Configure optional features to create a unique username.
3. (Optional) Configure a password that authenticates the username to the external authentication service.

Example:

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        delimiter delimiter-character;
        domain-name domain-name-string;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
```

```
        user-prefix user-prefix-string;
    }
}
```

Client Configuration Information Exchanged Between the External Authentication Server, DHCP Application, and DHCP Client

When the DHCP application receives a response from an external authentication server, the response might include information in addition to the IP address and subnet mask. The DHCP service uses the information and sends it to the DHCP client.

The DHCP application can either send the information in its original form or the application might merge the information with local configuration specifications.

For example, if the authentication response includes an address pool name and a local configuration specifies DHCP attributes for that pool, the DHCP service merges the authentication results and the attributes in the reply that the server sends to the client.

A local configuration is optional—a client can be fully configured by the external authentication service. However, if the external authentication service does not provide client configuration, you must configure the local address assignment pool to provide the configuration for the client.

When a local configuration specifies options, the extended DHCP application adds the local configuration options to the offer PDU the server sends to the client. If the two sets of options overlap, the options in the authentication response from the external service take precedence.

When you use RADIUS to provide the authentication, the additional information might be in the form of RADIUS attributes and Juniper Networks VSAs. Table 14 on page 268 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 14: Information in Authentication Grant

Attribute Number	Attribute Name	Description
RADIUS attribute 8	Framed-IP-Address	Client IP address

Table 14: Information in Authentication Grant *(Continued)*

Attribute Number	Attribute Name	Description
RADIUS attribute 9	Framed-IP-Netmask	Subnet mask for client IP address (DHCP option 1)
Juniper Networks VSA 26-4	Primary-DNS	Primary domain server (DHCP option 6)
Juniper Networks VSA 26-5	Secondary-DNS	Secondary domain server (DHCP option 6)
Juniper Networks VSA 26-6	Primary-WINS	Primary WINS server (DHCP option 44)
Juniper Networks VSA 26-7	Secondary-WINS	Secondary WINS server (DHCP option 44)
RADIUS attribute 27	Session-Timeout	Lease time
RADIUS attribute 88	Framed-Pool	Address assignment pool name
Juniper Networks VSA 26-109	DHCP-Guided-Relay-Server	DHCP relay server

Example-Configuring DHCP with External Authentication Server

To configure authentication at DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent levels.

1. Specify that you want to configure authentication.

```
[edit system services dhcp-local-server]
user@host# edit authentication
```

2. (Optional) Specify the optional information you want to include in the username.

```
[edit system services dhcp-local-server authentication username-include]
user@host# set username-include circuit-type
user@host# set username-include domain-name example.com
user@host# set username-include mac-address
user@host# set username-include user-prefix wallybrown
```

3. Configure an optional password that the extended DHCP application presents to the external AAA authentication service to authenticate the specified username.

```
[edit system services dhcp-local-server authentication]
user@host# set password $ABC123
```

The following example shows a sample configuration that creates a unique username. The username is shown after the configuration.

```
authentication {
    username-include {
        circuit-type;
        domain-name example.com;
        mac-address 2001:db8::/32;
        user-prefix wallybrown;
    }
}
```

The resulting unique username is:

```
wallybrown.2001:db8::/32.enet@example.com
```

Specifying Authentication Support

Include the `authentication` statement at hierarchy levels given in Table 15 on page 271. You can configure either global authentication support or group-specific support.

Table 15: Supported Hierarchy Levels for Authentication Support

Supported Hierarchy Level	Hierarchy Level
DHCP local server	`[edit system services dhcp-local-server]`
DHCP relay agent	`[edit forwarding-options dhcp-relay]`
DHCPv6 local server	`[edit system services dhcp-local-server dhcpv6]`
DHCPv6 relay agent	`[edit forwarding-options dhcp-relay dhcpv6]`

Creating Unique Usernames for DHCP Clients

You can configure the extended DHCP application to include additional information in the username that is passed to the external AAA authentication service when the DHCP client logs in. This additional information enables you to construct usernames that uniquely identify subscribers (DHCP clients).

To configure unique usernames, use the `username-include` statement. You can include any or all of the additional statements.

```
authentication {
    username-include {
        circuit-type;
        client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        routing-instance-name;
        user-prefix user-prefix-string;
```

```
    }
}
```

NOTE: If you do not include a username in the authentication configuration, the router (or switch) does not perform authentication; however, the IP address is provided by the local pool if it is configured.

When you use the DHCPv6 local server, you must configure authentication and the client username; otherwise client login fails.

The following list describes the optional information that you can include as part of the username:

- `circuit-type`—The circuit type used by the DHCP client, for example `enet`.
- `client-id`—The client identifier option (option 1). (DHCPv6 local server DHCPv6 relay agent only)
- `delimiter`—The delimiter character that separates components that make up the concatenated username. The default delimiter is a period (.). The semicolon (;) is not supported as a delimiter character.
- `domain-name`—The client domain name as a string. The router adds the @ delimiter to the username.
- `interface-description`—The description of the device (physical) interface or the logical interface.
- `interface-name`—The interface name, including the interface device and associated VLAN IDs.
- `logical-system-name`—The name of the logical system, if the receiving interface is in a logical system.
- `mac-address`—The client MAC address, in a string of the format *xxxx*.*xxxx*.*xxxx*.
- `option-60`—The portion of the option 60 payload that follows the length field. (Not supported for DHCPv6 local server)
- `option-82 <circuit-id> <remote-id>`—The specified contents of the option 82 payload. (Not supported for DHCPv6 local server)
  - `circuit-id`—The payload of the Agent Circuit ID suboption.
  - `remote-id`—The payload of the Agent Remote ID suboption.
  - Both `circuit-id` and `remote-id`—The payloads of both suboptions, in the format: `circuit-id[delimiter]remote-id`.
  - Neither `circuit-id` or `remote-id`—The raw payload of the option 82 from the PDU is concatenated to the username.

NOTE: For DHCP relay agent, the option 82 value used in creating the username is based on the option 82 value that is encoded in the outgoing (relayed) PDU.

- `relay-agent-interface-id`—The Interface-ID option (option 18). (DHCPv6 local server or DHCPv6 relay agent only)
- `relay-agent-remote-id`—The DHCPv6 Relay Agent Remote-ID option (option 37). (DHCPv6 local server or DHCPv6 relay agent only)
- `relay-agent-subscriber-id`—(On routers only) The DHCPv6 Relay Agent Subscriber-ID option (option 38). (DHCPv6 local server or DHCPv6 relay agent only)
- `routing-instance-name`—The name of the routing instance, if the receiving interface is in a routing instance.
- `user-prefix`—A string indicating the user prefix.
- `vlan-tags`—The subscriber VLAN tags. Includes the outer VLAN tag and, if present, the inner VLAN tag. You can use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

The router (switch) creates the unique username by including the specified additional information in the following order, with the fields separated by a delimiter.

For DHCP local server and DHCP relay agent:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]routing-instance-
name[delimiter]circuit-type[delimiter]interface-
name[delimiter]option-82[delimiter]option-60@domain-name
```

For DHCPv6 local server:

```
user-prefix[delimiter]mac-address[delimiter]logical-system-name[delimiter]routing-instance-
name[delimiter]circuit-type[delimiter]interface-name[delimiter]relay-agent-remote-
id[delimiter]relay-agent-subscriber-id[delimiter]relay-agent-interface-id[delimiter]client-
id@domain-name
```

Grouping Interfaces with Common DHCP Configurations

You use the group feature to group a set of interfaces and then apply a common DHCP configuration to the named interface group. The extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent all support interface groups.

The following steps create a DHCP local server group; the steps are similar for the DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent.

To configure a DHCP local server interface group:

1. Specify that you want to configure DHCP local server.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Create the group and assign a name.

```
[edit system services dhcp-local-server]
user@host# edit group boston
```

3. Specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the *interface interface-name* statement to specify multiple interfaces within the group, but you cannot use the same interface in more than one group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1
user@host# set interface fe-1/0/1.2
```

4. (Optional) You can use the `upto` option to specify a range of interfaces for a group.

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

5. (Optional) You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
[edit system services dhcp-local-server group boston]
user@host# set interface fe-1/0/1.1 upto fe-1/0/1.102
user@host# set interface fe-1/0/1.6 exclude
user@host# set interface fe-1/0/1.70 upto fe-1/0/1.80 exclude
```

Example- 2

To configure an interface group, use the `group` statement.

You can specify the names of one or more interfaces on which the extended DHCP application is enabled. You can repeat the `interface` *`interface-name`* statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group. For example:

1. The extended DHCP applications enable you to group together a set of interfaces and apply a common DHCP configuration to the named interface group.

```
group boston {
    interface 192.168.10.1;
    interface 192.168.15.5;
}
```

2. You can use the *upto* option to specify a range of interfaces on which the extended DHCP application is enabled. For example:

```
group quebec {
    interface 192.168.10.1 upto 192.168.10.255;
}
```

3.

You can use the `exclude` option to exclude a specific interface or a specified range of interfaces from the group. For example:

```
group paris {
    interface 192.168.100.1 exclude;
    interface 192.168.100.100 upto 192.168.100.125 exclude;
}
```

Example:

```
group group-name {
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
        }
    }
    interface interface-name <upto upto-interface-name> <exclude>;
}
```

RELATED DOCUMENTATION

Centrally Configure DHCP Options on a RADIUS Server | 277

IP Address Assignment Pool | 27

Centrally Configure DHCP Options on a RADIUS Server

IN THIS SECTION

- RADIUS-Sourced Options | 277
- Client-Sourced Options Configuration | 278
- Data Flow for RADIUS-Sourced DHCP Options | 279
- Multiple VSA 26-55 Instances Configuration | 280
- DHCP Options That Cannot Be Centrally Configured | 281

DHCP management on Junos OS devices support central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options) and traditional client-sourced options configuration. Read the following sections for information on central configuration of DHCP options on the RADIUS server.

RADIUS-Sourced Options

Subscriber management (on the routers) or DHCP management (on the switches) enables you to centrally configure DHCP options on a RADIUS server and then distribute the options on a per-subscriber or per DHCP-client basis. This method results in RADIUS-sourced DHCP options—the DHCP options originate at the RADIUS server and are sent to the subscriber (or DHCP client). This differs from the traditional client-sourced method (also called DHCP-sourced) of configuring DHCP options, in which the options originate at the client and are sent to the RADIUS server. The subscriber management (DHCP management) RADIUS-sourced DHCP options are also considered to be *opaque*, because DHCP local server performs minimal processing and error checking for the DHCP options string before passing the options to the subscriber (DHCP client).

Subscriber management (or DHCP management) uses Juniper Networks VSA 26-55 (DHCP-Options) to distribute the RADIUS-sourced DHCP options. The RADIUS server includes VSA 26-55 in the Access-Accept message that the server returns during subscriber authentication or DHCP client authentication. The RADIUS server sends the Access-Accept message to the RADIUS client, and then on to DHCP local server for return to the DHCP subscriber. The RADIUS server can include multiple instances of VSA 26-55 in a single Access-Accept message. The RADIUS client concatenates the multiple instances and uses the result as a single instance.

There is no CLI configuration required to enable subscriber management (DHCP management) to use the centrally configured DHCP options—the procedure is triggered by the presence of VSA 26-55 in the RADIUS Access-Accept message.

When building the offer packet for the DHCP client, DHCP local server uses the following sequence:

1. Processes any RADIUS-configured parameters that are passed as separate RADIUS attributes; for example, RADIUS attribute 27 (Session Timeout).
2. Processes any client-sourced parameters; for example, RADIUS attributes 53 (DHCP Message Type) and 54 (Server Identifier).
3. Appends (without performing any processing) the opaque DHCP options string contained in the VSA 26-55 received from the RADIUS server.

Client-Sourced Options Configuration

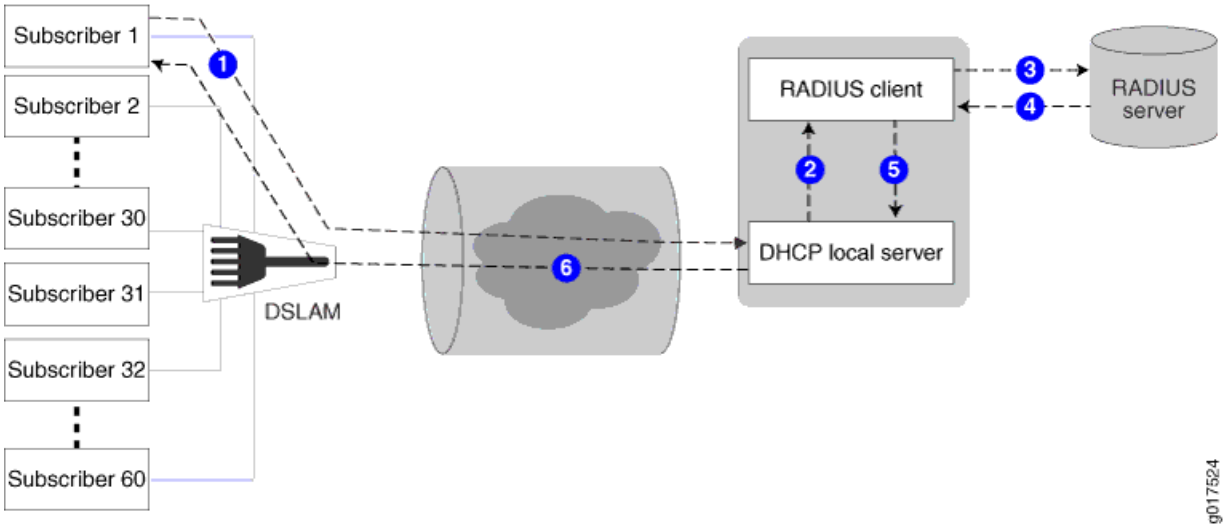
In addition to supporting central configuration of DHCP options directly on the RADIUS server (RADIUS-sourced options), subscriber management (DHCP management) also supports the traditional client-sourced options configuration, in which the router's (switch's) DHCP component sends the options to the RADIUS server. The client-sourced DHCP options method is supported for both DHCP local server and DHCP relay agent; however, the RADIUS-sourced central configuration method is supported on DHCP local server only. Both the RADIUS-sourced and client-sourced methods support DHCPv4 and DHCPv6 subscribers (clients).

NOTE: You can use the RADIUS-sourced and client-sourced methods simultaneously on DHCP local server. However, you must ensure that the central configuration method does not include options that override client-sourced DHCP options, because this can create unpredictable results.

Data Flow for RADIUS-Sourced DHCP Options

Figure 14 on page 279 shows the procedure subscriber management (DHCP management) uses when configuring DHCP options for subscribers (DHCP clients).

Figure 14: DHCP Options Data Flow



The following general sequence describes the data flow when subscriber management (DHCP management) uses RADIUS-sourced DHCP options and VSA 26-55 to configure a DHCP subscriber (client):

1. The subscriber (DHCP client) sends a DHCP discover message (or DHCPv6 solicit message) to the DHCP local server. The message includes client-sourced DHCP options.
2. The DHCP local server initiates authentication with the Junos OS RADIUS client.
3. The RADIUS client sends an Access-Request message on behalf of the subscriber (DHCP client) to the external RADIUS server. The message includes the subscriber's (DHCP client's) client-sourced DHCP options.
4. The external RADIUS server responds by sending an Access-Accept message to the RADIUS client. The Access-Accept message includes the RADIUS-sourced opaque DHCP options in VSA 26-55.
5. The RADIUS client sends the DHCP options string to DHCP local server. If there are multiple VSA 26-55 instances, the RADIUS client first assembles them into a single options string.
6. DHCP local server processes all options into the DHCP offer (or DHCPv6 reply) message, except for the RADIUS-sourced VSA 26-55 DHCP options. After processing all other options, DHCP local

server then appends the unmodified VSA 26-55 DHCP options to the message and sends the message to the subscriber (DHCP client).

7. The subscriber (DHCP client) is configured with the DHCP options.
8. The following operations occur after the subscriber (DHCP client) receives the DHCP options:
   - Accounting—The RADIUS client sends Acct-Start and Interim-Accounting requests to the RADIUS server, including the RADIUS-sourced DHCP options in VSA 26-55. By default, the DHCP options are included in accounting requests.
   - Renewal—When the subscriber (DHCP client) renews, the cached DHCP options value is returned in the DHCP renew (or DHCPv6 ACK) message. The originally assigned DHCP options cannot be modified during a renew cycle.
   - Logout—When the subscriber (DHCP client) logs out, the RADIUS client sends an Acct-Stop message to the RADIUS server, including the RADIUS-sourced VSA 26-55.

Multiple VSA 26-55 Instances Configuration

VSA 26-55 supports a maximum size of 247 bytes. If your RADIUS-sourced DHCP options field is greater than 247 bytes, you must break the field up and manually configure multiple instances of VSA 26-55 for the RADIUS server to return. When using multiple instances for an options field, you must place the instances in the packet in the order in which the fragments are to by reassembled by the RADIUS client. The fragments can be of any size of 247 bytes or less.

BEST PRACTICE: For ease of configuration and management of your DHCP options, you might want to have one DHCP option per VSA 26-55 instance, regardless of the size of the option field.

When the RADIUS client returns a reassembled opaque options field in an accounting request to the RADIUS server, the client uses 247-byte fragments. If you had originally created instances of fewer than 247 bytes, the returned fragments might not be the same as you originally configured on the RADIUS server.

NOTE: If you are configuring Steel-Belted Radius (SBR) to support multiple VSA 26-55 instances, ensure that you specify VSA 26-55 with the `RO` flags in the Subscriber Management RADIUS dictionary file. The `R` value indicates a multivalued reply attribute and the `O` value indicates an ordered attribute.

DHCP Options That Cannot Be Centrally Configured

Table 16 on page 281 shows the DHCP options that you must not centrally configure on the RADIUS server.

Table 16: Unsupported Opaque DHCP Options

DHCP Option	Option Name	Comments
Option 0	Pad Option	Not supported.
Option 51	IP Address Lease Time	Value is provided by RADIUS attribute 27 (Session-Timeout).
Option 52	Option Overload	Not supported.
Option 53	DHCP Message Type	Value is provided by DHCP local server.
Option 54	Server Identifier	Value is provided by DHCP local server.
Option 55	Parameter Request List	Value is provided by DHCP local server.
Option 255	End	Value is provided by DHCP local server.
–	DHCP magic cookie	Not supported.

RELATED DOCUMENTATION

- DHCP with External Authentication Server
- DHCP Overview
- IP Address Assignment Pool

CHAPTER 7

Managing DHCP Services

Group-Specific DHCP Configurations | 283

DHCP Snooping | 287

DHCP Auto Logout | 296

Additional Configurations for DHCP Clients | 300

Dynamic Reconfiguration of DHCP Servers and Clients | 305

DHCP Liveness Detection | 315

Secure DHCP Message Exchange | 343

DHCP Active Server Groups | 349

Suppressing DHCP Routes | 353

Group-Specific DHCP Configurations

IN THIS SECTION

- Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces | **283**
- Configuring Group-Specific DHCP Local Server Options | **285**
- Configuring Group-Specific DHCP Relay Options | **285**
- Configuring DHCP Server Configuration with Optional Pool Matching Using Groups | **286**

You use the group feature to group a set of interfaces and then apply a common DHCP configuration such as extended DHCP local server, DHCPv6 local server, DHCP relay agent, and DHCPv6 relay agent to the named interface group. For more information, read this topic.

Guidelines for Configuring Interface Ranges for Groups of DHCP Interfaces

This topic describes guidelines to consider when configuring interface ranges for named interface groups for DHCP local server and DHCP relay. The guidelines refer to the following *configuration statement*:

```
user@host# set interface  interface-name upto upto-interface-name
```

- The start subunit, `interface` *`interface-name`* , serves as the key for the stanza. The remaining configuration settings are considered attributes.
- If the subunit is not included, an implicit `.0` subunit is enforced. The implicit subunit is applied to all interfaces when autoconfiguration is enabled. For example, `interface ge-2/2/2` is treated as `interface ge-2/2/2.0`.
- Ranged entries contain the `upto` option, and the configuration applies to all interfaces within the specified range. The start of a ranged entry must be less than the end of the range. Discrete entries apply to a single interface, except in the case of autoconfiguration, in which a `0` (zero) subunit acts as a wildcard.

- Interface stanzas defined within the same router or switch context are dependent and can constrain each other—both DHCP local server and DHCP relay are considered. Interface stanzas defined across different router (switch) contexts are independent and do not constrain one another.
- Each interface stanza, whether discrete or ranged, has a unique start subunit across a given router context. For example, the following configuration is not allowed within the same group because `ge-1/0/0.10` is the start subunit for both.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.10
```

- Two groups cannot share interface space. For example, the following configuration is not allowed because the three stanzas share the same space and interfere with one another—interface `ge-1/0/0.26` is common to all three.

```
dhcp-relay group diamond interface ge-1/0/0.10 upto ge-1/0/0.30
dhcp-local-server group ruby interface ge-1/0/0.26
dhcp-relay group sapphire interface ge-1/0/0.25 upto ge-1/0/0.35
```

- Two ranges cannot overlap, either within a group or across groups. Overlapping occurs when two interface ranges share common subunit space but neither range is a proper subset of the other. The following ranges overlap:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.20 upto ge-1/0/0.40
```

- A range can contain multiple nested ranges. A nested range is a proper subset of another range. When ranges are nested, the smallest matching range applies.

  In the following example, the three ranges nest properly:

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.12 upto ge-1/0/0.15 exclude
interface ge-1/0/0.25 upto ge-1/0/0.29 exclude
```

- Discrete interfaces take precedence over ranges. In the following example, interface `ge-1/0/0.20` takes precedence and enforces an interface client limit of `5`.

```
interface ge-1/0/0.10 upto ge-1/0/0.30
interface ge-1/0/0.15 upto ge-1/0/0.25 exclude
interface ge-1/0/0.20 overrides interface-client-limit 5
```

Configuring Group-Specific DHCP Local Server Options

You can include the following statements at the `[edit system services dhcp-local-server group group-name]` hierarchy level to set group-specific DHCP local server configuration options. Statements configured at the `[edit system services dhcp-local-server group group-name]` hierarchy level apply only to the named group of interfaces, and override any global DHCP local server settings configured with the same statements at the `[edit system services dhcp-local-server]` hierarchy level.

DHCPv6 local server supports the same set of statements with the exception of the `dynamic-profile` statement.

- `authentication`—Configure the parameters the router sends to the external AAA server.
- `dynamic-profile`—Specify the dynamic profile that is attached to a group of interfaces.
- `interface`—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- `liveness-detection`—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see DHCP Liveness Detection Overview.
- `overrides`—Override the default configuration settings for the extended DHCP local server. For information, see *Overriding the Default DHCP Local Server Configuration Settings*.

Configuring Group-Specific DHCP Relay Options

You can include the following statements at the `[edit forwarding-options dhcp-relay group group-name]` hierarchy level to set group-specific DHCP relay agent configuration options. Group-specific statements apply only to the named group of interfaces, and override any global DHCP relay agent settings for the same statement.

Include the statements at the `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level to configure group-specific options for DHCPv6 relay agent.

- `active-server-group`—Configure an active server group to apply a common DHCP relay agent configuration for a named group of DHCP server addresses. For information, see *Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups*.
- `authentication`—Configure the parameters the router (or switch) sends to the external AAA server.
- `dynamic-profile`—Specify the dynamic profile that is attached to a group of interfaces.
- `interface`—Specify one or more interfaces, or a range of interfaces, that are within the specified group.
- `liveness-detection`—Configure bidirectional failure detection timers and authentication criteria for static routes, or Layer 2 liveness detection using ARP and Neighbor Discovery packets. For more information, see DHCP Liveness Detection Overview.
- `overrides`—Override the default configuration settings for the extended DHCP relay agent. For information, see *Overriding the Default DHCP Relay Configuration Settings*.
- `relay-agent-interface-id`—(DHCPv6 only) Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.
- `relay-agent-remote-id`—(DHCPv6 only) Insert the DHCPv6 Relay Agent Remote-ID option (option 37) in DHCPv6 packets destined for the DHCPv6 server.
- `relay-option`—Configure selective processing, which uses DHCP options in client packets to identify and filter client traffic, and to specify the action DHCP relay agent takes with the traffic. For more information, see *Using DHCP Option Information to Selectively Process DHCP Client Traffic*.
- `relay-option-82`—(DHCPv4 only) Enable or disable the insertion of option 82 information in packets destined for a DHCP server. For information, see *Using DHCP Relay Agent Option 82 Information*.
- `service-profile`—Specify the default subscriber service, (or default profile) which is activated when the subscriber (or DHCP client) logs in and no other service is activated by a RADIUS server or a provisioning server. For more information, see *Default Subscriber Service Overview* .

Configuring DHCP Server Configuration with Optional Pool Matching Using Groups

The following example shows an extended DHCP local server configuration that includes optional pool matching and interface groups. This configuration specifies that the DHCP local server uses option 82 information to match the named address range for client IP address assignment. The option 82 matching

must also be included in the address-assignment pool configuration. The DHCP local server uses the default pool match configuration of `ip-address-first`.

```
[edit system services]
dhcp-local-server {
    group group_one {
        interface fe-0/0/2.0;
        interface fe-0/0/2.1;
    }
    group group_two {
        interface fe-0/0/3.0;
        interface fe-0/0/3.1;
    }
    pool-match-order {
        ip-address-first:
        option-82:
    }
}
```

RELATED DOCUMENTATION

- DHCP Server Configuration | 51
- DHCP Server Options | 77
- DHCP Relay Agent | 156
- DHCP Relay Agent Information Option (Option 82) | 198

DHCP Snooping

IN THIS SECTION

- DHCP Snooping Support | 288
- Example: Configuring DHCP Snooping Support for DHCP Relay Agent | 290
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent | 293

DHCP snooping on Junos OS device validates DHCP messages and drops invalid traffic. You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives. For more information, read this topic.

DHCP Snooping Support

IN THIS SECTION

- What is DHCP Snooping | **288**
- Benefits of DHCP Snooping | **288**
- Configuring DHCP Snooping | **289**

DHCP snooping provides additional security by identifying the incoming DHCP packets and rejecting DHCP traffic determined to be unacceptable from untrusted devices in the network.

What is DHCP Snooping

DHCP allocates IP addresses dynamically, leasing addresses to devices so that the addresses can be reused when they are no longer needed by the devices to which they were assigned. Hosts and end devices that require IP addresses obtained through DHCP must communicate with a DHCP server across the LAN.

DHCP snooping looks into incoming DHCP packets and examines DHCP messages. It extracts their IP addresses and lease information allocated to clients and builds up a database. Using this database, it can determine if the packets arriving are from the valid clients—that is—the IP addresses of the clients was assigned by the DHCP server. In this way, DHCP snooping acts as a guardian of network security by keeping track of valid IP addresses assigned to downstream network devices by a trusted DHCP server (the server is connected to a trusted network port).

Benefits of DHCP Snooping

- DHCP snooping provides an extra layer of security via dynamic IP source filtering.
- DHCP snooping can prevent rogue DHCP activity in the network by filtering out DHCP packets that are arriving on the wrong ports, or with incorrect contents.

Configuring DHCP Snooping

In the default DHCP snooping configuration, all traffic is snooped.

On Junos OS device, DHCP snooping is enabled in a routing instance when you configure the following options in that routing instance:

- `dhcp-relay` statement at the `[edit forwarding-options]` hierarchy level
- `dhcp-local-server` statement at the `[edit system services]` hierarchy level
- You can optionally use the `forward-snooped-clients` statement to evaluate the snooped traffic and to determine if the traffic is forwarded or dropped, based on whether or not the interface is configured as part of a group.

The router discards snooped packets by default if there is no subscriber associated with the packet. To enable normal processing of snooped packets, you must explicitly configure the `allow-snooped-clients` statement at the `[edit forwarding-options dhcp-relay]` hierarchy level.

You can configure DHCP snooping support for a specific routing instance for the following:

- DHCPv4 relay agent—Override the router's (or switch's) default snooping configuration and specify that DHCP snooping is enabled or disabled globally, for a named group of interfaces, or for a specific interface within a named group.

  In a separate procedure, you can set a global configuration to specify whether the DHCPv4 relay agent forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces. The router also uses the global DHCP relay agent snooping configuration to determine whether to forward or drop snooped BOOTREPLY packets. A renew request may be unicast directly to the DHCP server. This is a BOOTPREQUEST packet and is snooped.

- DHCPv6 relay agent—As you can with snooping support for the DHCPv4 relay agent, you can override the default DHCPv6 relay agent snooping configuration on the router to explicitly enable or disable snooping support globally, for a named group of interfaces, or for a specific interface with a named group of interfaces.

  In multi-relay topologies where more than one DHCPv6 relay agent is between the DHCPv6 client and the DHCPv6 server, snooping enables intervening DHCPv6 relay agents between the client and the server to correctly receive and process the unicast traffic from the client and forward it to the server. The DHCPv6 relay agent snoops incoming unicast DHCPv6 packets by setting up a filter with UDP port 547 (the DHCPv6 UDP server port) on a per-forwarding table basis. The DHCPv6 relay agent then processes the packets intercepted by the filter and forwards the packets to the DHCPv6 server.

  Unlike the DHCPv4 relay agent, the DHCPv6 relay agent does not support global configuration of forwarding support for DHCPv6 snooped packets.

- DHCP local server—Configure whether DHCP local server forwards or drops snooped packets for all interfaces, only configured interfaces, or only nonconfigured interfaces.
- You can also disable snooping filters. In the preceding configurations, all DHCP traffic is forwarded to the slower routing plane of the routing instance before it is either forwarded or dropped. Disabling snooping filters causes DHCP traffic that can be forwarded directly from the faster hardware control plane to bypass the routing control plane.

Example: Configuring DHCP Snooping Support for DHCP Relay Agent

IN THIS SECTION

- Requirements | **290**
- Overview | **290**
- Configuration | **291**

This example shows how to configure DHCP snooping support for DHCP relay agent.

Requirements

- Configure DHCP relay agent. See *Extended DHCP Relay Agent Overview*.

Overview

In this example, you configure DHCP snooping support for DHCP relay agent by completing the following operations:

- Override the default DHCP snooping configuration and enable DHCP snooping support for the interfaces in group **frankfurt**.
- Configure DHCP relay agent to forward snooped packets to only configured interfaces.

NOTE: By default, DHCP snooping is disabled globally.

Configuration

IN THIS SECTION

- Procedure | 291

Procedure

Step-by-Step Procedure

To configure DHCP relay support for DHCP snooping:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Specify the named group of interfaces on which DHCP snooping is supported.

```
[edit forwarding-options dhcp-relay]
user@host# edit group frankfurt
```

3. Specify the interfaces that you want to include in the group. DHCP relay agent considers these as the configured interfaces when determining whether to forward or drop traffic.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# set interface fe-1/0/1.3 upto fe-1/0/1.9
```

4. Specify that you want to override the default configuration for the group.

```
[edit forwarding-options dhcp-relay group frankfurt]
user@host# edit overrides
```

5. Enable DHCP snooping support for the group.

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# set allow-snooped-clients
```

6. Return to the `[edit forwarding-options dhcp-relay]` hierarchy level to configure the forwarding action and specify that DHCP relay agent forward snooped packets on only configured interfaces:

```
[edit forwarding-options dhcp-relay group frankfurt overrides]
user@host# up 2
```

7. Enable DHCP snooped packet forwarding for DHCP relay agent.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

8. Specify that snooped packets are forwarded on only configured interfaces (the interfaces in group `frankfurt`).

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set configured-interfaces
```

Results

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
    forward-snooped-clients configured-interfaces;
    group frankfurt {
        overrides {
            allow-snooped-clients;
        }
        interface fe-1/0/1.3 {
```

```
            upto fe-1/0/1.9;
        }
    }
}
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

You can configure how DHCP relay agent handles DHCP snooped packets. Depending on the configuration, DHCP relay agent either forwards or drops the snooped packets it receives.

DHCP relay uses a two-part configuration to determine how to handle DHCP snooped packets. This topic describes how you use the `forward-snooped-clients` statement to manage whether DHCP relay agent forwards or drops snooped packets, depending on the type of interface on which the packets are snooped. In the other part of the DHCP relay agent snooping configuration, you enable or disable the DHCP relay snooping feature.

Table 17 on page 293 shows the action the router or switch takes on snooped packets when DHCP snooping is enabled by the `allow-snooped-clients` statement.

The router or switch also uses the configuration of the DHCP relay agent forwarding support to determine how to handle snooped BOOTREPLY packets.

Table 17: 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 17: 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 18 on page 294 shows the action the router (or switch) takes on snooped packets when DHCP snooping is disabled by the `no-allow-snooped-clients` statement.

Table 18: 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 19 on page 294 shows the action the router (or switch) takes for the snooped BOOTREPLY packets.

Table 19: Actions for Snooped BOOTREPLY Packets

forward-snooped-clients Configuration	Action
`forward-snooped-clients` not configured	snooped **BOOTREPLY** packets dropped if client is not found
`forward-snooped-clients` all configurations	snooped **BOOTREPLY** packets forwarded if client is not found

Configured interfaces have been configured with the **group** statement in the `[edit forwarding-options dhcp-relay]` hierarchy. Non-configured interfaces are in the logical system/routing instance but have not been configured by the **group** statement.

To configure DHCP snooped packet forwarding and BOOTREPLY snooped packet forwarding for DHCP relay agent:

1. Specify that you want to configure DHCP relay agent.

```
[edit]
user@host# edit forwarding-options dhcp-relay
```

2. Enable DHCP snooped packet forwarding.

```
[edit forwarding-options dhcp-relay]
user@host# edit forward-snooped-clients
```

3. Specify the interfaces that are supported for snooped packet forwarding.

```
[edit forwarding-options dhcp-relay forward-snooped-clients]
user@host# set (all-interfaces | configured-interfaces | non-configured-interfaces)
```

For example, to configure DHCP relay agent to forward DHCP snooped packets on only configured interfaces:

```
[edit]
forwarding-options {
    dhcp-relay {
        forward-snooped-clients configured-interfaces;
    }
}
```

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Security Services Administration Guide

DHCP Server | 49
DHCP Relay Agent | 156
DHCP Client | 234

DHCP Auto Logout

IN THIS SECTION

- DHCP Auto Logout Overview | 296
- Automatically Logging Out DHCP Clients | 298

DHCP local server and DHCP relay agent support Auto logout feature. Auto logout releases and returns IP addresses to the address pool if DHCP clients are no longer using these addresses. It improves the efficiency of DHCP IP address assignment. For more information, read this topic.

DHCP Auto Logout Overview

IN THIS SECTION

- Auto Logout Overview | 296
- How DHCP Identifies and Releases Clients | 297
- Option 60 and Option 82 Requirements | 298

This topic provides an introduction to the DHCP auto logout feature and includes the following sections:

Auto Logout Overview

Auto logout is supported for DHCP local server and DHCP relay agent. It improves the efficiency of DHCP IP address assignment by allowing IP addresses to be immediately released and returned to the

address pool when DHCP clients are no longer using the addresses. DHCP can then assign the addresses to other clients. Without auto logout, an IP address is blocked for the entire lease period, and DHCP must wait until the address lease time expires before reusing the address.

Auto logout is particularly useful when DHCP uses long lease times for IP address assignments and to help avoid allocating duplicate IP addresses for a single client.

For example, you might have an environment that includes set-top boxes (STB) that are often upgraded or replaced. Each time a STB is changed, the new STB repeats the DHCP discover process to obtain client configuration information and an IP address. DHCP views the new STB as a completely new client and assigns a new IP address— the previous IP address assigned to the client (the old STB) remains blocked and unavailable until the lease expires. If auto logout is configured in this situation, DHCP recognizes that the new STB is actually the same client and then immediately releases the original IP address. DHCP relay agent acts as a proxy client for auto logout and sends a DHCP release message to the DHCP server.

How DHCP Identifies and Releases Clients

The auto logout feature requires that DHCP explicitly identify clients. By default, DHCP local server and DHCP relay agent identify clients based on MAC address or Client Identifier, and subnet. However, in some cases this type of identification might not be sufficient. For example, in the previous STB example, each STB has a different MAC address, so DHCP incorrectly assumes that an upgraded or replacement STB is a new client.

In order to explicitly identify clients, auto logout uses a secondary identification method when the primary identification method is unsuccessful— the primary method is considered unsuccessful if the MAC address or Client Identifier does not match that of an existing client. Subscriber management supports two secondary identification methods that you can configure.

- Incoming interface method— DHCP views a new client connection on the interface as if it comes from the same client. DHCP deletes the existing client binding before creating a binding for the newly connected device. This method allows only one client device to connect on the interface.

  NOTE: The incoming interface method differs from the `overrides interface-client-limit 1` statement, which retains the existing binding and rejects the newly connected client.

- Option 60 and option 82 method— DHCP considers two clients as different if they have the same option 60 and option 82 information, but different subnets.

DHCP local server and DHCP relay agent perform the following operations when auto logout is enabled and the secondary identification method identifies a duplicate client (that is, the Discover packet is from an existing client).

- DHCP local server immediately releases the existing address.
- DHCP relay agent immediately releases the existing client and then sends a DHCP release packet to the DHCP server. Sending the release packet ensures that DHCP relay and the DHCP server are synchronized.

  If the DHCP relay receives a Discover message from an existing client, the DHCP relay forwards the Discover message to the DHCP server. The DHCP relay preserves the binding if the client' s existing IP address is returned by the DHCP server. This behavior is not applicable if the proxy-mode override or client-discover-match functionality are enabled.

  NOTE: If the DHCP relay agent is in snoop mode, DHCP relay releases the client but does not send a release packet to the DHCP server if the discover packet is for a passive client (a client added as a result of snooped packets) or if the discover packet is a snooped packet.

Option 60 and Option 82 Requirements

DHCP local server requires that the received discover packet include both DHCP option 60 and option 82. If either option is missing, the DHCP local server cannot perform the secondary identification method and auto logout is not used.

DHCP relay agent requires that the received discover packet contain DHCP option 60. DHCP relay determines the option 82 value based on the guidelines provided in *DHCP Relay Agent Option 82 Value for Auto Logout*.

Automatically Logging Out DHCP Clients

You can configure the extended DHCP local server and extended DHCP relay to automatically log out DHCP clients. Auto logout immediately releases an existing client when DHCP receives a discover packet from a client whose identity matches an existing client. DHCP then releases the existing client IP address without waiting for the normal lease expiration.

NOTE: When the existing client is released, the new client undergoes the normal authentication process. The new client might not receive the same IP address as the original client.

To configure DHCP client auto logout:

1. Specify that you want to configure override options.

- For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

2. Enable auto logout and specify the secondary identification method you want to use when the primary identification method is unsuccessful.

   - For example, to configure DHCP local server to use the incoming interface method:

```
[edit system services dhcp-local-server overrides]
user@host# set client-discover-match incoming-interface
```

   - For example, to configure DHCP relay agent to use the option 60 and option 82 method:

```
[edit forwarding-options dhcp-relay overrides]
user@host# set client-discover-match option60-and-option82
```

NOTE: If you change the auto logout configuration, existing clients continue to use the auto logout setting that was configured when they logged in. New clients use the new setting.

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information | 199

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 156

Additional Configurations for DHCP Clients

IN THIS SECTION

- Specifying the Maximum Number of DHCP Clients Per Interface | 300
- DHCP Local Server Handling of Client Information Request Messages | 301
- Enabling Processing of Client Information Requests | 302
- Sending Release Messages When Clients Are Deleted | 303

Specifying the Maximum Number of DHCP Clients Per Interface

By default, there is no limit to the number of DHCP local server or DHCP relay clients allowed on an interface. However, you can override the default setting and specify the maximum number of clients allowed per interface, in the range 1 through 500,000. When the number of clients on the interface reaches the specified limit, no additional DHCP Discover PDUs or DHCPv6 Solicit PDUs are accepted. When the number of clients subsequently drops below the limit, new clients are again accepted.

NOTE: The maximum number of DHCP (and DHCPv6) local server clients or DHCP (and DHCPv6) relay clients can also be specified by Juniper Networks VSA 26-143 during client login. The VSA-specified value always takes precedence if the `interface-client-limit` statement specifies a different number.

If the VSA-specified value differs with each client login, DHCP uses the largest limit set by the VSA until there are no clients on the interface.

To configure the maximum number of DHCP clients allowed per interface:

1. Specify that you want to configure override options.
   - For DHCP local server:

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

- For DHCPv6 local server:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit overrides
```

- For DHCP relay agent:

```
[edit forwarding-options dhcp-relay]
user@host# edit overrides
```

- For DHCPv6 relay agent:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit overrides
```

2. Configure the maximum number of clients allowed per interface. (DHCP local server, DHCPv6 local server, DHCP relay agent and DHCPv6 relay agent all support the `interface-client-limit` statement.)

```
[edit system services dhcp-local-server overrides]
user@host# set interface-client-limit number
```

NOTE: For DHCP local server and DHCP relay agent, you can use either the `interface-client-limit` statement or the `client-discover-match incoming-interface` statement to set a limit of one client per interface. The `interface-client-limit` statement with a value of 1 retains the existing client and rejects any new client connections. The `client-discover-match incoming-interface` statement deletes the existing client and allows a new client to connect.

DHCP Local Server Handling of Client Information Request Messages

DHCP clients that already have externally provided addresses may solicit further configuration information from a DHCP server by sending a DHCP inform or DHCPv6 information-request message that indicates what information is desired. These message types can be collectively referred to as information request messages. By default, DHCP local server and DHCPv6 local server ignore any DHCP information requests that they receive. You can override this default behavior to enable processing of these messages.

If you enable processing of information requests, DHCP local server responds to the client with a DHCP acknowledgment message that includes the requested information—if it is available. DHCPv6 local server responds in the same manner but uses a DHCP reply message. No subscriber management or DHCP-management is applied as a result of the DHCP information request message.

By default, DHCP relay and DHCP relay proxy automatically forward DHCP information request messages without modification if the messages are received on an interface configured for a DHCP server group. DHCP relay and relay proxy drop information request messages received on any other interfaces. You cannot disable this default DHCP relay and relay proxy behavior.

The information requested by these clients is typically configured with the `dhcp-attributes` statement for an address pool defined by the `address-assignment pool` *`pool-name`* statement at the `[edit access]` hierarchy level.

When you enable processing of DHCP information requests, you can optionally specify the name of the pool from which the local server retrieves the requested configuration information for the client. If you do not do specify a local pool, then the local server requests that AAA selects and returns only the name of the relevant pool.

NOTE: PPP interfaces are not supported on EX Series switches.

When DHCPv6 is configured over PPP interfaces, the PPP RADIUS authentication data can be used to select the pool from which the response information is taken. Additionally other RADIUS attributes can also be inserted into the DHCPv6 reply message. If an overlap exists between RADIUS attributes and local pool attributes, the RADIUS values are used instead of the local configuration data. If no RADIUS information is received from the underlying PPP interface, then the behavior is the same as described previously for non-PPP interfaces.

Enabling Processing of Client Information Requests

Configure one or more local address pools if you want to use a local pool rather than one provided by AAA. See DHCPv6 Address-Assignment Pools. For processing information request messages, the address configuration is not necessary. For DHCP local server, you must specify the IPv4 family; for DHCPv6 local server, you must specify the IPv6 family.

See *Configuring DHCP Client-Specific Attributes Applied When Clients Obtain an Address* for details about how to configure the information sought by clients that send information request messages.

By default, DHCP local server and DHCPv6 local server do not respond to information request (DHCP inform and DHCPv6 information-request) messages from the client. You can enable DHCP local server

and DHCPv6 local server to process these messages and respond to them with an acknowledgment (ack or reply message, respectively) and the requested information.

DHCP relay agent automatically forwards the information request messages without modification to the configured server group by means of the interfaces configured for the respective server group. The messages are dropped if they are received on an unconfigured interface. DHCP relay proxy also supports forwarding these messages. You cannot disable forwarding of the information request messages.

To enable processing of DHCP client information request messages:

1. Specify that you want to configure override options.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides]
     user@host# set process-inform
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides]
     user@host# set process-inform
     ```

2. (Optional) Specify a pool name from which DHCP information is returned to the client.
   - For DHCP local server:

     ```
     [edit system services dhcp-local-server overrides process-inform]
     user@host# set pool pool-name
     ```

   - For DHCPv6 local server:

     ```
     [edit system services dhcp-local-server dhcpv6 overrides process-inform]
     user@host# set pool pool-name
     ```

Sending Release Messages When Clients Are Deleted

By default, when DHCP relay and relay proxy delete a client, they do not send a release message to the DHCP server. You can override the default behavior and configure DHCP relay and relay proxy to send a

release message whenever they delete a client. The release message sent by DHCP relay and relay proxy includes option 82 information.

NOTE: You must include the `send-release-on-delete` statement to configure DHCP relay and relay proxy to send the release message when the `client-discover-match` statement is included.

You can use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to override the default behavior for DHCPv6 relay agent.

To send a release message:

1. Specify that you want to configure override options.
   - For DHCP relay agent:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit overrides
     ```

   - For DHCPv6 relay agent:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# edit overrides
     ```

2. Specify that you want DHCP relay and relay proxy (or DHCPv6 relay agent) to send a release message when clients are deleted.

   ```
   [edit forwarding-options dhcp-relay overrides]
   user@host# set send-release-on-delete
   ```

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

Dynamic Reconfiguration of DHCP Servers and Clients

IN THIS SECTION

- Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients | 305
- Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview | 309
- Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings | 310
- Configuring Dynamic Reconfiguration Attempts for DHCP Clients | 311
- Configuring Deletion of the Client When Dynamic Reconfiguration Fails | 312
- Configuring a Token for DHCP Local Server Authentication | 313
- Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect | 314

Junos OS allows you to perform different types of DHCP services such as attaching dynamic profiles, using external authentication services with DHCP, specifying maximum number of clients, managing client information request messages, dynamic reconfiguration of clients and so on. For more information, read this topic.

Understanding Dynamic Reconfiguration of Extended DHCP Local Server Clients

IN THIS SECTION

- Default Client/Server Interaction | 306
- Dynamic Client/Server Interaction for DHCPv4 | 307
- Dynamic Client/Server Interaction for DHCPv6 | 307
- Manually Forcing the Local Server to Initiate the Reconfiguration Process | 308
- Action Taken for Events That Occur During a Reconfiguration | 308
- Benefits of Dynamic Reconfiguration of DHCP Local Server Clients | 309

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 20 on page 308 lists the actions taken in response to several different events.

Table 20: Action Taken for Events That Occur During a Reconfiguration

Event	Action
Server receives a discover (DHCPv4) or solicit (DHCPv6) message from the client.	Server drops packet and deletes client.
Server receives a request, renew, rebind, or init-reboot message from the client.	DHCPv4—Server sends NAK message and deletes client. DHCPv6—Server drops packet and deletes client. Server replies to renew message with lease time of zero (0).
Server receives a release or decline message from the client.	Server deletes client.
The client lease times out.	Server deletes client.
The `clear dhcp server binding` command is issued.	Server deletes client.
The `request dhcp server reconfigure` (DHCPv4) or `request dhcpv6 server reconfigure` (DHCPv6) command is issued.	Command is ignored.
GRES or DHCP restart occurs.	Reconfiguration process is halted.

Benefits of Dynamic Reconfiguration of DHCP Local Server Clients

- Enable the DHCP local server to dynamically reconfigure DHCP clients, avoiding extended outages because of server configuration changes that otherwise require the server to wait for the client to renews its lease or rebind to the server.

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

The DHCP local server can initiate reconfiguration of its clients to avoid extended outages because of server configuration changes. You can enable dynamic reconfiguration for all DHCP clients or only the DHCP clients serviced by a specified group of interfaces, and you can modify the behavior accordingly.

Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements. You can provide the statements at the `[edit system services dhcp-local-server reconfigure]` hierarchy level for all DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 reconfigure]` hierarchy level for all DHCPv6 clients. To override this global configuration for only the DHCP clients serviced by a specified group of interfaces, you can include the statements with different values at the `[edit system services dhcp-local-server group` *`group-name`* `reconfigure]` hierarchy level for DHCPv4 clients, and at the `[edit system services dhcp-local-server dhcpv6 group` *`group-name`* `reconfigure]` hierarchy level for DHCPv6 clients.

To configure dynamic reconfiguration of DHCP clients:

1. Enable dynamic reconfiguration with default values for all clients.

   For DHCPv4:

   ```
   [edit system services dhcp-local-server]
   user@host# set reconfigure
   ```

   For DHCPv6:

   ```
   [edit system services dhcp-local-server dhcpv6]
   user@host# set reconfigure
   ```

2. (Optional) Enable dynamic reconfiguration for only the clients serviced by a group of interfaces.

For DHCPv4:

```
[edit system services dhcp-local-server group-name]
user@host# set reconfigure
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name]
user@host# set reconfigure
```

3. (Optional) Configure how the server attempts reconfiguration.

   See *Configuring Dynamic Reconfiguration Attempts for DHCP Clients*.

4. (Optional) Configure the response to a failed reconfiguration.

   See *Configuring Deletion of the Client When Dynamic Reconfiguration Fails*.

5. (Optional) Configure the behavior in response to a RADIUS-initiated disconnect.

   See *Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect*.

6. (Optional) Configure a token for rudimentary server authentication.

   See *Configuring a Token for DHCP Local Server Authentication*.

7. (Optional) Prevent DHCPv6 clients from binding if they do not support reconfigure messages.

   See *Preventing Binding of Clients That Do Not Support Reconfigure Messages*.

Requesting DHCP Local Server to Initiate Reconfiguration of Client Bindings

You can request that the DHCP local server initiate reconfiguration of all of clients or only specified clients.

To request reconfiguration of all clients:

- Specify the `all` option.

```
user@host> request dhcp server reconfigure all
```

You can use any of the following methods to request reconfiguration of specific clients:

- Specify the IP address of the DHCPv4 client.

```
user@host> request dhcp server reconfigure 192.168.27.3
```

- Specify the MAC address of a DHCPv4 client.

```
user@host> request dhcp server reconfigure 00:00:5E:00:53:67
```

- Specify an interface; reconfiguration is attempted for all clients on this interface.

```
user@host> request dhcp server reconfigure interface fe-0/0/0.100
```

- Specify a logical system; reconfiguration is attempted for all clients or the specified clients in this logical system.

```
user@host> request dhcp server reconfigure all logical-system ls-bldg5
```

- Specify a routing instance; reconfiguration is attempted for all clients or the specified clients in this routing instance.

```
user@host> request dhcp server reconfigure all routing-instance ri-boston
```

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

You can configure how many attempts the local server makes to initiate reconfiguration of the DHCP client by sending forcerenew or reconfigure messages. You can also specify how long the server waits between attempts. By default, eight attempts are made and the initial interval is two seconds.

Each successive attempt doubles the interval between attempts. For example, if the first value is 2, the first retry is attempted 2 seconds after the first attempt fails. The second retry is attempted 4 seconds after the first retry fails. The third retry is attempted 8 seconds after the second retry fails, and so on. A group configuration takes precedence over a DHCP local server configuration.

(Optional) To configure DHCP local server reconfiguration behavior for all DHCP clients:

1. Specify the number of reconfiguration attempts.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set attempts 5
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set attempts 5
```

2. Specify the interval between reconfiguration attempts.

   For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set timeout 8
```

   For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set timeout 8
```

To override the global configuration for a particular group of clients, include the statements at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Configuring Deletion of the Client When Dynamic Reconfiguration Fails

You can configure the local server to delete the client when the maximum number of reconfiguration attempts has been made without success. By default, the client's original configuration is restored.

(Optional) To configure the DHCP local server to delete the client when reconfiguration is not successful, for all clients:

- Specify the client deletion.

For DHCPv4:

```
[edit system services dhcp-local-server reconfigure]
user@host# set clear-on-terminate
```

For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure]
user@host# set clear-on-terminate
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure]` hierarchy level.

Configuring a Token for DHCP Local Server Authentication

You can configure an authentication token to provide rudimentary protection against inadvertently instantiated DHCP servers. You can configure the local server to include a constant, unencoded token in the DHCP forcerenew message as part of the authentication option it sends to clients. If the service provider has previously configured the DHCP client with a token, then the client can compare that token against the newly received token. If the tokens do not match, the DHCP client discards the forcerenew message. This functionality corresponds to RFC 3118, *Authentication for DHCP Messages*, section 4.

(Optional) To configure the DHCP local server to include a token in the forcerenew message sent to the client, for all clients:

- Specify the token.

  For DHCPv4:

  ```
  [edit system services dhcp-local-server reconfigure]
  user@host# set token token-value
  ```

  For DHCPv6:

  ```
  [edit system services dhcp-local-server dhcpv6 reconfigure]
  user@host# set token token-value
  ```

(Optional) For only a particular group of clients:

- Specify the token.

  For DHCPv4:

```
[edit system services dhcp-local-server group group-name reconfigure]
user@host# set token token-value
```

  For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
user@host# set token token-value
```

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

You can configure the local server to reconfigure the client when the client receives a RADIUS-initiated disconnect. By default, the client is deleted when a RADIUS-initiated disconnect is received.

(Optional) To configure the DHCP local server to reconfigure the client instead of deleting the client when a RADIUS-initiated disconnect is received, for all clients:

- Specify the RADIUS-initiated disconnect trigger.

  For DHCPv4:

```
[edit system services dhcp-local-server reconfigure trigger]
user@host# set radius-disconnect
```

  For DHCPv6:

```
[edit system services dhcp-local-server dhcpv6 reconfigure trigger]
user@host# set radius-disconnect
```

To override the global configuration for a particular group of clients, include the statement at the `[edit system services dhcp-local-server group group-name reconfigure trigger]` hierarchy level or the `[edit system services dhcpv6 dhcp-local-server group group-name reconfigure trigger]` hierarchy level.

Release History Table

Release	Description
14.1	Starting in Junos OS Release 14.1, you can modify the behavior of the process in which the DHCP local server initiates reconfiguration of its clients by including the appropriate configuration statements.

RELATED DOCUMENTATION

DHCP Overview | 2

IP Address Assignment Pool | 27

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

DHCP Liveness Detection

IN THIS SECTION

- DHCP Liveness Detection Overview | 316
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD | 318
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients | 320
- Configuring Detection of DHCP Local Server Client Connectivity with BFD | 324
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients | 326
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets | 331

DHCP liveness detection for DHCP client IP sessions utilizes an active liveness detection protocol to conduct liveness detection checks for relevant clients. When configured with a liveness detection protocol, if a given client fails to respond to a configured number of consecutive liveness detection requests, the client binding is deleted and its resources released. For more information, read this topic.

DHCP Liveness Detection Overview

IN THIS SECTION

- Benefits of DHCP Liveness Detection | 317

Unlike PPP, DHCP does not define a native keepalive mechanism as part of either the DHCPv4 or DHCPv6 protocols. Without a keepalive mechanism, DHCP local server, DHCP relay, and DHCP relay proxy are unable to quickly detect if any of them has lost connectivity with a subscriber or a DHCP client. Instead, they must rely on standard DHCP subscriber session or DHCP client session termination messages.

DHCP clients often do not send DHCP release messages before exiting the network. The discovery of their absence is dependent on existing DHCP lease time and release request mechanisms. These mechanisms are often insufficient when serving as session health checks for clients in a DHCP subscriber access or a DHCP-managed network. Because DHCP lease times are typically too long to provide an adequate response time for a session health failure, and configuring short DHCP lease times can pose an undue burden on control plane processing, implementing a DHCP liveness detection mechanism enables better monitoring of bound DHCP clients. When configured with a liveness detection protocol, if a given subscriber (or client) fails to respond to a configured number of consecutive liveness detection requests, the subscriber (or client) binding is deleted and its resources released.

DHCP liveness detection for DHCP subscriber IP or DHCP client IP sessions utilizes an active liveness detection protocol to institute liveness detection checks for relevant clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

Examples of liveness detection protocols include Bidirectional Forwarding Detection (BFD) for both DHCPv4 and DHCPv6 subscribers, IPv4 Address Resolution Protocol (ARP) for DHCPv4 subscribers, and IPv6 Neighbor Unreachability Detection (NUD) using Neighbor Discovery (ND) packets for DHCPv6 subscribers.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. In earlier releases, only BFD is supported for all platforms.

The two liveness detection methods are mutually exclusive.

When configuring BFD liveness detection, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 liveness detection either globally or per DHCPv4 or DHCPv6 group.
- DHCPv4 or DHCPv6 subscriber access clients that do not support BFD are not affected by the liveness detection configuration. These clients can continue to access the network (after they are validated) even if BFD liveness detection is enabled on the router (or switch).
- When configured, DHCPv4 or DHCPv6 initiates liveness detection checks for clients that support BFD when those clients enter a bound state.
- After protocol-specific messages are initiated for a BFD client, they are periodically sent to the subscriber (or client) IP address of the client and responses to those liveness detection requests are expected within a configured amount of time.
- If liveness detection responses are not received from clients that support BFD within the configured amount of time for a configured number of consecutive attempts, the liveness detection check is deemed to have failed. A configured failure action to clear the client binding is applied.
- The only failure action supported for Layer 2 Liveness detection is `clear-binding`.

When configuring DHCP ARP and ND Layer 2 liveness detection on MX Series, keep the following in mind:

- You can configure liveness detection for both DHCP local server and DHCP relay.
- You can configure DHCPv4 and DHCPv6 ARP and ND liveness detection globally, per DHCPv4 or DHCPv6 group, and per dual-stack group.
- ARP/ND liveness detection applies only to DHCP clients that:
  - Are directly connected over dynamic VLANs.
  - Have permanent Layer 2 entries.
- DHCPv6 clients must have a unique source MAC address and link-local address. Only single liveness detection entry is used for all IPv6 addresses associated with a specific client session.

Benefits of DHCP Liveness Detection

Using DHCP liveness detection, IP sessions are acted upon as soon as liveness detection checks fail. This faster response time serves to:

- Provide more accurate time-based accounting of subscriber (or DHCP client) sessions.
- Better preserve router (switch) resources.

- Help to reduce the window of vulnerability to some security attacks.

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP relay clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.
   - For DHCP global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection
     ```

   - For DHCP group configuration:

     ```
     [edit forwarding-options dhcp-relay group group-name]
     user@host# edit liveness-detection
     ```

   NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name` hierarchy level.

2. (Optional) Specify that you want to use DHCP relay proxy mode.

   ```
   [edit forwarding-options dhcp-relay group group-name]
   user@host# set overrides proxy-mode
   ```

3. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit method
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit method
```

4. Specify the liveness detection method that you want DHCP to use.

> **NOTE**: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.
>
> Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit bfd
```

5. Configure the liveness detection method as desired.

   See *Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients* for an example of how to globally configure DHCP relay liveness detection with BFD.

6. Configure the action the router takes when a liveness detection failure occurs.

- For DHCP global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

- For DHCP group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

IN THIS SECTION

- Requirements | 320
- Overview | 321
- Configuration | 321

This example shows how to configure liveness detection for DHCP relay agent subscribers using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers.
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP relay agent. See *Extended DHCP Relay Agent Overview*.

Overview

In this example, you configure liveness detection for DHCP relay agent subscribers by completing the following operations:

1. Enable liveness detection globally for DHCP relay subscribers.
2. Specify BFD as the liveness detection method for all dynamically created DHCP relay subscribers.
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit forwarding-options dhcp-relay dhcpv6]` or `[edit forwarding-options dhcp-relay dhcpv6 group group-name]` hierarchy level.

Configuration

IN THIS SECTION

- Procedure | 321

Procedure

Step-by-Step Procedure

To configure liveness detection for DHCP relay:

1. Specify that you want to configure liveness detection.

```
[edit forwarding-options dhcp-relay]
user@host# edit liveness-detection
```

2. Specify that you want to configure the liveness detection method.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit method
```

3. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit bfd
```

4. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set detection-time threshold 50000
```

5. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set holddown-interval 50
```

6. Configure the BFD minimum transmit and receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-interval 45000
```

7. Configure the minimum receive interval (in milliseconds).

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

8. Configure a multiplier value for the detection time.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set multiplier 100
```

9. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set no-adaptation
```

10. Configure the BFD session mode.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set session-mode automatic
```

11. Configure the threshold and minimum interval for the BFD transmit interval.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

12. Configure the BFD protocol version you want to detect.

```
[edit forwarding-options dhcp-relay liveness-detection method bfd]
user@host# set version automatic
```

13. Configure the action the router takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit forwarding-options dhcp-relay liveness-detection]
user@host# edit failure-action action
```

Results

From configuration mode, confirm your configuration by entering the `show forwarding-options` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it. The following output also shows a range of configured interfaces in group frankfurt.

```
[edit]
user@host# show forwarding-options
dhcp-relay {
    liveness-detection {
```

```
        failure-action clear-binding-if-interface-up;
        method {
            bfd {
                version automatic;
                minimum-interval 45000;
                minimum-receive-interval 60000;
                multiplier 100;
                no-adaptation;
                transmit-interval {
                    minimum-interval 45000;
                    threshold 60000;
                }
                detection-time {
                    threshold 50000;
                }
                session-mode automatic;
                holddown-interval 50;
            }
        }
    }
    }
```

If you are done configuring the device, enter `commit` from configuration mode.

Configuring Detection of DHCP Local Server Client Connectivity with BFD

You can configure liveness detection with Bidirectional Forwarding Detection (BFD) for DHCP subscriber IP sessions or DHCP client IP sessions to check the connectivity of DHCP local server clients. Clients must respond to liveness detection requests within a specified amount of time. If the responses are not received within that time for a given number of consecutive attempts, then the liveness detection check fails and a failure action is implemented.

NOTE: You can also configure DHCP liveness detection for DHCP relay.

To configure liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

- For DHCP global configuration:

```
[edit system services dhcp-local-server]
user@host# edit liveness-detection
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name]
user@host# edit liveness-detection
```

NOTE: Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

2. Specify that you want to configure the liveness detection method.

- For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit method
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit method
```

3. Specify the liveness detection method that you want DHCP to use.

NOTE: In releases earlier than Junos OS Release 17.4R1, the only method supported for liveness detection on all platforms is BFD.

Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection. The two liveness detection methods are mutually exclusive. See DHCP Liveness Detection Using ARP and Neighbor Discovery Packets for information about configuring ARP and ND Layer 2 liveness detection.

- For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection method]
user@host# edit bfd
```

- For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit bfd
```

4. Configure the liveness detection method as desired.

   See *Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients* for an example of how to configure DHCPv4 groups for DHCP local server liveness detection with BFD.

5. Configure the action the router takes when a liveness detection failure occurs.

   - For DHCP global configuration:

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit failure-action action
```

   - For DHCP group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection]
user@host# edit failure-action action
```

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

IN THIS SECTION

- Requirements | 327
- Overview | 327
- Configuration | 327

This example shows how to configure group liveness detection for DHCP local server subscribers or DHCP clients using Bidirectional Forwarding Detection (BFD) as the liveness detection method.

Requirements

This example uses the following hardware and software components:

- Juniper Networks MX Series routers
- Juniper Networks EX Series switches
- Junos OS Release 12.1 or later

Before you begin:

- Configure DHCP local server. See *Understanding Differences Between Legacy DHCP and Extended DHCP*.

Overview

In this example, you configure group liveness detection for DHCP local server subscribers (clients) by completing the following operations:

1. Enable liveness detection for DHCP local server subscriber (or DHCP client) groups.
2. Specify BFD as the liveness detection method for all dynamically created DHCP local server subscribers (clients).
3. Configure BFD-specific statements to define how the protocol behaves.
4. Configure the action the router (switch) takes when a liveness detection failure occurs.

NOTE: This example explains how to configure liveness detection for a DHCPv4 network. Liveness detection is also supported for DHCPv6 configurations. To configure DHCPv6 liveness detection, include the `liveness-detection` statement, and any subsequent configuration statements, at the `[edit system services dhcp-local-server dhcpv6]` or `[edit system services dhcp-local-server dhcpv6 group group-name]` hierarchy level.

Configuration

IN THIS SECTION

- Procedure | 328

Procedure

Step-by-Step Procedure

To configure group liveness detection for DHCP local server:

1. Specify that you want to configure liveness detection.

```
[edit system services dhcp-local-server ]
user@host# edit liveness-detection
```

2. Specify that you want to configure liveness detection for a specific DHCP local server group.

```
[edit system services dhcp-local-server liveness-detection]
user@host# edit group local_group_1
```

3. Specify that you want to configure the liveness detection method.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit method
```

4. Specify BFD as the liveness detection method that you want DHCP to use.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method]
user@host# edit bfd
```

5. Configure the detection time threshold (in milliseconds) at which a trap is produced.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set detection-time threshold 30000
```

6. Configure the time (in milliseconds) for which BFD holds a session up notification.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set holddown-interval 50
```

7. Configure the BFD minimum transmit and receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum transmit and receive interval if you configure the `minimum-interval` for the BFD `transmit-interval` statement and the `minimum-receive-interval`.

```
[edit system services dhcp-local-servergroup local_group_1  liveness-detection method bfd]
user@host# set minimum-interval 45000
```

8. Configure the minimum receive interval (in milliseconds).

NOTE: You do not need to configure the BFD minimum receive interval if you configure the BFD minimum transmit and receive interval.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set minimum-receive-interval 60000
```

9. Configure a multiplier value for the detection time.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set multiplier 100
```

10. Disable the ability for BFD interval timers to change or adapt to network situations.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set no-adaptation
```

11. Configure the BFD session mode.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set session-mode automatic
```

12. Configure the threshold and minimum interval for the BFD transmit interval.

NOTE: You do not need to configure the transmit interval values if you have already configured the minimum transmit and receive interval for BFD.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set transmit-interval threshold 60000 minimum-interval 45000
```

13. Configure the BFD protocol version you want to detect.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection method bfd]
user@host# set version automatic
```

14. Configure the action the router (switch) takes when a liveness detection failure occurs. In this example, the failure action is to clear the client session only when a liveness detection failure occurs and the local interface is detected as being up.

```
[edit system services dhcp-local-server group local_group_1 liveness-detection]
user@host# edit failure-action action
```

Results

From configuration mode, confirm your configuration by entering the `show system` command. If the output does not display the intended configuration, repeat the instructions in this example to correct it.

```
[edit]
user@host# show system
services {
    dhcp-local-server {
        group local_group_1 {
            liveness-detection {
                failure-action clear-binding-if-interface-up;
                method {
                    bfd {
                        version automatic;
                        minimum-interval 45000;
                        minimum-receive-interval 60000;
                        multiplier 100;
```

```
                    no-adaptation;
                    transmit-interval {
                        minimum-interval 45000;
                        threshold 60000;
                    }
                    detection-time {
                        threshold 30000;
                    }
                    session-mode automatic;
                    holddown-interval 50;
                }
            }
        }
    }
}
}
```

If you are done configuring the device, enter `commit` from configuration mode.

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

IN THIS SECTION

- How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works | **331**
- Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets | **336**
- Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets | **339**
- Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets | **342**

How DHCP Liveness Detection with ARP and Neighbor Discovery Packets Works

IN THIS SECTION

- Send Functionality | **333**

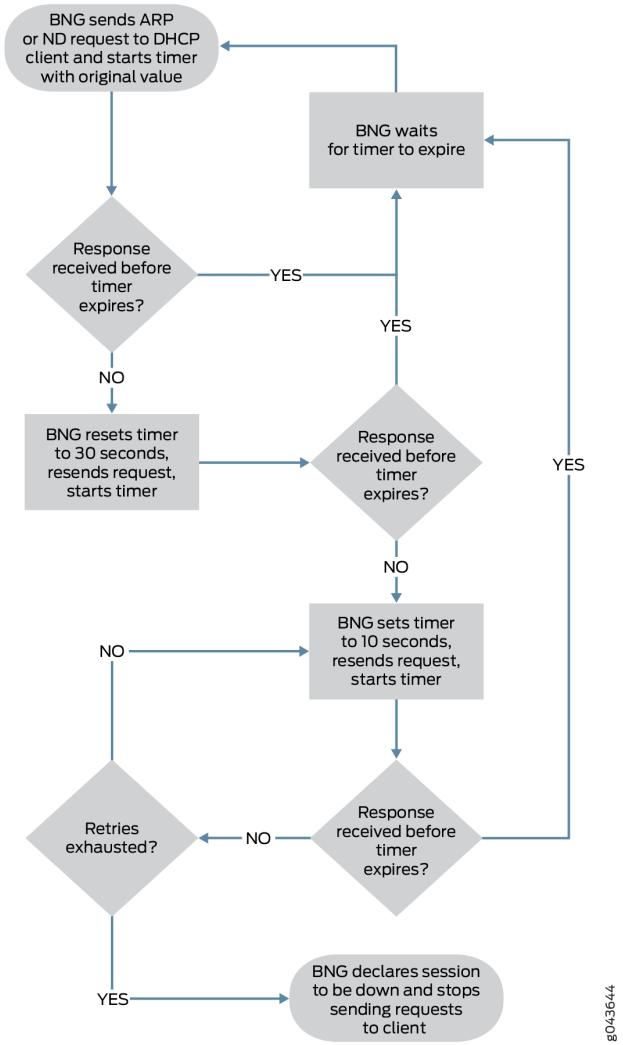
- Receive Functionality | 334

Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients. This Layer 2 liveness detection offers separate mechanisms for the DHCP client host and for the router acting as a broadband network gateway (BNG) to determine the validity and state of the DHCP client sessions. These mechanisms are referred to as the *send* functionality and the *receive* functionality. You can configure Layer 2 liveness detection for DHCP local server and DHCP relay clients.

Send Functionality

The BNG uses the send functionality to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions. *Figure 1* illustrates the send functionality.

Figure 15: Layer 2 Liveness Detection Send Behavior Flow



1. The BNG sends request packets to the each DHCP client at a configurable interval, then waits for a response. The BNG retries the requests when it does not receive a timely response. It sends ARP requests for DHCPv4 clients and Neighbor Discovery (ND) requests for DHCPv6 clients.
2. If the BNG receives a response from the client before the interval times out, it waits for the timer to expire and then sends another request to that client.

3. If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt; the timer is not configurable.

4. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

5. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This timer value is not configurable.

6. If the BNG receives a response from the client before the timer expires, then the BNG waits for the timer to run down, resets it to the original, configurable value, sends another request, and starts the timer.

7. If the BNG does not receive a response within the 10-second interval, it sends another request and starts the 10-second timer again. The BNG continues to send requests at 10-second intervals until it receives a response from the client before the interval times out or it exhausts the number of retry attempts.

   The first retry attempt uses the 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

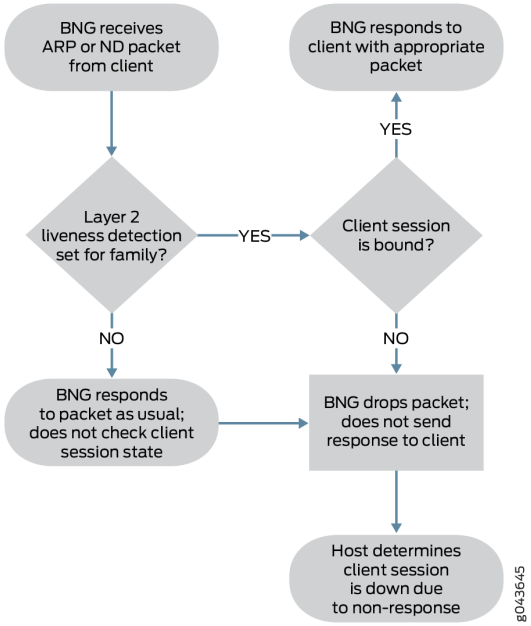
8. If the BNG never sends a response from a client within the interval before the retries are exhausted, then the liveness detection check fails and the clear-binding failure action is implemented. The client session is cleared.

Receive Functionality

The receive functionality enables a DHCP client host to determine the state of the DHCPv4 or DHCPv6 client session from the perspective of a BNG. The BNG conducts a host connectivity check on its

directly connected DHCPv4 and DHCPv6 clients when it receives ARP or ND packets. *Figure 2* illustrates the receive functionality.

Figure 16: Layer 2 Liveness Detection Receive Behavior Flow



When the BNG receives either of these packets, it does the following:

1. Checks whether Layer 2 liveness detection for subscriber management is enabled globally for the relevant address family, inet or inet6.
2. If Layer 2 liveness detection is not enabled, then the BNG responds as usual to the received packets without checking the state of the client session.
3. If liveness detection is enabled for the family, then the BNG checks whether the client session is still in the bound state.
4. If the client session is bound, the BNG responds to the client with the appropriate ARP or ND packet.
5. If the session is not bound, the BNG drops the received packet. It does not send an ARP or ND response packet to the host, enabling the host to determine that the BNG considers the session to be down.

The usefulness of the receive functionality depends on the ability of the DHCP client host to reclaim resources from the stale client based on the absence of a response packet from the BNG for an unbound client session. If this capability requires a change in the client implementation, you may want to use the send functionality.

Configuring BNG Detection of DHCP Local Server Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 local server liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit system services dhcp-local-server]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit system services dhcp-local-server liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

- For DHCPv4 group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv4 dual-stack-group configuration:

```
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv4 global configuration:

```
[edit system services dhcp-local-server liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 group configuration:

```
[edit system services dhcp-local-server group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 dual-stack-group configuration:

```
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 local server liveness detection:

1. Specify that you want to configure the liveness detection method.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit liveness-detection method
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6 liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv6 global configuration:

```
[edit system services dhcp-local-server dhcpv6 liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv6 group configuration:

```
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

Configuring BNG Detection of DHCP Relay Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the send functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP relay clients.

The send functionality enables the BNG to determine whether a client session is down based on a lack of response from the DHCP client to the ARP or ND request packets it sends to the client.

NOTE: DHCP liveness detection can also be configured using Bidirectional Forwarding Detection (BFD). BFD liveness detection and ARP/ND liveness detection are mutually exclusive.

To configure the send functionality for DHCPv4 relay liveness detection:

1. Specify that you want to configure the liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit liveness-detection method
     ```

   - For DHCPv4 group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit group group-name liveness-detection method
     ```

   - For DHCPv4 dual-stack-group configuration:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# edit dual-stack-group dual-stack-group-name liveness-detection method
     ```

2. Specify the Layer 2 liveness detection method.
   - For DHCPv4 global configuration:

     ```
     [edit forwarding-options dhcp-relay liveness-detection method]
     user@host# set layer2-liveness-detection
     ```

- For DHCPv4 group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv4 dual-stack-group configuration:

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv4 global configuration:

```
[edit forwarding-options dhcp-relay liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 group configuration:

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv4 dual-stack-group configuration:

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-
detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

To configure the send functionality for DHCPv6 relay liveness detection:

1. Specify that you want to configure the liveness detection method.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit liveness-detection method
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# edit group group-name liveness-detection method
```

2. Specify the Layer 2 liveness detection method.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
user@host# set layer2-liveness-detection
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
user@host# set layer2-liveness-detection
```

3. (Optional) Configure the number of retry attempts and the interval timer.

- For DHCPv6 global configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

- For DHCPv6 group configuration:

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
user@host# edit layer2-liveness-detection
user@host# set max-consecutive-retries number
user@host# set transmit-interval seconds
```

Configuring DHCP Host Detection of Client Connectivity with ARP and ND Packets

This procedure shows you how to configure the receive functionality of Layer 2 liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients to check the connectivity of DHCP local server clients.

The receive functionality enables the DHCP client host to determine whether a client session is down based on a lack of response from the BNG to the ARP or ND packets it sends to the BNG. You configure the receive functionality globally for DHCP per address family as an override to the global subscriber management configuration.

Enable Layer 2 liveness detection globally per address family.

- For DHCPv4:

```
[edit system services subscriber-management overrides]
user@host# set interfaces family inet layer2-liveness-detection
```

- For DHCPv6:

```
[edit system services subscriber-management overrides]
user@host# set interfaces family inet6 layer2-liveness-detection
```

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

Release History Table

Release	Description
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.
17.4R1	Starting in Junos OS Release 17.4R1, the use of ARP packets for DHCPv4 and ND packets for DHCPv6 is supported on MX Series routers for Layer 2 liveness detection in addition to BFD liveness detection.

17.4R1	Starting in Junos OS Release 17.4R1, you can configure liveness detection using IPv4 Address Resolution Protocol (ARP) for DHCPv4 clients and IPv6 Neighbor Unreachability Detection for DHCPv6 clients.

RELATED DOCUMENTATION

- DHCP Overview | 2
- IP Address Assignment Pool | 27
- DHCP Server | 49
- DHCP Relay Agent | 156
- DHCPv6 Server | 109
- DHCPv6 Relay Agent | 222

Secure DHCP Message Exchange

IN THIS SECTION

- DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs | 344
- Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances | 345

Junos OS allows you to use the DHCP relay agent to provide secure message exchange between different virtual routing and forwarding instances (VRFs). To enable secure exchange of DHCP messages, you must configure both the server side and the client side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information. For more information, read this topic.

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs

In some service provider networks, the service network in which the DHCP server resides is isolated from the actual subscriber network. This separation of the service and subscriber networks can sometimes introduce potential security issues, such as route leaking.

Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different virtual routing and forwarding instances (VRFs). The DHCP relay agent can ensure that there is no direct routing between the client VRF and the DHCP server VRF, and that only acceptable DHCP packets are relayed across the two VRFs. Subscriber management supports the cross-VRF message exchange for both DHCP and DHCPv6 packets.

To exchange DHCP messages between different VRFs, you must enable both the server-side and the client-side of the DHCP relay agent to recognize and forward acceptable traffic based on DHCP option information in the packets. The message exchange uses the following DHPP options to identify the traffic to be relayed.

- Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets
- Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets

Statistics for DHCP packets using the cross-VRF message exchange are counted in the client VRF.

The following list describe how DHCP relay agent exchanges messages between the DHCP clients and DHCP server in different VRFs:

- Packets from DHCP client to DHCP server—DHCP relay agent receives the DHCP packet from the client in the client VRF, and then inserts the appropriate DHCP option 82 suboption 1 or DHCPv6 option 18 attribute into the packet. The relay agent then forwards the packet to the DHCP server in the server's VRF.
- Packets from DHCP server to DHCP client—DHCP relay agent receives the DHCP reply message from the DHCP server in the server VRF. The relay agent derives the client's interface, including VRF, from the DHCP option 82 suboption 1 or DHCPv6 option 18 attribute in the packet in the DHCP server VRF. The relay agent then forwards the reply message to the DHCP client in the client's VRF.

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances

IN THIS SECTION

- Client-Side Support | 346
- Server-Side Support | 347
- DHCP Local Server Support | 348

Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

You can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing instances. This type of configuration is for a *stateless* DHCP relay connection between a DHCP server and a DHCP client, when the DHCP server resides in a network that must be isolated from the client network.

A stateless DHCP relay agent does not maintain dynamic state information about the DHCP clients and does not maintain a static route for the traffic to flow between the client and server routing instances.

To enable the DHCP message exchange between the two VRFs, you configure each side of the DHCP relay to recognize and forward acceptable traffic based on the DHCP option information in the packets. The acceptable traffic is identified by either the Agent Circuit ID (DHCP option 82 suboption 1) for DHCPv4 packets or the Relay Agent Interface-ID (DHCPv6 option 18) for DHCPv6 packets.

The following list provides an overview of the tasks required to create the DHCP message exchange between the different VRFs:

- Client-side support—Configure the DHCP relay agent `forward-only` statement to specify the VRF location of the DHCP server, to which the DHCP relay agent forwards the client packets with the appropriate DHCP option information. The `forward-only` statement ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations (such as creating dynamic interfaces or maintaining leases).

  You can optionally configure a specific logical system and routing instance for the server VRF. If you do not specify a logical system or routing instance, then DHCP uses the local logical system and routing instance from which the configuration is added.

- Server-side support—Configure the DHCP relay agent `forward-only-replies` statement so the DHCP relay agent forwards the reply packets that have the appropriate DHCP option information. This statement also ensures that DHCP relay agent does not create a new session or perform any other subscriber management operations.

  NOTE: You do not need to configure the `forward-only-replies` statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

- DHCP local server support—Configure the DHCP local server to support option 82 information in DHCP NAK and forcerenew messages. By default, the two message types do not support option 82.
- Additional support—Ensure that the following required support is configured:
  - Proxy ARP support must be enabled on the server-facing interface in the DHCP server VRF so that the DHCP relay agent can receive and respond to the ARP requests for clients and the client-facing interface in the DHCP server VRF.
  - Routes must be available to receive the DHCP packets from the DHCP server in the server VRF for the clients reachable in the client VRF.

The following procedures describe the configuration tasks for creating the DHCP message exchange between the DHCP server and clients in different VRFs.

Client-Side Support

To configure support on the client side of the DHCP relay agent:

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Specify the DHCP server VRF to which the DHCP relay agent forwards the packets from the DHCP client. DHCP relay agent forwards the acceptable packets that have the appropriate DHCP option information, but does not perform any additional subscriber management operations. You can configure the `forward-only` statement globally or for a named group of interfaces, and for DHCPv4 or DHCPv6. You can specify the current, default, or a specific logical system or routing instance for the server VRF.

The following example configures the `forward-only` statement globally for DHCPv4, and specifies the default logical system and routing instance:

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only logical-system default routing-instance default
```

NOTE: For local DHCPv4 clients, the DHCP relay agent adds the Agent Circuit ID option. However, if the Agent Circuit ID option is already present in the packet, you must ensure that the DHCP server supports the option 82 Vendor-Specific Information suboption (suboption 9).

If the `forward-only` statement is configured at the `[edit forwarding-options dhcp-relay relay-option]` hierarchy level, then that relay-option action takes precedence over the configuration of the `forward-only` statement for the DHCP cross-VRF message exchange.

Server-Side Support

To configure the cross-VRF message exchange support on the server side of the DHCP relay:

NOTE: You do not need to configure the `forward-only-replies` statement if the DHCP client and DHCP server reside in the same logical system/routing instance.

1. Enable DHCP relay agent configuration.

```
[edit forwarding-options]
user@host# edit dhcp-relay
```

2. Configure the DHCP relay agent to forward the DHCP packets from the DHCP server VRF to the client. DHCP relay agent only forwards the packets, and does not perform any additional subscriber management operations. You can configure the `forward-only-replies` statement globally for DHCPv4 and DHCPv6.

   The following example configures the `forward-only-replies` statement globally for DHCPv4.

```
[edit forwarding-options dhcp-relay]
user@host# set forward-only-replies
```

DHCP Local Server Support

To configure the DHCP local server to support option 82 information in NAK and forcerenew messages; the cross-VRF message exchange feature uses the option 82 or DHCPv6 option 18 information to determine the client VRF:

1. Enable DHCP local server configuration.

```
[edit system services]
user@host# edit dhcp-local-server
```

2. Specify that you want to configure an override option.

```
[edit system services dhcp-local-server]
user@host# edit overrides
```

3. Configure DHCP local server to override the default behavior and support option 82 information in DHCP NAK and forcerenew messages. You can configure the override action globally, for a group of interfaces, or for a specific interface.

```
[edit system services dhcp-local-server overrides]
user@host# set include-option-82 forcerenew nak
```

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

Release History Table

Release	Description
14.2	Starting in Junos OS Release 14.2, you can use the DHCP relay agent to provide additional security when exchanging DHCP messages between different virtual routing and forwarding instances (VRFs).
14.2	Starting in Junos OS Release 14.2, you can configure DHCP relay agent to provide additional security when exchanging DHCP messages between a DHCP server and DHCP clients that reside in different virtual routing and forwarding instances (VRFs).

RELATED DOCUMENTATION

DHCP Overview | 2

Using DHCP Relay Agent Option 82 Information

DHCP Server | 49

DHCP Relay Agent | 156

DHCP Client | 234

DHCPv6 Server | 109

DHCPv6 Relay Agent | 222

DHCPv6 Client | 255

DHCP Active Server Groups

IN THIS SECTION

- Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups | 349

You can apply a common DHCP or DHCPv6 relay configuration to a set of DHCP server IP addresses configured as a server group. For this, you must configure a group of DHCP server addresses, and apply them as an active server group. For more information, read this topic.

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups

You can apply a common DHCP or DHCPv6 relay configuration to a set of IP addresses configured as a server group. An active server group is sometimes referred to as a trusted group of servers.

You can configure active server groups globally or at the group level (configured with the `group`. When you apply the active server group at the group level, it overrides a global active server group configuration.

To configure a group of DHCP server addresses and apply them as an active server group:

1. Specify the name of the server group.

   - For DHCPv4 servers:

     ```
     [edit forwarding-options dhcp-relay]
     user@host# set server-group server-group-name
     ```

   - For DHCPv6 servers:

     ```
     [edit forwarding-options dhcp-relay dhcpv6]
     user@host# set server-group server-group-name
     ```

2. Add the IP addresses of the DHCP servers belonging to the group.

   ```
   [edit forwarding-options dhcp-relay server-group server-group-name]
   user@host# set ip-address1
   user@host# set ip-address2
   ```

   NOTE: Starting in Junos OS Release 18.4R1, up to 32 server IP addresses are supported per DHCPv4 server group. In earlier releases, a maximum of 5 server IP addresses are supported for DHCPv4 servers. Configuring more than the maximum number of server addresses results in a commit check failure.

3. Apply the server group as an active server group.

   - At global level (DHCPv4)

     ```
     [edit forwarding-options dhcp-relay]
     user@host# set active-server-group server-group-name
     ```

   - At group-level (DHCPv6)

     ```
     [edit forwarding-options dhcp-relay group interface-group-name]
     user@host# set active-server-group server-group-name
     ```

- At global level (DHCPv6)

```
[edit forwarding-options dhcp-relay dhcpv6]
user@host# set active-server-group server-group-name
```

- At group-level (DHCPv6)

```
[edit forwarding-options dhcp-relay dhcpv6 group interface-group-name]
user@host# set active-server-group server-group-name
```

For example, you might want to direct certain DHCP client traffic to a DHCP server. You can configure an interface group for each set of clients, specifying the DHCP relay interfaces for the group. In each of these groups, you specify an active server group to which each client groups traffic is forwarded. After a DHCP server group is created and server IP addresses are added to the group, the device used as the DHCP relay agent can forward messages to specific servers.

- Three groups of DHCP server addresses are configured, Default, Campus-A, and Campus-B.
- The Default group is applied as the global active server group for the overall DHCP relay configuration.
- The Campus-A server group is assigned as the active server group for interface group Campus-A-v10-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-A-v10-DHCP-RELAY is forwarded to DHCP servers 198.51.100.100 and 198.51.100.101.
- The Campus-B server group is assigned as the active server group for interface group Campus-B-v200-DHCP-RELAY. DHCP traffic received on the interfaces in Campus-B-v200-DHCP-RELAY is forwarded to DHCP servers 198.51.100.55 and 198.51.100.56.
- All other DHCP traffic is forwarded to DHCP server 203.0.113.1.

```
[edit forwarding-options dhcp-relay]
#
# Server groups
user@host# set server-group Default 203.0.113.1
user@host# set server-group Campus-A 198.51.100.100
user@host# set server-group Campus-A 198.51.100.101
user@host# set server-group Campus-B 198.51.100.55
user@host# set server-group Campus-B 198.51.100.56
#
# Default server group applied globally.
user@host# set active-server-group Default
```

```
#
# Interface groups with application of active server groups
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.1
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.2
user@host# set group Campus-A-v10-DHCP-RELAY interface ge-1/1/0.3
user@host# set group Campus-A-v10-DHCP-RELAY active-server-group Campus-A
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.4
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/2/0.5
user@host# set group Campus-B-v200-DHCP-RELAY interface ge-2/1/0.6
user@host# set group Campus-B-v200-DHCP-RELAY active-server-group Campus-B
```

Note the following:

- In some configurations, servers in an active server group maintain redundant information about the DHCP clients. If the binding server later becomes inaccessible, the client is unable to renew the lease from that server. When the client attempts to rebind to a server, other servers in the group with the client information can reply with an ACK message. By default, instead of forwarding the ACK to the DHCP client, the relay agent drops any such ACKs that it receives from any server other than the binding server because the new server address does not match the expected server address in the DHCP client entry. Consequently the lease cannot be extended by any of the redundant servers.
- Starting in Junos OS Release 16.2R1, you can enable a DHCPv4 relay agent to forward DHCP request (renew or rebind) ACKs from any server in the active server group (thus, any trusted server). The relay agent updates the client entry with the new server address. Because the servers in the group are expected to mirror the client information exactly, the lease option is expected to be the same as for the original server and the relay agent does not need to verify the lease option.
- Starting in Junos OS Release 18.4R1, this capability is extended to allow a DHCP relay agent to forward DHCP information request (DHCPINFORM) ACK messages from any server in the active server group.

To enable ACK forwarding from any server in the active server group:

- Enable forwarding for the active server group.

```
[edit forwarding-options dhcp-relay active-server-group]
user@host# set allow-server-change
```

Release History Table

Release	Description
18.4R1	Starting in Junos OS Release 18.4R1

16.2R1	Starting in Junos OS Release 16.2R1

RELATED DOCUMENTATION

- Group-Specific DHCP Configurations | 283
- DHCP Overview | 2
- IP Address Assignment Pool | 27
- DHCP Server | 49
- DHCP Relay Agent | 156
- DHCPv6 Server | 109
- DHCPv6 Relay Agent | 222

Suppressing DHCP Routes

IN THIS SECTION

- Suppressing DHCP Access, Access-Internal, and Destination Routes | 353
- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default | 354

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. However, you can override the default behavior and prevent DHCP from automatically installing the route information. For more information, read this topic.

Suppressing DHCP Access, Access-Internal, and Destination Routes

During the DHCP client binding operation, the DHCP process adds route information for the DHCP sessions by default. The DHCP process adds the following routes:

- DHCPv4 sessions—access-internal and destination routes.
- DHCPv6 sessions—access-internal and access routes.

An access route represents a network behind an attached video services router, and is set to a preference of 13.

An access internal route is a /32 route that represents a directly attached end user, and is set to a preference of 12.

These routes are used by the DHCP application on a video services router to represent either the end users or the networks behind the attached video services router.

In some scenarios, you might want to override the default behavior and prevent DHCP from automatically installing the route information.

For example, DHCP relay installs destination (host) routes by default—this action is required in certain configurations to enable address renewals from the DHCP server to work properly. However, the default installation of destination routes might cause a conflict when you configure DHCP relay with static subscriber interfaces.

To avoid such configuration conflicts you can override the default behavior and prevent DHCP relay from installing the routes.

Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default

You can use the route suppression option to override the default route installation behavior. You can configure route suppression and prevent DHCP from installing specific types of routes for:

- DHCP local server and DHCP relay agent
- DHCPv4 and DHCPv6 sessions
- Globally or for named interface groups

For DHCPv4 you can override the installation of destination routes only or access-internal routes (the access-internal option prevents installation of both destination and access-internal routes). For DHCPv6 you can specify access routes, access-internal routes, or both.

Example:

- For DHCP local server route suppression (for example, a global configuration):

```
[edit system services dhcp-local-server]
user@host# set route-suppression access-internal
```

- For DHCP relay (for example, a group-specific configuration):

```
[edit forwarding-options dhcp-relay group southeast]
user@host# set route-suppression destination
```

- For DHCPv6 local server (for example, a group-specific configuration):

```
[edit system services dhcp-local-server group southern3]
user@host# set dhcpv6 route-suppression access access-internal
```

- For DHCPv6 relay (for example, a global configuration):

```
[edit forwarding-options dhcp-relay]
user@host# set dhcpv6 route-suppression access
```

Note the following while configuring route suppression option:

- You cannot suppress access-internal routes when the subscriber is configured with both IA_NA and IA_PD addresses over IP demux interfaces—the IA_PD route relies on the IA_NA route for next hop connectivity.
- The `no-arp` statement supported in legacy DHCP is replaced by the `route-suppression` statement.

RELATED DOCUMENTATION

DHCP Server | 49

DHCP Client | 234

DHCP Relay Agent | 156

DHCP Overview | 2

CHAPTER 8

Configuration Statements

access-profile | 363

active-server-group | 365

address-assignment (Address-Assignment Pools) | 367

address-pool | 370

address-pool (Access) | 372

allow-no-end-option (DHCP Relay Agent) | 374

allow-snooped-clients | 376

always-write-giaddr | 378

always-write-option-82 | 380

always-write-option-82 | 382

apply-secondary-as-giaddr | 383

attempts (DHCP Local Server) | 385

authentication (DHCP Local Server) | 388

authentication (DHCP Relay Agent) | 390

authentication-order (Access Profile) | 392

authentication-server | 394

bfd | 396

boot-server (DHCP) | 398

circuit-id (DHCP Relay Agent) | 399

circuit-type | 403

circuit-type (DHCP Local Server) | 405

circuit-type (DHCP Relay Agent) | 407

classification-key (DHCP Local Server) | 408

classification-key (DHCP Relay Agent) | 410

clear-on-abort (DHCP Local Server) | 413

client-discover-match (DHCP Local Server) | 416

client-ia-type | 418

client-id (DHCP Local Server) | 420

client-id (DHCP Relay Agent) | 422

client-identifier (DHCP Client) | 424

client-identifier (DHCPv6 Client) | 426

client-type | 428

delegated-pool (DHCP Local Server) | 430

delimiter (DHCP Local Server) | 432

delimiter (DHCP Relay Agent) | 434

detection-time | 437

dhcp | 439

dhcp (DHCP Client) | 441

dhcp-attributes (Access IPv4 Address Pools) | 444

dhcp-attributes (Access IPv6 Address Pools) | 446

dhcp-client | 449

dhcp-local-server | 451

dhcp-local-server (System Services) | 464

dhcp-relay | 470

dhcp-service | 486

dhcpv6 (DHCP Local Server) | 489

dhcpv6 (DHCP Relay Agent) | 496

dhcpv6 (System Services) | 504

dhcpv6-client | 510

disable-relay | 512

domain (Domain Map) | 514

domain-name (DHCP) | 516

domain-name (DHCP Local Server) | 517

domain-name (DHCP Relay Agent) | 520

domain-name-server (Routing Instances and Access Profiles) | 522

domain-name-server-inet (Routing Instances and Access Profiles) | 524

domain-name-server-inet6 (Routing Instances and Access Profiles) | 526

domain-search | 528

drop (DHCP Relay Agent Option) | 529

dual-stack (DHCP Local Server Overrides) | 531

dual-stack (DHCP Relay Agent Overrides) | 533

dual-stack-group (DHCP Local Server) | 535

dual-stack-group (DHCP Relay Agent) | 537

dual-stack-interface-client-limit (DHCP Local Server and Relay Agent) | 541

dynamic-pool | 543

dynamic-profile (DHCP Local Server) | 545

dynamic-profile (DHCP Relay Agent) | 547

dynamic-server | 549

excluded-address (Address-Assignment Pools) | 551

excluded-address (Address-Assignment Pools) | 552

external-authority | 554

failure-action | 556

force-discover (DHCP Client) | 558

forward-only (DHCP Relay Agent) | 559

forward-snooped-clients (DHCP Local Server) | 562

forward-snooped-clients (DHCP Relay Agent) | 563

group (DHCP Local Server) | 566

group (DHCP Relay Agent) | 571

group (System Services DHCP) | 578

holddown-interval | 582

host-name (DHCP Relay Agent) | 584

include-irb-and-l2 | 585

interface (DHCP Local Server) | 589

interface (DHCP Relay Agent) | 592

interface (System Services DHCP) | 595

interface-client-limit (DHCP Local Server) | 597

interface-client-limit (DHCP Relay Agent) | 599

interface-delete (Subscriber Management or DHCP Client Management) | 602

interface-name (DHCP Local Server) | 604

interface-traceoptions (System Services DHCP) | 605

ip-address-first | 608

keep-incoming-circuit-id (DHCP Relay Agent) | 610

keep-incoming-remote-id (DHCP Relay Agent) | 611

layer2-liveness-detection (Send) | 613

layer2-unicast-replies | 616

lease-time | 618

lease-time (dhcp-client) | 620

liveness-detection | 621

local-server-group (DHCP Relay Agent Option) | 624

location (DHCP Relay Agent) | 626

log | 627

logical-system-name (DHCP Local Server) | 630

mac-address (DHCP Local Server) | 631

mac-address (DHCP Relay Agent) | 633

maximum-hop-count | 635

maximum-lease-time (DHCP) | 637

method | 638

minimum-interval | 640

minimum-receive-interval | 643

minimum-wait-time | 645

multiplier | 646

name-server (Access) | 648

name-server (System Services) | 650

next-server | 652

no-adaptation | 653

no-allow-snooped-clients | 655

no-bind-on-request (DHCP Relay Agent) | 657

no-listen | 659

no-vlan-interface-name | 660

on-demand-address-allocation | 663

option (DHCP server) | 665

option-60 (DHCP Local Server) | 667

option-60 (DHCP Relay Agent) | 669

option-82 (DHCP Local Server Authentication) | 672

option-82 (DHCP Local Server Pool Matching) | 674

option-82 (DHCP Relay Agent) | 675

option-number (DHCP Relay Agent Option) | 677

overrides (DHCP Local Server) | 679

overrides (DHCP Relay Agent) | 683

overrides (DHCP Relay Agent) | 686

overrides (System Services DHCP) | 688

password (DHCP Local Server) | 690

password (DHCP Relay Agent) | 693

pool (DHCP Local Server Overrides) | 695

pool (System) | 698

pool-match-order | 700

preferred-prefix-length | 702

prefix (DHCP Client) | 703

prefix (DHCP Relay Agent) | 704

process-inform | 707

profile (Access) | 709

protocol-master | 717

proxy-mode | 720

radius-disconnect (DHCP Local Server) | 722

rapid-commit (DHCPv6 Client) | 724

rapid-commit (DHCPv6 Local Server) | 725

reauthenticate (DHCP Local Server) | 727

reconfigure (DHCP Local Server) | 730

reconfigure (DHCP Local Server) | 732

relay-agent-interface-id (DHCP Local Server) | 735

relay-agent-interface-id (DHCPv6 Relay Agent) | 737

relay-agent-option-79 | 739

relay-agent-remote-id (DHCP Local Server) | 741

relay-agent-remote-id (DHCPv6 Relay Agent Username) | 743

relay-option (DHCP Relay Agent) | 745

relay-option-82 | 747

relay-server-group (DHCP Relay Agent Option) | 750

remote-id (DHCP Relay Agent) | 752

replace-ip-source-with (DHCP Relay Agent) | 755

replace-ip-source-with (DHCP Relay Agent) | 756

req-option | 758

retransmission-attempt (DHCP Client) | 760

retransmission-attempt (DHCP Client) | 762

retransmission-attempt (DHCPv6 Client) | 764

retransmission-interval (DHCP Client) | 765

retransmission-interval (DHCP Client) | 767

retransmission-interval (DHCP Client) | 769

route-suppression (DHCP Local Server and Relay Agent) | 771

routing-instance-name (DHCP Local Server) | 773

routing-instance-name (DHCP Relay Agent) | 775

send-release-on-delete (DHCP Relay Agent) | 777

server-address | 779

server-address (dhcp-client) | 781

server-group | 783

server-identifier | 785

service-profile (DHCP Local Server) | 787

service-profile (DHCP Relay Agent) | 789

services (System Services) | 791

session-mode | 799

short-cycle-protection (DHCP Local Server and Relay Agent) | 801

source-address-giaddr | 803

source-ip-change (Forwarding Options) | 805

static-binding | 806

strict (DHCP Local Server) | 808

sub-prefix-length | 810

threshold (detection-time) | 812

threshold (transmit-interval) | 814

timeout (DHCP Local Server) | 816

token (DHCP Local Server) | 818

trace (DHCP Relay Agent) | 820

traceoptions (Address-Assignment Pool) | 822

traceoptions (DHCP) | 825

traceoptions (DHCP Server) | 828

transmit-interval | 832

trigger (DHCP Local Server) | 834

trust-option-82 | 836

update-router-advertisement | 838

update-server | 839

update-server (dhcp-client) | 841

update-server (dhcpv6-client) | 842

use-interface | 843

use-interface-description | 844

use-primary (DHCP Local Server) | 847

use-primary (DHCP Relay Agent) | 849

use-vlan-id | 852

use-vlan-id (DHCP Relay Agent) | 854

user-defined-option-82 | 856

user-id | 858

user-prefix (DHCP Local Server) | 859

username-include (DHCP Local Server) | 862

username-include (DHCP Relay Agent) | 864

vendor-id | 867

vendor-option | 869

vendor-option | 871

version (BFD) | 873

wins-server (System) | 875

access-profile

IN THIS SECTION

- Syntax | 363
- Hierarchy Level | 363
- Description | 364
- Options | 364
- Required Privilege Level | 364
- Release Information | 364

Syntax

```
access-profile profile-name;
```

Hierarchy Level

```
[edit],
[edit forwarding-options dhcp-relay]
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name]
[edit forwarding-options dhcp-relay dhcpv6]
[edit forwarding-options dhcp-relay dhcpv6 group group-name]
[edit logical-systems logical-system-name routing-instances routing-instance-name]
[edit interfaces interface-name auto-configure vlan-ranges],
[edit interfaces interface-name auto-configure stacked-vlan-ranges],
[edit routing-instances routing-instances-name]
[edit system services dhcp-local-server]
[edit system services dhcp-local-server group group-name]
[edit system services dhcp-local-server dhcpv6]
```

```
[edit system services dhcp-local-server dhcpv6 group group-name]
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name]
```

Description

After you have created the access profile that specifies authentication and accounting parameters, you must specify where the profile is used. Authentication and accounting will not run unless you specify the profile. You can attach access profiles globally at the `[edit]` hierarchy level, or you can apply them to DHCP clients or subscribers, VLANs, or to a routing instance.

Options

profile-name—Name of the access profile that you configured at the `[edit access profile name]` hierarchy level.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

- *RADIUS Servers and Parameters for Subscriber Access*
- *Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution*
- *Configuring Access Components for the PPPoE Wholesale Network Solution*

active-server-group

IN THIS SECTION

- Syntax | 365
- Hierarchy Level | 365
- Description | 366
- Options | 366
- Required Privilege Level | 366
- Release Information | 367

Syntax

```
active-server-group server-group-name <allow-server-change>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[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 dhcpv6],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relaygroup 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 dhcpv6],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name],
```

```
[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 dhcpv6],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name]
```

Description

Apply a DHCP relay agent configuration to the named group of DHCP server addresses. The server group itself is configured with the `server-group` statement. You can apply an active server group globally or for specific groups of interfaces, configured with the `group` statement. An active server group applied to an interface group overrides a global configuration.

Options

allow-server-change (Optional) (DHCPv4 only) Enable the relay agent to accept and forward a DHCP request (renew or rebind) ACK message to the client from any DHCP local server in the active server group. Starting in Junos OS Release 18.4R1, this option also applies to DHCP information request (DHCPINFORM) ACK messages.

- **Default:** Forward ACK messages from only the original binding server.

server-group-name Name of the group of DHCP or DHCPv6 server addresses to which the DHCP or DHCPv6 relay agent configuration applies.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

`allow-server-change` option added in Junos OS Release 16.2R1.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- *Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups*
- *Configuring Group-Specific DHCP Relay Options*

address-assignment (Address-Assignment Pools)

IN THIS SECTION

- Syntax | **367**
- Hierarchy Level | **368**
- Description | **368**
- Options | **369**
- Required Privilege Level | **370**
- Release Information | **370**

Syntax

```
address-assignment {
    abated-utilization percentage;
    abated-utilization-v6 percentage;
    high-utilization percentage;
```

```
    high-utilization-v6 percentage;
    neighbor-discovery-router-advertisement ndra-pool-name;
    pool pool-name {
        active-drain;
        family family {
            dhcp-attributes {
                protocol-specific attributes;
            }
            excluded-address ip-address;
            excluded-range name low minimum-value high maximum-value;
            host hostname {
                hardware-address mac-address;
                ip-address ip-address;
            }
            network ip-prefix/<prefix-length>;
            prefix ipv6-prefix;
            range range-name {
                high upper-limit;
                low lower-limit;
                prefix-length prefix-length;
            }
        }
        hold-down;
        link pool-name;
    }
}
```

Hierarchy Level

```
[edit access]
```

Description

Configure address-assignment pools that can be used by different client applications.

NOTE: Support for subordinate statements is platform-specific. See individual statement topics for support information.

Options

abated-utilization (ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCP address pools or linked set of address pools. No SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

- **Values:** *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

abated-utilization-v6 (ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate SNMP traps for DHCPv6 address pools or linked set of address pools. No SNMP traps are generated unless a value is configured. Default: Abated utilization is not set. Delete the abated-utilization value to unset.

- **Values:** *percentage*—Threshold below which an SNMP trap clear is generated. Range: 1 through 98.

high-utilization (ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCP address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

- **Values:** *percentage*—Percentage used to generate a trap. Range: 2 through 99.

high-utilization-v6 (ACX Series, MX Series only) Starting in Junos OS Release 11.2, generate an SNMP trap when the DHCPv6 address pool or linked set of address pools use surpasses the specified percentage. Default: High utilization is not set. Delete the high-utilization value to unset.

- **Values:** *percentage*—Percentage used to generate a trap. Range: 2 through 99.

neighbor-discovery-router-advertisement (M Series, MX Series, SRX Series, T Series only) Configure the name of the address-assignment pool used to assign the router advertisement prefix.

- **Values:** *ndra-pool-name*—Name of the address-assignment pool.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

- Address-Assignment Pools Overview
- Address-Assignment Pool Configuration Overview
- Configuring an Address-Assignment Pool for L2TP LNS with Inline Services
- Configuring Address-Assignment Pool Usage Threshold Traps
- Configuring an Address-Assignment Pool Used for Router Advertisements

address-pool

IN THIS SECTION

- Syntax | 371
- Hierarchy Level | 371
- Description | 371
- Options | 371
- Required Privilege Level | 372

Release Information | 372

Syntax

```
address-pool pool-name {
    address address-or-prefix;
    address-range <low lower-limit> <high upper-limit>;
}
```

Hierarchy Level

```
[edit access]
```

Description

Allocate IP addresses for clients.

NOTE: This statement is not supported for L2TP LNS on MX Series routers.

Options

pool-name Name assigned to an address pool.

address (EX Series, M Series, PTX Series, T Series only) Configure the IP address or prefix value for clients.

- **Values:** *address-or-prefix*—An address or prefix value.

address-range Configure the address range.

- Values:
  - high *upper-limit*—Upper limit of an address range.
  - low *lower-limit*—Lower limit of an address range.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring the Address Pool for L2TP Network Server IP Address Allocation

address-pool (Access)

IN THIS SECTION

- Syntax | 373
- Hierarchy Level | 373
- Description | 373
- Options | 373
- Required Privilege Level | 374
- Release Information | 374

Syntax

```
address-pool pool-name {
    address address or address prefix;
    address-range {
        high upper-limit;
        low lower-limit;
        mask network-mask;
    }
    primary-dns IP address;
    primary-wins IP address;
    secondary-dns IP address;
    secondary-wins IP address;
}
```

Hierarchy Level

```
[edit access]
```

Description

Create an address-pool for L2TP clients.

Options

- `pool-name`—Name assigned to the address-pool.
- `address`—Configure subnet information for the address-pool.
- `address-range`—Defines the address range available for clients.
- `primary-dns`—Specify the primary-dns IP address.
- `secondary-dns`—Specify the secondary-dns IP address.

- `primary-wins`—Specify the primary-wins IP address.
- `secondary-wins`—Specify the secondary-wins IP address.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

access-control

allow-no-end-option (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 375
- Hierarchy Level | 375
- Description | 375
- Required Privilege Level | 375
- Release Information | 375

Syntax

```
allow-no-end-option;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ...]
```

Description

Enable a DHCP relay agent to process packets sent from clients without DHCP Option-255 (end-of-options).

The default behavior in Junos OS is to drop packets that do not include Option 255. To override this default behavior, configure the `allow-no-end-option` CLI statement at the `[edit forwarding-options dhcp-relay overrides]` hierarchy level.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 14.1X53.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Overriding the Default DHCP Relay Configuration Settings

DHCP Snooping Support | 288

allow-snooped-clients

IN THIS SECTION

- Syntax | 376
- Hierarchy Level | 376
- Description | 377
- Default | 377
- Required Privilege Level | 377
- Release Information | 377

Syntax

```
allow-snooped-clients;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[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 ...]
```

Description

Explicitly enable DHCP snooping support on the DHCP relay agent.

Use the statement at the `[edit ... dhcpv6]` hierarchy levels to explicitly enable snooping support on the router for DHCPv6 relay agent.

Default

DHCP snooping is disabled by default.

NOTE: On EX4300 and EX9200 switches, the `allow-snooped-clients` statement is enabled by default at the `[edit forwarding-options dhcp-relay overrides]` hierarchy level.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.2.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- *Overriding the Default DHCP Relay Configuration Settings*
- DHCP Snooping Support
- Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

always-write-giaddr

IN THIS SECTION

- Syntax | 378
- Hierarchy Level | 378
- Description | 379
- Required Privilege Level | 379
- Release Information | 379

Syntax

```
always-write-giaddr;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

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.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

dhcp-relay | 470

always-write-option-82

IN THIS SECTION

- Syntax | 380
- Hierarchy Level | 380
- Description | 381
- Required Privilege Level | 381
- Release Information | 381

Syntax

```
always-write-option-82;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

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:

- 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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

Extended DHCP Relay Agent Overview

always-write-option-82

IN THIS SECTION

- Syntax | 382
- Hierarchy Level | 382
- Description | 382
- Required Privilege Level | 383
- Release Information | 383

Syntax

```
always-write-option-82 {
    apply-groups;
        apply-groups-except;
    }
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides]
```

Description

Override the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server. Using this option allows 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 the DHCP packets, the DHCP relay agent 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, the DHCP relay agent 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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

RELATED DOCUMENTATION

replace-ip-source-with (DHCP Relay Agent) | 755

overrides (DHCP Relay Agent) | 686

apply-secondary-as-giaddr

IN THIS SECTION

- Syntax | 384
- Hierarchy Level | 384
- Description | 384
- Required Privilege Level | 385
- Release Information | 385

Syntax

```
apply-secondary-as-giaddr;
```

Hierarchy Level

For platforms without ELS:

```
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface]
```

For platforms with ELS:

```
[edit forwarding-options dhcp-relay overrides]
[edit forwarding-options dhcp-relay group name interface name overrides]
```

Description

Configures the interfaces on a switch that are DHCP relay agents to be enabled for smart DHCP relay. Smart DHCP relay enables you to configure alternative IP addresses for the gateway interface so that if the server fails to reply to the requests sent from the primary gateway address, the switch can resend the requests using the alternative gateway addresses. To use this feature, you must configure an IRB interface or Layer 3 subinterface with multiple IP addresses and configure that interface to be a relay agent. This feature is not supported for EVPN-VXLAN deployments.

Depending on where you configure this statement, it enables smart relay on all the interfaces that are relay agents or on specific interfaces. To enable smart relay on all the interfaces that are relay agents, configure this statement at the following locations:

- Junos OS with ELS: configure it under `edit forwarding-options dhcp-relay overrides`.
- Junos OS without ELS: configure it directly under the **bootp** statement.

To enable smart relay on specific interfaces that are relay agents, configure this statement at the following locations:

- Junos OS with ELS: configure it under `edit forwarding-options dhcp-relay group` *name* `interface` *name* `overrides`.
- Junos OS without ELS: configure it directly under the **interface** statement.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 14.1X53-D26.

RELATED DOCUMENTATION

Configuring DHCP and BOOTP Relay | 194

attempts (DHCP Local Server)

IN THIS SECTION

- Syntax | 386
- Hierarchy Level | 386
- Description | 387
- Options | 387
- Required Privilege Level | 387
- Release Information | 387

Syntax

```
attempts attempt-count;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

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

attempt-count—Maximum number of attempts.

- **Range:** 1 through 10
- **Default:** 8

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the `[edit ... dhcpv6 ...]` hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

> *Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview*
>
> *Configuring Dynamic Reconfiguration Attempts for DHCP Clients*

authentication (DHCP Local Server)

IN THIS SECTION

- Syntax | 388
- Hierarchy Level | 389
- Description | 389
- Required Privilege Level | 389
- Release Information | 389

Syntax

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name ;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
    }
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[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 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 ...]
```

Description

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

authentication (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 390
- Hierarchy Level | 391
- Description | 391
- Required Privilege Level | 391
- Release Information | 391

Syntax

```
authentication {
    password password-string;
    username-include {
        circuit-type;
        client-id;
        delimiter delimiter-character;
        domain-name domain-name-string;
        interface-description  (device-interface | logical-interface);
        interface-name;
        logical-system-name;
        mac-address;
        option-60;
        option-82 <circuit-id> <remote-id>;
        relay-agent-interface-id;
        relay-agent-remote-id;
        relay-agent-subscriber-id;
        routing-instance-name;
        user-prefix user-prefix-string;
        vlan-tags;
    }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay 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 ...]
```

Description

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group dual-stack-group-name]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

dhcp-relay | 470

Specifying Authentication Support

authentication-order (Access Profile)

IN THIS SECTION

- Syntax | 392
- Hierarchy Level | 392
- Description | 393
- Default | 393
- Options | 393
- Required Privilege Level | 394
- Release Information | 394

Syntax

```
authentication-order [(none | ldap | password | radius | s6a | secureid)];
```

Hierarchy Level

```
[edit access profile profile-name]
```

Description

Configure the order of authentication, authorization, and accounting (AAA) methods to use while sending authentication messages.

Default

Not enabled

Options

`none`—No authentication for specified users.

When you enable `none` authentication option, the SRX Series device no longer requires the RADIUS server to authenticate the initiator again with the common shared password used for IKEv2 configuration payload. This is because, the SRX Series device already authenticates the remote peer using a certificated-based authentication. You can use this AAA profile in different combinations, but ensure that it is not used where you do not use a pre-authentication.

For example: Consider a scenario, where to establish a connection from a client to secure gateway IPsec tunnels, client is authenticated using certificates method as per IKE protocol. For simplicity, if you do not prefer dependency on RADIUS server and use local pool for address acquisition without any additional authentication, you can configure the “aaa” profile in IKE gateway hierarchy and set the `authentication-order` value as `none` in the access profile, as follows:

```
set access profile profile-name authentication-order none
set security ike gateway gateway name aaa access-profile profile-name
```

`ldap`—Light weight directory access protocol.

`password`—Locally configured password in access profile.

`radius`—RADIUS authentication.

`s6a`—S6a authentication

`securid`—RSA Secure ID authentication.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

`none` option introduced in Junos OS Release 20.3R1.

RELATED DOCUMENTATION

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch
- Configuring 802.1X RADIUS Accounting (CLI Procedure)

authentication-server

IN THIS SECTION

- Syntax | 395
- Hierarchy Level | 395
- Description | 395
- Options | 395
- Required Privilege Level | 395
- Release Information | 395

Syntax

```
authentication-server [server-addresses];
```

Hierarchy Level

```
[edit access                profile                profile-name                radius]
```

Description

Configure the RADIUS server for authentication. To configure multiple RADIUS servers, include multiple server addresses. The servers are tried in order and in a round-robin fashion until a valid response is received from one of the servers or until all the configured retry limits are reached.

Options

server-addresses—Configure one or more RADIUS server addresses.

Required Privilege Level

admin—To view this statement in the configuration.
admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

Statement introduced in Junos OS Release 14.1X53-D20 for OCX Series switches.

RELATED DOCUMENTATION

- Example: Connecting a RADIUS Server for 802.1X to an EX Series Switch
- show network-access aaa statistics authentication

bfd

IN THIS SECTION

- Syntax | 396
- Hierarchy Level | 397
- Description | 397
- Required Privilege Level | 397
- Release Information | 397

Syntax

```
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;
}
```

Hierarchy Level

```
[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 group-name liveness-detection method],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method],
[edit forwarding-options dhcp-relay group group-name liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method]
```

Description

Configure Bidirectional Forwarding Detection (BFD) as the liveness detection method.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

boot-server (DHCP)

IN THIS SECTION

- Syntax | 398
- Hierarchy Level | 398
- Description | 398
- Options | 399
- Required Privilege Level | 399
- Release Information | 399

Syntax

```
boot-server (address | hostname);
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

Configure the name of the boot server advertised to DHCP clients. The client uses a boot file located on the boot server to complete DHCP setup.

Options

- *address*—IP address of a DHCP boot server.
- *hostname*—Hostname of a DHCP boot server.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

boot-file

circuit-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 400
- Hierarchy Level | 400
- Description | 400
- Required Privilege Level | 402
- Release Information | 402

Syntax

```
circuit-id {
    include-irb-and-l2;
    keep-incoming-circuit-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-option-82]
```

Description

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.

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

`include-irb-and-l2` , `no-vlan-interface-name`, and `use-vlan-id` options added in Junos OS Release 14.1.

Release History Table

Release	Description
21.2R1	Starting with Junos OS Release 21.2R1, QFX Series switches support the circuit-id CLI statement in a stateless DHCP relay configuration. You can configure stateless DHCP relay using the forward-only CLI statement at the [edit forwarding-options dhcp-relay] hierarchy level.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

Configuring Option 82 Information

circuit-type

IN THIS SECTION

- Syntax | 403
- Hierarchy Level | 404
- Description | 404
- Required Privilege Level | 404
- Release Information | 404

Syntax

```
circuit-type;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name  routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[edit system services dhcp-local-server authenticationusername-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

Description

Specify that the circuit type is concatenated with the username during the subscriber authentication process.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

circuit-type (DHCP Local Server)

IN THIS SECTION

- Syntax | 405
- Hierarchy Level | 405
- Description | 406
- Required Privilege Level | 406
- Release Information | 406

Syntax

```
circuit-type;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[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]
```

Description

Specify that the circuit type is concatenated with the username during the subscriber authentication or client authentication process.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

circuit-type (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 407
- Hierarchy Level | 407
- Description | 408
- Required Privilege Level | 408
- Release Information | 408

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 group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-
include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[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 ...]
```

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.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *`dual-stack-group-name`*`]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

classification-key (DHCP Local Server)

IN THIS SECTION

- Syntax | 409
- Hierarchy Level | 409

- Description | 409
- Options | 410
- Required Privilege Level | 410
- Release Information | 410

Syntax

```
classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
}
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group
dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-
name ],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-
name ],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name ]
```

Description

Different mechanisms to identify a single household.

Options

circuit-id	Circuit-id as key.
mac-address	MAC address of client.
remote-id	Remote-id as key.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.3.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

classification-key (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **411**
- Hierarchy Level | **411**
- Description | **412**
- Options | **412**
- Required Privilege Level | **413**

- Release Information | 413

Syntax

```
classification-key {
    circuit-id circuit-id;
    mac-address mac-address;
    remote-id remote-id;
}
```

Hierarchy Level

[edit bridge-domains *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit bridge-domains *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* bridge-domains *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* bridge-domains *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name routing-instances name* bridge-domains *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name routing-instances name* bridge-domains *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name routing-instances name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name routing-instances name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name routing-instances name* system services dhcp-local-server dual-stack-group *dual-stack-group-name*],

```
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dhcpv6
group name ddual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay dual-
stack-group dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-
name ],
[edit logical-systems name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-
group dual-stack-group-name ],
[edit logical-systems name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-
group-name ],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name
dual-stack-group dual-stack-group-name ],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay dual-stack-group
dual-stack-group-name ],
[edit routing-instances name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group ],
[edit routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-
name ],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-
name ],
[edit routing-instances name vlans name forwarding-options dhcp-relay dhcpv6 group name dual-
stack-group dual-stack-group-name ],
[edit routing-instances name vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-
group-name ],
[edit system services dhcp dhcp-local-server dual-stack-group dual-stack-group-name ],
[edit vlans name forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-
group-name ],
[edit vlans name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ]
```

Description

Different mechanisms to identify a single household.

Options

circuit-id	Circuit-id as key
mac-address	MAC address of client

remote-id	Remote-id as key

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.3.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

clear-on-abort (DHCP Local Server)

IN THIS SECTION

- Syntax | **414**
- Hierarchy Level | **414**
- Description | **415**
- Default | **415**
- Required Privilege Level | **415**
- Release Information | **415**

Syntax

```
clear-on-abort;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the `[edit ... dhcpv6 ...]` hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Configuring Deletion of the Client When Dynamic Reconfiguration Fails

client-discover-match (DHCP Local Server)

IN THIS SECTION

- Syntax | 416
- Hierarchy Level | 416
- Description | 417
- Default | 417
- Options | 417
- Required Privilege Level | 417
- Release Information | 417

Syntax

```
client-discover-match <option60-and-option82 | incoming-interface>;
```

Hierarchy Level

```
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server group group-name interface interface-name overrides]
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server ... overrides],
[edit logical-systems logical-system-name system services dhcp-local-server ...overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server ...overrides]
```

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.

Default

By default, DHCP uses the `option60-and-option82` option.

Options

`incoming-interface` (Optional) 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.

> **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.

`option60-and-option82` (Optional) Use option 60 and option 82 information to identify subscribers.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.4.

`incoming-interface` option added in Junos OS Release 13.3.

RELATED DOCUMENTATION

- *Understanding Differences Between Legacy DHCP and Extended DHCP*
- *Overriding the Default DHCP Local Server Configuration Settings*
- *DHCP Auto Logout Overview*
- *Allowing Only One DHCP Client Per Interface*

client-ia-type

IN THIS SECTION

- Syntax | **418**
- Hierarchy Level | **419**
- Description | **419**
- Options | **419**
- Required Privilege Level | **419**
- Release Information | **419**

Syntax

```
client-ia-type {
    ia-na;
    ia-pd;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client]
```

Description

Configure the DHCPv6 client identity association type.

Options

ia-na Identity association for nontemporary address

ia-pd Identity association for prefix delegation

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

DHCPv6 Client Overview | 256

client-id (DHCP Local Server)

IN THIS SECTION

- Syntax | 420
- Hierarchy Level | 420
- Description | 421
- Options | 421
- Required Privilege Level | 422
- Release Information | 422

Syntax

```
client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  group group-
name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication username-include],
[edit system services dhcp-local-server dhcp authentication username-include],
[edit system services dhcp-local-server dhcp group group-name 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 dual-stack-group <group-name> authentication username-
include]
```

Description

Specify that the client identifier (DHCP option 61) is concatenated with the username during the subscriber authentication or client authentication process.

Options

exclude-headers

By default, all headers that are part of the client identifier format in option 61 are included in the username string used for RADIUS authentication. Configure the `exclude-headers` option to exclude the use of headers in the username string.

use-automatic-ascii-hex-encoding

By default, all components of the client identifier are converted to ASCII hex to encode the username. Configure the `use-automatic-ascii-hex-encoding` option to use ASCII hex encoding only if there are non-ASCII characters in the client identifier.

Use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.6.

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients

client-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 422
- Hierarchy Level | 423
- Description | 423
- Options | 423
- Required Privilege Level | 423
- Release Information | 424

Syntax

```
client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...]
```

Description

Specify that the client identifier (DHCP option 61) is concatenated with the username during the subscriber authentication or client authentication process.

Options

exclude-headers

By default, all headers that are part of the client identifier format in option 61 are included in the username string used for RADIUS authentication. Configure the `exclude-headers` option to exclude the use of headers in the username string.

use-automatic-ascii-hex-encoding

By default, all components of the client identifier are converted to ASCII hex to encode the username. Configure the `use-automatic-ascii-hex-encoding` option to use ASCII hex encoding only if there are non-ASCII characters in the client identifier.

Use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

client-identifier (DHCP Client)

IN THIS SECTION

- Syntax | **424**
- Hierarchy Level | **425**
- Description | **425**
- Options | **425**
- Required Privilege Level | **426**
- Release Information | **426**

Syntax

```
client-identifier {
    hardware-type type-number
    user-id {ascii ascii hexadecimal hexadecimal;
    use-interface-description {logical |device};
```

```
    prefix [host-name routing-instance-name];
}
```

Hierarchy Level

```
[edit interfaces name unit name family
inet dhcp],
[edit interfaces interface-range name unit
name family inet dhcp],
```

Description

The DHCP server identifies a client by a client-identifier value.

Options

hardware-type Specify the type of hardware used for the interface on which the client access. Ethernet is the common hardware type and the value for Ethernet is 1.

- **Default:** Zero
- **Range:** Zero through 255

ascii Client identifier as an ASCII string

hexadecimal Client identifier as a hexadecimal string

prefix Add prefix to client-id option

- Values:
  - host-name—Add router host name to client-id option
  - logical-system-name—Add logical system name to client-id option
  - routing-instance-name—Add routing instance name to client-id option

use-interface-description Use the interface description

- Values:
  - device—Use the device interface description
  - logical—Use the logical interface description

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

The option `hardware-type` is added in Junos OS Release 20.2R1.

RELATED DOCUMENTATION

DHCPv6 Client Overview | 256

client-identifier (DHCPv6 Client)

IN THIS SECTION

Syntax | 427

- Hierarchy Level | 427
- Description | 427
- Options | 427
- Required Privilege Level | 428
- Release Information | 428

Syntax

```
client-identifier duid-type (duid-ll | duid-llt | vendor);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client]
```

Description

The DHCPv6 server identifies a client by a client-identifier value.

Options

duid-type The DHCPv6 client is identified by a DHCP unique identifier (DUID).

duid-ll Link Layer address.

duid-llt Link Layer address plus time.

vendor Vendor-assigned unique ID based on the enterprise number.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

DHCPv6 Client Overview | 256

client-type

IN THIS SECTION

- Syntax | 429
- Hierarchy Level | 429
- Description | 429
- Options | 429
- Required Privilege Level | 429
- Release Information | 430

Syntax

```
client-type (autoconfig | stateful);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit logical-systems logical -system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client]
```

Description

The type of DHCPv6 client.

Options

- autoconfig—Autoconfig client type for router advertisement
- stateful— Stateful client type for address assignment

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

DHCPv6 Client Overview | 256

delegated-pool (DHCP Local Server)

IN THIS SECTION

- Syntax | 430
- Hierarchy Level | 430
- Description | 431
- Options | 431
- Required Privilege Level | 431
- Release Information | 431

Syntax

```
delegated-pool pool-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 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],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 ...],
[edit logical-systems logical-system-name system services system services dhcp-local-server
dhcpv6 ...],
[edit routing-instances routing-instance-name system services system services dhcp-local-server
dhcpv6 ...]
```

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

pool-name	Name of the address-assignment pool.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Specifying the Delegated Address-Assignment Pool to Be Used for DHCPv6 Prefix Delegation

Overriding the Default DHCP Local Server Configuration Settings

delimiter (DHCP Local Server)

IN THIS SECTION

- Syntax | 432
- Hierarchy Level | 432
- Description | 433
- Options | 433
- Required Privilege Level | 434
- Release Information | 434

Syntax

```
delimiter delimiter-character;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-name
authentication username-include],
```

```
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group group-
name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[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]
```

Description

Specify the character used as the delimiter between the concatenated components of the username.

Options

delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

- **Default:** . (period)

NOTE: When you include the *interface-description* in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is

configured as “Backbone connection/PHL01”, you cannot use the forward slash (/) as the delimiter.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

delimiter (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 435
- Hierarchy Level | 435
- Description | 436
- Options | 436
- Required Privilege Level | 436
- Release Information | 436

Syntax

```
delimiter delimiter-character;
```

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 group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
```

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

delimiter-character—Character that separates components that make up the concatenated username. You cannot use the semicolon (;) as a delimiter.

- **Default:** . (period)

> **NOTE**: When you include the *interface-description* in the username, the delimiter must not be a character that is part of the interface description. For example, if the text description is configured as “Backbone connection/PHL01”, you cannot use the forward slash (/) as the delimiter.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *dual-stack-group-name*`]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

detection-time

IN THIS SECTION

- Syntax | 437
- Hierarchy Level | 437
- Description | 438
- Required Privilege Level | 438
- Release Information | 438

Syntax

```
detection-time {
    threshold milliseconds;
}
```

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
```

```
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Description

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

dhcp

IN THIS SECTION

- Syntax | 439
- Hierarchy Level | 440
- Description | 440
- Required Privilege Level | 440
- Release Information | 441

Syntax

```
dhcp {
    boot-file filename;
    boot-server (address | hostname);
    default-lease-time seconds;
    domain-name domain-name;
    domain-search [domain-list];
    maximum-lease-time seconds;
    name-server {
        address;
    }
    next-servernext-server
    option option-identifier-code ;
    pool address/prefix-length {
        address-range {
            low address;
            high address;
        }
        exclude-address {
            address;
        }
    }
    router {
        address;
```

```
    }
    static-binding mac-address {
        fixed-address {
            address;
        }
        host-name hostname;
        client-identifier (ascii client-id | hexadecimal client-id);
    }
    wins-server {
        address;
    }
}
```

Hierarchy Level

```
[edit system services]
[edit logical-systems logical -system-name system services]
```

Description

Configure a router, or a switch as a DHCP server. A DHCP server can allocate network addresses and deliver configuration information to client hosts on a TCP/IP network.

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.

Release Information

Statement introduced before Junos OS Release 7.4.

The `logical-systems` option is introduced in Junos OS Release 18.4R1.

dhcp (DHCP Client)

IN THIS SECTION

- Syntax (EX Series) | **441**
- Syntax (SRX Series) | **442**
- Hierarchy level (EX Series) | **442**
- Hierarchy level (SRX Series) | **442**
- Description | **443**
- Options | **443**
- Required Privilege Level | **443**
- Release Information | **444**

Syntax (EX Series)

```
dhcp {
    client-identifier duid-type (duid-ll | duid-llt | vendor);
    no-dns-install;
    rapid-commit;
    options name;
}
```

Syntax (SRX Series)

```
dhcp {
    client-identifier {
        (ascii string | hexadecimal string);
    }
    force-discover;
    lease-time (length | infinite);
    metric;
    no-dns-install;
    options;
    requested-options;
    retransmission-attempt value;
    retransmission-interval seconds;
    server-address server-address;
    update-server;
    vendor-id vendor-id ;
}
```

Hierarchy level (EX Series)

```
[edit interfaces interface-name unit logical-unit-number family inet]
[edit logical-systems name interfaces interface-name unit logical-unit-number family inet]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet]
```

Hierarchy level (SRX Series)

```
[edit interfaces interface-name unit logical-unit-number family inet]
```

Description

Configure a Dynamic Host Configuration Protocol (DHCP) client for an IPv4 interface for logical systems and tenant systems.

The remaining statements are described separately.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

Options

client-identifier duid-type	Identify a client by a client-identifier value. This statement is mandatory.
no-dns-install	Do not add DNS information to the DHCP client even after it is learned from the DHCP server.
options	Specify options requested by the DHCPv4 client.
force-discover	Send DHCPDISCOVER after DHCPREQUEST retransmission failure
lease-time	Specify lease time in seconds requested in DHCP client protocol packet (60 through 2147,,483,647 seconds for SRX devices)
metric	client initiated default-route metric (0..255 for SRX Series devices)
requested-options	Specify the DHCP options.

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.

Release Information

Statement introduced in Junos OS Release 9.0.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

Understanding Interfaces

Configuring a DHCP Client | 235

dhcp-attributes (Access IPv4 Address Pools)

IN THIS SECTION

- Syntax | 444
- Hierarchy Level | 446
- Description | 446
- Required Privilege Level | 446
- Release Information | 446

Syntax

```
dhcp-attributes {
    boot-file boot-file-name;
    boot-server boot-server-name;
    domain-name domain-name;
    grace-period seconds;
    maximum-lease-time (seconds | infinite);
    name-server ipv4-address;
    netbios-node-type (b-node | h-node | m-node | p-node);
    next-server next-server-name;
```

```
    option dhcp-option-identifier-code {
        array {
            byte [8-bit-value];
            flag [ false| off |on |true];
            integer [32-bit-numeric-values];
            ip-address [ip-address];
            short [signed-16-bit-numeric-value];
            string [character string value];
            unsigned-integer [unsigned-32-bit-numeric-value];
            unsigned-short [16-bit-numeric-value];
        }
        byte 8-bit-value;
        flag (false | off | on | true);
        integer 32-bit-numeric-values;
        ip-address ip-address;
        short signed-16-bit-numeric-value;
        string character string value;
        unsigned-integer unsigned-32-bit-numeric-value;
        unsigned-short 16-bit-numeric-value;
    }
    option-match {
        option-82 {
            circuit-id match-value {
                range range-name;
            }
            remote-id match-value;
                range range-name;
            }
        }
    }
    propagate-ppp-settings [interface-name];
    propagate-settings interface-name;
    router ipv4-address;
    server-identifier ip-address;
    sip-server {
        ip-address ipv4-address;
        name sip-server-name;
    }
    tftp-server server-name;
    wins-server ipv4-address;
}
```

Hierarchy Level

```
[edit access address-assignment pool pool-name family inet]
```

Description

Configure attributes for IPv4 address pools that can be used by different clients. The DHCP attributes for this statement uses standard IPv4 DHCP options.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

dhcp-attributes (Access IPv6 Address Pools)

IN THIS SECTION

Syntax | 447

- Hierarchy Level | 448
- Description | 448
- Options | 448
- Required Privilege Level | 448
- Release Information | 449

Syntax

```
dhcp-attributes {
    dns-server ipv6-address;
    grace-period seconds;
    maximum-lease-time (seconds | infinite);
    option dhcp-option-identifier-code {
        array {
            byte [8-bit-value];
            flag [ false| off |on |true];
            integer [32-bit-numeric-values];
            ip-address [ip-address];
            short [signed-16-bit-numeric-value];
            string [character string value];
            unsigned-integer [unsigned-32-bit-numeric-value];
            unsigned-short [16-bit-numeric-value];
        }
        byte 8-bit-value;
        flag (false | off | on | true);
        integer 32-bit-numeric-values;
        ip-address ip-address;
        short signed-16-bit-numeric-value;
        string character string value;
        unsigned-integer unsigned-32-bit-numeric-value;
        unsigned-short 16-bit-numeric-value;
    }
    propagate-ppp-settings [interface-name];
    sip-server-address ipv6-address;
    sip-server-domain-name domain-name;
}
```

Hierarchy Level

```
[edit access address-assignment pool pool-name family inet6]
```

Description

Configure attributes for address pools that can be used by different clients.

Options

- `dns-server` *IPv6-address*—Specify a DNS server to which clients can send DNS queries.
- `grace-period` *seconds* —Specify the grace period offered with the lease.
- **Range:** 0 through 4,294,967,295 seconds
- **Default:** 0 (no grace period)
- `maximum-lease-time` *seconds*—Specify the maximum length of time in seconds for which a client can request and hold a lease on a DHCP server.
- **Range:** 30 through 4,294,967,295 seconds
- **Default:** 86,400 seconds (24 hours)
- `option` *dhcp-option-identifier-code*—Specify the DHCP option identifier code.
- `propagate-ppp-settings` [*interface-name*—Specify PPP interface name for propagating DNS or WINS settings.
- `sip-server-address` *IPv6-address*—Specify the IPv6 address of the SIP outbound proxy server.
- `sip-server-domain-name` *domain-name*—Specify the domain name of the SIP outbound proxy server.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

dhcp-client

IN THIS SECTION

- Syntax | 449
- Hierarchy Level | 450
- Description | 450
- Options | 450
- Required Privilege Level | 451
- Release Information | 451

Syntax

```
dhcp-client {
    client-identifier {
        prefix {
            host-name;
            logical-system-name;
            routing-instance-name;
        }
```

```
        use-interface-description (device | logical);
        user-id (ascii string| hexadecimal string);
    }
    force-discover;
    lease-time (length | infinite);
    no-dns-install;
    options no-hostname;
    retransmission-attempt value;
    retransmission-interval seconds;
    server-address server-address;
    update-server;
    vendor-id vendor-id ;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family]
```

Description

Configure the Dynamic Host Configuration Protocol (DHCP) client.

Options

- **force-discover**—Forces the DHCP client to send a DHCP discover packet after one to three failed `dhcp-request` attempts. The `force-discover` option ensures that the DHCP server will assign the same or a new IP address to the client.
- **lease-time**—Specify the time to negotiate and exchange DHCP information.
  - **infinite**—Lease never expires.
  - **length**—Number of seconds.
- **no-dns-install**—Do not add DNS information to the DHCP client (resolve.conf) even after learn from DHCP server

- **retransmission-attempt**—Specify the number of times the device attempts to retransmit a DHCP packet fallback. Range is 0-6.
- **server-address**—Specify the preferred DHCP server address that is sent to DHCP clients.
- **update-server**—Propagate TCP/IP settings to a local DHCP server.
- **vendor-id**—Vendor class ID for the DHCP client.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.4R1 and Junos OS Release 15.1X49-D60, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to align with other Junos platforms. There is no change in the functionality.

RELATED DOCUMENTATION

DHCP Overview | 2

dhcp-local-server

IN THIS SECTION

Syntax | 452

- Hierarchy Level | 463
- Description | 463
- Required Privilege Level | 464
- Release Information | 464

Syntax

```
dhcp-local-server {
    access-profile profile-name;
    allow-active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
    }
    allow-bulk-leasequery {
        max-connections number-of-connections;
        max-empty-replies number-of-replies;
        restricted-requestor;
        timeout seconds;
    }
    allow-leasequery {
        restricted-requestor;
    }
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name ;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
```

```
            vlan-tags;
        }
    }
    dhcpv6 {
        access-profile profile-name;
        allow-active-leasequery {
            idle-timeout seconds;
            peer-address address;
            timeout seconds;
        }
        allow-bulk-leasequery {
            max-connections number-of-connections;
            max-empty-replies number-of-replies;
            restricted-requestor;
            timeout seconds;
        }
        allow-leasequery {
            restricted-requestor;
        }
        authentication {
            ...
        }
        duplicate-clients incoming-interface;
        group group-name {
            access-profile profile-name;
            authentication {
                ...
            }
            interface interface-name {
                access-profile profile-name;
                exclude;
                overrides {
                    asymmetric-lease-time seconds;
                    asymmetric-prefix-lease-time seconds;
                    delay-advertise {
                        based-on (option-15 | option-16 | option-18 | option-37) {
                            equals {
                                ascii ascii-string;
                                hexadecimal hexadecimal-string;
                            }
                            not-equals {
                                ascii ascii-string;
                                hexadecimal hexadecimal-string;
```

```
                        }
                        starts-with {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                    }
                    delay-time seconds;
                }
                dual-stack dual-stack-group-name;
                interface-client-limit number;
                multi-address-embedded-option-response;
                process-inform {
                    pool pool-name;
                }
                protocol-attributes attribute-set-name;
                rapid-commit;
            }
            service-profile dynamic-profile-name;
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
            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;
                }
                layer2-liveness-detection {
                    max-consecutive-retries number;
```

```
                    transmit-interval interval;
                }
            }
        }
        overrides {
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            delay-advertise {
                based-on (option-15 | option-16 | option-18 | option-37) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
                delay-time seconds;
            }
            delegated-pool;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            multi-address-embedded-option-response;
            process-inform {
                pool pool-name;
            }
            protocol-attributes attribute-set-name;
            rapid-commit;
        }
        route-suppression;
        server-duid-type type;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    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;
                }
                layer2-liveness-detection {
                    max-consecutive-retries number;
                    transmit-interval interval;
                }
            }
        }
        overrides {
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            delay-advertise {
                based-on (option-15 | option-16 | option-18 | option-37) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
                delay-time seconds;
            }
            delegated-pool;
            dual-stack dual-stack-group-name;
```

```
            include-option-82 {
                forcerenew;
                nak;
            }
            interface-client-limit number;
            multi-address-embedded-option-response;
            process-inform {
                pool pool-name;
            }
            protocol-attributes attribute-set-name;
            rapid-commit;
        }
        reconfigure {
            attempts attempt-count;
            clear-on-terminate;
            strict;
            support-option-pd-exclude;
            timeout timeout-value;
            token token-value;
             trigger {
                radius-disconnect;
            }
        }
        reauthenticate (<lease-renewal> <remote-id-mismatch >);
        requested-ip-network-match subnet-mask;
        route-suppression;
        server-duid-type type;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    dual-stack-group name {
        access-profile access-profile;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-description  (device-interface | logical-interface);
                interface-name ;
                logical-system-name;
                mac-address;
                relay-agent-interface-id;
```

```
                relay-agent-remote-id;
                routing-instance-name;
                user-prefix user-prefix-string;
                vlan-tags;
            }
        }
        classification-key {
            circuit-id circuit-id;
            mac-address mac-address;
            remote-id remote-id;
        }
        dual-stack-interface-client-limit number;
        dynamic-profile profile-name {
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        liveness-detection {
            failure-action (clear-binding | clear-binding-if-interface-up | log-only);
            method {
                layer2-liveness-detection {
                    max-consecutive-retries number;
                    transmit-interval interval;
                }
            }
        }
        on-demand-address-allocation;
        protocol-primary (inet | inet6);
        reauthenticate (<lease-renewal> <remote-id-mismatch >);
        service-profile service-profile;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    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;
```

```
            overrides {
                asymmetric-lease-time seconds;
                client-discover-match (option60-and-option82 | incoming-interface);
                delay-offer {
                    based-on (option-60 | option-77 | option-82) {
                        equals {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                        not-equals {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                        starts-with {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                    }
                    delay-time seconds;
                }
                include-option-82 {
                    forcerenew;
                    nak;
                }
                dual-stack dual-stack-group-name;
                interface-client-limit number;
                process-inform {
                    pool pool-name;
                }
                protocol-attributes attribute-set-name;
            }
            service-profile dynamic-profile-name;
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
            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;
                }
                layer2-liveness-detection {
                    max-consecutive-retries number;
                    transmit-interval interval;
                }
            }
        }
        overrides {
            asymmetric-lease-time seconds;
            client-discover-match  (option60-and-option82 | incoming-interface);
            delay-offer {
                based-on (option-60 | option-77 | option-82) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
                delay-time seconds;
            }
            include-option-82 {
                forcerenew;
                nak;
            }
            dual-stack dual-stack-group-name;
```

```
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            protocol-attributes attribute-set-name;
        }
        requested-ip-network-match subnet-mask
        route-suppression;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    on-demand-address-allocation;
    overrides {
        asymmetric-lease-time seconds;
        client-discover-match  <option60-and-option82 | incoming-interface>;
        delay-offer {
            based-on (option-60 | option-77 | option-82) {
                equals {
```

```
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
    }
    pool-match-order {
        external-authority;
        ip-address-first;
        option-82;
    }
    protocol-primary;
    reauthenticate (<lease-renewal> <remote-id-mismatch >);
    reconfigure {
        attempts attempt-count;
        clear-on-terminate;
        strict;
        timeout timeout-value;
        token token-value;
         trigger {
            radius-disconnect;
        }
    }
    requested-ip-network-match subnet-mask;
    route-suppression;
    service-profile dynamic-profile-name;
```

```
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

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]
```

Description

Configure Dynamic Host Configuration Protocol (DHCP) local server options on the router or switch to enable the router or switch to function as an extended DHCP local server. The DHCP local server receives DHCP request and reply packets from DHCP clients and then responds with an IP address and other optional configuration information to the client.

The extended DHCP local server is incompatible with the DHCP server on J Series routers and, therefore, is not supported on J Series routers. Also, the DHCP local server and the DHCP/BOOTP relay server, which are configured under the `[edit forwarding-options helpers]` hierarchy level, cannot both be enabled on the router or switch at the same time. The extended DHCP local server is fully compatible with the extended DHCP relay feature.

The `dhcpv6` stanza configures the router or switch to support Dynamic Host Configuration Protocol for IPv6 (DHCPv6). The DHCPv6 local server is fully compatible with the extended DHCP local server and the extended DHCP relay feature.

NOTE: When you configure the `dhcp-local-server` statement at the routing instance hierarchy level, you must use a routing instance type of `virtual-router`.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

Understanding Differences Between Legacy DHCP and Extended DHCP

DHCPv6 Local Server Overview

dhcp-local-server (System Services)

IN THIS SECTION

- Syntax | 464
- Hierarchy Level | 469
- Description | 469
- Options | 469
- Required Privilege Level | 469
- Release Information | 469

Syntax

```
dhcp-local-server {
    dhcpv6 {
```

```
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix;
            }
        }
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        group group-name {
            authentication {
                password password;
                username-include {
                    circuit-type;
                    client-id;
                    delimiter delimiter-character;
                    domain-name domain-name;
                    interface-name;
                    logical-system-name;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix;
                }
            }
            dynamic-profile {
```

```
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile;
        }
        interface interface-name {
            dynamic-profile {
                profile-name;
                aggregate-clients {
                    merge;
                    replace;
                }
                junos-default-profile;
                use-primary dynamic-profile-name;
            }
            exclude;
            overrides {
                delegated-pool pool-name;
                interface-client-limit number;
                process-inform {
                    pool pool-name;
                }
                rapid-commit ;
            }
            service-profile service-profile-name
            trace ;
            upto interface-name;
        }
        liveness-detection {
            failure-action {
                 clear-binding;
                clear-binding-if-interface-up;
                log-only;
            }
            method {
                bfd {
                    detection-time {
                        threshold milliseconds;
                    }
                    holddown-interval interval;
```

```
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    session-mode (automatic | multihop | single-hop);
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                version (0 | 1 | automatic);
            }
        }
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        reconfigure {
            attempts number;
            clear-on-abort;
            strict;
            timeout number;
            token token-name;
            trigger {
                radius-disconnect;
            }
        }
        service-profile service-profile-name;
    }
    liveness-detection {
        failure-action {
             clear-binding;
            clear-binding-if-interface-up;
            log-only;
        }
        method {
            bfd {
                detection-time {
                    threshold milliseconds;
                }
```

```
                    holddown-interval interval;
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    session-mode (automatic | multihop | single-hop);
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                version (0 | 1 | automatic);
            }
        }
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        reconfigure {
            attempts number;
            clear-on-abort;
            strict;
            timeout number;
            token token-name;
            trigger {
                radius-disconnect;
            }
        }
        service-profile service-profile-name;
    }
    group group-name {
        interface interface-name {
            exclude;
            upto upto-interface-name;
        }
    }
}
```

Hierarchy Level

```
[edit system services]
```

Description

Configure DHCP Local Server for DHCPv6, forwarding snoop (unicast) packets, and setting traceoptions.

NOTE: SRX Series devices do not support client authentication.

Options

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

dhcp-relay

IN THIS SECTION

- Syntax | 470
- Hierarchy Level | 485
- Description | 485
- Required Privilege Level | 485
- Release Information | 486

Syntax

```
dhcp-relay {
    access-profile profile-name;
    active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
        topology-discovery;
    }
    active-server-group server-group-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            option-60;
            option-82 <circuit-id> <remote-id>;
            routing-instance-name;
            user-prefix user-prefix-string;
```

```
            vlan-tags;
        }
    }
    bulk-leasequery {
        attempts number-of-attempts;
        timeout seconds;
    }
    dhcpv6 {
        access-profile profile-name;
        active-leasequery {
            idle-timeout seconds;
            peer-address address;
            timeout seconds;
            topology-discovery;
        }
        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-description  (device-interface | logical-interface);
                interface-name interface-name;
                logical-system-name;
                mac-address mac-address;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
                routing-instance-name;
                user-prefix user-prefix-string;
                vlan-tags;
            }
        }
        bulk-leasequery {
            attempts number-of-attempts;
            timeout seconds;
            trigger automatic;
        }
        duplicate-clients incoming-interface;
        dynamic-profile profile-name {
```

```
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-name>;
        }
        forward-only-replies;
        }
        forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-
interfaces);
        group group-name {
            access-profile profile-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;
                    interface-description  (device-interface | logical-interface);
                    interface-name interface-name;
                    logical-system-name;
                    mac-address mac-address;
                    relay-agent-interface-id;
                    relay-agent-remote-id;
                    relay-agent-subscriber-id;
                    routing-instance-name;
                    user-prefix user-prefix-string;
                    vlan-tags;
                }
            }
            dynamic-profile profile-name {
                aggregate-clients (merge | replace);
                use-primary primary-profile-name;
            }
            forward-only {
                logical-system <current | default | logical-system-name>;
                routing-instance <current | default | routing-instance-name>;
            }
            interface interface-name {
                access-profile profile-name;
```

```
                dynamic-profile profile-name {
                    aggregate-clients (merge | replace);
                    use-primary primary-profile-name;
                }
                exclude;
                overrides {
                    allow-snooped-clients;
                    asymmetric-lease-time seconds;
                    asymmetric-prefix-lease-time seconds;
                    client-negotiation-match incoming-interface;
                    delay-authentication;
                    delete-binding-on-renegotiation;
                    dual-stack dual-stack-group-name;
                    interface-client-limit number;
                    no-allow-snooped-clients;
                    no-bind-on-request;
                    relay-source interface-name;
                    send-release-on-delete;
                }
                service-profile dynamic-profile-name;
                short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
                trace;
                upto upto-interface-name;
            }
            }
            lease-time-validation {
                lease-time-threshold seconds;
                violation-action action;
            }
            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;
                }
                layer2-liveness-detection {
                    max-consecutive-retries number;
                    transmit-interval interval;
                }
            }
        }
        overrides {
            allow-snooped-clients;
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-negotiation-match incoming-interface;
            delay-authentication;
            delete-binding-on-renegotiation;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            no-allow-snooped-clients;
            no-bind-on-request;
            relay-source interface-name;
            send-release-on-delete;
        }
        relay-agent-interface-id {
            include-irb-and-l2;
            keep-incoming-interface-id ;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82 <strict>;
            use-vlan-id;
        }
        relay-agent-remote-id {
            include-irb-and-l2;
            keep-incoming-interface-id ;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82 <strict>;
            use-vlan-id;
        }
```

```
            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;
                }
            }
            remote-id-mismatch disconnect;
            route-suppression;
            service-profile dynamic-profile-name;
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
        }
        leasequery {
            attempts number-of-attempts;
            timeout seconds;
        }
        lease-time-validation {
            lease-time-threshold seconds;
            violation-action action;
        }
        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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
            route-suppression;
            service-profile dynamic-profile-name;
        }
    }
    no-snoop;
    overrides {
        allow-snooped-clients;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-authentication;
        delete-binding-on-renegotiation;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        no-allow-snooped-clients;
        no-bind-on-request;
        relay-source interface-name;
        send-release-on-delete;
    }
    relay-agent-interface-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    relay-agent-remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id ;
        no-vlan-interface-name;
```

```
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82 <strict>;
            use-vlan-id;
        }
        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-vendor-specific{
            host-name;
            location;
        remote-id-mismatch disconnect;
        route-suppression;
        server-group {
            server-group-name {
                server-ip-address;
            }
        }
        server-response-time seconds;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    dual-stack-group dual-stack-group-name {
        access-profile profile-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
```

```
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    classification-key {
        circuit-id circuit-id;
        mac-address mac-address;
        remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    protocol-primary (inet | inet6);
    relay-agent-interface-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    relay-agent-remote-id {
```

```
            include-irb-and-l2;
            keep-incoming-remote-id ;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82 <strict>;
            use-vlan-id;
        }
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    duplicate-clients-in-subnet (incoming-interface | option-82):
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    forward-only-replies;
    forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
    group group-name {
        access-profile profile-name;
        active-server-group server-group-name;
        authentication {
            password password-string;
            username-include {
                circuit-type;
                delimiter delimiter-character;
                domain-name domain-name-string;
                interface-description  (device-interface | logical-interface);
                interface-name interface-name;
                logical-system-name;
                mac-address;
                option-60;
                option-82 [circuit-id] [remote-id];
                routing-instance-name;
                user-prefix user-prefix-string;
                }
            vlan-tags;
        }
        dynamic-profile profile-name {
```

```
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-name>;
        }
        forward-only {
            logical-system <current | default | logical-system-name>;
            routing-instance <current | default | routing-instance-name>;
        }
        interface interface-name {
            access-profile profile-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 {
                allow-no-end-option;
                allow-snooped-clients;
                always-write-giaddr;
                always-write-option-82;
                asymmetric-lease-time seconds;
                client-discover-match <option60-and-option82 | incoming-interface>;
                delay-authentication;
```

```
                delete-binding-on-renegotiation;
                disable-relay;
                dual-stack dual-stack-group-name;
                interface-client-limit number;
                layer2-unicast-replies;
                no-allow-snooped-clients;
                no-bind-on-request;
                proxy-mode;
                relay-source
                replace-ip-source-with;
                send-release-on-delete;
                trust-option-82;
            }
            service-profile dynamic-profile-name;
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
            trace;
            upto upto-interface-name;
        }
        overrides {
            allow-no-end-option
            allow-snooped-clients;
            always-write-giaddr;
            always-write-option-82;
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-discover-match (option60-and-option82 | incoming-interface);
            delay-authentication;
            delete-binding-on-renegotiation;
            disable-relay;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            layer2-unicast-replies;
            no-allow-snooped-clients;
            no-bind-on-request;
            proxy-mode;
            relay-source
            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-id-override
        }
        remote-id-mismatch disconnect;
        route-suppression:
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    leasequery {
        attempts number-of-attempts;
        timeout seconds;
    }
    lease-time-validation {
        lease-time-threshold seconds;
        violation-action action;
    }
    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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    no-snoop;
    overrides {
        allow-no-end-option
        allow-snooped-clients;
        always-write-giaddr;
        always-write-option-82;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match (option60-and-option82 | incoming-interface);
        delay-authentication;
        delete-binding-on-renegotiation;
        disable-relay;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
        no-bind-on-request;
        proxy-mode;
        relay-source
        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-id-override
    }
    }
    remote-id-mismatch disconnect;
    route-suppression:
    server-group {
        server-group-name {
            server-ip-address;
        }
    }
    server-response-time seconds;
    service-profile dynamic-profile-name;
```

```
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options],
[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]
```

Description

Configure extended Dynamic Host Configuration Protocol (DHCP) relay and DHCPv6 relay options on the router or switch to 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 client authentication. You can attach dynamic profiles and configure authentication support on a global basis or for a specific group of interfaces.

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

DHCPv6 Relay Agent Overview

DHCP Relay Proxy Overview

Specifying Authentication Support

dhcp-service

IN THIS SECTION

- Syntax | 486
- Hierarchy Level | 488
- Description | 488
- Required Privilege Level | 488
- Release Information | 488

Syntax

```
dhcp-service {
    accept-max-tcp-connections max-tcp-connections;
    dhcp-snooping-file(local_pathname | remote_URL) {
        write-interval interval;
    }
    dhcpv6-snooping-file {
        location;
        write-interval seconds;
```

```
    }
    (disable | enable);
    interface-traceoptions {
        file filename <files number> <match regular-expression > <size maximum-file-size> <world-
readable | no-world-readable>;
        flag flag;
        level  (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
    log {
        session {
            client;
            all;
            dhcpv6 {
                client;
                server;
                relay;
                dynamic-server;
                all;
            }
            server;
            relay;
        }
    }
    ltv-syslog-interval seconds;
    persistent-storage {
        backup-interval backup-interval;
        file-name;
    }
    request-max-tcp-connections max-tcp-connections;
    traceoptions {
        file filename <files number> <match regular-expression > <size maximum-file-size> <world-
readable | no-world-readable>;
        flag flag;
        level  (all | error | info | notice | verbose | warning);
        no-remote-trace;
    }
}
```

Hierarchy Level

```
[edit system processes]
```

Description

Enable DHCP services on the device. DHCP services automate network-parameter assignment to network devices. The DHCP service process is enabled by default. However, by default, IP-MAC bindings in the DHCP snooping database do not persist through device reboots. You can inprove performance after rebooting by configuring the IP-MAC bindings to persist, by configuring a storage location for the DHCP database file. When specifying the location for the DHCP database, you must also specify how frequently the switch writes the database entries into the DHCP snooping database file.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 13.2X50-D10.

Support for log option introduced in Junos OS Release 19.1R1 for SRX Series devices.

RELATED DOCUMENTATION

- Configuring Persistent Bindings in the DHCP or DHCPv6 (ELS)

dhcpv6 (DHCP Local Server)

IN THIS SECTION

- Syntax | 489
- Hierarchy Level | 495
- Description | 495
- Required Privilege Level | 495
- Release Information | 496

Syntax

```
dhcpv6 {
    access-profile profile-name;
    allow-active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
    }
    allow-bulk-leasequery {
        max-connections number-of-connections;
        max-empty-replies number-of-replies;
        restricted-requestor;
        timeout seconds;
    }
    allow-leasequery {
        restricted-requestor;
    }
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
```

```
            interface-description  (device-interface | logical-interface);
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    duplicate-clients incoming-interface;
    group group-name {
        access-profile profile-name;
        authentication {
        ...
        interface interface-name {
            access-profile profile-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 {
                asymmetric-lease-time seconds;
                asymmetric-prefix-lease-time seconds;
```

```
                client-negotiation-match incoming-interface;
                delay-advertise {
                    based-on (option-15 | option-16 | option-18 | option-37) {
                        equals {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                        not-equals {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                        starts-with {
                            ascii ascii-string;
                            hexadecimal hexadecimal-string;
                        }
                    }
                    delay-time seconds;
                }
                delete-binding-on-renegotiation;
                interface-client-limit number;
                multi-address-embedded-option-response;
                process-inform {
                    pool pool-name;
                }
                protocol-attributes attribute-set-name;
                rapid-commit;
            }
            service-profile dynamic-profile-name;
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
            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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        delegated-pool;
        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
```

```
            rapid-commit;
        }
        route-suppression;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    }
    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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
```

```
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        delegated-pool;
        delete-binding-on-renegotiation;
        interface-client-limit number;
        multi-address-embedded-option-response;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
        reconfigure {
            attempts attempt-count;
            clear-on-terminate;
            strict;
            timeout timeout-value;
            token token-value;
             trigger {
                radius-disconnect;
            }
        }
    }
    reauthenticate (<lease-renewal> <remote-id-mismatch >);
    reconfigure {
        attempts attempt-count;
        clear-on-terminate;
        strict;
        support-option-pd-exclude;
        timeout timeout-value;
        token token-value;
         trigger {
            radius-disconnect;
        }
    }
    requested-ip-network-match subnet-mask;
    route-suppression;
```

```
    server-duid-type type;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Description

Configure DHCPv6 local server options on the router or switch to enable the router or switch to function as a server for the DHCP protocol for IPv6. The DHCPv6 local server sends and receives packets using the IPv6 protocol and informs IPv6 of the routing requirements of router clients. The local server works together with the AAA service framework to control subscriber access (or DHCP client access) and accounting.

The DHCPv6 local server is fully compatible with the extended DHCP local server and DHCP relay agent.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.6.

RELATED DOCUMENTATION

DHCPv6 Local Server Overview

dhcpv6 (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 496
- Hierarchy Level | 503
- Description | 503
- Required Privilege Level | 504
- Release Information | 504

Syntax

```
dhcpv6 {
    access-profile profile-name;
    active-leasequery {
        idle-timeout seconds;
        peer-address address;
        timeout seconds;
        topology-discovery;
    }
    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-description  (device-interface | logical-interface);
            interface-name interface-name;
            logical-system-name;
            mac-address mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    bulk-leasequery {
        attempts number-of-attempts;
        timeout seconds;
        trigger automatic;
    }
    duplicate-clients incoming-interface;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    forward-only-replies;
    }
    forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
    group group-name {
        access-profile profile-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;
            interface-description  (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    interface interface-name {
        access-profile profile-name;
        dynamic-profile profile-name {
            aggregate-clients (merge | replace);
            use-primary primary-profile-name;
        }
        exclude;
        overrides {
            allow-snooped-clients;
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-negotiation-match incoming-interface;
            delay-authentication;
            delete-binding-on-renegotiation;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            no-allow-snooped-clients;
            no-bind-on-request;
            relay-source interface-name;
            send-release-on-delete;
        }
        service-profile dynamic-profile-name;
```

```
            short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
            trace;
            upto upto-interface-name;
        }
        }
        lease-time-validation {
            lease-time-threshold seconds;
            violation-action action;
        }
        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;
                }
                layer2-liveness-detection {
                    max-consecutive-retries number;
                    transmit-interval interval;
                }
            }
        }
        overrides {
            allow-snooped-clients;
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-negotiation-match incoming-interface;
            delay-authentication;
            delete-binding-on-renegotiation;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
```

```
            no-allow-snooped-clients;
            no-bind-on-request;
            relay-source interface-name;
            send-release-on-delete;
        }
        relay-agent-interface-id {
            include-irb-and-l2;
            keep-incoming-interface-id ;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82;
        }
        relay-agent-remote-id {
            include-irb-and-l2;
            keep-incoming-interface-id ;
            no-vlan-interface-name;
            prefix prefix;
            use-interface-description (logical | device);
            use-option-82 <strict>;
        }
        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;
            }
        }
        remote-id-mismatch disconnect;
        route-suppression;
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
```

```
    }
    leasequery {
        attempts number-of-attempts;
        timeout seconds;
    }
    lease-time-validation {
        lease-time-threshold seconds;
        violation-action action;
    }
    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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
            route-suppression;
            service-profile dynamic-profile-name;
        }
    }
    no-snoop;
    overrides {
        allow-snooped-clients;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-negotiation-match incoming-interface;
        delay-authentication;
```

```
        delete-binding-on-renegotiation;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        no-allow-snooped-clients;
        no-bind-on-request;
        relay-source interface-name;
        send-release-on-delete;
    }
    relay-agent-interface-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82;
    }
    relay-agent-remote-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
    }
    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-vendor-specific{
```

```
        host-name;
        location;
    remote-id-mismatch disconnect;
    route-suppression;
    server-group {
        server-group-name {
            server-ip-address;
        }
    }
    server-response-time seconds;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[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]
```

Description

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.

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

Support for `forward-snooped-clients` introduced in Junos OS Release 15.1X53-D56 for EX Series switches and Junos OS Release 17.1R1.

RELATED DOCUMENTATION

dhcp-relay | 470

DHCPv6 Relay Agent Overview

Specifying Authentication Support

dhcpv6 (System Services)

IN THIS SECTION

- Syntax | 505
- Hierarchy Level | 509
- Description | 509
- Options | 509
- Required Privilege Level | 509
- Release Information | 509

Syntax

```
dhcpv6 {
    authentication {
        password password;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name;
            interface-name;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile-name;
    }
    group group-name {
        authentication {
            password password;
            username-include {
                circuit-type;
                client-id;
                delimiter delimiter-character;
                domain-name domain-name;
                interface-name;
                logical-system-name;
                relay-agent-interface-id;
                relay-agent-remote-id;
                relay-agent-subscriber-id;
```

```
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
        }
        junos-default-profile;
        use-primary dynamic-profile;
    }
    interface interface-name {
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        exclude;
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        service-profile service-profile-name
        trace ;
        upto interface-name;
    }
    liveness-detection {
        failure-action {
             clear-binding;
            clear-binding-if-interface-up;
            log-only;
        }
        method {
```

```
                bfd {
                    detection-time {
                        threshold milliseconds;
                    }
                    holddown-interval interval;
                    minimum-interval milliseconds;
                    minimum-receive-interval milliseconds;
                    multiplier number;
                    no-adaptation;
                    session-mode (automatic | multihop | single-hop);
                    transmit-interval {
                        minimum-interval milliseconds;
                        threshold milliseconds;
                    }
                version (0 | 1 | automatic);
            }
        }
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        reconfigure {
            attempts number;
            clear-on-abort;
            strict;
            timeout number;
            token token-name;
            trigger {
                radius-disconnect;
            }
        }
        service-profile service-profile-name;
    }
    liveness-detection {
        failure-action {
             clear-binding;
            clear-binding-if-interface-up;
            log-only;
        }
```

```
        method {
            bfd {
                detection-time {
                    threshold milliseconds;
                }
                holddown-interval interval;
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
                session-mode (automatic | multihop | single-hop);
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
            version (0 | 1 | automatic);
        }
    }
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
```

Hierarchy Level

```
[edit system services]
```

Description

Configure DHCPv6 server to provide IPv6 addresses to clients.

NOTE: SRX Series devices do not support client authentication.

Options

- `duplicate-clients-on-interface`—Allow duplicate clients on different interfaces in a subnet.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

dhcpv6-client

IN THIS SECTION

- Syntax | 510
- Hierarchy Level | 511
- Description | 511
- Options | 511
- Required Privilege Level | 512
- Release Information | 512

Syntax

```
dhcpv6-client {
    client-ia-type {
        ia-na;
        ia-pd;
    }
    client-identifier duid-type (duid-ll | duid-llt | vendor);
    client-type (autoconfig | stateful);
    rapid-commit;
    req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain |
sip-server |time-zone | vendor-spec);
    retransmission-attempt number;
    update-router-advertisement {
        interface interface-name;
    }
    update-server;
    vendor-id <model-number>:<serial-number>;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet6]
[edit logical-systems name interfaces name unit name family inet6]
[edit tenants tenant-name interfaces name unit name family inet6]
```

Description

Configure the Dynamic Host Configuration Protocol version 6 (DHCPv6) client.

NOTE: Starting in Junos OS Release 18.1R1, DHCPv4 and DHCPv6 clients are supported on management interfaces (fxp0 and em0) configured in the non-default management routing instance, `mgmt_junos`.

Options

client-ia-type	Identity association type for DHCPv6 client. This statement is mandatory.
client-identifier duid-type	Identity a client by a client-identifier value. This statement is mandatory.
client-type	Identify the type of DHCPv6 client. This statement is mandatory.
rapid-commit	The use of the two-message exchange for address assignment.
req-option	Specify options requested by the DHCPv6 client.
retransmission-attempt number	Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.
update-router-advertisement	Specify the interface used to delegate prefixes.
update-server	Propagate TCP/IP settings to the DHCPv6 server.

For detailed information about these commands, see CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

DHCP Overview | 2

Minimum DHCPv6 Client Configuration on SRX Series Devices | 258

disable-relay

IN THIS SECTION

- Syntax | 513
- Hierarchy Level | 513
- Description | 513
- Required Privilege Level | 513
- Release Information | 514

Syntax

```
disable-relay;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

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.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

domain (Domain Map)

IN THIS SECTION

- Syntax | 514
- Hierarchy Level | 515
- Description | 515
- Required Privilege Level | 515
- Release Information | 515

Syntax

```
domain {
    delimiter [delimiter-character];
    map domain-map-name {
        aaa-logical-system logical-system-name {
            aaa-routing-instance routing-instance-name;
        }
        aaa-routing-instance routing-instance-name;
        access-profile profile-name;
        address-pool pool-name;
        dynamic-profile profile-name;

        strip-domain;
```

```
        target-logical-system logical-system-name {
            target-routing-instance routing-instance-name;
        }
        target-routing-instance routing-instance-name;
        tunnel-profile profile-name;
    }
    parse-direction (left-to-right | right-to-left);
    parse-order (domain-first | realm-first);
    realm-delimiter [delimiter-character];
    realm-parse-direction  (left-to-right | right-to-left);
}
```

Hierarchy Level

```
[edit access]
```

Description

Configure a domain map, which is used to map access options and session parameters for subscriber sessions.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring a Domain Map

domain-name (DHCP)

IN THIS SECTION

- Syntax | **516**
- Hierarchy Level | **516**
- Description | **517**
- Options | **517**
- Required Privilege Level | **517**
- Release Information | **517**

Syntax

```
domain-name domain-name;
```

Hierarchy Level

```
[edit system services dhcp
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

Configure the name of the domain in which clients search for a DHCP server host. This is the default domain name that is appended to hostnames that are not fully qualified.

Options

domain-name—Name of the domain.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring a DHCP Server on Switches | 66

domain-name (DHCP Local Server)

IN THIS SECTION

- Syntax | 518
- Hierarchy Level | 518

- Description | 519
- Options | 519
- Required Privilege Level | 519
- Release Information | 519

Syntax

```
domain-name domain-name-string;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication username-include],
[edit routing-instances routing-instance-name 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]
```

Description

Specify the domain name that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options

domain-name-string—Domain name formatted string.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

domain-name (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 520
- Hierarchy Level | 520
- Description | 521
- Options | 521
- Required Privilege Level | 521
- Release Information | 522

Syntax

```
domain-name domain-name-string;
```

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 group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-
include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-
include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication
```

```
username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication
username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name authentication username-include]
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
authentication username-include]
```

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

domain-name-string—Domain name formatted string.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *`dual-stack-group-name`*`]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

domain-name-server (Routing Instances and Access Profiles)

IN THIS SECTION

- Syntax | **523**
- Hierarchy Level | **523**
- Description | **523**
- Options | **523**
- Required Privilege Level | **523**
- Release Information | **524**

Syntax

```
domain-name-server dns-address;
```

Hierarchy Level

```
[edit access];
[edit access profile]
```

Description

Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the `[edit access]` hierarchy level or for an access profile at the `[edit access profile profile-name]` hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is less preferred than one configured with the "domain-name-server-inet" on page 524 statement. That is, the server with the address configured with the "domain-name-server-inet" on page 524 takes precedence over a server configured with this statement.

Options

dns-address	IPv4 address of the DNS name server.

Required Privilege Level

admin—To view this statement in the configuration

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Configuring DNS Name Server Addresses for Subscriber Management

DNS Name Server Address Overview

domain-name-server-inet (Routing Instances and Access Profiles)

IN THIS SECTION

- Syntax | 524
- Hierarchy Level | 525
- Description | 525
- Options | 525
- Required Privilege Level | 525
- Release Information | 525

Syntax

```
domain-name-server-inet dns-address;
```

Hierarchy Level

```
[edit access],
[edit access profile]
```

Description

Configure an IPv4 address for a DNS name server. You can configure an address globally for a routing instance at the `[edit access]` hierarchy level or for an access profile at the `[edit access profile` *`profile-name`*`]` hierarchy level. You can configure more than one address by including the statement multiple times.

NOTE: A DNS name server address configured with this statement is higher in preference than one configured with the "domain-name-server" on page 522 statement. That is, the server with the address configured with the "domain-name-server-inet" on page 524 takes precedence over a server configured with the "domain-name-server" on page 522 statement.

Options

dns-address	IPv4 address of the DNS name server.

Required Privilege Level

admin—To view this statement in the configuration

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Configuring DNS Name Server Addresses for Subscriber Management

DNS Name Server Address Overview

domain-name-server-inet6 (Routing Instances and Access Profiles)

IN THIS SECTION

- Syntax | 526
- Hierarchy Level | 526
- Description | 527
- Options | 527
- Required Privilege Level | 527
- Release Information | 527

Syntax

```
domain-name-server-inet6 dns-address;
```

Hierarchy Level

```
[edit access],
[edit access profile]
```

Description

Configure an IPv6 address for a DNS name server. You can configure an address globally for a routing instance at the `[edit access]` hierarchy level or for an access profile at the `[edit access profile` *`profile-name`*`]` hierarchy level. You can configure more than one address by including the statement multiple times.

Options

dns-address	IPv6 address of the DNS name server.

Required Privilege Level

admin—To view this statement in the configuration

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

> *Configuring DNS Name Server Addresses for Subscriber Management*
>
> *DNS Name Server Address Overview*

domain-search

IN THIS SECTION

- Syntax | 528
- Hierarchy Level | 528
- Description | 528
- Options | 529
- Required Privilege Level | 529
- Release Information | 529

Syntax

```
domain-search [domain-list ];
```

Hierarchy Level

```
[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

Configure a list of domains to search (in the case where you want to configure access to multiple DNS servers for redundancy, and/or to resolve hosts that the previous server could not).

Options

domain-list List of domain servers to search. The list can contain up to six domain names, separated by a space, with a total of up to 256 characters.

For example to search `domain1.net`, and if it fails to resolve the host, `domain2.net`, and if fails to resolve the host, `domain3.net`, you would configure the following domain list at the `domain-search` hierarchy level:

```
[edit system]
set domain-search [domain1.net domain2.net domain3.net]
```

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

drop (DHCP Relay Agent Option)

IN THIS SECTION

- Syntax | 530
- Hierarchy Level | 530
- Description | 530
- Required Privilege Level | 530
- Release Information | 531

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 group-name relay-option (default-action | equals | starts-
with)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action | equals
| starts-with)],
[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 ...]
```

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.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic

dual-stack (DHCP Local Server Overrides)

IN THIS SECTION

- Syntax | 531
- Hierarchy Level | 531
- Description | 532
- Options | 532
- Required Privilege Level | 532
- Release Information | 532

Syntax

```
dual-stack dual-stack-group-name;
```

Hierarchy Level

```
[edit logical-systems name routing-instances routing-instance-name system services dhcp-local-
server ...],
[edit logical-systems name system services dhcp-local-server ...],
```

```
[edit routing-instances name system services dhcp-local-server ...],
[edit system services dhcp-local-server group group-name interface interface-name overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server overrides]
```

Description

Assigns the specified dual-stack group to both legs (DHCP and DHCPv6) of the DHCP dual stack. The dual-stack group defines the common configuration settings for DHCP and DHCPv6 subscribers on both legs. These settings take precedence over all other configurations, such as those specified in global, group, or interface settings.

Options

dual-stack-group-name	Name of the globally configured dual-stack group.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement in the configuration.

Release Information

Statement introduced in Junos OS Release 17.3R1.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

Configuring Single-Session DHCP Dual-Stack Support

dual-stack (DHCP Relay Agent Overrides)

IN THIS SECTION

- Syntax | 533
- Hierarchy Level | 533
- Description | 534
- Options | 534
- Required Privilege Level | 534
- Release Information | 534

Syntax

```
dual-stack dual-stack-group-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[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 ...]
```

Description

Assigns the specified dual-stack group to both legs (DHCP and DHCPv6) of the DHCP dual stack. The dual-stack group defines the common configuration settings for DHCP and DHCPv6 subscribers on both legs. These settings take precedence over all other configurations, such as those specified in global, group, or interface settings.

Options

dual-stack-group-name	Name of the globally configured dual-stack group.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement in the configuration.

Release Information

Statement introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

Configuring Single-Session DHCP Dual-Stack Support

dual-stack-group (DHCP Local Server)

IN THIS SECTION

- Syntax | 535
- Hierarchy Level | 536
- Description | 536
- Options | 537
- Required Privilege Level | 537
- Release Information | 537

Syntax

```
dual-stack-group name {
    access-profile access-profile;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name ;
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    classification-key {
        circuit-id circuit-id;
        mac-address mac-address;
```

```
        remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
        method {
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    on-demand-address-allocation;
    protocol-primary (inet | inet6);
    reauthenticate (<lease-renewal> <remote-id-mismatch >);
    service-profile service-profile;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server],
[edit logical-systems name system services dhcp-local-server],
[edit routing-instances name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Description

Specifies common configuration settings that are used for both legs (DHCP and DHCPv6) of the DHCP local server dual-stack, and names the dual-stack group.

When applied, the dual-stack configuration takes precedence over all other configurations, such as those specified in global, group, or interface settings.

Options

name Name of the dual-stack group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement in the configuration.

Release Information

Statement introduced in Junos OS Release 17.3R1.

RELATED DOCUMENTATION

- *Single-Session DHCP Dual-Stack Overview*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets
- *Configuring RADIUS Reauthentication for DHCP Subscribers*
- *RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers*

dual-stack-group (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 538
- Hierarchy Level | 539
- Description | 540

- Options | 540
- Required Privilege Level | 540
- Release Information | 540

Syntax

```
dual-stack-group name {
    access-profile profile-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            interface-name;
            logical-system-name;
            mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    classification-key {
        circuit-id circuit-id;
        mac-address mac-address;
        remote-id remote-id;
    }
    dual-stack-interface-client-limit number;
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    liveness-detection {
        failure-action (clear-binding | clear-binding-if-interface-up | log-only);
```

```
        method {
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    protocol-primary (inet | inet6);
    relay-agent-interface-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    relay-agent-remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[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]
```

Description

Specifies common configuration settings that are used for both legs (DHCP and DHCPv6) of the DHCP dual stack, and names the dual stack group.

The group is assigned to each leg of the DHCP dual-stack with the "dual-stack" on page 533 statement in the `overrides` stanza. When applied, the dual-stack configuration takes precedence over all other configurations, such as those specified in global, group, or interface settings.

Options

name	Name of the dual-stack group.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement in the configuration.

Release Information

Statement introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

Configuring Single-Session DHCP Dual-Stack Support

DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

dual-stack-interface-client-limit (DHCP Local Server and Relay Agent)

IN THIS SECTION

- Syntax | 541
- Hierarchy Level | 541
- Description | 542
- Options | 542
- Required Privilege Level | 542
- Release Information | 542

Syntax

```
dual-stack-interface-client-limit number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay dual-stack-group
dual-stack-group-name ],
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-
group dual-stack-group-name ],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-
name ],
[edit routing-instances name forwarding-options dhcp-relay dual-stack-group dual-stack-group-
name ],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-
```

```
name ],
[edit system services dhcp dhcp-local-server dual-stack-group dual-stack-group-name ],
```

Description

Limit the number of clients allowed on an interface.

NOTE: For dual-stack subscribers, always use this statement instead of the "interface-client-limit" on page 599 (DHCP Relay Agent) or "interface-client-limit" on page 597 (DHCP Local Server) statements.

Options

number Maximum number of dual-stack subscribers that can log in per interface.

- **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.

Release Information

Statement introduced in Junos OS Release 17.3R1.

RELATED DOCUMENTATION

Single-Session DHCP Dual-Stack Overview

dynamic-pool

IN THIS SECTION

- Syntax | 543
- Hierarchy Level | 544
- Description | 544
- Options | 544
- Required Privilege Level | 544
- Release Information | 544

Syntax

```
dynamic-pool <dynamic-pool>{
    family {
        inet6 {
            from-interface <interface>;
            delegated-prefix-length <network-prefix-length>;
            range <range-name> {
                masked-low <masked-low>;
                masked-high <masked-high>;
                prefix-length <prefix-length>;
            }
            dhcp-attributes {
                dns-server <address>;
                t1-percentage <t1-percentage>;
                t2-percentage <t2-percentage>;
                preferred-lifetime <preferred-lifetime>;
                valid-lifetime <valid-lifetime>;
            }
        }
    }
}
```

Hierarchy Level

```
[edit access address-assignment (Access)]
```

Description

Configure the dynamic pool updated by the client running on the WAN interface.

Options

The remaining statements are explained separately.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 15.1X49-D70.

RELATED DOCUMENTATION

address-assignment (Access)

IP Address Assignment Pool | **27**

dynamic-profile (DHCP Local Server)

IN THIS SECTION

- Syntax | 545
- Hierarchy Level | 545
- Description | 546
- Options | 546
- Required Privilege Level | 546
- Release Information | 546

Syntax

```
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[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 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 ...]
```

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.2.

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.

RELATED DOCUMENTATION

> *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
>
> *Configuring a Default Subscriber Service*

dynamic-profile (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 547
- Hierarchy Level | 547
- Description | 548
- Options | 548
- Required Privilege Level | 548
- Release Information | 548

Syntax

```
dynamic-profile profile-name {
    aggregate-clients (merge | replace);
    use-primary primary-profile-name;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-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 ...]
```

Description

Specify the dynamic profile that is attached to all interfaces, to a named group of interfaces, or to a specific interface.

M120 and M320 routers do not support DHCPv6.

Options

profile-name—Name of the dynamic profile.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.2.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *`dual-stack-group-name`*`]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

dhcp-relay | 470

Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

Grouping Interfaces with Common DHCP Configurations

Configuring a Default Subscriber Service

dynamic-server

IN THIS SECTION

- Syntax | 549
- Hierarchy Level | 550
- Description | 550
- Options | 550
- Required Privilege Level | 550
- Release Information | 550

Syntax

```
dhcpv6 {
    dynamic-server {
        group <group> {
            neighbor-discovery-router-advertisement <ndra-pool>;
            interface <interface> {
                overrides {
                    delegated-pool <delegated-pool>;
                    ia-na-pool <ia-na-pool>;
                    process-inform {
                        pool <pool>;
                    }
                }
            }
        }
    }
}
```

Hierarchy Level

```
[edit system services]
```

Description

Configure the server running on a LAN interface.

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.

Release Information

Statement introduced in Junos OS Release 15.1X49-D70.

RELATED DOCUMENTATION

dhcp-local-server (System Services) | 464

dhcp-client | 449

excluded-address (Address-Assignment Pools)

IN THIS SECTION

- Syntax | 551
- Hierarchy Level | 551
- Description | 551
- Required Privilege Level | 552
- Release Information | 552

Syntax

```
excluded-address ip-address;
```

Hierarchy Level

```
[edit access address assignment-address pool]
```

Description

Allows you to exclude select IPv4 or IPv6 addresses from a DHCP address pool. Within a configured address pool, you can specifically exclude up to 20 addresses. Junos OS will not assign these excluded addresses to any clients. If you configure an excluded address that has already been assigned to a DHCP client, that excluded address will be revoked from the client.

NOTE: Excluded addresses must match the address family of the configured address pool. For example, you cannot exclude an IPv4 address within an IPv6 address pool.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 15.1X49-D20.

RELATED DOCUMENTATION

pool

Preventing Addresses from Being Allocated from an Address Pool

excluded-address (Address-Assignment Pools)

IN THIS SECTION

- Syntax | 553
- Hierarchy Level | 553
- Description | 553
- Options | 553
- Required Privilege Level | 553
- Release Information | 554

Syntax

```
excluded-address ip-address;
```

Hierarchy Level

```
[edit access address-assignment pool name family (inet | inet6)],
[edit logical-systems name access address-assignment pool name family (inet | inet6)],
[edit logical-systems name routing-instances name access address-assignment pool name family (inet
| inet6)],
[edit routing-instances name access address-assignment pool name family (inet | inet6)]
```

Description

Specify an address to exclude from consideration when addresses are allocated from the corresponding address pool. If an address that you configure for exclusion has already been allocated, the subscriber that has that address is logged out. The address is then deallocated and marked for exclusion from future allocation.

Options

ip-address IPv4 or IPv6 address to exclude from the address pool for the specified family.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 18.1R1.

RELATED DOCUMENTATION

Preventing Addresses from Being Allocated from an Address Pool

Address-Assignment Pools Overview

Address-Assignment Pool Configuration Overview

external-authority

IN THIS SECTION

- Syntax | 554
- Hierarchy Level | 554
- Description | 555
- Required Privilege Level | 555
- Release Information | 555

Syntax

```
external-authority;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server pool-match-order],
```

```
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

Description

Specify that an external authority (for example, RADIUS or Diameter) provides the address assignment.

When RADIUS is the external authority, the router uses the Framed-IPv6-Pool attribute (RADIUS attribute 100) to select the pool. When Diameter is the external authority, the router uses the Diameter counterpart of RADIUS Framed-IPv6-Pool attribute.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

RELATED DOCUMENTATION

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Understanding Differences Between Legacy DHCP and Extended DHCP*
- *Address-Assignment Pools Overview*

failure-action

IN THIS SECTION

- Syntax | 556
- Hierarchy Level | 556
- Description | 557
- Options | 557
- Required Privilege Level | 557
- Release Information | 557

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 group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection]
```

Description

Configure the action the router (or switch) takes when a liveness detection failure occurs.

Options

- **Default:** `clear-binding`

`clear-binding`—The DHCP client session is cleared when a liveness detection failure occurs, except when `maintain-subscribers interface-delete` setting is configured and active.

`clear-binding-if-interface-up`—The DHCP client session is cleared only when a liveness detection failure occurs and the local interface is detected as being up. Use this setting to distinguish failures from between a liveness detection failure due to a local network error, and a host disconnecting from the network. If the client binding is in the maintain-binding Finite State Machine (FSM) state when the liveness detection failure detection occurs, then the binding is not deleted. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

`log-only`—A message is logged to indicate the event; no action is taken and DHCP is left to manage the failure and maintain the client binding. Not supported for Layer 2 ARP/ND liveness detection on MX Series routers.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

DHCP Liveness Detection Overview

Configuring Detection of DHCP Local Server Client Connectivity with BFD

Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD
Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

force-discover (DHCP Client)

IN THIS SECTION

- Syntax | 558
- Hierarchy Level | 558
- Description | 558
- Required Privilege Level | 559
- Release Information | 559

Syntax

```
force-discover;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number dhcp-client]
```

Description

Forces the DHCP client to send a DHCP discover packet after one to three failed `dhcp-request` attempts. The `force-discover` option ensures that the DHCP server will assign the same or a new IP address to the client.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 15.1X49-D80.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

RELATED DOCUMENTATION

- DHCP Client | 234
- DHCPv6 Client | 255
- Minimum DHCP Client Configuration | 235

forward-only (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 560
- Hierarchy Level | 560
- Description | 560
- Default | 560
- Options | 560
- Required Privilege Level | 561
- Release Information | 561

Syntax

```
forward-only {
    logical-system <current | default | logical-system-name>;
    routing-instance <current | default | routing-instance-name>;
}
```

Hierarchy Level

```
[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 ...]
```

Description

Specify the VRF location of the DHCP server when configuring secure DHCP traffic between the DHCP server and DHCP client when the two reside in different VRFs.

Default

Logical system and routing instance from where the configuration is applied.

Options

logical-system (Optional) Logical system in which the DHCP server resides.

- `current`—Logical system from which the configuration is applied.
- `default`—Root logical system.
- *`logical-system-name`*—A specific logical system.

routing-instance (Optional) Routing instance in which the DHCP server resides.

- `current`—Routing instance from which the configuration is applied.
- `default`—Root routing instance.
- *`logical-system-name`*—A specific routing instance.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Releases 13.3R3, 14.1R2, and 14.2R1.

RELATED DOCUMENTATION

DHCP Message Exchange Between DHCP Clients and DHCP Server in Different VRFs

Configuring DHCP Message Exchange Between DHCP Server and Clients in Different Virtual Routing Instances

forward-snooped-clients (DHCP Local Server)

IN THIS SECTION

- Syntax | 562
- Hierarchy Level | 562
- Description | 562
- Options | 563
- Required Privilege Level | 563
- Release Information | 563

Syntax

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Description

Configure how the DHCP local server filters and handles DHCP snooped packets on the specified interfaces.

Options

`all-interfaces`—Perform the action on all interfaces.

`configured-interfaces`—Perform the action only on interfaces that are configured as part of an interface group.

`non-configured-interfaces`—Perform the action only on interfaces that are not configured as part of a group.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Snooping Support

Configuring DHCP Snooped Packets Forwarding Support for DHCP Local Server

forward-snooped-clients (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 564
- Hierarchy Level | 564
- Description | 564

- Options | 565
- Required Privilege Level | 565
- Release Information | 565

Syntax

```
forward-snooped-clients (all-interfaces | configured-interfaces | non-configured-interfaces);
```

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]
```

Description

Configure how DHCP relay agent filters and handles DHCP snooped packets on the specified 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.

The router (or switch) also uses this statement to determine how to handle snooped BOOTREPLY packets received on non-configured interfaces.

Options

`all-interfaces`—Perform the action on all interfaces.

- **Default:** On EX Series switches, the action is performed on all interfaces by default.

`configured-interfaces`—Perform the action only on interfaces that are configured as part of an interface group.

`non-configured-interfaces`—Perform the action only on interfaces that are not part of a group.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

Support at the [`edit forwarding-options dhcp-relay dhcpv6`] hierarchy level introduced in Junos OS Release 15.1X53-D56 for EX Series switches and Junos OS Release 17.1R1.

RELATED DOCUMENTATION

DHCP Snooping Support

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

group (DHCP Local Server)

IN THIS SECTION

- Syntax | 566
- Hierarchy Level | 570
- Description | 570
- Options | 570
- Required Privilege Level | 571
- Release Information | 571

Syntax

```
group group-name {
    access-profile profile-name;
    authentication {
        password password-string;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name-string;
            interface-description  (device-interface | logical-interface);
            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;
            vlan-tags;
        }
    }
```

```
    dynamic-profile profile-name <aggregate-clients (merge | replace) | use-primary primary-profile-
name>;
    interface interface-name {
        access-profile profile-name;
        exclude;
        overrides {
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-discover-match <option60-and-option82>;
            client-negotiation-match incoming-interface;
            delay-advertise {
                based-on (option-15 | option-16 | option-18 | option-37) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
                delay-time seconds;
            }
            delay-offer {
                based-on (option-60 | option-77 | option-82) {
                    equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    not-equals {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                    starts-with {
                        ascii ascii-string;
                        hexadecimal hexadecimal-string;
                    }
                }
                delay-time seconds;
```

```
            }
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit;
        }
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
        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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82>;
        client-negotiation-match incoming-interface;
```

```
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        delay-offer {
            based-on (option-60 | option-77 | option-82) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        delegated-pool;
        delete-binding-on-renegotiation;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        protocol-attributes attribute-set-name;
        rapid-commit;
```

```
    }
    reconfigure {
        attempts attempt-count;
        clear-on-terminate;
        strict;
        timeout timeout-value;
        token token-value;
         trigger {
            radius-disconnect;
        }
    }
    route-suppression;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[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 ...]
```

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

- *Understanding Differences Between Legacy DHCP and Extended DHCP*
- *Grouping Interfaces with Common DHCP Configurations*
- *Specifying Authentication Support*
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

group (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **572**
- Hierarchy Level | **576**
- Description | **576**
- Options | **577**
- Required Privilege Level | **577**

- Release Information | 577

Syntax

```
group group-name {
    access-profile profile-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;
            interface-description  (device-interface | logical-interface);
            interface-name interface-name;
            logical-system-name;
            mac-address mac-address;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix-string;
            vlan-tags;
        }
    }
    dynamic-profile profile-name {
        aggregate-clients (merge | replace);
        use-primary primary-profile-name;
    }
    forward-only {
        logical-system <current | default | logical-system-name>;
        routing-instance <current | default | routing-instance-name>;
    }
    interface interface-name {
        access-profile profile-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 {
            allow-no-end-option;
            allow-snooped-clients;
            always-write-giaddr;
            always-write-option-82;
            asymmetric-lease-time seconds;
            asymmetric-prefix-lease-time seconds;
            client-discover-match <option60-and-option82 | incoming-interface>;
            client-negotiation-match incoming-interface;
            delay-authentication;
            delete-binding-on-renegotiation;
            disable-relay;
            dual-stack dual-stack-group-name;
            interface-client-limit number;
            layer2-unicast-replies;
            no-allow-snooped-clients;
            no-bind-on-request;
            proxy-mode;
            relay-source
            replace-ip-source-with;
            send-release-on-delete;
            trust-option-82;
        }
```

```
        service-profile dynamic-profile-name;
        short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
        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;
            }
            layer2-liveness-detection {
                max-consecutive-retries number;
                transmit-interval interval;
            }
        }
    }
    overrides {
        allow-snooped-clients;
        always-write-giaddr;
        always-write-option-82;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82>;
        client-negotiation-match incoming-interface;
        disable-relay;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
```

```
        no-bind-on-request;
        proxy-mode;
        relay-source
        replace-ip-source-with;
        send-release-on-delete;
        trust-option-82;
    }
    relay-agent-interface-id {
        include-irb-and-l2;
        keep-incoming-interface-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    relay-agent-remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-option-82 <strict>;
        use-vlan-id;
    }
    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);
        }
        server-id-override
    }
    remote-id-mismatch disconnect;
    route-suppression;
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
}
```

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 ...]
```

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- Configuring DHCP Relay Agent
- *Configuring Group-Specific DHCP Relay Options*
- *Grouping Interfaces with Common DHCP Configurations*
- *Specifying Authentication Support*
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

group (System Services DHCP)

IN THIS SECTION

- Syntax | 578
- Hierarchy Level | 580
- Description | 580
- Options | 581
- Required Privilege Level | 581
- Release Information | 581

Syntax

```
group group-name {
    authentication {
        password password;
        username-include {
            circuit-type;
            client-id;
            delimiter delimiter-character;
            domain-name domain-name;
            interface-name;
            logical-system-name;
            relay-agent-interface-id;
            relay-agent-remote-id;
            relay-agent-subscriber-id;
            routing-instance-name;
            user-prefix user-prefix;
        }
    }
    dynamic-profile {
        profile-name;
        aggregate-clients {
            merge;
            replace;
```

```
        }
        junos-default-profile;
        use-primary dynamic-profile;
    }
    interface interface-name {
        dynamic-profile {
            profile-name;
            aggregate-clients {
                merge;
                replace;
            }
            junos-default-profile;
            use-primary dynamic-profile-name;
        }
        exclude;
        overrides {
            delegated-pool pool-name;
            interface-client-limit number;
            process-inform {
                pool pool-name;
            }
            rapid-commit ;
        }
        service-profile service-profile-name
        trace ;
        upto interface-name;
    }
    liveness-detection {
        failure-action {
             clear-binding;
            clear-binding-if-interface-up;
            log-only;
        }
        method {
            bfd {
                detection-time {
                    threshold milliseconds;
                }
                holddown-interval interval;
                minimum-interval milliseconds;
                minimum-receive-interval milliseconds;
                multiplier number;
                no-adaptation;
```

```
                session-mode (automatic | multihop | single-hop);
                transmit-interval {
                    minimum-interval milliseconds;
                    threshold milliseconds;
                }
            version (0 | 1 | automatic);
        }
    }
    overrides {
        delegated-pool pool-name;
        interface-client-limit number;
        process-inform {
            pool pool-name;
        }
        rapid-commit ;
    }
    reconfigure {
        attempts number;
        clear-on-abort;
        strict;
        timeout number;
        token token-name;
        trigger {
            radius-disconnect;
        }
    }
    service-profile service-profile-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6]
```

Description

Configure a group of interfaces that have a common configuration.

The remaining statements are explained separately. See CLI Explorer.

Options

- *group-name*—Name of the group.

> **NOTE**: SRX Series devices do not support DHCP client authentication.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

DHCP Server | 49

DHCP Server Configuration | 51

holddown-interval

IN THIS SECTION

- Syntax | 582
- Hierarchy Level | 582
- Description | 583
- Options | 583
- Required Privilege Level | 583
- Release Information | 583

Syntax

```
holddown-interval milliseconds;
```

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Description

Configure the time (in milliseconds) for which Bidirectional Forwarding Detection (BFD) holds a session up notification.

Options

milliseconds—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.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

host-name (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 584
- Hierarchy Level | 584
- Description | 584
- Required Privilege Level | 585
- Release Information | 585

Syntax

```
host-name name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82]
```

Description

Supports the addition of vendor-specific hostname in the option 82, suboption 9 field of DHCPv4 control messages on server-facing interfaces. The hostname can be a string of characters such as **Juniper-AB-1**.

Junos OS automatically adds the remaining vendor-specific information as per RFC 4243, *Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option*. The Juniper Networks enterprise ID is 2636. The hostname is option-data 1 (the location is

option-data 2). The DHCPv4 relay strips the suboption data from replies from the server before it relays the packets out the client facing interface.

This feature can be useful, in conjunction with operator-developed tools, for troubleshooting DHCP servers and providing service assurances. For example, a central DHCP server can log the information, and operators can query the hostname to track and troubleshoot subscriber IP information and network attachment points.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Command introduced in Junos OS Release 16.2.

include-irb-and-l2

IN THIS SECTION

- Syntax | **586**
- Hierarchy Level | **586**
- Description | **586**
- Required Privilege Level | **588**
- Release Information | **588**

Syntax

```
include-irb-and-l2;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Description

Include both the integrated routing and bridging (IRB) interface name and Layer 2 interface name in the `circuit-id` or `remote-id` value in the DHCP option 82 information. VLAN tags are global.

For leasequery and bulk leasequery operations that involve integrated routing and bridging (IRB) interfaces, you must configure DHCP relay agent to include the layer 2 interface name along with IRB name in the circuit ID of option 82. DHCP relay agent uses the layer 2 interface name when using leasequery or bulk leasequery to restore the lease database.

When you configure the `include-irb-and-l2` statement without including the `no-vlan-interface` statement, the format is as follows:

- Bridge domain:

```
(fe | ge)-fpc/pic/port.subunit:bridge-domain-name+irb.subunit
```

- VLAN:

```
(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit
```

NOTE: For remote systems, the *subunit* is required and is used to differentiate an interface.

When you configure both the `include-irb-and-l2` statement and the `use-vlan-id` statement, the format is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan-id-vlan-id+irb.subunit
```

NOTE: The *svlan-id-vlan-id* represents the VLANs associated with the bridge domain.

When you configure both the `include-irb-and-l2` and `no-vlan-interface-name` statements, the format is as follows:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

When you configure both the `include-irb-and-l2` and `use-interface-description` statements, the format displays the description for the Layer 2 interface:

```
l2_descr:vlan-name+irb.subunit
```

If you configure both the `include-irb-and-l2` and `use-interface-description` statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name:

```
(fe | ge)-fpc/pic/port.subunit:vlan-name+irb.subunit
```

When you configure the `include-irb-and-l2` statement with both the `no-vlan-interface-name` and `use-interface-description` statements, the format displays as follows:

```
l2_descr+irb.subunit
```

If you configure the `include-irb-and-l2` statement with both the `no-vlan-interface-name` and `use-interface-description` statements, and no description is found for the Layer 2 interface, the format displays as follows:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 14.1.

NOTE: The EX Series switches that support the `include-irb-and-l2` statement are the EX4300, EX4600, and EX9200 switches.

RELATED DOCUMENTATION

- *Including a Textual Description in DHCP Options*
- *Using DHCP Relay Agent Option 82 Information*
- *Configuring DHCPv6 Relay Agent Options*

interface (DHCP Local Server)

IN THIS SECTION

- Syntax | 589
- Hierarchy Level | 590
- Description | 591
- Options | 591
- Required Privilege Level | 591
- Release Information | 592

Syntax

```
interface interface-name {
    access-profile profile-name;
    exclude;
    overrides {
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82 | incoming-interface>;
        client-negotiation-match  incoming-interface;
        delay-advertise {
            based-on (option-15 | option-16 | option-18 | option-37) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
```

```
            }
            delay-time seconds;
        }
        delay-offer {
            based-on (option-60 | option-77 | option-82) {
                equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                not-equals {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
                starts-with {
                    ascii ascii-string;
                    hexadecimal hexadecimal-string;
                }
            }
            delay-time seconds;
        }
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        rapid-commit;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-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 ...]
```

Description

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` *`interface-name`* 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.

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 supports only static DHCP configurations.

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.

`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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.0.

Options `upto` and `exclude` introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Understanding Differences Between Legacy DHCP and Extended DHCP

Grouping Interfaces with Common DHCP Configurations

Specifying Authentication Support

interface (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 592
- Hierarchy Level | 593
- Description | 593
- Options | 594
- Required Privilege Level | 594
- Release Information | 594

Syntax

```
interface dhcp-interface-name {
    access-profile profile-name;
    exclude;
    overrides {
        allow-no-end-option
        allow-snooped-clients;
        always-write-giaddr;
```

```
        always-write-option-82;
        asymmetric-lease-time seconds;
        asymmetric-prefix-lease-time seconds;
        client-discover-match <option60-and-option82 | incoming-interface>;
        client-negotiation-match incoming-interface;
        disable-relay;
        dual-stack dual-stack-group-name;
        interface-client-limit number;
        layer2-unicast-replies;
        no-allow-snooped-clients;
        proxy-mode;
        relay-source
        replace-ip-source-with;
        send-release-on-delete;
        trust-option-82;
    }
    service-profile dynamic-profile-name;
    short-cycle-protection <lockout-min-time seconds> <lockout-max-time seconds>;
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay 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 ...]
```

Description

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` *interface-name* 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.

EX Series switches do not support DHCPv6.

> **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. .

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Options `upto` and `exclude` introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- *Grouping Interfaces with Common DHCP Configurations*
- *Specifying Authentication Support*

interface (System Services DHCP)

IN THIS SECTION

- Syntax | 595
- Hierarchy Level | 596
- Description | 596
- Options | 596
- Required Privilege Level | 596
- Release Information | 596

Syntax

```
interface interface-name {
    exclude;
    overrides {
        interface-client-limit number;
    }
    trace;
    upto upto-interface-name;
}
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Description

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 interface-name statement to specify multiple interfaces within a group, but you cannot specify the same interface in more than one group.

Options

- *interface-name*—Name of the interface.
- `trace`—Enable tracing of the interface specified by the *interface-name* argument.
- `upto` *upto-interface-name*—The 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*.

Required Privilege Level

security—To view this statement in the configuration.

security-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Server Configuration | 51

DHCP Server Options | 77

interface-client-limit (DHCP Local Server)

IN THIS SECTION

- Syntax | 597
- Hierarchy Level | 597
- Description | 598
- Default | 599
- Options | 599
- Required Privilege Level | 599
- Release Information | 599

Syntax

```
interface-client-limit number;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server group group-name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
overrides],
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server dhcpv6 overrides],
[edit system services dhcp-local-server dhcpv6 group group-name overrides],
[edit system services dhcp-local-server dhcpv6 group interface interface-name group-name
overrides],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server group group-name interface interface-name overrides]
```

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.

NOTE: Do not use this statement for dual-stack subscribers. Instead, use the "dual-stack-interface-client-limit" on page 541 statement for dual-stack subscribers.

Default

No limit

Options

number—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.

Release Information

Statement introduced in Junos OS Release 9.2.

RELATED DOCUMENTATION

Specifying the Maximum Number of DHCP Clients Per Interface

Overriding the Default DHCP Local Server Configuration Settings

interface-client-limit (DHCP Relay Agent)

IN THIS SECTION

Syntax | 600

- Hierarchy Level | **600**
- Description | **601**
- Default | **601**
- Options | **601**
- Required Privilege Level | **601**
- Release Information | **602**

Syntax

```
interface-client-limit number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
```

```
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

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.

M120 and M320 routers do not support DHCPv6.

NOTE: Do not use this statement for dual-stack subscribers. Instead, use the "dual-stack-interface-client-limit" on page 541 statement for dual-stack subscribers.

Default

`No limit`

Options

number—Maximum number of clients allowed.

- **Range:** 1 through 500,000

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.2.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

dhcp-relay | 470

Extended DHCP Relay Agent Overview

Configuring Group-Specific DHCP Relay Options

Overriding the Default DHCP Relay Configuration Settings

interface-delete (Subscriber Management or DHCP Client Management)

IN THIS SECTION

- Syntax | 603
- Hierarchy Level | 603
- Description | 603
- Required Privilege Level | 603
- Release Information | 603

Syntax

```
interface-delete;
```

Hierarchy Level

```
[edit system services subscriber-management maintain-subscriber]
```

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.

Release Information

Statement introduced in Junos OS Release 11.1.

RELATED DOCUMENTATION

Configuring the Router to Maintain DHCP Subscribers During Interface Delete Events

interface-name (DHCP Local Server)

IN THIS SECTION

- Syntax | 604
- Hierarchy Level | 604
- Description | 605
- Required Privilege Level | 605
- Release Information | 605

Syntax

```
interface-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...],
[edit system services dhcp-local-server 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]
```

Description

Specify that the interface name is concatenated with the username during the subscriber authentication or DHCP client authentication process. Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients

interface-traceoptions (System Services DHCP)

IN THIS SECTION

- Syntax | 606
- Hierarchy Level | 606
- Description | 606
- Options | 606
- Required Privilege Level | 608
- Release Information | 608

Syntax

```
interface-traceoptions {
    file {
        filename ;
        files number;
        match regular-expression;
        size maximum-file-size;
        (world-readable | no-world-readable);
    }
    flag flag;
    level (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

Description

Configure extended DHCP local server tracing operations that can be enabled on a specific interface or group of interfaces. You use the `interface` *interface-name* `trace` statement at the `[edit system services group` *group-name*`]` hierarchy level to enable the tracing operation on the specific interfaces.

Options

file-name—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 `jdhcpd` in the directory `/var/log`. If you include the `file` statement, you must specify a filename.

`files` *`number`*—(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. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

- **Range:** 2 through 1000
- **Default:** 3 files

`flag` *`flag`*—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:

- `all`—Trace all events
- `dhcpv6-packet`—Trace DHCPv6 packet decoding operations.
- `dhcpv6-packet-option`—Trace DHCPv6 option decoding operations.
- `dhcpv6-state`—Trace changes in state for DHCPv6 operations.
- `packet`—Trace packet decoding operations
- `packet-option`—Trace DHCP option decoding operations
- `state`—Trace changes in state

`match` *`regular-expression`*—(Optional) Refine the output to include lines that contain the regular expression.

`no-remote-trace`—Disable remote tracing.

`no-world-readable`—(Optional) Disable unrestricted file access.

`size` *`size`*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option.

- **Syntax:** `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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Server Configuration | 51

DHCP Server Options | 77

ip-address-first

IN THIS SECTION

- Syntax | 608
- Hierarchy Level | 609
- Description | 609
- Required Privilege Level | 609
- Release Information | 609

Syntax

```
ip-address-first;
```

Hierarchy Level

```
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

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.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use

Understanding Differences Between Legacy DHCP and Extended DHCP

Address-Assignment Pools Overview

keep-incoming-circuit-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 610
- Hierarchy Level | 610
- Description | 610
- Required Privilege Level | 611
- Release Information | 611

Syntax

```
keep-incoming-circuit-id ;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id]
```

Description

Specify that the `jdhcpd` process keeps the incoming circuit ID and prepends the ID with the locally generated ID (in the format, `generated-id + incoming-id`) before sending the leasequery packet to the DHCP server.

This configuration is required for leasequery and bulk leasequery operations when subscriber authentication is based on the circuit ID, and enables leasequery and bulk leasequery to restore the agent circuit identifier/agent remote identifier (ACI/ARI) pair and to use the circuit ID to authenticate subscribers.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

keep-incoming-remote-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **612**
- Hierarchy Level | **612**
- Description | **612**
- Required Privilege Level | **613**
- Release Information | **613**

Syntax

```
keep-incoming-remote-id ;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
[edit forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-82 XXXcircuit-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 relay-agent-remote-id],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-82 circuit-id],
```

Description

Specify that the `jdhcpd` process keeps the incoming remote ID and prepends the ID with the locally generated ID (in the format, `generated-id + incoming-id`) before sending the leasequery packet to the DHCPv6 server.

This configuration is required for leasequery and bulk leasequery operations when subscriber authentication is based on the remote ID, and enables leasequery and bulk leasequery to restore the agent circuit identifier/agent remote identifier (ACI/ARI) pair and to use the remote ID to authenticate subscribers.

Use the statement at the `[edit ... dhcpv6]` hierarchy level to configure DHCPv6 support.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

layer2-liveness-detection (Send)

IN THIS SECTION

- Syntax | **613**
- Hierarchy Level | **614**
- Description | **614**
- Options | **615**
- Required Privilege Level | **615**
- Release Information | **616**

Syntax

```
layer2-liveness-detection {
    max-consecutive-retries number;
```

```
    transmit-interval seconds;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection method],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection
method],
[edit forwarding-options dhcp-relay group group-name liveness-detection method],
[edit forwarding-options dhcp-relay liveness-detection method],


[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method],
[edit system services dhcp-local-server dhcpv6 liveness-detection method],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection
method],
[edit system services dhcp-local-server group group-name liveness-detection method],
[edit system services dhcp-local-server liveness-detection method],
```

Description

Configure a router acting as a broadband network gateway (BNG) to conduct a host connectivity check on its directly connected DHCPv4 and DHCPv6 clients to determine the validity and state of the DHCP client session, and to clean up inactive sessions.

The BNG sends ARP or ND request packets to the each DHCP client at a configurable interval, then waits for a response. If it receives a response from a client before the interval times out, it sends another request to the client when the timer expires.

If the BNG does not receive a response before the interval times out, it sets the timer to 30 seconds and sends another request. This is the first retry attempt.

If it receives a response from a client before the 30-second interval times out, it sends another request to the client when the timer expires. If the 30-second timer expires before a response is received, the BNG sets the timer to 10 seconds and sends another request. This is the second retry attempt. If the BNG does not receive a response within this interval it resets the timer to 10 seconds and sends another

request. The BNG continues to send requests at 10-second intervals until it either receives a response from the client before the interval times out or exhausts the number of retry attempts.

The first retry attempt uses a 30-second interval. Subsequent retries occur at 10-second intervals. The number of possible 10-second retries is therefore the total number of retries minus 1. For example, if you configure 5 retries, there is one 30-second retry and up to four 10-second retries.

If the BNG attempts all the retries and never receives a response from a client within the interval, the client session is declared to be down.

NOTE: The only option to the `failure-action` statement supported by Layer 2 liveness detection is `clear-binding`.

Options

max-consecutive-retries *number*

Maximum number of consecutive times that the router sends an ARP request packet in the absence of an ARP response packet.

- **Range:** 3 through 6 retries
- **Default:** 3 retries

transmit-interval *seconds*

Initial interval that the router waits for an ARP response after sending an ARP request packet to the client or waits for an ND response packet after sending an NG request packet to the client.

- **Range:** 300 through 1800 seconds
- **Default:** 300 seconds

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.4R1.

RELATED DOCUMENTATION

- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets
- DHCP Liveness Detection Overview

layer2-unicast-replies

IN THIS SECTION

- Syntax | 616
- Hierarchy Level | 616
- Description | 617
- Required Privilege Level | 617
- Release Information | 617

Syntax

```
layer2-unicast-replies;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
```

```
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

dhcp-relay | 470

lease-time

IN THIS SECTION

- Syntax | 618
- Hierarchy Level | 618
- Description | 618
- Default | 619
- Options | 619
- Required Privilege Level | 619
- Release Information | 619

Syntax

```
lease-time (length | infinite);
```

Hierarchy Level

```
[edit interfaces interface-name                unit                logical-unit-
number            family     inet dhcp]
```

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.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

DHCP Client | **234**

DHCPv6 Client | **255**

lease-time (dhcp-client)

IN THIS SECTION

- Syntax | 620
- Hierarchy Level | 620
- Description | 620
- Options | 620
- Required Privilege Level | 621
- Release Information | 621

Syntax

```
lease-time seconds;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Specify the time to negotiate and exchange Dynamic Host Configuration Protocol (DHCP) information.

Options

seconds Request time to negotiate and exchange information.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-client` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

RELATED DOCUMENTATION

DHCP Overview | 2

liveness-detection

IN THIS SECTION

- Syntax | 622
- Hierarchy Level | 622
- Description | 623
- Required Privilege Level | 623
- Release Information | 623

Syntax

```
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;
        }
        layer2-liveness-detection {
            max-consecutive-retries number;
            transmit-interval interval;
        }
    }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name ],
[edit forwarding-options dhcp-relay group group-name],
[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 dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server group group-name]
```

Description

Configure bidirectional failure detection timers and authentication criteria for static routes.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- DHCP Liveness Detection Overview
- Configuring Detection of DHCP Local Server Client Connectivity with BFD
- Configuring Detection of DHCP Relay or DHCP Relay Proxy Client Connectivity with BFD
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

local-server-group (DHCP Relay Agent Option)

IN THIS SECTION

- Syntax | 624
- Hierarchy Level | 624
- Description | 625
- Options | 625
- Required Privilege Level | 625
- Release Information | 625

Syntax

```
local-server-group local-server-group;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option (default-action | equals | starts-with)],
[edit forwarding-options dhcp-relay group group-name relay-option (default-action | equals | starts-with)],
[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 ...]
```

Description

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.

The `local-server-group` option is not supported for DHCPv6 relay agent.

Options

local-server-group	Name of DHCP local server group.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic

location (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 626
- Hierarchy Level | 626
- Description | 626
- Required Privilege Level | 627
- Release Information | 627

Syntax

```
location name;
```

Hierarchy Level

```
[edit forwarding-optionsdhcp-relay relay-option-82 vendor-specific],
[edit forwarding-options dhcp-relaygroup group-name relay-option-82 vendor-specific]
```

Description

Supports the addition of a vendor-specific location in the option 82, suboption 9 field of DHCPv4 control messages on server-facing interfaces. The location should be specified as interface, vlan ID, and if applicable, svlan ID. For example, **<ifd-name>:<vlan>** (ae0:100) or **<ifd-name>:<svlan> -<vlan>** (ae0:100-10).

Junos OS automatically adds the remaining vendor-specific information as per RFC 4243, *Vendor-Specific Information Suboption for the Dynamic Host Configuration Protocol (DHCP) Relay Agent Option*. The Juniper Networks enterprise ID is 2636. The the location is option-data 2 (the hostname is

option-data 1). The DHCPv4 relay strips the suboption data from replies from the server before it relays the packets out the client facing interface.

This feature can be useful, in conjunction with operator-developed tools, for troubleshooting DHCP servers and providing service assurances. For example, a central DHCP server can log the information, and operators can query the hostname to track and troubleshoot subscriber IP information and network attachment points.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Command introduced in Junos OS Release 16.2.

log

IN THIS SECTION

- Syntax | **628**
- Hierarchy Level | **628**
- Description | **628**
- Options | **629**
- Required Privilege Level | **629**
- Release Information | **630**

Syntax

```
log {
    session {
        client;
        all;
        dhcpv6 {
            client;
            server;
            relay;
            dynamic-server;
            all;
        }
        server;
        relay;
    }
}
```

Hierarchy Level

```
[edit system processes dhcp-service]
```

Description

Enable DHCP session log on the device. Session logs include the information on the session creation, deletion and renew events. You can use the session logs for monitoring and troubleshooting purposes.

DHCP logs are written to system syslog that you define using the following command:

`set system syslog ( file filename | host destination) user logging-level`

Example:

```
syslog {
        host 10.10.10.10 {
        user any;
```

```
    }
    file file-1 {
        user any;
    }
}
```

In the example:

Syslog messages are stored on the host with IP address 10.10.10.10 for all severity levels.

Syslog messages are stored in the file file-1 at /var/log/<file-name> for all severity levels.

Options

- `session`—Logs of the DHCP sessions.
- `client`—Log sessions of the DHCP client.
- `all`—Log sessions of the DHCP client, server and relay.
- `dhcpv6`—Log sessions of the DHCPv6.
- `client`—Log sessions of the DHCPv6 client.
- `dynamic-server`—Log sessions of the DHCPv6 dynamic server.
- `all`—Log sessions of the DHCPv6 client, server, relay and dynamic server.
- `server`—Log sessions of the DHCP server.
- `relay`—Log sessions of the DHCP relay.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 19.1R1.

RELATED DOCUMENTATION

dhcp-service | 486

logical-system-name (DHCP Local Server)

IN THIS SECTION

- Syntax | 630
- Hierarchy Level | 630
- Description | 631
- Required Privilege Level | 631
- Release Information | 631

Syntax

```
logical-system-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server dhcpv6 authentication username-include],
[edit system services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
[edit logical-systems 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 ...]
```

Description

Specify that the logical system name be concatenated with the username during the subscriber authentication or DHCP client process. No logical system name is concatenated if the configuration is in the default logical system.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

mac-address (DHCP Local Server)

IN THIS SECTION

- Syntax | 632
- Hierarchy Level | 632

- Description | 632
- Required Privilege Level | 633
- Release Information | 633

Syntax

```
mac-address;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[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]
```

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or DHCP client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

RELATED DOCUMENTATION

Specifying Authentication Support

mac-address (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 634
- Hierarchy Level | 634
- Description | 634

Required Privilege Level | 635
Release Information | 635

Syntax

```
mac-address;
```

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 group-name authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[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 ...]
```

Description

Specify that the MAC address from the client PDU be concatenated with the username during the subscriber authentication or client authentication process.

For DHCPv6 clients, because the DHCPv6 packet format has no specific field for the client MAC address, the MAC address is derived from among several sources with the following priority:

- Client DUID Type 1 or Type 3.
- Option 79 (client link-layer address), if present.
- The packet source address if the client is directly connected.
- The link local address.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support for DHCPv6 added in Junos OS Release 17.2 for MX Series Routers.

RELATED DOCUMENTATION

Specifying Authentication Support

maximum-hop-count

IN THIS SECTION

- Syntax | 635
- Hierarchy Level | 636
- Description | 636
- Options | 636
- Required Privilege Level | 636
- Release Information | 636

Syntax

```
maximum-hop-count number;
```

Hierarchy Level

```
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (interface-name | interface-group)]
```

Description

Set the maximum allowed number of hops. This value is compared against the hops field in the BOOTP request message. BOOTP request messages that have a number in the hops field that exceeds `maximum-hop-count` are not forwarded. If you omit the `maximum-hop-count` statement, the default value is four hops.

Options

number—Maximum number of hops for BOOTP request messages.

- **Range:** 1 through 16
- **Default:** 4

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

maximum-lease-time (DHCP)

IN THIS SECTION

- Syntax | 637
- Hierarchy Level | 637
- Description | 637
- Options | 638
- Required Privilege Level | 638
- Release Information | 638

Syntax

```
maximum-lease-time seconds;
```

Hierarchy Level

```
[edit system services dhcp],
```

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

seconds—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

Release Information

Statement introduced before Junos OS Release 7.4.

method

IN THIS SECTION

- Syntax | 638
- Hierarchy Level | 639
- Description | 639
- Required Privilege Level | 640
- Release Information | 640

Syntax

```
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;
    }
    layer2-liveness-detection {
        max-consecutive-retries number;
        transmit-interval interval;
    }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection],
[edit forwarding-options dhcp-relay dhcpv6 liveness-detection],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name liveness-detection],
[edit forwarding-options dhcp-relay group group-name liveness-detection],
[edit forwarding-options dhcp-relay liveness-detection],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection],
[edit system services dhcp-local-server dhcpv6 liveness-detection],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name liveness-detection],
[edit system services dhcp-local-server group group-name liveness-detection],
[edit system services dhcp-local-server liveness-detection]
```

Description

Configure the liveness detection method.

NOTE: The "bfd" on page 396 stanza is not available at the `[edit forwarding-options dhcp-relay dual-stack-group` *`dual-stack-group-name`* `liveness-detection method]` or `[edit system services dhcp-local-server dual-stack-group` *`dual-stack-group-name`* `liveness-detection` hierarchy levels.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- DHCP Liveness Detection Overview
- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients
- DHCP Liveness Detection Using ARP and Neighbor Discovery Packets

minimum-interval

IN THIS SECTION

Syntax | 641

- Hierarchy Level | 641
- Description | 642
- Options | 642
- Required Privilege Level | 642
- Release Information | 642

Syntax

```
minimum-interval milliseconds;
```

Hierarchy Level

```
[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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server group group-name liveness-detection method bfd transmit-
interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd
transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-
interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd
transmit-interval]
```

Description

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.

Options

`milliseconds` — Specify the minimum interval value for BFD liveliness detection.

- **Range:** 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

minimum-receive-interval

IN THIS SECTION

- Syntax | 643
- Hierarchy Level | 643
- Description | 644
- Options | 644
- Required Privilege Level | 644
- Release Information | 644

Syntax

```
minimum-receive-interval milliseconds;
```

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

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

milliseconds — Specify the minimum receive interval value.

- **Range:** 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

minimum-wait-time

IN THIS SECTION

- Syntax | 645
- Hierarchy Level | 645
- Description | 645
- Options | 646
- Required Privilege Level | 646
- Release Information | 646

Syntax

```
minimum-wait-time seconds;
```

Hierarchy Level

```
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface (interface-name | interface-group)]
```

Description

To set the minimum allowed number of seconds in the secs field of the BOOTP message, include the minimum-wait-time statement. This setting configures a minimum number of seconds since the client sent its first BOOTP request. BOOTP messages that have a smaller number in the secs field than the allowed minimum are not forwarded. The default value for the minimum wait time is zero (0).

The default value for the minimum wait time is zero (0) seconds. If the minimum wait time is 0 and the secs field in the BOOTP request message is 0, the device forwards the packet.

Options

seconds Minimum wait time the BOOTP client has waited before packets are forwarded.

- **Range:** 0 to 30,000
- **Default:** 0

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

multiplier

IN THIS SECTION

Syntax | 647

- Hierarchy Level | 647
- Description | 647
- Options | 648
- Required Privilege Level | 648
- Release Information | 648

Syntax

```
multiplier number;
```

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Description

Configure the number of hello packets not received by the neighbor before Bidirectional Forwarding Detection (BFD) declares the neighbor down.

Options

number Maximum allowable number of hello packets missed by the neighbor.

- **Range:** 1 through 255
- **Default:** 3

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

name-server (Access)

IN THIS SECTION

- Syntax | 649
- Hierarchy Level | 649
- Description | 649
- Required Privilege Level | 649

Release Information | 649

Syntax

```
name-server address
```

Hierarchy Level

```
[edit access address-assignment pool <name> family (inet | inet6) dhcp-attributes]
```

Description

Specify the DNS server IP address for an address-assignment pool.

Required Privilege Level

access—To view this statement in the configuration.

access-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

address-assignment (Access)

name-server (System Services)

IN THIS SECTION

- Syntax | 650
- Hierarchy Level | 650
- Description | 651
- Options | 651
- Required Privilege Level | 651
- Release Information | 651

Syntax

```
name-server {
    address {
        routing-instance routing-instance;
    }
}
```

Hierarchy Level

```
[edit system],
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

Configure one or more Domain Name System (DNS) name servers.

Options

address Address of the name server. To configure multiple name servers, include a maximum of three *address* options.

routing-instance *routing-instance* Configure name of the routing instance through which the name server is reachable.

> **NOTE**: The only routing instance supported is `mgmt_junos`. Also, this routing instance command is not supported on SRX Series devices.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

`routing-instance` options introduced in Junos OS Release 19.2R1 under the `[edit system]` hierarchy level only.

RELATED DOCUMENTATION

- Configuring a DNS Name Server for Resolving Hostnames into Addresses

next-server

IN THIS SECTION

- Syntax | 652
- Hierarchy Level | 652
- Description | 652
- Options | 653
- Required Privilege Level | 653
- Release Information | 653

Syntax

```
next-server next-server;
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool pool-id],
[edit system services dhcp static-binding mac-address]
```

Description

(J Series Services Routers only) Specify the IP address for the next DHCP server used for communication after a DHCP boot client establishes initial contact.

Options

next-server—The IP address of the DHCP server that is used as the “siaddr” in a DHCP protocol packet.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.4.

no-adaptation

IN THIS SECTION

- Syntax | **653**
- Hierarchy Level | **654**
- Description | **654**
- Required Privilege Level | **654**
- Release Information | **654**

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

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.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

no-allow-snooped-clients

IN THIS SECTION

- Syntax | 655
- Hierarchy Level | 655
- Description | 656
- Required Privilege Level | 656
- Release Information | 656

Syntax

```
no-allow-snooped-clients;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit forwarding-options dhcp-relay overrides],
[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 ...]
```

Description

Explicitly disable DHCP snooping support on DHCP relay agent.

Use the statement at the `[edit ... dhcpv6]` hierarchy levels to explicitly disable snooping support for DHCPv6 relay agent.

NOTE: In Junos OS Release 10.0 and earlier, DHCP snooping is *enabled* by default. In Release 10.1 and later, DHCP snooping is *disabled* by default.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.2.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Overriding the Default DHCP Relay Configuration Settings

DHCP Snooping Support

Configuring DHCP Snooped Packets Forwarding Support for DHCP Relay Agent

no-bind-on-request (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 657
- Hierarchy Level | 657
- Description | 658
- Required Privilege Level | 658
- Release Information | 658

Syntax

```
no-bind-on-request;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name overrides],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (*stray* requests). Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

M120 and M320 routers do not support DHCPv6.

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.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- *Overriding the Default DHCP Relay Configuration Settings*
- *Disabling Automatic Binding of Stray DHCP Requests*

no-listen

IN THIS SECTION

- Syntax | 659
- Hierarchy Level | 659
- Description | 660
- Required Privilege Level | 660
- Release Information | 660

Syntax

```
no-listen;
```

Hierarchy Level

```
[edit forwarding-options helpers bootp interface (interface-name | interface-group)],
[edit forwarding-options helpers domain interface interface-name],
[edit forwarding-options helpers port port-number interface interface-name],
[edit forwarding-options helpers tftp interface interface-name]
```

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.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

Configuring DNS and TFTP Packet Forwarding

Configuring Port-based LAN Broadcast Packet Forwarding

Configuring Routers, Switches, and Interfaces as DHCP and BOOTP Relay Agents

no-vlan-interface-name

IN THIS SECTION

- Syntax | **661**
- Hierarchy Level | **661**
- Description | **661**
- Required Privilege Level | **663**
- Release Information | **663**

Syntax

```
no-vlan-interface-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

Description

When you do not want bridge domain or VLAN tag information, do not include the VLAN ID nor the VLAN interface name (the default) in the circuit or remote ID value in the DHCP option 82 information.

NOTE: The `no-vlan-interface-name` statement is mutually exclusive with the `use-interface-description` and `use-vlan-id` statements.

When you configure the `no-vlan-interface-name` statement only, the format displays only the Layer 3 interface:

```
irb.subunit
```

NOTE: The *subunit* is required and used to differentiate the interface for remote systems.

When you configure the `no-vlan-interface-name` and `use-interface-description` statements, the format displays the IRB interface description:

```
irb_descr
```

If you configure the `no-vlan-interface-name` and `use-interface-description` statements, and no description for the IRB interface is found, the format displays the IRB interface name:

```
irb.subunit
```

When you configure the `no-vlan-interface-name` and `include-irb-and-l2` statements, the format displays the Layer 2 logical interface name and the IRB interface name:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

When you configure the `no-vlan-interface-name`, `include-irb-and-l2` and `use-interface-name` statements, the format displays the Layer 2 interface description and the IRB interface name:

```
l2_descr+irb.subunit
```

If you configure the `no-vlan-interface-name`, `include-irb-and-l2` and `use-interface-name` statements, and no description for the Layer 2 interface is found, the format displays the Layer 2 logical interface name and the IRB interface name:

```
(fe | ge)-fpc/pic/port.subunit+irb.subunit
```

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 14.1.

NOTE: The EX Series switches that support the `no-vlan-interface-name` statement are the EX4300, EX4600, and EX9200 switches.

RELATED DOCUMENTATION

Including a Textual Description in DHCP Options

Using DHCP Relay Agent Option 82 Information

Configuring DHCPv6 Relay Agent Options

on-demand-address-allocation

IN THIS SECTION

- Syntax | 664
- Hierarchy Level | 664
- Description | 664
- Required Privilege Level | 664
- Release Information | 665

Syntax

```
on-demand-address-allocation;
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-group
dual-stack-group-name],
[edit logical-systems name system services dhcp-local-server dual-stack-group dual-stack-group-
name],
[edit routing-instances name system services dhcp-local-server dual-stack-group dual-stack-group-
name],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name]
```

Description

Enables an address or prefix to be allocated on demand when a dual-stack subscriber session is established. Starting in Junos OS Release 18.1R1, when reauthentication is configured, enables per-family address allocation as each family's DHCP session is established. In earlier released, applies only to the second family of the dual stack.

NOTE: You must configure `on-demand-address-allocation` if you also configure reauthentication for dual-stack, single-session DHCP subscribers. This is true whether you enable reauthentication with the `reauthenticate` statement or the Reauthenticate-On-Renew VSA (26-206).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.3R1.

RELATED DOCUMENTATION

- *Configuring RADIUS Reauthentication for DHCP Subscribers*
- *RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers*
- *Single-Session DHCP Dual-Stack Overview*
- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution*
- *Configuring Access Components for the PPPoE Wholesale Network Solution*
- *Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*

option (DHCP server)

IN THIS SECTION

- Syntax | **666**
- Hierarchy Level | **666**
- Description | **666**
- Options | **666**
- Required Privilege Level | **667**
- Release Information | **667**

Syntax

```
option {
    [ (id-number option-type option-value) | (id-number array option-type option-value) ];
}
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

Configure one or more user-defined options that are not included in the Junos default implementation of the DHCP server. For example, if a client requests a DHCP option that is not included in the DHCP server, you can create a user-defined option that enables the server to respond to the client's request.

Options

- *id-number*—Any whole number. The ID number is used to index the option and must be unique across a DHCP server.
- *option-type*—Any of the following types: `byte`, `byte-stream`, `flag`, `integer`, `ip-address`, `short`, `string`, `unsigned-integer`, `unsigned-short`.
- `array`—An option can include an array of values.
- *option-value*—Value associated with an option. The option value must be compatible with the option type (for example, an `On` or `Off` value for a `flag` type).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4. Statement introduced in Junos OS Release 9.0 .

option-60 (DHCP Local Server)

IN THIS SECTION

- Syntax | 667
- Hierarchy Level | 667
- Description | 668
- Required Privilege Level | 668
- Release Information | 668

Syntax

```
option-60;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

option-60 (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 669
- Hierarchy Level | 670
- Description | 671
- Required Privilege Level | 671
- Release Information | 671

Syntax

```
option-60 {
    default-action {
        drop drop;
        forward-only forward-only;
        local-server-group local-server-group;
    }
    equals {
        ascii name {
            drop drop;
            forward-only forward-only;
            local-server-group local-server-group;
        }
        hexadecimal name {
            drop drop;
            forward-only forward-only;
            local-server-group local-server-group;
        }
    }
    not-present {
        drop drop;
        forward-only forward-only;
        local-server-group local-server-group;
    }
```

```
    equals {
        ascii name {
            drop drop;
            forward-only forward-only;
            local-server-group local-server-group;
        }
        hexadecimal name {
            drop drop;
            forward-only forward-only;
            local-server-group local-server-group;
        }
    }
}
```

Hierarchy Level

```
[edit bridge-domains name forwarding-options dhcp-relay group name relay-option],
[edit bridge-domains name forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay group name relay-option],
[edit forwarding-options dhcp-relay relay-option],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay group name relay-
option],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay relay-option],
[edit logical-systems name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name forwarding-options dhcp-relay relay-option],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-
relay group name relay-option],
[edit logical-systems name routing-instances name bridge-domains name forwarding-options dhcp-
relay relay-option],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay group name relay-
option],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay relay-option],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay group
name relay-option],
[edit logical-systems name routing-instances name vlans name forwarding-options dhcp-relay relay-
option],
[edit logical-systems name vlans name forwarding-options dhcp-relay group name relay-option],
[edit logical-systems name vlans name forwarding-options dhcp-relay relay-option],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay group name relay-
```

```
option],
[edit routing-instances name bridge-domains name forwarding-options dhcp-relay relay-option],
[edit routing-instances name forwarding-options dhcp-relay group name relay-option],
[edit routing-instances name forwarding-options dhcp-relay relay-option],
[edit routing-instances name vlans name forwarding-options dhcp-relay group name relay-option],
[edit routing-instances name vlans name forwarding-options dhcp-relay relay-option],
[edit vlans name forwarding-options dhcp-relay group name relay-option],
[edit vlans name forwarding-options dhcp-relay relay-option]
```

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.

Release Information

Statement introduced in Junos OS Release 9.1.

Statement updated in Junos OS Release 17.4R1 for MX Series.

RELATED DOCUMENTATION

Specifying Authentication Support

DHCPv4 and DHCPv6 Forward-Only Action for Relay Traffic with Unknown DHCP Server Address

option-82 (DHCP Local Server Authentication)

IN THIS SECTION

- Syntax | 672
- Hierarchy Level | 672
- Description | 673
- Options | 673
- Required Privilege Level | 673
- Release Information | 673

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
```

```
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[edit system services dhcp-local-server authentication username-include],
[edit system services dhcp-local-server group group-name authentication username-include]
```

Description

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.

Options

`circuit-id`—(Optional) Agent Circuit ID suboption (suboption 1).

`remote-id`—(Optional) Agent Remote ID suboption (suboption 2).

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

option-82 (DHCP Local Server Pool Matching)

IN THIS SECTION

- Syntax | 674
- Hierarchy Level | 674
- Description | 674
- Required Privilege Level | 675
- Release Information | 675

Syntax

```
option-82;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server pool-match-order],
[edit logical-systems logical-system-name system services dhcp-local-server pool-match-order],
[edit routing-instances routing-instance-name system services dhcp-local-server pool-match-order],
[edit system services dhcp-local-server pool-match-order]
```

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.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

- *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
- *Understanding Differences Between Legacy DHCP and Extended DHCP*
- *Address-Assignment Pools Overview*

option-82 (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **676**
- Hierarchy Level | **676**
- Description | **676**
- Options | **677**
- Required Privilege Level | **677**
- Release Information | **677**

Syntax

```
option-82 <circuit-id> <remote-id>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication username-include],
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
```

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.

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.

Options

`circuit-id`—(Optional) The string for the Agent Circuit ID suboption (suboption 1).

`remote-id`—(Optional) The string for the Agent Remote ID suboption (suboption 2).

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

option-number (DHCP Relay Agent Option)

IN THIS SECTION

- Syntax | **678**
- Hierarchy Level | **678**
- Description | **678**
- Options | **678**
- Required Privilege Level | **679**
- Release Information | **679**

Syntax

```
option-number option-number;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option],
[edit forwarding-options dhcp-relay dhcpv6 relay-option],
[edit forwarding-options dhcp-relay group group-name relay-option],
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option],
[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 ...]
```

Description

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.

Use the `[edit forwarding-options dhcp-relay dhcpv6]` hierarchy level to configure the DHCPv6 relay agent support.

Options

option-number—The DHCP or DHCPv6 option in the incoming traffic.

NOTE: EX Series switches do not support the User Class Options.

- 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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic

overrides (DHCP Local Server)

IN THIS SECTION

- Syntax | **680**
- Hierarchy Level | **681**
- Description | **681**
- Required Privilege Level | **682**
- Release Information | **682**

Syntax

```
asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    client-negotiation-match incoming-interface;
    delay-advertise {
        based-on (option-15 | option-16 | option-18 | option-37) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
        }
        delay-time seconds;
    }
    delay-offer {
        based-on (option-60 | option-77 | option-82) {
            equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            not-equals {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
            starts-with {
                ascii ascii-string;
                hexadecimal hexadecimal-string;
            }
        }
        delay-time seconds;
    }
    delegated-pool;
```

```
    delete-binding-on-renegotiation;
    dual-stack dual-stack-group-name;
    include-option-82 {
        forcerenew;
        nak;
    }
    interface-client-limit number;
    multi-address-embedded-option-response;
    process-inform {
        pool pool-name;
    }
    protocol-attributes attribute-set-name;
    rapid-commit;
}
```

Hierarchy Level

```
[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 ...]
```

Description

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.

- 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.

> **NOTE**: By default, `jdhcp` does not process DHCPINFORM message. Only after you enable the overrides command using the `set system services dhcp-local-server overrides process-inform` statement, `jdhcp` starts processing the DHCPINFORM message.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

The `interface-client-limit` statement is not supported in the `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

The *`asymmetric-prefix-lease-time`*, `delegated-pool`, *`multi-address-embedded-option-response`*, and `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.

Release Information

Statement introduced in Junos OS Release 9.2.

Support for the `allow-no-end` option introduced in Junos OS Release 14.1X53-D15 for EX Series switches.

RELATED DOCUMENTATION

- *Understanding Differences Between Legacy DHCP and Extended DHCP*
- *Overriding the Default DHCP Local Server Configuration Settings*
- Configuring a DHCP Server on Switches

overrides (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 683
- Hierarchy Level | 684
- Description | 684
- Required Privilege Level | 685
- Release Information | 685

Syntax

```
overrides {
    allow-no-end-option;
    allow-snooped-clients;
    always-write-giaddr;
    always-write-option-82;
    asymmetric-lease-time seconds;
    asymmetric-prefix-lease-time seconds;
    client-discover-match <option60-and-option82 | incoming-interface>;
    client-negotiation-match incoming-interface;
    delay-authentication;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack dual-stack-group-name;
    interface-client-limit number;
    layer2-unicast-replies;
    no-allow-snooped-clients;
```

```
    no-bind-on-request;
    proxy-mode;
    relay-source
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-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 ...]
```

Description

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.

M120 and M320 routers do not support DHCPv6.

The following statements are supported at both the `[edit ... dhcp-relay]` and `[edit ... dhcpv6]` hierarchy levels.

- `allow-snooped-clients`
- `asymmetric-lease-time`
- `delete-binding-on-renegotiation`

- dual-stack
- interface-client-limit
- no-allow-snooped-clients
- no-bind-on-request
- relay-source
- send-release-on-delete

The following statements are supported at the [edit ... dhcpv6] hierarchy levels only.

- asymmetric-prefix-lease-time

All other statements are supported at the [edit ... dhcp-relay] hierarchy levels only.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Support at the [edit ... dhcpv6] hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Overriding the Default DHCP Relay Configuration Settings

overrides (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 686
- Hierarchy Level | 687
- Description | 687
- Options | 687
- Required Privilege Level | 688
- Release Information | 688

Syntax

```
overrides {
    allow-no-end-option;
     always-write-option-82;
    asymmetric-lease-time;
    bootp-support;
    delete-binding-on-renegotiation;
    disable-relay;
    dual-stack;
    no-bind-on-request;
    relay-source;
    replace-ip-source-with;
    send-release-on-delete;
    trust-option-82;
    user-defined-option-82;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Description

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.

Options

allow-no-end-option — Accept packets without end-of-option.

asymmetric-lease-time — Provides a way to send the DHCP client a lease that is shorter than the actual lease granted by the DHCP local server.

- **Range:** 600 through 86,400 seconds.

bootp-support — Allows send bootp request from a remote client to a DHCP server for an IP address.

delete-binding-on-renegotiation — Allows DHCP relay agent to delete binding information for a specific client when a DHCP DISCOVER packet is received from the client.

disable-relay — Disable DHCP relay processing.

dual-stack — Specify the dual stack group to use.

no-bind-on-request — Explicitly disable automatic binding of received DHCP request messages that have no entry in the database (stray requests).

relay-source — Specify the interface for relay source.

send-release-on-delete — Always send RELEASE to the server when a binding is deleted.

trust-option-82 — Allow processing of DHCP client packets that have a gateway IP address giaddr of 0 and contain option 82 information.

user-defined-option-82 Specify user defined description for option-82.

The remaining statements are explained separately. see CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

RELATED DOCUMENTATION

replace-ip-source-with (DHCP Relay Agent) | 755

always-write-option-82 | 382

overrides (System Services DHCP)

IN THIS SECTION

- Syntax | 689
- Hierarchy Level | 689
- Description | 689
- Options | 690
- Required Privilege Level | 690
- Release Information | 690

Syntax

```
overrides {
    interface-client-limit number;
}
```

Hierarchy Level

```
[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]
```

Description

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.

- 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 dhcpv6 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 dhcpv6 group group-name interface interface-name]` hierarchy level.
- Use the DHCPv6 hierarchy levels to override DHCPv6 configuration options.

Options

`interface-client-limit` *number*—Sets the maximum number of 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.

- **Range:** 1 through 500,000
- **Default:** No limit

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Additional Configurations for DHCP Clients | 300

password (DHCP Local Server)

IN THIS SECTION

- Syntax | 691
- Hierarchy Level | 691
- Description | 692
- Options | 692

Required Privilege Level | 692
Release Information | 692

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6
authentication],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name authentication],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
```

```
authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dhcpv6 group group-name authentication],
[edit system services dhcp-local-server group group-name authentication]
```

Description

Configure the password that is sent to the external AAA authentication server for subscriber authentication or DHCP client authentication.

Options

password-string—Authentication password.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

password (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 693
- Hierarchy Level | 693
- Description | 694
- Options | 694
- Required Privilege Level | 694
- Release Information | 694

Syntax

```
password password-string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
authentication],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
```

```
options dhcp-relay dhcpv6 authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name authentication],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
authentication],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name authentication]
```

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

password-string—Authentication password.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the [edit ... dual-stack-group *dual-stack-group-name* authentication] hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Specifying Authentication Support

Example-Configuring DHCP with External Authentication Server

pool (DHCP Local Server Overrides)

IN THIS SECTION

- Syntax | 695
- Hierarchy Level | 695
- Description | 697
- Options | 697
- Required Privilege Level | 697
- Release Information | 697

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]

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.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Enabling Processing of Client Information Requests

Overriding the Default DHCP Local Server Configuration Settings

pool (System)

IN THIS SECTION

- Syntax | 698
- Hierarchy Level | 698
- Description | 699
- Options | 699
- Required Privilege Level | 699
- Release Information | 699

Syntax

```
pool address/prefix-length {
    address-range {
        low address;
        high address;
    }
    exclude-address {
        address;
    }
}
```

Hierarchy Level

```
[edit system services dhcp],
```

Description

For J Series Services Routers and EX Series switches only. Configure a pool of IP addresses for DHCP clients on a subnet. When a client joins the network, the DHCP server dynamically allocates an IP address from this pool.

Options

`address-range`—Lowest and highest IP addresses in the pool that are available for dynamic address assignment. If no range is specified, the pool will use all available addresses within the subnet specified. (Broadcast addresses, interface addresses, and excluded addresses are not available.)

`exclude-address`—Addresses within the range that are not used for dynamic address assignment. You can exclude one or more addresses within the range.

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

address-assignment (Address-Assignment Pools) | 367

pool-match-order

IN THIS SECTION

- Syntax | 700
- Hierarchy Level | 700
- Description | 701
- Default | 701
- Required Privilege Level | 701
- Release Information | 701

Syntax

```
pool-match-order {
    external-authority;
    ip-address-first;
    option-82;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server],
[edit logical-systems logical-system-name system services dhcp-local-server],
[edit routing-instances routing-instance-name system services dhcp-local-server],
[edit system services dhcp-local-server]
```

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

> *Configuring How the Extended DHCP Local Server Determines Which Address-Assignment Pool to Use*
>
> *Understanding Differences Between Legacy DHCP and Extended DHCP*

preferred-prefix-length

IN THIS SECTION

- Syntax | 702
- Hierarchy Level | 702
- Description | 702
- Required Privilege Level | 703
- Release Information | 703

Syntax

```
preferred-prefix-length preferred-prefix-length;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client prefix-delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client prefix-delegating]
```

Description

Allows you to configure DHCPv6 client preferred prefix length. If preferred-prefix-length is configured, the DHCPv6 client checks the prefix length in the ADVERTISE packet and if the check fails, a sysolg is created.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

sub-prefix-length | 810

prefix (DHCP Client)

IN THIS SECTION

- Syntax | 703
- Hierarchy Level | 704
- Description | 704
- Required Privilege Level | 704
- Release Information | 704

Syntax

```
prefix {
    host-name;
    logical-system-name;
```

```
    routing-instance-name;
}
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-
identifier]
```

Description

Specify a prefix as a client identifier.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

prefix (DHCP Relay Agent)

IN THIS SECTION

Syntax | 705

- Hierarchy Level | 705
- Description | 705
- Options | 706
- Required Privilege Level | 706
- Release Information | 706

Syntax

```
prefix prefix;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)]
```

Description

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.

Options

prefix—Any of the following:

- `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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... relay-agent-remote-id]` and `[edit ... remote-id]` hierarchy levels introduced in Junos OS Release 14.1.

RELATED DOCUMENTATION

Including a Prefix in DHCP Options

Using DHCP Relay Agent Option 82 Information

Configuring DHCPv6 Relay Agent Options

process-inform

IN THIS SECTION

- Syntax | 707
- Hierarchy Level | 707
- Description | 708
- Default | 709
- Required Privilege Level | 709
- Release Information | 709

Syntax

```
process-inform {
    pool pool-name;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name interface interface-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name interface interface-name overrides],
```

```
[edit logical-systems logical-system-name system services dhcp-local-server overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name interface interface-name overrides],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
overrides],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
interface interface-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name interface interface-name overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
overrides],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
interface interface-name overrides],
[edit system services dhcp-local-server overrides],
[edit system services dhcp-local-server dhcpv6 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],
[edit system services dhcp-local-server group group-name overrides],
[edit system services dhcp-local-server group group-name interface interface-name overrides]
```

Description

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

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.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Enabling Processing of Client Information Requests

Overriding the Default DHCP Local Server Configuration Settings

profile (Access)

IN THIS SECTION

- Syntax | **710**
- Hierarchy Level | **715**
- Description | **716**
- Options | **716**
- Required Privilege Level | **716**
- Release Information | **716**

Syntax

```
profile profile-name {
    accounting {
        address-change-immediate-update
        accounting-stop-on-access-deny;
        accounting-stop-on-failure;
        ancp-speed-change-immediate-update;
        coa-immediate-update;
        coa-no-override service-class-attribute;
        duplication;
        duplication-filter;
        duplication-vrf {
            access-profile-name profile-name;
            vrf-name vrf-name;
        }
        immediate-update;
        order [ accounting-method ];
        send-acct-status-on-config-change;
        statistics (time | volume-time);
        update-interval minutes;
        wait-for-acct-on-ack;
    }
    accounting-order (radius | [accounting-order-data-list]);
    authentication-order [ authentication-methods ];
    client client-name {
        chap-secret chap-secret;
        group-profile profile-name;
        ike {
            allowed-proxy-pair {
                remote remote-proxy-address local local-proxy-address;
            }
            pre-shared-key (ascii-text character-string | hexadecimal hexadecimal-digits);
            ike-policy policy-name;
            interface-id string-value;
        }
        l2tp {
            aaa-access-profile profile-name;
            interface-id interface-id;
            lcp-renegotiation;
            local-chap;
```

```
            maximum-sessions number;
            maximum-sessions-per-tunnel number;
            multilink {
                drop-timeout milliseconds;
                fragment-threshold bytes;
            }
            override-result-code session-out-of-resource;
            ppp-authentication (chap | pap);
            ppp-profile profile-name;
            service-profile profile-name(parameter)&profile-name;
            sessions-limit-group limit-group-name;
            shared-secret shared-secret;
        }
        pap-password pap-password;
        ppp {
            cell-overhead;
            encapsulation-overhead bytes;
            framed-ip-address ip-address;
            framed-pool framed-pool;
            idle-timeout seconds;
            interface-id interface-id;
            keepalive seconds;
            primary-dns primary-dns;
            primary-wins primary-wins;
            secondary-dns secondary-dns;
            secondary-wins secondary-wins;
        }
        user-group-profile profile-name;
    }
    domain-name-server;
    domain-name-server-inet;
    domain-name-server-inet6;
    local {
        flat-file-profile profile-name;
    }
    preauthentication-order preauthentication-method;
    provisioning-order  (gx-plus | jsrc | pcrf);
    radius {
        accounting-server [ ip-address ];
        attributes {
            exclude {
                attribute-name packet-type;
                standard-attribute number {
```

```
                    packet-type [ access-request | accounting-off | accounting-on | accounting-
start | accounting-stop ];
                }
                vendor-id id-number {
                    vendor-attribute vsa-number {
                        packet-type [ access-request | accounting-off | accounting-on |
accounting-start | accounting-stop ];
                    }
                }
            }
            ignore {
                dynamic-iflset-name;
                framed-ip-netmask;
                idle-timeout;
                input-filter;
                logical-system:routing-instance;
                output-filter;
                session-timeout;
                standard-attribute number;
                vendor-id id-number {
                    vendor-attribute vsa-number;
                }
            }
        }
        authentication-server [ ip-address ];
        options {
            accounting-session-id-format (decimal | description);
            calling-station-id-delimiter delimiter-character;
            calling-station-id-format {
                agent-circuit-id;
                agent-remote-id;
                interface-description;
                interface-text-description;
                mac-address;
                nas-identifier;
                stacked-vlan;
                vlan;
            }
            chap-challenge-in-request-authenticator;
            client-accounting-algorithm (direct | round-robin);
            client-authentication-algorithm  (direct | round-robin);
            coa-dynamic-variable-validation;
            ethernet-port-type-virtual;
```

```
            interface-description-format {
                exclude-adapter;
                exclude-channel;
                exclude-sub-interface;
            }
            juniper-access-line-attributes;
            nas-identifier identifier-value;
            nas-port-extended-format {
                adapter-width width;
                ae-width width;
                port-width width;
                pw-width width;
                slot-width width;
                stacked-vlan-width width;
                vlan-width width;
                atm {
                    adapter-width width;
                    port-width width:
                    slot-width width;
                    vci-width width:
                    vpi-width width;
                }
            }
            nas-port-id-delimiter delimiter-character;
            nas-port-id-format {
                agent-circuit-id;
                agent-remote-id;
                interface-description;
                interface-text-description;
                nas-identifier;
                order {
                    agent-circuit-id;
                    agent-remote-id;
                    interface-description;
                    interface-text-description;
                    nas-identifier;
                    postpend-vlan-tags;
                }
                postpend-vlan-tags;
            }
            nas-port-type {
                ethernet {
                    port-type;
```

```
                }
            }
            override {
                calling-station-id remote-circuit-id;
                nas-ip-address tunnel-client-gateway-address;
                nas-port tunnel-client-nas-port;
                nas-port-type tunnel-client-nas-port-type;
            }
            remote-circuit-id-delimiter;
            remote-circuit-id-fallback {
            remote-circuit-id-format;
                agent-circuit-id;
                agent-remote-id;
            }
            revert-interval interval;
            service-activation {
                dynamic-profile (optional-at-login | required-at-login);
                extensible-service (optional-at-login | required-at-login);
            }
            vlan-nas-port-stacked-format;
        }
        preauthentication-server ip-address;
    }
    radius-server server-address {
        accounting-port port-number;
        accounting-retry number;
        accounting-timeout seconds;
        dynamic-request-port
        port port-number;
        preauthentication-port port-number;
        preauthentication-secret password;
        retry attempts;
        routing-instance routing-instance-name;
        secret password;
        max-outstanding-requests value;
         source-address source-address;
        timeout seconds;
    }
    service {
        accounting {
            statistics (time | volume-time);
            update-interval minutes;
        }
```

```
        accounting-order (activation-protocol | local | radius);
    }
    session-limit-per-username number;
    session-options {
        client-idle-timeout minutes;
        client-idle-timeout-ingress-only;
        client-session-timeoutminutes;
        pcc-context {
            input-service-filter-name filter-name;
            input-service-set-name service-set-name;
            ipv6-input-service-filter-name filter-name;
            ipv6-input-service-set-name service-set-name;
            ipv6-output-service-filter-name filter-name;
            ipv6-output-service-set-name service-set-name;
            output-service-filter-name filter-name;
            output-service-set-name service-set-name;
            profile-name pcef-profile-name;
        }
        strip-user-name {
            delimiter [ delimiter ];
            parse-direction (left-to-right | right-to-left);
        }
    }
    subscriber username {
        delegated-pool delegated-pool-name;
        framed-ip-address ipv4-address;
        framed-ipv6-pool ipv6-pool-name;
        framed-pool ipv4-pool-name;
        password password;
        target-logical-system logical-system-name <target-routing-instance (default | routing-
instance-name>;
        target-routing-instance (default | routing-instance-name);
    }
}
```

Hierarchy Level

```
[edit access]
```

Description

Configure a subscriber access profile that includes subscriber access, L2TP, or PPP properties.

Options

profile-name—Name of the profile.

For CHAP, the name serves as the mapping between peer identifiers and CHAP secret keys. This entity is queried for the secret key whenever a CHAP challenge or response is received.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

- *Configuring the PPP Challenge Handshake Authentication Protocol*
- *Configuring the PPP Password Authentication Protocol*
- *Configuring Access Profiles for L2TP or PPP Parameters*
- *Configuring L2TP Properties for a Client-Specific Profile*
- Configuring an L2TP Access Profile on the LNS
- Configuring an L2TP LNS with Inline Service Interfaces
- *Configuring PPP Properties for a Client-Specific Profile*
- Configuring Service Accounting with JSRC

Configuring Service Accounting in Local Flat Files

AAA Service Framework Overview

Enabling Direct PCC Rule Activation by a PCRF for Subscriber Management

protocol-master

IN THIS SECTION

- Syntax | 717
- Hierarchy Level | 717
- Description | 719
- Options | 719
- Required Privilege Level | 719
- Release Information | 719

Syntax

```
protocol-master (inet | inet6);
```

Hierarchy Level

```
[edit bridge-domains name forwarding-options dhcp-relay dhcpv6 group group-name dual-stack-group
dual-stack-group-name],
[edit bridge-domains name forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay dhcpv6 group name dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dhcpv6 group name
dual-stack-group dual-stack-group-name],
[edit logical-systems name bridge-domains name forwarding-options dhcp-relay dual-stack-group
```

dual-stack-group-name],
[edit logical-systems *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* forwarding-options dhcp-relay dual-stack-group],
[edit logical-systems *name* *routing-instances* *name* bridge-domains *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* bridge-domains *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* system services dhcp-local-server dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* vlans *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* *routing-instances* *name* vlans *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* system services dhcp-local-server dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* vlans *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit logical-systems *name* vlans *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* bridge-domains *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* system services dhcp-local-server dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* vlans *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit routing-instances *name* vlans *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*],
[edit system services dhcp-local-server dual-stack-group *dual-stack-group-name*],
[edit vlans *name* forwarding-options dhcp-relay dhcpv6 group *name* dual-stack-group *dual-stack-group-name*],
[edit vlans *name* forwarding-options dhcp-relay dual-stack-group *dual-stack-group-name*]

Description

Select family as protocol primary. In some customer use cases, CPE devices have reachability to multiple BNG routers for load sharing. The CPE's DHCP client broadcasts a DHCP protocol handshake to the reachable routers; more than one router may respond. In a DHCP dual-stack environment, the DHCPv4 and DHCPv6 protocol handshakes are independent of each other, meaning that each arm of the subscriber session could connect to a different router. You can avoid this situation by specify the primary protocol. For a given dual-stack subscriber, this configuration causes the rejection of any binding attempt from the secondary address family client when a binding is not currently active for the primary protocol family. If bindings are currently active for both arms when the primary protocol family binding is released or deleted, then the binding for the secondary address family is also torn down.

Options

inet INET family has protocol primary behavior.

inet6 INET6 family has protocol primary behavior.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.3.

RELATED DOCUMENTATION

- *Configuring Access Profile Options for Interactions with RADIUS Servers*
- *Attaching Access Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces*
- *Configuring Access Components for the DHCP Layer 3 Wholesale Network Solution*
- *Configuring Access Components for the PPPoE Wholesale Network Solution*

proxy-mode

IN THIS SECTION

- Syntax | **720**
- Hierarchy Level | **720**
- Description | **721**
- Required Privilege Level | **721**
- Release Information | **721**

Syntax

```
proxy-mode;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name  overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay  overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay  overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name  overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay  overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
```

```
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

Enable DHCP relay proxy mode on the extended DHCP relay. Proxy mode supports all extended DHCP relay functionality.

You cannot configure both the DHCP relay proxy and the extended DHCP local server on the same interface.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.5.

RELATED DOCUMENTATION

- *DHCP Relay Proxy Overview*
- *Extended DHCP Relay Agent Overview*
- *Enabling DHCP Relay Proxy Mode*

radius-disconnect (DHCP Local Server)

IN THIS SECTION

- Syntax | 722
- Hierarchy Level | 722
- Description | 723
- Default | 723
- Required Privilege Level | 723
- Release Information | 723

Syntax

```
radius-disconnect;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name reconfigure trigger],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure
trigger],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure trigger],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
```

```
name reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure
trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure trigger],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure trigger],
[edit system services dhcp-local-server reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 reconfigure trigger],
[edit system services dhcp-local-server group group-name reconfigure trigger],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure trigger]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

rapid-commit (DHCPv6 Client)

IN THIS SECTION

- Syntax | 724
- Hierarchy Level | 724
- Description | 725
- Required Privilege Level | 725
- Release Information | 725

Syntax

```
rapid-commit;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6dhcpv6-
client]
```

Description

Used to signal the use of the two-message exchange for address assignment.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

DHCPv6 Client Overview | 256

Understanding DHCPv6 Client and Server Identification | 257

rapid-commit (DHCPv6 Local Server)

IN THIS SECTION

- Syntax | 726
- Hierarchy Level | 726
- Description | 726
- Default | 726
- Required Privilege Level | 726
- Release Information | 727

Syntax

```
rapid-commit;
```

Hierarchy Level

```
[edit system services dhcp-local-server dhcpv6 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],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 ...],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 ...],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 ...]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Configuring DHCPv6 Rapid Commit (MX Series, EX Series)

Overriding the Default DHCP Local Server Configuration Settings

reauthenticate (DHCP Local Server)

IN THIS SECTION

- Syntax | **727**
- Hierarchy Level | **728**
- Description | **728**
- Options | **729**
- Required Privilege Level | **729**
- Release Information | **730**

Syntax

```
reauthenticate (<lease-renewal> <remote-id-mismatch >);
```

Hierarchy Level

```
[edit logical-systems name routing-instances name system services dhcp-local-server],
[edit logical-systems name routing-instances name system services dhcp-local-server dhcpv6],
[edit logical-systems name routing-instances name system services dhcp-local-server dual-stack-
group name],
[edit logical-systems name system services dhcp-local-server],
[edit logical-systems name system services dhcp-local-server dhcpv6],
[edit logical-systems name system services dhcp-local-server dual-stack-group name],
[edit routing-instances name system services dhcp-local-server ],
[edit routing-instances name system services dhcp-local-server dhcpv6],
[edit routing-instances name system services dhcp-local-server
dual-stack-group name],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server dual-stack-group name]
```

Description

Enable DHCP client reauthentication, that is, trigger jdhcpd to request reauthentication from authd, which in turn reissues the RADIUS Access-Request for subscriber authentication. The purpose of the reauthentication is to change characteristics of the subscriber session, such as activating subscriber services or changing attributes. You can use reauthentication as an alternative to a RADIUS CoA request.

Starting in Junos OS Release 18.1R1, reauthentication can be triggered by discover and solicit messages in addition to the previously supported renew and rebind messages. The release also introduces reauthentication support for dual-stack, single-session subscribers.

You can specify that reauthentication occurs in response to all DHCP renew, rebind, discover, or solicit messages or only in response to discover and solicit messages that include a new (different) Agent Remote ID for the DHCP client.

You can use the Juniper Networks VSA, Reauthentication-On-Renew (26-206) as an alternative to the CLI configuration to enable reauthentication. The `reauthenticate` statement overrides the VSA when the VSA is present with a value of disable.

NOTE: Reauthentication for dual-stack, single-session subscribers requires that the `on-demand-address-allocation` statement is configured for the dual-stack group. This is true whether you enable reauthentication with the `reauthenticate` statement or the Reauthenticate-On-Renew VSA (26-206).

NOTE: You cannot configure both the `reauthenticate` statement and the *remote-id-mismatch* statement at the global level, `[edit system services dhcp-local-server]`. However, DHCP precedence rules do permit you to configure both statements when they are at different levels. For example, you can configure `reauthenticate` at the global level and *remote-id-mismatch* for DHCPv6 at the `[edit system services dhcp-local-server dhcpv6]` or for a specific group at the `[edit system services dhcp-local-server group name]` hierarchy level, and so on.

NOTE: Reauthentication does not support Extensible Services Subscriber Management (essmd) services. Activation or deactivation of any such service causes the request to fail.

Options

lease-renewal Reauthenticate when a renew, rebind, discover, or solicit message is received from the DHCP client.

remote-id-mismatch Reauthenticate when a discover or solicit message is received from the DHCP client with a new value for the DHCP client's Agent Remote ID. The change in value corresponds to a change in subscriber service plan. The Agent Remote ID is conveyed in option 82, suboption 2 for DHCPv4 clients and in option 37 for DHCPv6 clients.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.4R1.

Support at the `[edit ... system services dhcp-local-server dual-stack-group]` hierarchy level introduced in Junos OS Release 18.1R1.

RELATED DOCUMENTATION

Configuring RADIUS Reauthentication for DHCP Subscribers

RADIUS Reauthentication As an Alternative to RADIUS CoA for DHCP Subscribers

reconfigure (DHCP Local Server)

IN THIS SECTION

- Syntax | **730**
- Hierarchy Level | **731**
- Description | **731**
- Options | **732**
- Required Privilege Level | **732**
- Release Information | **732**

Syntax

```
reconfigure {
    attempts attempt-count;
    clear-on-terminate;
    strict;
    support-option-pd-exclude;
    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]
```

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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Options

support-option-pd-exclude Request to exclude prefix option in the reconfigure message.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the `[edit ... dhcpv6 ...]` hierarchy levels introduced in Junos OS Release 10.4.

`support-option-pd-exclude` statement introduced in Junos OS Release 17.3 for the MX Series.

RELATED DOCUMENTATION

Dynamic Reconfiguration of DHCP Servers and Clients

reconfigure (DHCP Local Server)

IN THIS SECTION

Syntax | 733

- Hierarchy Level | 733
- Description | 733
- Options | 734
- Required Privilege Level | 734
- Release Information | 734

Syntax

```
reconfigure {
    attempts number;
    clear-on-abort;
    strict;
    timeout number;
    token token-name;
    trigger {
        radius-disconnect;
    }
}
```

Hierarchy Level

```
[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]
```

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.

Options

`attempts` *number*—Configure maximum number of attempts 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.

- **Range:** 1 through 10 attempts
- **Default:** 8 attempts

`clear-on-abort` —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.

`strict` —Configure the system to only allow packets that contain the reconfigure accept option.

`timeout` *seconds*—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. Each successive attempts 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.

- **Range:** 1 through 10 seconds
- **Default:** 2 seconds

`token` *token-name*—Configure a plain-text token for all DHCP clients or only the clients specified by the specified group of interfaces. The default is null (empty string).

`trigger` — Specify DHCP reconfigure trigger.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

DHCP Overview | 2

DHCP Server Configuration | 51

relay-agent-interface-id (DHCP Local Server)

IN THIS SECTION

- Syntax | 735
- Hierarchy Level | 735
- Description | 736
- Required Privilege Level | 736
- Release Information | 736

Syntax

```
relay-agent-interface-id;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  group group-
name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name 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]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.6.

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients

relay-agent-interface-id (DHCPv6 Relay Agent)

IN THIS SECTION

- Syntax | 737
- Hierarchy Level | 737
- Description | 738
- Required Privilege Level | 738
- Release Information | 738

Syntax

```
relay-agent-interface-id {
    include-irb-and-l2;
    keep-incoming-interface-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-option-82 <strict>;
    use-vlan-id;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group dual-
stack-group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 ...],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group ],
```

Description

Insert the DHCPv6 Relay Agent Interface-ID option (option 18) in DHCPv6 packets destined for the DHCPv6 server.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group dual-stack-group-name]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

dhcp-relay | 470

Extended DHCP Relay Agent Overview

DHCPv6 Relay Agent Overview

Inserting DHCPv6 Interface-ID Option (Option 18) In DHCPv6 Packets

relay-agent-option-79

IN THIS SECTION

- Syntax | 739
- Hierarchy Level | 739
- Description | 739
- Required Privilege Level | 740
- Release Information | 740

Syntax

```
relay-agent-option-79;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6]
```

Description

Configure the DHCPv6 client link layer option (option 79) to include the source MAC address in DHCPv6 requests from clients before the messages are forwarded to a DHCPv6 server. In a dual-stack network environment in which devices act as both DHCPv4 and DHCPv6 clients, the client MAC address can be used to associate DHCPv4 and DHCPv6 messages with the same client interface. The client MAC address also provides network operators with additional information for event debugging and logging related to the client at the relay agent and the server.

You can configure `relay-agent-option-79` to enable DHCPv6 option 79 for a layer 3 DHCPv6 relay agent (LDRA). When DHCPv6 option 79 is enabled, the relay agent reads the source MAC address of DHCPv6

Solicit and DHCPv6 Request messages that it receives from a client. The relay agent encapsulates the Solicit and Request messages within a DHCPv6 Relay-Forward message, and inserts the client MAC address as option 79 in the Relay-Forward header before relaying the message to the server.

You can also configure DHCPv6 option 79 for a lightweight DHCPv6 relay agent (LDRA). An LDRA resides on the same IPv6 link as the DHCPv6 client and relay agent or server and acts as a layer 2 relay agent. To configure DHCPv6 option 79 for an LDRA, use the *option-79* statement.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 18.2R1.

Release History Table

Release	Description
21.2R1	Starting with Junos OS Release 21.2R1, QFX Series switches support the relay-agent-option-79 CLI statement in a stateless DHCPv6 relay configuration. You can configure stateless DHCPv6 relay using the forward-only CLI statement at the [edit forwarding-options dhcp-relay dhcpv6] hierarchy level.

RELATED DOCUMENTATION

Inserting the DHCPv6 Client MAC Address Option (Option 79) In DHCPv6 Packets | 227

relay-agent-remote-id (DHCP Local Server)

IN THIS SECTION

- Syntax | 741
- Hierarchy Level | 741
- Description | 742
- Required Privilege Level | 742
- Release Information | 742

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  group group-
name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6  group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name 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]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.6.

For MX Series routers only, `enterprise-id` and `remote-id` options introduced in Junos OS Release 12.3R3.

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.

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients

relay-agent-remote-id (DHCPv6 Relay Agent Username)

IN THIS SECTION

- Syntax | 743
- Hierarchy Level | 743
- Description | 744
- Required Privilege Level | 744
- Release Information | 744

Syntax

```
relay-agent-remote-id;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication
username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6
authentication username-include],
```

```
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name authentication username-include]
```

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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

For MX Series routers only, `enterprise-id` and `remote-id` options introduced in Junos OS Release 12.3R3.

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.

Support at the `[edit ... dual-stack-group dual-stack-group-name]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

DHCPv6 Relay Agent Overview

Creating Unique Usernames for DHCP Clients

relay-option (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 745
- Hierarchy Level | 746
- Description | 746
- Required Privilege Level | 746
- Release Information | 746

Syntax

```
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;
    }
}
```

Hierarchy Level

```
[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 ...]
```

Description

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.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic

relay-option-82

IN THIS SECTION

- Syntax | 747
- Syntax (QFX Series) | 748
- Hierarchy Level | 748
- Description | 749
- Required Privilege Level | 749
- Release Information | 750

Syntax

```
relay-option-82 {
    circuit-id {
        include-irb-and-l2;
        keep-incoming-circuit-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    server-id-override;
    vendor-specific{
        host-name;
        location;
```

```
    }
}
```

Syntax (QFX Series)

```
relay-option-82 {
    circuit-id {
        include-irb-and-l2;
        keep-incoming-circuit-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    remote-id {
        include-irb-and-l2;
        keep-incoming-remote-id ;
        no-vlan-interface-name;
        prefix prefix;
        use-interface-description (logical | device);
        use-vlan-id;
    }
    server-id-override;
    link-selection;
    vendor-specific{
        host-name;
        location;
    }
}
```

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]
```

Description

Enable or disable the insertion of the DHCP relay agent information option (option 82) in DHCP packets destined for a DHCP server.

To enable insertion of option 82 information in DHCP packets, you must specify at least one of the `circuit-id` or `remote-id` statements.

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.

Starting in Junos OS Release 21.2R1, on QFX Series devices, we've introduced `link-selection` statement at the `edit forwarding-options dhcp-relay relay-option-82` hierarchy level, which allows DHCP relay to add suboption 5 to option 82. Suboption 5 allows DHCP proxy clients and relay agents to request an IP address for a specific subnet from a specific IP address range and scope. Earlier to this release, the DHCP relay drops packets during the renewal DHCP process as the DHCP Server uses the leaf's address as a destination to acknowledge DHCP renewal message.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

`link-selection` option added in Junos OS Release 21.2R1.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

dhcp-relay | 470

relay-server-group (DHCP Relay Agent Option)

IN THIS SECTION

- Syntax | 750
- Hierarchy Level | 751
- Description | 751
- Options | 751
- Required Privilege Level | 751
- Release Information | 751

Syntax

```
relay-server-group relay-server-group;
```

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 group-name relay-option (default-action | equals | starts-
with),
[edit forwarding-options dhcp-relay dhcpv6 group group-name relay-option (default-action | equals
| starts-with),
[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 ...]
```

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

relay-server-group	Name of DHCP server group.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3.

RELATED DOCUMENTATION

Using DHCP Option Information to Selectively Process DHCP Client Traffic

remote-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 752
- Hierarchy Level | 752
- Description | 753
- Required Privilege Level | 754
- Release Information | 755

Syntax

```
remote-id {
    include-irb-and-l2;
    keep-incoming-remote-id ;
    no-vlan-interface-name;
    prefix prefix;
    use-interface-description (logical | device);
    use-vlan-id;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-82],
[edit forwarding-options dhcp-relay group group-name relay-option-82],
[edit logical-systems logical-system-name forwarding-options dhcp-relay ... relay-option-82],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
```

```
options dhcp-relay ... relay-option-82],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82]
```

Description

Specify the Agent Remote ID suboption (suboption 2) 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.

NOTE: For Layer 3 interfaces, when you configure relay-option-82 only, the Agent Remote 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 Remote 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.

The format of the Agent Remote 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 Remote 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. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 14.1.

Release History Table

Release	Description
21.2R1	Starting with Junos OS Release 21.2R1, QFX Series switches support the remote-id CLI statement in a stateless DHCP relay configuration. You can configure stateless DHCP relay using the forward-only CLI statement at the [edit forwarding-options dhcp-relay] hierarchy level.

RELATED DOCUMENTATION

Using DHCP Relay Agent Option 82 Information

Configuring Option 82 Information

replace-ip-source-with (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 755
- Hierarchy Level | 756
- Description | 756
- Required Privilege Level | 756
- Release Information | 756

Syntax

```
replace-ip-source-with giaddr;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides]
```

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr) 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.

Release Information

Statement introduced in Junos OS Release 15.1X49-D100.

RELATED DOCUMENTATION

overrides (DHCP Relay Agent) | 686

replace-ip-source-with (DHCP Relay Agent)

IN THIS SECTION

Syntax | 757

- Hierarchy Level | 757
- Description | 757
- Required Privilege Level | 758
- Release Information | 758

Syntax

```
replace-ip-source-with giaddr;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

Replace the IP source address in DHCP relay request and release packets with the gateway IP address (giaddr).

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.6.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Configure DHCP Relay Agent to Replace Request and Release Packets with Gateway IP address

req-option

IN THIS SECTION

- Syntax | **759**
- Hierarchy Level | **759**
- Description | **759**
- Options | **759**
- Required Privilege Level | **760**
- Release Information | **760**

Syntax

```
req-option (dns-server | domain | fqdn | nis-domain | nis-server | ntp-server | sip-domain | sip-server | time-zone | vendor-spec);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-client]
```

Description

The configuration options requested by the DHCPv6 client.

Options

dns-server	Specify a DNS server.
domain	Specify a domain name.
fqdn	Specify a fully qualified domain name.
nis-domain	Specify a Network Information Service (NIS) domain.
nis-server	Specify a Network Information Service (NIS) server.
ntp-server	Specify a Network Time Protocol (NTP) server.
sip-domain	Specify a Session Initiation Protocol (SIP) domain.
sip-server	Specify a Session Initiation Protocol (SIP) server.

time-zone	Specify a time zone.
vendor-spec	Specify vendor specification.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

retransmission-attempt (DHCP Client)

IN THIS SECTION

- Syntax | **761**
- Hierarchy Level | **761**
- Description | **761**
- Options | **761**
- Required Privilege Level | **761**
- Release Information | **762**

Syntax

```
retransmission-attempt number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

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

number Number of retransmit attempts.

Range:

- - For IPv4 — 0 through 50000 from Junos OS Release 17.3R1 onwards and 0 through 6 on Junos OS earlier releases.
  - For IPv6 — 0 through 9.
- **Default:** 4

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.5.

RELATED DOCUMENTATION

Configuring a DHCP Client | 235

interfaces

unit

family

retransmission-attempt (DHCP Client)

IN THIS SECTION

- Syntax | 762
- Hierarchy Level | 763
- Description | 763
- Options | 763
- Required Privilege Level | 763
- Release Information | 763

Syntax

```
retransmission-attempts number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Specify the number of times the device attempts to retransmit a Dynamic Host Control Protocol (DHCP) packet fallback.

Options

number Number of attempts to retransmit the packet.

Range: 0 through 6

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

RELATED DOCUMENTATION

Understanding DHCP Client Operation | 234

Minimum DHCP Client Configuration | 235

retransmission-attempt (DHCPv6 Client)

IN THIS SECTION

- Syntax | 764
- Hierarchy Level | 764
- Description | 765
- Options | 765
- Required Privilege Level | 765
- Release Information | 765

Syntax

```
retransmission-attempt number;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client]
```

Description

Specify the number of times the device retransmits a DHCPv6 client packet if a DHCPv6 server fails to respond. After the specified number of attempts, no further attempts at reaching a server are made.

Options

number Number of retransmit attempts.

- **Range:** 0 through 50000 (from Junos OS Release 20.3R1 onwards)
- **Range:** 0 through 9

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

retransmission-interval (DHCP Client)

IN THIS SECTION

- Syntax | **766**
- Hierarchy Level | **766**

- Description | 766
- Options | 766
- Required Privilege Level | 767
- Release Information | 767

Syntax

```
retransmission-interval  seconds;
```

Hierarchy Level

```
[edit interfaces interface-name  unit                logical-unit-number  family inet dhcp]
```

Description

Specify the time between successive retransmissions of the client DHCP request if a DHCP server fails to respond.

Options

seconds 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.

Release Information

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

Configuring a DHCP Client | 235

retransmission-interval (DHCP Client)

IN THIS SECTION

- Syntax | 767
- Hierarchy Level | 768
- Description | 768
- Options | 768
- Required Privilege Level | 768
- Release Information | 768

Syntax

```
retransmission-interval seconds;
```

Hierarchy Level

```
[edit interfaces   interface-name  unit logical-unit-number         family family-name dhcp]
```

Description

Specify the time between successive retransmission attempts.

Options

seconds—Number of seconds between successive retransmission.

- **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.

Release Information

Statement introduced in Release 8.5 of Junos OS.

retransmission-interval (DHCP Client)

IN THIS SECTION

- Syntax | 769
- Hierarchy Level | 769
- Description | 769
- Options | 770
- Required Privilege Level | 770
- Release Information | 770

Syntax

```
retransmission-interval seconds;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Specify the initial retransmission interval. Successive retransmission intervals are doubled as per RFC2131.

NOTE: Though the SRX series devices implement the exponential backoff, as described in RFC 2131, the retransmit attempt does not stop when the retransmission interval reaches 64 seconds. The packet is transmitted till the retransmission attempt is reached. For example, if you

configure the `retransmission-attempt` to 5 and the `retransmission-interval` to 20, the sequence of retransmission-interval is 20, 40, 80, 160, 320.

Options

seconds Number of seconds before initial retransmission.

Range: The range is 4 through 64. The default is 4 seconds.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

RELATED DOCUMENTATION

Understanding DHCPv6 Client and Server Identification | 257

route-suppression (DHCP Local Server and Relay Agent)

IN THIS SECTION

- Syntax | 771
- Hierarchy Level | 771
- Description | 772
- Options | 772
- Required Privilege Level | 772
- Release Information | 772

Syntax

```
route-suppression (access | access-internal | destination);
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit logical-systems logical-system-name ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name...],
[edit routing-instances routing-instance-name ...],
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dhcpv6],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server dhcpv6 group group-name]
```

Description

Configure the jdhcpd process to suppress the installation of access, access-internal, or destination routes during client binding.

> **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.

Options

access (DHCPv6 only) Suppress installation of access routes. You can use the `access` and `access-internal` options in the same statement for DHCPv6.

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.

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.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 13.2.

RELATED DOCUMENTATION

- Preventing DHCP from Installing Access, Access-Internal, and Destination Routes by Default

routing-instance-name (DHCP Local Server)

IN THIS SECTION

- Syntax | 773
- Hierarchy Level | 773
- Description | 774
- Required Privilege Level | 774
- Release Information | 775

Syntax

```
routing-instance-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  authentication
```

```
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[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]
```

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

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

Specifying Authentication Support

routing-instance-name (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 775
- Hierarchy Level | 775
- Description | 776
- Required Privilege Level | 776
- Release Information | 777

Syntax

```
routing-instance-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 group-name authentication username-include],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name authentication username-
include],
```

```
[edit forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include],
[edit tenants tenant-name routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include]
[edit routing-instances routing-instance-name forwarding-options dhcp-relay authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-name authentication username-include],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name authentication username-include]
```

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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *`dual-stack-group-name`*`]` hierarchy level introduced in Junos OS Release 15.1.

The `tenants` option is introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

send-release-on-delete (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **777**
- Hierarchy Level | **778**
- Description | **778**
- Required Privilege Level | **779**
- Release Information | **779**

Syntax

```
send-release-on-delete;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 overrides],
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay dhcpv6 group group-name overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

Description

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.

M120 and M320 routers do not support DHCPv6.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.2.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

- *Extended DHCP Relay Agent Overview*
- *Overriding the Default DHCP Relay Configuration Settings*
- *Sending Release Messages When Clients Are Deleted*

server-address

IN THIS SECTION

- Syntax | **780**
- Hierarchy Level | **780**
- Description | **780**
- Default | **780**
- Options | **780**
- Required Privilege Level | **780**
- Release Information | **781**

Syntax

```
server-address  ip-address;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family inet dhcp]
```

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

ip-address	DHCP server address.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.5.

RELATED DOCUMENTATION

- Configuring a DHCP Client | 235
- *interfaces*
- unit
- family

server-address (dhcp-client)

IN THIS SECTION

- Syntax | 781
- Hierarchy Level | 782
- Description | 782
- Options | 782
- Required Privilege Level | 782
- Release Information | 782

Syntax

```
server address ip-address;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Specify the preferred DHCP server address that is sent to DHCP clients.

Options

ip-address DHCP server address.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

server-group

IN THIS SECTION

- Syntax | 783
- Hierarchy Level | 783
- Description | 784
- Options | 784
- Required Privilege Level | 784
- Release Information | 784

Syntax

```
server-group {
    server-group-name {
        server-ip-address;
    }
}
```

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 forwarding-options dhcp-relay dhcpv6],
[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 dhcpv6],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6]
```

Description

Specify the name of a group of DHCP server addresses for use by the extended DHCP relay agent. Apply the group with the `active-server-group` statement globally for all interfaces or for a named group of interfaces configured with the `group` statement. This mechanism enables you to apply different DHCP relay configurations for different groups of servers, with a common configuration for the servers within a server group.

Options

server-group-name	Name of the group of DHCP or DHCPv6 server addresses.
server-ip-address	IP address of the DHCP server belonging to this named server group. Use IPv6 addresses when configuring DHCPv6 support. Starting in Junos OS Release 18.4R1, you can configure up to 32 server IP addresses per group for DHCPv4 servers. In earlier releases, you can configure only up to 5 server IP addresses for DHCPv4 servers. For DHCPv6 servers, you can configure only up to 32 addresses in all releases. The configuration fails commit check if you configure more than the maximum number of server addresses.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

Extended DHCP Relay Agent Overview

Configuring Active Server Groups to Apply a Common DHCP Relay Agent Configuration to Named Server Groups

server-identifier

IN THIS SECTION

- Syntax | 785
- Hierarchy Level | 785
- Description | 786
- Default | 786
- Options | 786
- Required Privilege Level | 786
- Release Information | 786

Syntax

```
server-identifier address;
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

Description

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).

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.

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.

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.

Release Information

Statement introduced before Junos OS Release 7.4.

service-profile (DHCP Local Server)

IN THIS SECTION

- Syntax | 787
- Hierarchy Level | 787
- Description | 788
- Options | 788
- Required Privilege Level | 788
- Release Information | 788

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

```
[edit system services dhcp-local-server],
[edit system services dhcp-local-server dual-stack-group dual-stack-group-name],
[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 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 ...]
```

Description

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.

- 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` *`group-name`*`]` 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` *`group-name`* `interface` *`interface-name`*`]` hierarchy level.
- For DHCPv6 clients, use the `service-profile` statement at the `[edit system services dhcp-local-server dhcpv6]` hierarchy level.

Options

`dynamic-profile-name`—Name of the dynamic profile that defines the service.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.2.

RELATED DOCUMENTATION

> *Understanding Differences Between Legacy DHCP and Extended DHCP*
>
> *Default Subscriber Service Overview*

service-profile (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 789
- Hierarchy Level | 789
- Description | 790
- Options | 790
- Required Privilege Level | 790
- Release Information | 790

Syntax

```
service-profile dynamic-profile-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name],
[edit forwarding-options dhcp-relay dhcpv6 groupgroup-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-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 ...]
```

Description

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.

- 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 group-name]` 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 group-name interface interface-name]` hierarchy level.

Options

dynamic-profile-name—Name of the dynamic service profile.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.2.

Support at the `[edit ... dhcpv6 ...]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the [edit ... dual-stack-group *dual-stack-group-name*] hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

dhcp-relay | 470

Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

Grouping Interfaces with Common DHCP Configurations

Default Subscriber Service Overview

services (System Services)

IN THIS SECTION

- Syntax | 791
- Hierarchy Level | 798
- Description | 798
- Required Privilege Level | 798
- Release Information | 798

Syntax

```
services {
    dhcp { # DHCP is not supported on a DCF
        dhcp_services;
    }
    dtcp-only
    finger {
        connection-limit limit;
        rate-limit limit;
    }
    flow-tap-dtcp {
```

```
        ssh {
            connection-limit limit;
            rate-limit limit;
        }
    }
    ftp {
        authentication-order [authentication-methods];
        connection-limit limit;
        rate-limit limit;
    }
    grpc {
        request-response {
            grpc {
                ssl {
                    address ip-address;
                    local-certificate local-certificate;
                    port port;
                }
                max-connections max-connections;
            }
        }
        notification {
            port port;
            max-connections max-connections;
            allow-clients {
                address ip-address;
            }
        }
        traceoptions {
            file <filename> <files number> <match regex> <size size> <world-readable | no-world-
readable>;
            flag flag;
            no-remote-trace;
        }
    }
    netconf {
        flatten-commit-results;
        hello-message {
            yang-module-capabilities {
                advertise-native-yang-modules;
                advertise-custom-yang-modules;
                advertise-standard-yang-modules;
            }
```

```
        }
        netconf-monitoring {
            netconf-state-schemas {
                retrieve-custom-yang-modules;
                retrieve-standard-yang-modules;
            }
        }
        notification;
        rfc-compliant;
        ssh {
            client-alive-count-max number;
            client-alive-interval seconds;
            connection-limit limit;
            port port;
            rate-limit limit;
        }
        tls {
            client-identity client-id {
                fingerprint fingerprint;
                map-type (san-dirname-cn | specified);
                username username;
            }
            default-client-identity {
                map-type (san-dirname-cn | specified);
                username username;
            }
            local-certificate local-certificate;
            traceoptions {
                file <filename> <files files> <match match> <size size> <(world-readable | no-
world-readable)>;
                flag name;
                level (all | error | info | notice | verbose | warning);
                no-remote-trace;
            }
        }
        traceoptions {
            file <filename> <files number> <match regular-expression> <size size> <world-
readable | no-world-readable>;
            flag flag;
            no-remote-trace;
            on-demand;
        }
        yang-compliant;
```

```
        yang-modules {
            device-specific;
            emit-extensions;
        }
    }
    outbound-https {
        client client-id {
            address {
                port port;
                trusted-cert trusted-cert;
            }
            device-id device-id;
            reconnect-strategy (in-order | sticky);
            secret password;
            waittime seconds;
        }
    }
    service-deployment {
        servers address {
            port-number port-number;
        }
        source-address address;
    }
    ssh {
        authentication-order  [method 1 method2...];
        authorized-keys-command authorized-keys-command;
        authorized-keys-command-user authorized-keys-command-user;
        ciphers [ cipher-1 cipher-2 cipher-3 ...];
        client-alive-count-max number;
        client-alive-interval seconds;
        connection-limit limit;
        fingerprint-hash (md5 | sha2-256);
        hostkey-algorithm (algorithm | no-algorithm);
        key-exchange [algorithm1 algorithm2...];
        log-key-changes log-key-changes;
        macs [algorithm1 algorithm2...];
        max-pre-authentication-packets number;
        max-sessions-per-connection number;
        no-challenge-response;
        no-password-authentication;
        no-passwords;
        no-public-keys;
        no-tcp-forwarding;
```

```
        port port-number;
        protocol-version [v2];
        rate-limit number;
        rekey {
            data-limit bytes;
            time-limit minutes;
        }
        root-login (allow | deny | deny-password);
        sftp-server;
        }
    tcp-forwarding;
    resource-monitor {
        free-fw-memory-watermark number;
        free-heap-memory-watermark number;
        free-nh-memory-watermark number;
        high-threshold number;
        no-logging;
        no-throttle;
        resource-category jtree {
            resource-category jtree (continguous-pages | free-dwords | free-pages) {
                low-watermark number;
                high-watermark number;
            }
        }
        subscribers-limit {
            client-type (any | dhcp | l2tp | pppoe) {
                chassis {
                    limit limit;
                }
                fpc slot-number {
                    limit limit;
                    pic number {
                        limit limit;
                        port number {
                            limit limit;
                        }
                    }
                }
            }
        }
        traceoptions {
            file filename <files number> <match regular-expression> <size maximum-file-size>
<world-readable | no-world-readable>;
```

```
            flag flag;
            no-remote-trace;
        }
    }
    subscriber-management {
        enable;
        enforce-strict-scale-limit-license;
        gres-route-flush-delay;
        }
        overrides {
            event {
                catastrophic-failure {
                    reboot (master | standby);
                }
            }
            interfaces {
                family (inet | inet6) {
                    layer2-liveness-detection;
                }
            }
            no-unsolicited-ra;
            ra-initial-interval-max seconds;
            ra-initial-interval-min seconds;
            shmlog {
                disable;
                file filename <files maximum-no-files> <size maximum-file-size>;
                filtering enable;
                log-name {
                    all;
                    logname {
                        <brief | detail | extensive | none | terse>;
                        <file-logging |no-file-logging>;
                    }
                    }
                log-type (debug | info | notice);
            |
        }
        redundancy {
            interface name {
                local-inet-address v4-address;
                local-inet6-address v6-address;
                shared-key string;
                virtual-inet-address virtual-v4-address;
```

```
                virtual-inet6-address virtual-v6-address;
            }
            no-advertise-routes-on-backup;
            protocol {
                pseudo-wire;
                vrrp;
            }
        }
        traceoptions {
            file filename <files number> <match regular-expression > <size maximum-file-size>
<world-readable | no-world-readable>;
            flag flag;
        }
    }
    telnet {
        authentication-order [authentication-methods];
        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-ssl {
        connection-limit limit;
        local-certificate name;
        rate-limit limit;
        ssl-renegotiation;
    }
}
```

Hierarchy Level

```
[edit system]
```

Description

Configure the router or switch so that users on remote systems can access the local router or switch through the DHCP server, DTCP over SSH, finger, outbound HTTPS, rlogin, SSH, telnet, Web management, Junos XML protocol SSL, and network utilities, or enable Junos OS to work with the Session and Resource Control (SRC) software. Also, enable configuration of third-party applications developed using the Juniper Extension Toolkit (JET) to run on Junos OS.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

`extension-service` option added in Junos OS Release 16.1 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.

`grpc` option added in Junos OS Release 16.2 for MX80, MX104, MX240, MX480, MX960, MX2010, MX2020, vMX Series.

RELATED DOCUMENTATION

Configuring the Junos OS to Work with SRC Software

Configuring Junos OS Enhanced Subscriber Management

session-mode

IN THIS SECTION

- Syntax | 799
- Hierarchy Level | 799
- Description | 800
- Options | 800
- Required Privilege Level | 800
- Release Information | 800

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Description

Configure the session mode.

Options

- **Default:** automatic

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 and passive DHCP clients.

single-hop Configure single hop BFD sessions and non-passive DHCP clients.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

short-cycle-protection (DHCP Local Server and Relay Agent)

IN THIS SECTION

- Syntax | 801
- Hierarchy Level | 801
- Description | 802
- Options | 802
- Required Privilege Level | 803
- Release Information | 803

Syntax

```
short-cycle-protection <lockout-max-time seconds> <lockout-min-time seconds>;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay],
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit forwarding-options dhcp-relay group group-name],
[edit forwarding-options dhcp-relay group group-name interface interface-name]
[edit logical-systems name forwarding-options dhcp-relay ...],
[edit logical-systems name routing-instances name forwarding-options dhcp-relay ...],
[edit routing-instances name forwarding-options dhcp-relay ...],
[edit logical-systems name system services dhcp-local-server ...],
[edit logical-systems name routing-instances name system services dhcp-local-server dhcp-local-
```

```
server...],
[edit routing-instances name system services dhcp-local-server ...],
[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 dual-stack-group dual-stack-group-name],
[edit system services dhcp-local-server group group-name],
[edit system services dhcp-local-server group group-name interface interface-name]
```

Description

Enable DHCP short-cycle protection to reduce resource usage associated with connection and authentication processing in highly scaled networks. You must configure both the minimum duration and the maximum duration for the lockout period.

The router detects short-lived client sessions and clients that repeatedly fail session negotiation, then locks them out from access by dropping subsequent DHCP discover or solicit messages from the client. The clients are tracked by the client identifier (client key), which can be a MAC address or some other unique value for DHCPv4 clients or the DUID for DHCPv6 clients. Locked-out clients are entered in the lockout database. If a locked-out client attempts another session before the grace time threshold is reached, it is locked out again. Each successive lockout period is increased exponentially up to the maximum lockout period. The grace time threshold is automatically set at whichever value is larger, 900 seconds or the configured maximum value.

Options

lockout-max-time *seconds*

Maximum length of any lockout period; the upper bound of the lockout range.

- **Range:** 1 through 86400

lockout-min-time *seconds*

Minimum length of any lockout period; the lower bound of the lockout period. The minimum value is the length of the first lockout period for a client. It cannot be greater than the maximum value. If you set it to the same value as the maximum, then the lockout period is fixed and does not increase for a client's subsequent lockouts.

- **Range:** 1 through 86400

Required Privilege Level

interface

Release Information

Statement introduced in Junos OS Release 18.2R1.

RELATED DOCUMENTATION

Configuring DHCP Short-Cycle Protection

DHCP Short Cycle Protection Against Frequent Brief or Failed Client Sessions

source-address-giaddr

IN THIS SECTION

- Syntax | 803
- Hierarchy Level | 804
- Description | 804
- Required Privilege Level | 804
- Release Information | 805

Syntax

```
source-address-giaddr;
```

Hierarchy Level

```
[edit forwarding-options helpers bootp],
[edit forwarding-options helpers bootp interface interface-name]
```

Description

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.

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.

When this statement is entered in the [**edit forwarding-options helpers bootp interface *interface-name***] 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.

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.

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.

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.

Required Privilege Level

interface—To view this statement in the configuration.
interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.1.

RELATED DOCUMENTATION

DHCP/BOOTP Relay for Switches Overview

source-ip-change (Forwarding Options)

IN THIS SECTION

- Syntax | 805
- Hierarchy Level | 805
- Description | 806
- Required Privilege Level | 806
- Release Information | 806

Syntax

```
source-ip-change;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay]
```

Description

For Dynamic Host Configuration Protocol (DHCP) client request forwarding, enable source IP change for the device to use address of egress interface as source IP address.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement changed from `vpn` to `source-ip-change` in Junos OS Release 15.1X49-D130 and later releases.

RELATED DOCUMENTATION

DHCP Overview | 2

static-binding

IN THIS SECTION

- Syntax | 807
- Hierarchy Level | 807
- Description | 807
- Options | 807
- Required Privilege Level | 808
- Release Information | 808

Syntax

```
static-binding mac-address {
    client-identifier (ascii client-id | hexadecimal client-id);
    fixed-address {
        address;
    }
    host-name client-hostname;
}
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp]
```

Description

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.

Options

mac-address—The MAC address of the client. This is a hardware address that uniquely identifies a client on the network.

`fixed-address` *address*—Fixed IP address assigned to the client. Typically a client has one address assigned, but you can assign more.

`host-name` *client-hostname*—Hostname of the client requesting the DHCP server. The name can include the local domain name. Otherwise, the name is resolved based on the `domain-name` statement.

`client-identifier (ascii` *client-id* | `hexadecimal` *client-id*)—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, *Assigned Numbers*. Either a client identifier or the client's MAC address must be configured to uniquely identify the client on the network.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

strict (DHCP Local Server)

IN THIS SECTION

- Syntax | 808
- Hierarchy Level | 809
- Description | 809
- Default | 809
- Required Privilege Level | 809
- Release Information | 810

Syntax

```
strict;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

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.

Release Information

Statement introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Preventing Binding of Clients That Do Not Support Reconfigure Messages

sub-prefix-length

IN THIS SECTION

- Syntax | 810
- Hierarchy Level | 810
- Description | 811
- Required Privilege Level | 811
- Release Information | 811

Syntax

```
sub-prefix-length sub-prefix-length;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client prefix-
delegating]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
```

```
family inet6 dhcpv6-client prefix-delegating]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client prefix-delegating]
```

Description

Allows you to configure DHCPv6 client sub prefix length. The DHCPv6 client separates the delegated prefix according to sub-prefix lengths. If the delegated prefix is not enough for all interfaces, the client sends out a syslog message.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.3X48-D30 and in Junos OS Release 15.1X49-D100.

The `logical-systems` and `tenants` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

preferred-prefix-length | 702

threshold (detection-time)

IN THIS SECTION

- Syntax | 812
- Hierarchy Level | 812
- Description | 813
- Options | 813
- Required Privilege Level | 813
- Release Information | 813

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[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 group-name liveness-detection method bfd detection-
time],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd
detection-time],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd detection-
time],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd
detection-time]
```

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.

NOTE: The threshold time must be greater than or equal to the `minimum-interval` or the `minimum-receive-interval`.

Options

milliseconds— Value for the detection time adaptation threshold.

- **Range:** 1 through 255,000

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

threshold (transmit-interval)

IN THIS SECTION

- Syntax | 814
- Hierarchy Level | 814
- Description | 815
- Options | 815
- Required Privilege Level | 815
- Release Information | 815

Syntax

```
threshold milliseconds;
```

Hierarchy Level

```
[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 group-name liveness-detection method bfd transmit-
interval],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd
transmit-interval],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd transmit-
interval],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd
transmit-interval]
```

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

milliseconds — Threshold value.

- **Range:** 0 through 4,294,967,295 (2^{32} – 1)

> **NOTE**: The threshold value specified in the `threshold` statement must be greater than the value specified in the `minimum-interval` statement for the `transmit-interval` statement.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients

Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

timeout (DHCP Local Server)

IN THIS SECTION

- Syntax | 816
- Hierarchy Level | 816
- Description | 817
- Options | 817
- Required Privilege Level | 817
- Release Information | 817

Syntax

```
timeout timeout-value;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
```

```
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

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

timeout-value—Initial retry timeout value.

- **Range:** 1 through 10 seconds
- **Default:** 2 seconds

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Configuring Dynamic Reconfiguration Attempts for DHCP Clients

token (DHCP Local Server)

IN THIS SECTION

- Syntax | 818
- Hierarchy Level | 818
- Description | 819
- Options | 819
- Required Privilege Level | 820
- Release Information | 820

Syntax

```
token token-value;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Description

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, *Authentication for DHCP Messages*, section 4.

Options

token-value—Plain-text alphanumeric string.

- **Default:** null (empty string)

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the `[edit ... dhcpv6 ...]` hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Configuring a Token for DHCP Local Server Authentication

trace (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 820
- Hierarchy Level | 821
- Description | 821
- Required Privilege Level | 821
- Release Information | 821

Syntax

```
trace;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit forwarding-options dhcp-relay group group-name  interface-name],
[edit  logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
interface interface-name],
[edit  logical-systems logical-system-name forwarding-options dhcp-relay group group-name
interface interface-name],
[edit  logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name interface interface-name],
[edit  logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group group-
name interface interface-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name]
```

Description

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.

EX Series switches do not support DHCPv6.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.4.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

- Configuring DHCP Relay Agent
- *DHCP Monitoring and Management*

traceoptions (Address-Assignment Pool)

IN THIS SECTION

- Syntax | 822
- Hierarchy Level | 823
- Description | 823
- Options | 823
- Required Privilege Level | 824
- Release Information | 824

Syntax

```
traceoptions {
    file filename {
        files number;
        size maximum-file-size;
        match regex;
        (world-readable | no-world-readable);
    }
    flag address-assignment;
    flag all;
    flag configuration;
    flag framework;
    flag ldap;
    flag local-authentication;
    flag radius;
}
```

Hierarchy Level

```
[edit system processes general-authentication-service]
```

Description

Configure tracing options.

Options

file *filename*—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 **/var/log**.

files *number*—(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.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

- **Range:** 2 through 1000
- **Default:** 3 files

`flag` *`flag`*—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:

- `address-assignment`—All address-assignment events
- `all`—All tracing operations
- `configuration`—Configuration events
- `framework`—Authentication framework events
- `ldap`—LDAP authentication events
- `local-authentication`—Local authentication events
- `radius`—RADIUS authentication events

`match` *regex*—(Optional) Refine the output to include lines that contain the regular expression.

`no-world-readable`—(Optional) Restrict access to the originator of the trace operation only.

`size` *size*—(Optional) Maximum size of each trace file, in kilobytes (KB), megabytes (MB), or gigabytes (GB). If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option 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

admin—To view this statement in the configuration.

admin-control—To add this statement to the configuration.

Release Information

Flag for tracing address-assignment pool operations introduced in Junos OS Release 9.0.

`option-name` option introduced in Junos OS Release 8.3.

Statement introduced in Junos OS Release 9.0.

RELATED DOCUMENTATION

> *Address-Assignment Pool Configuration Overview*

traceoptions (DHCP)

IN THIS SECTION

- Syntax | 825
- Hierarchy Level | 825
- Description | 826
- Options | 826
- Required Privilege Level | 828
- Release Information | 828

Syntax

```
traceoptions {
    file filename <files number> <match regular-expression > <size maximum-file-size> <world-
readable | no-world-readable>;
    flag flag;
    level  (all | error | info | notice | verbose | warning);
    no-remote-trace;
}
```

Hierarchy Level

```
[edit system processes dhcp-service]
[edit security dynamic-address]
```

Description

Define global tracing operations for extended DHCP local server and extended DHCP relay agent processes.

This statement replaces the deprecated `traceoptions` statements at the `[edit forwarding-options dhcp-relay]` and `[edit system services dhcp-local-server]` hierarchy levels.

NOTE: Traceoptions does not differentiate between a logical system and tenant system, and can be configured under the root logical system.

Options

`file` *`filename`*—Name of the file to receive the output of the tracing operation. Enclose the name within quotation marks. All files are placed in the directory `/var/log`.

`files` *`number`*—(Optional) Maximum number of trace files to create before overwriting the oldest one. If you specify a maximum number of files, you also must specify a maximum file size with the `size` option.

- **Range:** 2 through 1000
- **Default:** 3 files

`flag` *`flag`*—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements:

- `all`—Trace all events.
- `auth`—Trace authentication events.
- `database`—Trace database events.
- `fwd`—Trace firewall process events.
- `general`—Trace miscellaneous events.
- `ha`—Trace high availability-related events.
- `interface`—Trace interface operations.
- `io`—Trace I/O operations.
- `liveness-detection`—Trace liveness detection operations.

- `packet`—Trace packet and option decoding operations.
- `performance`—Trace performance measurement operations.
- `profile`—Trace profile operations.
- `rpd`—Trace routing protocol process events.
- `rtsock`—Trace routing socket operations.
- `security-persistence`—Trace security persistence events.
- `session-db`—Trace session database events.
- `state`—Trace changes in state.
- `statistics`—Trace baseline statistics.
- `ui`—Trace user interface operations.

`level`—Level of tracing to perform; also known as severity level. The option you configure enables tracing of events at that level and all higher (more restrictive) levels. You can specify any of the following levels:

- `all`—Match messages of all levels.
- `error`—Match error messages.
- `info`—Match informational messages.
- `notice`—Match notice messages about conditions requiring special handling.
- `verbose`—Match verbose messages. This is the lowest (least restrictive) severity level; when you configure `verbose`, messages at all higher levels are traced. Therefore, the result is the same as when you configure `all`.
- `warning`—Match warning messages.
- **Default:** `error`

`match` *`regular-expression`*—(Optional) Refine the output to include lines that contain the regular expression.

`no-remote-trace`—Disable remote tracing.

`no-world-readable`—(Optional) Disable unrestricted file access, allowing only the user `root` and users who have the Junos OS `maintenance` permission to access the trace files.

`size` *`maximum-file-size`*—(Optional) Maximum size of each trace file. By default, the number entered is treated as bytes. Alternatively, you can include a suffix to the number to indicate kilobytes (*`maximum-file-size`*`k`), megabytes (*`maximum-file-size`*`m`), or gigabytes (*`maximum-file-size`*`g`). If you specify a maximum file size, you also must specify a maximum number of trace files with the `files` option.

- **Range:** 10,240 through 1,073,741,824
- **Default:** 128 KB

`world-readable`—(Optional) Enable unrestricted file access.

Required Privilege Level

trace—To view this statement in the configuration.

trace-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

DHCP Monitoring and Management

traceoptions (DHCP Server)

IN THIS SECTION

- Syntax | 829
- Hierarchy Level | 829
- Description | 829
- Options | 829

Required Privilege Level | 832
Release Information | 832

Syntax

```
traceoptions {
    file filename <files number> <match regex> <size size> <world-readable | no-world-readable>;
    flag flag;
}
```

Hierarchy Level

```
[edit system services dhcp]
```

Description

Define tracing operations for DHCP processes.

Options

file ***filename***—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 **/var/log**.

files ***number***—(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.

If you specify a maximum number of files, you also must specify a maximum file size with the **size** option and a filename.

- **Range:** 2 through 1000
- **Default:** 3 files

`flag` *`flag`*—Tracing operation to perform. To specify more than one tracing operation, include multiple `flag` statements. You can include the following flags:

- `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:** *x*`k` to specify KB, *x*`m` to specify MB, or *x*`g` 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.

Release Information

Statement introduced in Junos OS Release 9.0.

transmit-interval

IN THIS SECTION

- Syntax | 832
- Hierarchy Level | 833
- Description | 833
- Required Privilege Level | 833
- Release Information | 833

Syntax

```
transmit-interval {
    threshold milliseconds;
```

```
    minimum-interval milliseconds;
}
```

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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd]
```

Description

Configure the Bidirectional Forwarding Detection (BFD) transmit interval.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients

trigger (DHCP Local Server)

IN THIS SECTION

- Syntax | 834
- Hierarchy Level | 834
- Description | 835
- Required Privilege Level | 835
- Release Information | 835

Syntax

```
trigger {
    radius-disconnect;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name reconfigure],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
```

```
services dhcp-local-server dhcpv6 group group-name reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
reconfigure],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
reconfigure],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6 group
group-name reconfigure],
[edit system services dhcp-local-server reconfigure],
[edit system services dhcp-local-server dhcpv6 reconfigure],
[edit system services dhcp-local-server group group-name reconfigure],
[edit system services dhcp-local-server dhcpv6 group group-name reconfigure]
```

Description

Configure behavior in response to a trigger for all DHCP clients or only the DHCP clients serviced by the specified group of interfaces.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 10.0.

Support at the [edit ... dhcpv6 ...] hierarchy levels introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

Configuring Reconfiguration of the Client on Receipt of RADIUS-Initiated Disconnect

radius-disconnect (DHCP Local Server) | 722

trust-option-82

IN THIS SECTION

- Syntax | 836
- Hierarchy Level | 836
- Description | 837
- Required Privilege Level | 837
- Release Information | 837

Syntax

```
trust-option-82;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay overrides],
[edit forwarding-options dhcp-relay group group-name overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay overrides],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name
overrides],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay overrides],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
overrides],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name
interface interface-name overrides]
```

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

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 8.3.

RELATED DOCUMENTATION

> *Enable Processing of Untrusted Packets So Option 82 Information Can Be Used*
>
> *Overriding the Default DHCP Relay Configuration Settings*

update-router-advertisement

IN THIS SECTION

- Syntax | 838
- Hierarchy Level | 838
- Description | 838
- Options | 839
- Required Privilege Level | 839
- Release Information | 839

Syntax

```
update-router-advertisement (interface interface-name);
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
[edit logical-systems logical-system-name interfaces interface-name unit logical-unit-number
family inet6 dhcpv6-client]
[edit tenants tenant-name interfaces interface-name unit logical-unit-number family inet6 dhcpv6-
client]
```

Description

Specify the interface used to delegate prefixes.

Options

interface *interface-name*	Interface on which to delegate prefixes

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

The `logical-systems` and `tenant` options are introduced in Junos OS Release 18.4R1.

update-server

IN THIS SECTION

- Syntax | 840
- Hierarchy Level | 840
- Description | 840
- Required Privilege Level | 840
- Release Information | 840

Syntax

```
update-server;
```

Hierarchy Level

```
[edit interfaces interface-name unit  logical-unit-number  family inet dhcp]
```

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.

Release Information

Statement introduced in Junos OS Release 8.5.

RELATED DOCUMENTATION

- Configuring a DHCP Client | 235
- Example: Configuring the Device as a DHCP Client | 238
- *interfaces*
- unit
- family

update-server (dhcp-client)

IN THIS SECTION

- Syntax | 841
- Hierarchy Level | 841
- Description | 841
- Required Privilege Level | 841
- Release Information | 842

Syntax

```
update-server;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Propagate DHCP options to a local DHCP server.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is changed to `dhcp` to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option `dhcp`.

update-server (dhcpv6-client)

IN THIS SECTION

- Syntax | 842
- Hierarchy Level | 842
- Description | 843
- Required Privilege Level | 843
- Release Information | 843

Syntax

```
update-server;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcpv6-client]
```

Description

Propagate TCP/IP settings to the DHCPv6 server.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

use-interface

IN THIS SECTION

- Syntax | 843
- Hierarchy Level | 844
- Description | 844
- Required Privilege Level | 844
- Release Information | 844

Syntax

```
use-interface-description {logical |device};
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-
identifier]
```

Description

The description configured at the physical or logical interface level is used for client identification.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

use-interface-description

IN THIS SECTION

- Syntax | 845
- Hierarchy Level | 845
- Description | 845
- Options | 846
- Required Privilege Level | 847

Release Information | 847

Syntax

```
use-interface-description (logical | device);
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay dhcpv6 group group-name (relay-agent-interface-id | relay-agent-remote-id)],
[edit forwarding-options dhcp-relay relay-option-82 (circuit-id | remote-id)],
[edit forwarding-options dhcp-relay group group-name relay-option-82 (circuit-id | remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay dhcpv6 (relay-agent-interface-id | relay-agent-remote-id)],
[edit logical-systems logical-system-name ... forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6  (relay-agent-interface-id | relay-agent-remote-id)],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay ... relay-option-82 (circuit-id | remote-id)],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-18],
[edit vlans vlan-name forwarding-options dhcp-security dhcpv6-options option-37]
```

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.

Release Information

Statement introduced in Junos OS Release 9.6.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... relay-agent-remote-id]` and `[edit ... remote-id]` hierarchy levels introduced in Junos OS Release 14.1.

Support at the `[edit vlans vlan-name dhcp-security dhcpv6-options option-18]` and `[edit vlans vlan-name dhcp-security dhcpv6-options option-37]` hierarchy levels introduced in Junos OS Release 14.1X53-D10 for EX Series switches.

RELATED DOCUMENTATION

Using DHCP Option 82 Information

Using DHCP Relay Agent Option 82 Information

Configuring DHCPv6 Relay Agent Options

use-primary (DHCP Local Server)

IN THIS SECTION

- Syntax | 848
- Hierarchy Level | 848
- Description | 848
- Options | 849
- Required Privilege Level | 849

- Release Information | 849

Syntax

```
use-primary primary-profile-name;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server dynamic-profile
profile-name],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
dynamic-profile profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server dynamic-profile
profile-name],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
dynamic-profile profile-name],
[edit system services dhcp-local-server dynamic-profile profile-name],
[edit system services dhcp-local-server group group-name dynamic-profile profile-name]
```

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

primary-profile-name—Name of the dynamic profile to configure as the primary dynamic profile

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.3.

RELATED DOCUMENTATION

Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

use-primary (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 850
- Hierarchy Level | 850
- Description | 851
- Options | 851
- Required Privilege Level | 851
- Release Information | 851

Syntax

```
use-primary primary-profile-name;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dhcpv6 group  group-name dynamic-profile profile-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name dynamic-profile profile-
name],
[edit forwarding-options dhcp-relay group  group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 dynamic-profile
profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dynamic-profile profile-
name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 group group-name
dynamic-profile profile-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name dynamic-
profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 group group-name dynamic-profile profile-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 dynamic-
profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dynamic-profile
profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 group  group-
name dynamic-profile profile-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group  group-name
dynamic-profile profile-name]
```

Description

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.

Use the statement at the `[edit ... dhcpv6]` hierarchy levels to configure DHCPv6 support.

EX Series switches do not support DHCPv6.

Options

primary-profile-name—Name of the dynamic profile to configure as the primary dynamic profile

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.3.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *dual-stack-group-name*`]` hierarchy level introduced in Junos OS Release 15.1.

RELATED DOCUMENTATION

Attaching Dynamic Profiles to DHCP Subscriber Interfaces or DHCP Client Interfaces

use-vlan-id

IN THIS SECTION

- Syntax | 852
- For Platforms with Enhanced Layer 2 Software (ELS) | 852
- For MX Series Platforms | 852
- Description | 853
- Required Privilege Level | 853
- Release Information | 853

Syntax

```
use-vlan-id;
```

For Platforms with Enhanced Layer 2 Software (ELS)

```
[edit forwarding-options helpers bootp dhcp-option82-circuit-id]
[edit forwarding-options helpers bootp interface  interface-name dhcp-option82-circuit-id]
```

For MX Series Platforms

```
[edit bridge-domains bridge-domain-name forwarding-options dhcp-security option-82 circuit-id]
```

Description

Use the VLAN ID rather than the VLAN name (the default) in the circuit ID or remote ID value in the DHCP option 82 information.

NOTE: The `use-vlan-id` statement is mutually exclusive with the `use-interface-description` and `no-vlan-interface-name` statements.

The `use-vlan-id` statement only applies to interfaces in a bridge domain. The format of the Agent Circuit ID or Agent Remote ID information for Fast Ethernet or Gigabit Ethernet interfaces is as follows:

```
(fe | ge)-fpc/pic/port.subunit:svlan_id-vlan_id
```

NOTE: The *subunit* is required and used to differentiate the interface for remote systems, and *svlan_id-vlan_id* represents the VLANs associated with the bridge domain.

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.3.

Hierarchy level `[edit vlans vlan-name forwarding-options dhcp-security]` introduced in Junos OS Release 13.2X50-D10. (See Using the Enhanced Layer 2 Software CLI for information about ELS.)

Hierarchy level `[edit bridge-domains bridge-domain-name forwarding-options dhcp-security]` introduced in Junos OS Release 14.1 for the MX Series.

NOTE: The EX Series switches that support the `use-vlan-id` statement are the EX4300, EX4600, and EX9200 switches.

RELATED DOCUMENTATION

- Example: Setting Up DHCP Option 82 Using the Same VLAN
- Example: Setting Up DHCP Option 82
- http://tools.ietf.org/html/rfc3046.

use-vlan-id (DHCP Relay Agent)

IN THIS SECTION

- Syntax | 854
- Hierarchy Level | 855
- Description | 855
- Required Privilege Level | 855
- Release Information | 856

Syntax

```
use-vlan-id;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay dhcpv6],
[edit forwarding-options dhcp-relay dhcpv6 group group-name],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-group-name],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name forwarding-options dhcp-relay dual-stack-group dual-
stack-group-name],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dhcpv6 ...],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay dual-stack-group dual-stack-group-name],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dhcpv6 ...],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay dual-stack-group ]
```

Description

Specify that the VLAN is identified by the VLAN ID, rather than the VLAN name, when you configure the DHCPv6 relay agent to include either of the following in packets it sends to a DHCPv6 server:

- DHCPv6 Interface-ID (option 18)
- DHCPv6 Remote-ID (option 37)

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 11.4.

RELATED DOCUMENTATION

DHCPv6 Relay Agent

Extended DHCP Relay Agent Overview

user-defined-option-82

IN THIS SECTION

- Syntax | 856
- Hierarchy Level | 856
- Description | 857
- Required Privilege Level | 857
- Release Information | 858

Syntax

```
user-defined-option-82 string;
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay group group-name interface interface-name overrides user-
defined-option82 string],
```

```
[edit forwarding-options dhcp-relay group group-name overrides user-defined-option82 string],
[edit forwarding-options dhcp-relay overrides user-defined-option82 string]
```

Description

Configure a custom text string to use as the interface description in the DHCP option 82 Agent Circuit ID (suboption 1) information. This text string is defined independently of the interface description that is configured using the `description` statement at the `[edit interfaces interface-name]` hierarchy level.

The custom text string is configured using the `user-defined-option-82` statement at the following hierarchy levels:

- To configure a custom string on an interface level:

  ```
  [edit forwarding-options dhcp-relay group group-name interface interface-name overrides user-defined-option82 string]
  ```

- To configure a custom string at the group level:

  ```
  [edit forwarding-options dhcp-relay group group-name overrides user-defined-option82 string]
  ```

- To configure a custom string globally:

  ```
  [edit forwarding-options dhcp-relay overrides user-defined-option82 string]
  ```

You can define a custom string up to 251 characters in length. To include the custom string in the DHCP option 82 Agent Circuit ID, you must configure the `user-defined` statement at the `[edit forwarding-options dhcp-relay group group-name relay-option-82 circuit-id]` hierarchy level.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 17.2.

Release History Table

Release	Description
21.2R1	Starting with Junos OS Release 21.2R1, QFX Series switches support the user-defined-option-82 CLI statement in a stateless DHCP relay configuration. You can configure stateless DHCP relay using the forward-only CLI statement at the [edit forwarding-options dhcp-relay] hierarchy level.

RELATED DOCUMENTATION

Including a Textual Description in DHCP Options

Using DHCP Relay Agent Option 82 Information

user-id

IN THIS SECTION

- Syntax | 858
- Hierarchy Level | 859
- Description | 859
- Required Privilege Level | 859
- Release Information | 859

Syntax

```
user-id {ascii ascii hexadecimal hexadecimal};
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client client-
identifier]
```

Description

Specify an ASCII or hexadecimal user ID for the Dynamic Host Configuration Protocol (DHCP) client.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

user-prefix (DHCP Local Server)

IN THIS SECTION

- Syntax | 860
- Hierarchy Level | 860
- Description | 861
- Options | 861
- Required Privilege Level | 861

Release Information | 861

Syntax

```
user-prefix user-prefix-string;
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication ],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server  authentication username-
include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6  authentication
username-include],
[edit logical-systems logical-system-name system services dhcp-local-server dhcpv6 group group-
name authentication username-include],
[edit logical-systems logical-system-name system services dhcp-local-server group group-name
authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server dhcpv6 group group-name authentication username-include],
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server group group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server authentication
username-include],
```

```
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6
authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server dhcpv6  group
group-name authentication username-include],
[edit routing-instances routing-instance-name system services dhcp-local-server group group-name
authentication username-include],
[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]
```

Description

Specify the user prefix that is concatenated with the username during the subscriber authentication or DHCP client authentication process.

Options

user-prefix-string—User prefix string.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

RELATED DOCUMENTATION

DHCP with External Authentication Server | 266

username-include (DHCP Local Server)

IN THIS SECTION

- Syntax | 862
- Hierarchy Level | 863
- Description | 863
- Options | 863
- Required Privilege Level | 864
- Release Information | 864

Syntax

```
username-include {
    circuit-type;
    client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interfaces-description (device-interface | logical-interface);
    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;
    vlan-tags;
}
```

Hierarchy Level

```
[edit logical-systems logical-system-name routing-instances routing-instance-name system
services dhcp-local-server ...],
[edit logical-systems logical-system-name system services dhcp-local-server ...],
[edit routing-instances routing-instance-name system services dhcp-local-server ...],
[edit system services dhcp-local-server authentication],
[edit system services dhcp-local-server group group-name 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 dual-stack-group group-name authentication]
```

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.

The following statements are not supported in the DHCPv6 hierarchy levels:

- **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**

Options

vlan-tags Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format *outer-vlan-tag-inner-vlan-tag*. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

`vlan-tags` option added in Junos OS Release 18.3R1 on MX Series routers.

RELATED DOCUMENTATION

Specifying Authentication Support

Creating Unique Usernames for DHCP Clients

username-include (DHCP Relay Agent)

IN THIS SECTION

- Syntax | **865**
- Hierarchy Level | **865**
- Description | **866**
- Options | **866**

Required Privilege Level | 867
Release Information | 867

Syntax

```
username-include {
    circuit-type;
    client-id <exclude-headers> <use-automatic-ascii-hex-encoding>;
    delimiter delimiter-character;
    domain-name domain-name-string;
    interface-description (device-interface | logical-interface);
    interface-name;
    logical-system-name;
    mac-address;
    option-60;
    option-82 <circuit-id> <remote-id>;
    relay-agent-interface-id;
    relay-agent-remote-id;
    relay-agent-subscriber-id;
    routing-instance-name;
    user-prefix user-prefix-string;
    vlan-tags;
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay authentication],
[edit forwarding-options dhcp-relay group group-name authentication],
[edit forwarding-options dhcp-relay dhcpv6 authentication],
[edit forwarding-options dhcp-relay dhcpv6 group group-name authentication],
[edit forwarding-options dhcp-relay dual-stack-group dual-stack-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 ...]
```

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:

- **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**

Options

vlan-tags Include the subscriber session VLAN tags in the username for interactions with an external authority. Both single-tagged and double-tagged VLANs are supported: The tags are added in the format *outer-vlan-tag-inner-vlan-tag*. The outer tag is always included; the inner tag is included for double-tagged VLANs.

Use this option instead of the `interface-name` option when the outer VLAN tag is unique across the system and you do not need the underlying physical interface name to be part of the format.

The remaining statements are explained separately. Search for a statement in CLI Explorer or click a linked statement in the Syntax section for details.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 9.1.

Support at the `[edit ... dhcpv6]` hierarchy levels introduced in Junos OS Release 11.4.

Support at the `[edit ... dual-stack-group` *`dual-stack-group-name`*`]` hierarchy level introduced in Junos OS Release 15.1.

`vlan-tags` option added in Junos OS Release 18.3R1 on MX Series routers.

RELATED DOCUMENTATION

Creating Unique Usernames for DHCP Clients

Specifying Authentication Support

vendor-id

IN THIS SECTION

- Syntax | 868
- Hierarchy Level | 868
- Description | 868
- Options | 868
- Required Privilege Level | 868
- Release Information | 868

Syntax

```
vendor-id vendor-id;
```

Hierarchy Level

```
[edit interfaces interface-name unit logical-unit-number family family dhcp-client]
```

Description

Configure a vendor class ID for the Dynamic Host Configuration Protocol (DHCP) client.

Options

vendor-id	Vendor class ID.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

Starting with Junos OS Release 17.3R1, on all SRX Series devices and vSRX instances, the CLI option `dhcp-clinet` at `[edit interfaces interface-name unit logical-unit-number family inet]` hierarchy is

changed to dhcp to keep consistent with other Junos platforms. There is no change in the functionality with the changed CLI option dhcp.

vendor-option

IN THIS SECTION

- Syntax | 869
- Hierarchy Level | 869
- Description | 870
- Required Privilege Level | 870
- Release Information | 870

Syntax

```
vendor-option {
    default-local-server-group local-server-group-name |
    default-relay-server-group server-group-name
    drop;
    equals
    starts-with
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-60]
```

Description

Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

NOTE: The `vendor-option` statement has been deprecated and might be removed from future product releases. We recommend that you phase out its use. See "option-number" on page 677.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 12.1.

Statement deprecated in Junos OS Release 12.3 for EX Series switches.

RELATED DOCUMENTATION

Configuring DHCP Relay Agent | **159**

Understanding the Extended DHCP Relay Agent for EX Series Switches

vendor-option

IN THIS SECTION

- Syntax | 871
- Hierarchy Level | 871
- Description | 872
- Options | 872
- Required Privilege Level | 873
- Release Information | 873

Syntax

```
vendor-option {
    (default-relay-server-group server-group-name | default-local-server-group local-server-group-name | drop);
    (equals | starts-with) (ascii match-string | hexadecimal match-hex) {
        (drop | local-server-group local-server-group-name | relay-server-group server-group-name);
    }
}
```

Hierarchy Level

```
[edit forwarding-options dhcp-relay relay-option-60],
[edit forwarding-options dhcp-relay group group-name relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay relay-option-60],
[edit logical-systems logical-system-name forwarding-options dhcp-relay group group-name relay-option-60],
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-60],
```

```
[edit logical-systems logical-system-name routing-instances routing-instance-name forwarding-
options dhcp-relay group group-name relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay relay-option-60],
[edit routing-instances routing-instance-name forwarding-options dhcp-relay group group-name relay-
option-60]
```

Description

Configure the match criteria when you use the DHCP vendor class identifier option (option 60) in DHCP client packets to forward client traffic to specific DHCP servers. The extended DHCP relay agent compares the option 60 vendor-specific strings received in DHCP client packets against the match criteria that you specify. If there is a match, you can define certain actions for the associated DHCP client packets.

The `vendor-option` statement enables you to specify either an exact, left-to-right match (with the `equals` statement) or a partial match (with the `starts-with` statement), and configure either an ASCII match string (with the `ascii` statement) or a hexadecimal match string (with the `hexadecimal` statement).

You can configure an unlimited number of match strings. Match strings do not support the use of wildcard attributes.

Options

equals—Exact, left-to-right match of the ASCII or hexadecimal match string with the option 60 string.

starts-with—Partial match of the ASCII or hexadecimal match string with the option 60 string. The option 60 string can contain a superset of the ASCII or hexadecimal match string, provided that the leftmost characters of the option 60 string entirely match the characters in the configured match string. When you use the `starts-with` statement, the longest match rule applies; that is, the router matches the string “test123” before it matches the string “test”.

ascii *match-string*—ASCII match string of 1 through 255 alphanumeric characters.

hexadecimal *match-hex*—Hexadecimal match string of 1 through 255 hexadecimal characters (0 through 9, a through f, A through F).

The remaining statements are explained separately. See CLI Explorer.

Required Privilege Level

interface—To view this statement in the configuration.

interface-control—To add this statement to the configuration.

Release Information

Statement introduced in JUNOS Release 9.0.

version (BFD)

IN THIS SECTION

- Syntax | 873
- Hierarchy Level | 874
- Description | 874
- Options | 874
- Required Privilege Level | 874
- Release Information | 875

Syntax

```
version (0 | 1 | automatic);
```

Hierarchy Level

```
[edit logical-systems logical-system-name protocols ldp oam bfd-liveness-detection],
[edit logical-systems logical-system-name 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 group-name liveness-detection method bfd],
[edit system services dhcp-local-server dhcpv6 group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay group group-name liveness-detection method bfd],
[edit forwarding-options dhcp-relay dhcpv6 group group-name liveness-detection method bfd],
[edit protocols ldp oam bfd-liveness-detection],
[edit protocols ldp oam fec address bfd-liveness-detection]
```

Description

Configure the BFD protocol version to detect.

Options

0	Use BFD protocol version 0.
1	Use BFD protocol version 1.
automatic	Autodetect the BFD protocol version.

- **Default:** `automatic`

Required Privilege Level

routing—To view this statement in the configuration.

routing-control—To add this statement to the configuration.

Release Information

Statement introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

- Example: Configuring Group Liveness Detection with BFD for DHCP Local Server Clients
- Example: Configuring Global Liveness Detection with BFD for DHCP Relay Agent Clients
- Configuring BFD for LDP LSPs

wins-server (System)

IN THIS SECTION

- Syntax | 875
- Hierarchy Level | 876
- Description | 876
- Options | 876
- Required Privilege Level | 876
- Release Information | 876

Syntax

```
wins-server {
    address;
}
```

Hierarchy Level

```
[edit system services dhcp],
[edit system services dhcp],
[edit system services dhcp pool],
[edit system services dhcp static-binding]
```

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

address—IPv4 address of the NetBIOS Name Server running WINS. To configure multiple servers, include multiple *address* options.

Required Privilege Level

system—To view this statement in the configuration.

system-control—To add this statement to the configuration.

Release Information

Statement introduced before Junos OS Release 7.4.

CHAPTER 9

Operational Commands

clear dhcp client binding | 879

clear dhcp client statistics | 881

clear dhcp relay binding | 883

clear dhcp relay statistics | 885

clear dhcp server binding | 886

clear dhcp server statistics | 888

clear dhcpv6 client binding | 890

clear dhcpv6 client statistics | 892

clear dhcpv6 relay binding | 893

clear dhcpv6 relay statistics | 898

clear dhcpv6 server binding | 901

clear dhcpv6 server binding (Local Server) | 905

clear dhcpv6 server statistics | 907

clear dhcpv6 server statistics (Local Server) | 909

clear system services dhcp binding | 910

clear system services dhcp conflict | 912

clear system services dhcp statistics | 914

request dhcp client renew | 915

request dhcp server reconfigure | 917

request dhcpv6 server reconfigure | 919

request dhcpv6 client renew | 922

request system services dhcp | 923

restart | 925

show captive-portal firewall | 942

show dhcp client binding | 946

show dhcp client statistics | 951

show dhcp relay binding | 956

show dhcp relay statistics | 960

show dhcp server binding | 963

show dhcp server statistics | 966

show dhcpv6 client binding | 969

show dhcpv6 client statistics | 973

show dhcpv6 relay binding | 977

show dhcpv6 relay statistics | 989

show dhcpv6 server binding (View) | 997

show dhcpv6 server statistics | 1003

show dhcpv6 server statistics (View) | 1010

show route protocol | 1015

show system services dhcp binding | 1023

show system services dhcp client | 1027

show system services dhcp conflict | 1032

show system services dhcp global | 1035

show system services dhcp pool | 1037

show system services dhcp relay-statistics | 1041

show system services dhcp statistics | 1044

clear dhcp client binding

IN THIS SECTION

- Syntax | 879
- Description | 879
- Options | 879
- Required Privilege Level | 880
- Output Fields | 880
- Release Information | 880

Syntax

```
clear dhcp client binding
[all|interface <interface-name>]
[routing-instance <routing-instance-name>]
```

Description

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the DHCP client table.

Options

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.

routing-instance <routing-instance-name>	(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, binding state is cleared for DHCP clients on the default routing instance.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

show dhcp client binding | 946

clear dhcp client statistics

IN THIS SECTION

- Syntax | 881
- Description | 881
- Options | 881
- Required Privilege Level | 882
- Output Fields | 882
- Release Information | 882

Syntax

```
clear dhcp client statistics
<all>
<interface>
<routing-instance>
```

Description

Clear all Dynamic Host Configuration Protocol (DHCP) client statistics.

Options

all	(Optional) Clear all the DHCP client statistics.
interface	(Optional) Clear the statistics for DHCP clients on the specified interface.

routing-instance	(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.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

show dhcp client statistics | 951

clear dhcp relay binding

IN THIS SECTION

- Syntax | 883
- Description | 883
- Options | 883
- Required Privilege Level | 884
- Output Fields | 884
- Release Information | 884

Syntax

```
clear dhcp relay binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>
```

Description

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table.

Options

all	(Optional) Clear the binding state for all DHCP clients.
ip-address	(Optional) Clear the binding state for the DHCP client, using the specified IP address.

mac-address	(Optional) Clear the binding state for the DHCP client, using the specified MAC address.
interface interface-name	(Optional) Clear the binding state for DHCP clients on the specified interface
routing-instance routing-instance-name	(Optional) Clear the binding state for DHCP clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for the default routing instance.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

Viewing and Clearing DHCP Bindings

show dhcp relay binding

clear dhcp relay statistics

IN THIS SECTION

- Syntax | 885
- Description | 885
- Options | 885
- Required Privilege Level | 886
- Output Fields | 886
- Release Information | 886

Syntax

```
clear dhcp relay statistics
<routing-instance routing-instance-name>
```

Description

Clear all Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options

routing-instance routing-instance-name	(Optional) Clear the DHCP relay statistics 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

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

show dhcp relay statistics | 960

clear dhcp server binding

IN THIS SECTION

- Syntax | 887
- Description | 887
- Options | 887
- Required Privilege Level | 887
- Output Fields | 888
- Release Information | 888

Syntax

```
clear dhcp server binding
<all | ip-address | mac-address>
<interface interface-name>
<routing-instance routing-instance-name>
```

Description

Clear the binding state of a Dynamic Host Configuration Protocol (DHCP) client from the client table on the DHCP local server.

Options

all	(Optional) Clear the binding state for all DHCP clients.
ip-address	(Optional) Clear the binding state for the DHCP client, using the specified IP address.
mac-address	(Optional) Clear the binding state for the DHCP client, using the specified MAC address.
interface interface-name	(Optional) Clear the binding state for DHCP clients on the specified interface.
routing-instance routing-instance-name	(Optional) Clear the binding state for DHCP clients on the specified routing instance.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

show dhcp server binding | 963

clear dhcp server statistics

IN THIS SECTION

- Syntax | 888
- Description | 889
- Options | 889
- Required Privilege Level | 889
- Output Fields | 889
- Release Information | 889

Syntax

```
clear dhcp server statistics
<routing-instance routing-instance-name>
```

Description

Clear all Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

routing-instance routing-instance-name	(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.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

show dhcp server statistics | 966

clear dhcpv6 client binding

IN THIS SECTION

- Syntax | 890
- Description | 890
- Options | 890
- Required Privilege Level | 891
- Output Fields | 891
- Release Information | 891

Syntax

```
clear dhcpv6 client binding
[all | interface interface-name]
[routing-instance routing-instance-name]
```

Description

Clear the binding state of a Dynamic Host Configuration Protocol (DHCPv6) client from the DHCPv6 client table.

Options

all	(Optional) Clear the binding state for all DHCPv6 clients.
interface *interface-name*	(Optional) Clear the binding state for DHCPv6 clients on the specified interface.

routing-instance *routing-instance-name*	(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance. If you do not specify a routing instance, the binding state is cleared for DHCPv6 clients on the default routing instance.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

show dhcpv6 client binding | 969

clear dhcpv6 client statistics

IN THIS SECTION

- Syntax | 892
- Description | 892
- Options | 892
- Required Privilege Level | 893
- Output Fields | 893
- Release Information | 893

Syntax

```
clear dhcpv6 client statistics
routing-instance routing-instance-name
```

Description

Clear all DHCPv6 client statistics.

Options

routing-instance *routing-instance-name*

(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.

Required Privilege Level

clear

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

show dhcpv6 client statistics | 973

clear dhcpv6 relay binding

IN THIS SECTION

- Syntax | 894
- Description | 894
- Options | 894
- Required Privilege Level | 895
- Output Fields | 895

Sample Output | 895
Release Information | 897

Syntax

```
clear dhcpv6 relay binding
<address>
<all>
<dual-stack>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Clear the binding state of Dynamic Host Configuration Protocol for IPv6 (DHCPv6) clients from the client table.

Options

address (Optional) Clear the binding state for the DHCPv6 client, using one of the following entries:

- *CID*—The specified Client ID (CID).
- *ipv6-prefix*—The specified IPv6 prefix.
- *session-id*—The specified session ID.

all (Optional) Clear the binding state for all DHCPv6 clients.

dual-stack	(Optional) Clear the binding state for DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.
interfaces-vlan	(Optional) Clear the binding state on the interface VLAN ID and S-VLAN ID.
interfaces-wildcard	(Optional) The set of interfaces on which to clear bindings. This option supports the use of the wildcard character (*).
interface ***interface-name***	(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
logical-system ***logical-system-name***	(Optional) Clear the binding state for DHCPv6 clients on the specified logical system.
routing-instance ***routing-instance-name***	(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level

view

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:db8:3c4d:15::/64   1           83720    BOUND    ge-1/0/0.0
```

```
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:db8:3c4d:16::/64    2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64    3           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d: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:db8:3c4d:15::/64
user@host> show dhcpv6 relay binding

Prefix                   Session Id  Expires  State    Interface    Client DUID
2001:db8:3c4d:16::/64    2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64    3           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d: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 dhcpv6 relay binding dual-stack all

The following command clears all DHCPv6 relay agent bindings for all DHCPv6 clients and the associated DHCPv4 bindings in the single-session DHCP dual stack. DHCPv4 clients created in a DHCPv4-only stack are not affected.

```
user@host> clear dhcpv6 relay binding dual-stack all
```

clear dhcv6p 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.*
```

Release Information

Command introduced in Junos OS Release 11.4.

Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Option `dual-stack` added in Junos OS Release 15.1.

RELATED DOCUMENTATION

Viewing and Clearing DHCP Bindings

show dhcpv6 relay binding | **977**

clear dhcpv6 relay statistics

IN THIS SECTION

- Syntax | **898**
- Description | **899**
- Options | **899**
- Required Privilege Level | **899**
- Output Fields | **899**
- Sample Output | **900**
- Release Information | **901**

Syntax

```
clear dhcpv6 relay statistics
<bulk-leasequery-connections>
<leasequery>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Clear all Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options

bulk-leasequery-connections	(Optional) Clear DHCPv6 relay bulk leasequery statistics.
leasequery	(Optional) Clear DHCPv6 relay individual leasequery statistics.
logical-system *logical-system-name*	(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 *routing-instance-name*	(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

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
```

Release Information

Command introduced in Junos OS Release 11.4.

`bulk-leasequery-connections` option introduced in Junos OS Release 16.1.

clear dhcpv6 server binding

IN THIS SECTION

- Syntax | **901**
- Description | **902**
- Options | **902**
- Required Privilege Level | **903**
- Output Fields | **903**
- Sample Output | **903**
- Release Information | **905**

Syntax

```
clear dhcpv6 server binding
<address>
```

```
<all>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<dual-stack>
```

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

address	(Optional) Clear the binding state for the DHCPv6 client, using one of the following entries: • *CID*—The specified Client ID (CID). • *ipv6-prefix*—The specified IPv6 prefix. • *session-id*—The specified session ID.
all	(Optional) Clear the binding state for all DHCPv6 clients.
interface *interface-name*	(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
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 DHCPv6 clients on the specified logical system.
routing-instance *routing-instance-name*	(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.
dual-stack	(Optional) Remove either both arms or single arm of dual-stack.

NOTE:

- The `dual-stack` command is added in the syntax removes both arms of the dual-stack with a single command entry.
- When the `dual-stack` command is not added in the syntax, the `clear dhcpv6 server binding` command clears only the family specific arm of the dual-stack.

Required Privilege Level

clear

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 binding dual-stack all

The following command clears all the dual-stack local server bindings.

```
user@host> clear dhcpv6 server binding dual-stack all
```

Release Information

Command introduced in Junos OS Release 9.6.

Options *interfaces-vlan* and *interfaces-wildcard* added in Junos OS Release 12.1.

Command updated with `dual-stack` statement in Junos OS Release 17.3.

RELATED DOCUMENTATION

Viewing and Clearing DHCP Bindings

No Link Title

clear dhcpv6 server binding (Local Server)

IN THIS SECTION

- Syntax | **905**
- Description | **906**
- Options | **906**
- Required Privilege Level | **906**
- Release Information | **906**

Syntax

```
clear dhcpv6 server binding
<all | client-id | ip-address | session-id>
<interface interface-name>
<routing-instance routing-instance-name>
```

Description

Clear the binding state of a DHCPv6 client from the client table on the DHCPv6 local server.

Options

- all—(Optional) Clear the binding state for all DHCPv6 clients.
- *client-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified client ID (option 1).
- *ip-address*—(Optional) Clear the binding state for the DHCPv6 client with the specified address.
- *session-id*—(Optional) Clear the binding state for the DHCPv6 client with the specified session ID.
- interface *interface-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Clear the binding state for DHCPv6 clients on the specified routing instance.

Required Privilege Level

clear

Release Information

Command introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

show dhcpv6 server binding (View) | 997

clear dhcpv6 server statistics

IN THIS SECTION

- Syntax | 907
- Description | 907
- Options | 907
- Required Privilege Level | 908
- Output Fields | 908
- Sample Output | 908
- Release Information | 908

Syntax

```
clear dhcpv6 server statistics
<bulk-leasequery-connections>
<interface interface-name>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Clear all extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options

bulk-leasequery-connections	(Optional) Clear DHCPv6 local server bulk leasequery statistics.

logical-system *logical-system-name*	(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.
routing-instance *routing-instance-name*	(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.

Required Privilege Level

clear

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
```

Release Information

Command introduced in Junos OS Release 9.6.

`bulk-leasequery-connections` option introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

show dhcpv6 server statistics | 1003

clear dhcpv6 server statistics (Local Server)

IN THIS SECTION

- Syntax | 909
- Description | 909
- Options | 909
- Required Privilege Level | 910
- Release Information | 910

Syntax

```
clear dhcpv6 server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Clear all DHCPv6 local server statistics.

Options

logical-system *logical-system-name*	(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.
routing-instance *routing-instance-name*	(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.

Required Privilege Level

clear

Release Information

Command introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

show dhcpv6 server statistics (View) | 1010

clear system services dhcp binding

IN THIS SECTION

- Syntax | 910
- Description | 911
- Options | 911
- Required Privilege Level | 911
- Output Fields | 911
- Sample Output | 911
- Release Information | 911

Syntax

```
clear system services dhcp binding
<address>
```

Description

(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

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
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

show system services dhcp binding | 1023

clear system services dhcp conflict

IN THIS SECTION

- Syntax | 912
- Description | 912
- Options | 913
- Required Privilege Level | 913
- Output Fields | 913
- Sample Output | 913
- Release Information | 913

Syntax

```
clear system services dhcp conflict
<address>
```

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

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
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

show system services dhcp conflict | 1032

clear system services dhcp statistics

IN THIS SECTION

- Syntax | 914
- Description | 914
- Options | 914
- Required Privilege Level | 915
- Output Fields | 915
- Sample Output | 915
- Release Information | 915

Syntax

```
clear system services dhcp statistics
```

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

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
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

show system services dhcp statistics | 1044

request dhcp client renew

IN THIS SECTION

- Syntax | 916
- Description | 916

- Options | 916
- Required Privilege Level | 916
- Output Fields | 917
- Release Information | 917

Syntax

```
request dhcp client renew
[all|interface <interface-name>]
routing-instance <routing-instance-name>
```

Description

Initiates a renew request for the specified clients if they are in the bound state.

Options

all	Initiate renew requests for all DHCP clients. If you specify a routing instance, renew requests are initiated for all DHCP clients within that routing instance.
interface <interface-name>	Initiate renew requests for DHCP clients on the specified interface.
routing-instance <routing-instance-name>	Initiate renew requests for DHCP clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level

view

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

request dhcpv6 client renew | 922

request dhcp server reconfigure

IN THIS SECTION

- Syntax | 917
- Description | 918
- Options | 918
- Required Privilege Level | 919
- Output Fields | 919
- Sample Output | 919
- Release Information | 919

Syntax

```
request dhcp server reconfigure (all | address | interface interface-name | logical-system
logical-system-name | routing-instance routing-instance-name)
```

Description

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.

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.

Options

all — Initiate reconfiguration for all DHCP clients.

address — Initiate reconfiguration for DHCP client with the specified IP address or MAC address.

interface ***interface-name*** — Initiate reconfiguration for all DHCP clients on this logical interface (clients whose initial login requests were received over the specified interface).

> **NOTE**: You cannot use the `interface` *`interface-name`* 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.

logical-system ***logical-system-name*** — Initiate reconfiguration for all DHCP clients on the specified logical system.

routing-instance ***routing-instance-name*** — Initiate reconfiguration reconfigured for all DHCP clients in the specified routing instance.

Required Privilege Level

view

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
```

Release Information

Command introduced in Junos OS Release 10.0.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

request dhcpv6 server reconfigure

IN THIS SECTION

- Syntax | 920
- Description | 920

- Options | 920
- Required Privilege Level | 921
- Output Fields | 921
- Sample Output | 921
- Release Information | 921

Syntax

```
request dhcpv6 server reconfigure (all | address | client-id | interface interface-name |
logical-system logical-system-name | routing-instance routing-instance-name | session-id)
```

Description

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.

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.

Options

all	Initiate reconfiguration for all DHCPv6 clients.
address	Initiate reconfiguration for DHCPv6 client with the specified IPv6 address.

client-id	Initiate reconfiguration for DHCPv6 client with the specified client ID.
interface *interface-name*	Initiate reconfiguration for all DHCPv6 clients on this logical interface (clients whose initial login requests were received over the specified interface).
logical-system *logical-system-name*	Initiate reconfiguration for all DHCPv6 clients on the specified logical system.
routing-instance *routing-instance-name*	Initiate reconfiguration reconfigured for all DHCPv6 clients in the specified routing instance.
session-id	Initiate reconfiguration for DHCPv6 client with the specified session ID.

Required Privilege Level

view

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 2001db8::2/16
```

Release Information

Command introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

Configuring Dynamic Reconfiguration of Extended Local Server Clients Overview

request dhcpv6 client renew

IN THIS SECTION

- Syntax | **922**
- Description | **922**
- Options | **923**
- Required Privilege Level | **923**
- Output Fields | **923**
- Release Information | **923**

Syntax

```
request dhcpv6 client renew
[all | interface interface-name]
routing-instance <routing-instance-name>
```

Description

Initiate a renew request for the specified DHCPv6 clients if they are in the bound state.

Options

all	Initiate renew requests for all DHCPv6 clients. If you specify a routing instance, renew requests are initiated for all DHCPv6 clients within that routing instance.
interface-name *interface-name*	Initiate renew requests for DHCPv6 clients on the specified interface.
routing-instance *routing-instance-name*	Initiate renew requests for DHCPv6 clients in the specified routing instance. If you do not specify a routing instance, renew requests are initiated on the default routing instance.

Required Privilege Level

view

Output Fields

This command produces no output.

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

request system services dhcp

IN THIS SECTION

- Syntax | 924
- Description | 924

- Options | 924
- Required Privilege Level | 924
- Output Fields | 925
- Release Information | 925

Syntax

```
request system services dhcp (release           interface-name          | renew
interface-name)
```

Description

Release or renew the acquired IP address for a specific interface.

To view the status of the Dynamic Host Configuration Protocol (DHCP) clients on the specified interfaces, enter the `show system services dhcp client` *interface-name* command.

Options

- `release` *interface-name* —Clears other resources received earlier from the server, and reinitializes the client state to INIT for the particular interface.
- `renew` *interface-name* —Reacquires an IP address from the server for the interface. When you use 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.

Required Privilege Level

maintenance

Output Fields

This command produces no output.

Release Information

Command introduced in Junos OS Release 8.5.

RELATED DOCUMENTATION

- dhcp (DHCP Client) | 441
- show system services dhcp client | 1027

restart

IN THIS SECTION

- Syntax | 926
- Syntax (ACX Series Routers) | 926
- Syntax (EX Series Switches) | 927
- Syntax (MX Series Routers) | 927
- Syntax (QFX Series) | 928
- Syntax (Routing Matrix) | 928
- Syntax (SRX Series) | 928
- Syntax (TX Matrix Routers) | 929
- Syntax (TX Matrix Plus Routers) | 929
- Syntax (QFX Series) | 930
- Syntax (Junos OS Evolved) | 930
- Description | 931
- Options | 931

- Required Privilege Level | **941**
- Output Fields | **941**
- Sample Output | **941**
- Release Information | **941**

Syntax

```
restart
<adaptive-services |ancpd-service | application-identification |audit-process | auto-
configuration |captive-portal-content-delivery |ce-l2tp-service |chassis-control | class-of-
service |clksyncd-service |database-replication|datapath-trace-service |dhcp-service | diameter-
service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | ethernet-connectivity-
fault-management |ethernet-link-fault-management |event-processing | firewall | general-
authentication-service | gracefully | iccp-service |idp-policy | immediately |interface-control
| ipsec-key-management | kernel-health-monitoring | kernel-replication | l2-learning | l2cpd-
service | l2tp-service | l2tp-universal-edge | lacp | license-service |link-management |local-
policy-decision-function |mac-validation |mib-process | mountd-service |mpls-traceroute |mspd |
multicast-snooping |named-service | nfsd-service | packet-triggered-subscribers |peer-selection-
service |pgm | pic-services-logging | pki-service |ppp | ppp-service | pppoe | protected-system-
domain-service | redundancy-interface-process | remote-operations | root-system-domain-service |
routing <logical-system logical-system-name>  | sampling | sbc-configuration-process | sdk-
service |service-deployment | services | snmp |soft |static-subscribers |statistics-service|
subscriber-management | subscriber-management-helper | tunnel-oamd |usb-control| vrrp |web-
management>
<gracefully | immediately | soft>
```

Syntax (ACX Series Routers)

```
restart
<adaptive-services |audit-process | auto-configuration | autoinstallation |chassis-control |
class-of-service |clksyncd-service |database-replication| dhcp-service | diameter-service | disk-
monitoring | dynamic-flow-capture | ethernet-connectivity-fault-management | ethernet-link-fault-
management |event-processing | firewall | general-authentication-service | gracefully |
immediately |interface-control | ipsec-key-management | l2-learning | lacp |link-management |mib-
```

```
process | mountd-service |mpls-traceroute |mspd | named-service | nfsd-service | pgm | pki-
service | ppp | pppoe | redundancy-interface-process | remote-operations | routing | sampling |
sdk-service |secure-neighbor-discovery | service-deployment | services | snmp |soft | statistics-
service| subscriber-management | subscriber-management-helper | tunnel-oamd | vrrp>
```

Syntax (EX Series Switches)

```
restart
<autoinstallation | chassis-control | class-of-service | database-replication | dhcp | dhcp-
service | diameter-service | dot1x-protocol | ethernet-link-fault-management | ethernet-
switching | event-processing | firewall | general-authentication-service | interface-control |
kernel-health-monitoring | kernel-replication | l2-learning | lacp | license-service | link-
management | lldpd-service | mib-process | mountd-service | multicast-snooping | pgm |
redundancy-interface-process | remote-operations | routing | secure-neighbor-discovery | service-
deployment | sflow-service | snmp | vrrp | web-management>
```

Syntax (MX Series Routers)

```
restart
<adaptive-services | ancpd-service | application-identification | audit-process | auto-
configuration | bbe-stats-service | captive-portal-content-delivery | ce-l2tp-service | chassis-
control | class-of-service | clksyncd-service | database-replication | datapath-trace-service |
dhcp-service | diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging |
ethernet-connectivity-fault-management | ethernet-link-fault-management | event-processing |
firewall | general-authentication-service | gracefully | iccp-service | idp-policy | immediately
|interface-control | ipsec-key-management |kernel-health-monitoring |  kernel-replication | l2-
learning | l2cpd-service | l2tp-service | l2tp-universal-edge | lacp | license-service | link-
management | local-policy-decision-function | mac-validation | mib-process | mountd-service |
mpls-traceroute | mspd | multicast-snooping |named-service | nfsd-service | packet-triggered-
subscribers |peer-selection-service | pgm | pic-services-logging | pki-service | ppp | ppp-
service | pppoe | protected-system-domain-service | redundancy-interface-process | remote-
operations | root-system-domain-service | routing | routing <logical-system logical-system-
name>  | sampling | sbc-configuration-process | sdk-service | service-deployment | services |
snmp |soft |static-subscribers |statistics-service| subscriber-management | subscriber-
management-helper | tunnel-oamd | usb-control | vrrp | web-management>
<all-members>
```

```
<gracefully | immediately | soft>
<local>
<member member-id>
```

Syntax (QFX Series)

```
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dialer-services |
diameter-service | dlsw | ethernet-connectivity | event-processing | fibre-channel | firewall |
general-authentication-service | igmp-host-services | interface-control | ipsec-key-management |
isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process | named-service | network-
access-service | nstrace-process | pgm | ppp | ppoe | redundancy-interface-process | remote-
operations |logical-system-name>  | routing | sampling |secure-neighbor-discovery | service-
deployment | snmp | usb-control | web-management>
<gracefully | immediately | soft>
```

Syntax (Routing Matrix)

```
restart
<adaptive-services | audit-process | chassis-control | class-of-service | disk-monitoring |
dynamic-flow-capture | ecc-error-logging | event-processing | firewall | interface-control |
ipsec-key-management | kernel-replication | l2-learning | l2tp-service | lacp | link-management
| mib-process | pgm | pic-services-logging | ppp | pppoe | redundancy-interface-process | remote-
operations | routing <logical-system logical-system-name>  | sampling | service-deployment |
snmp>
<all | all-lcc | lcc number>
<gracefully | immediately | soft>
```

Syntax (SRX Series)

```
restart
<application-identification |application-security |audit-process |commitd-service |chassis-
```

```
control | class-of-service |database-replication |datapath-trace-service |ddns |dhcp |dhcp-
service |dynamic-flow-capture |disk-monitoring |event-processing | ethernet-connectivity-fault-
management |ethernet-link-fault-management |extensible-subscriber-services |fipsd |firewall |
firewall-authentication-service |general-authentication-service |gracefully |gprs-process |idp-
policy |immediately |interface-control | ipmi |ipsec-key-management |jflow-service |jnu-
management |jnx-wmicd-service |jsrp-service |kernel-replication |l2-learning |l2cpd-service |
lacp |license-service |logical-system-service |mib-process |mountd-service |named-service |
network-security |network-security-trace |nfsd-service |ntpd-service |pgm |pic-services-logging |
profilerd |pki-service |remote-operations |rest-api |routing |sampling |sampling-route-record |
scc-chassisd |secure-neighbor-discovery |security-intelligence |security-log |services |service-
deployment |simple-mail-client-service |soft |snmp |static-routed |statistics-service |
subscriber-management |subscriber-management-helper |system-log-vital |tunnel-oamd |uac-service |
user-ad-authentication |vrrp |web-management >
```

Syntax (TX Matrix Routers)

```
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp-service |
diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | event-processing
| firewall | interface-control | ipsec-key-management | kernel-replication | l2-learning | l2tp-
service | lacp | link-management | mib-process |pgm | pic-services-logging | ppp | pppoe |
redundancy-interface-process | remote-operations | routing <logical-system logical-system-name>
| sampling | service-deployment | snmp| statistics-service>
<all-chassis | all-lcc | lcc number | scc>
<gracefully | immediately | soft>
```

Syntax (TX Matrix Plus Routers)

```
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dhcp-service |
diameter-service | disk-monitoring | dynamic-flow-capture | ecc-error-logging | event-processing
| firewall | interface-control | ipsec-key-management | kernel-replication | l2-learning | l2tp-
service | lacp | link-management | mib-process | pgm | pic-services-logging | ppp | pppoe |
redundancy-interface-process | remote-operations | routing <logical-system logical-system-name>
| sampling | service-deployment | snmp| statistics-service>
```

```
<all-chassis | all-lcc | all-sfc | lcc number | sfc number>
<gracefully | immediately | soft>
```

Syntax (QFX Series)

```
restart
<adaptive-services | audit-process | chassis-control | class-of-service | dialer-services |
diameter-service | dlsw | ethernet-connectivity | event-processing | fibre-channel | firewall |
general-authentication-service | igmp-host-services | interface-control | ipsec-key-management |
isdn-signaling | l2ald | l2-learning | l2tp-service | mib-process | named-service | network-
access-service | nstrace-process | pgm | ppp | pppoe | redundancy-interface-process | remote-
operations |logical-system-name>  | routing | sampling |secure-neighbor-discovery | service-
deployment | snmp | usb-control | web-management>
<gracefully | immediately | soft>
```

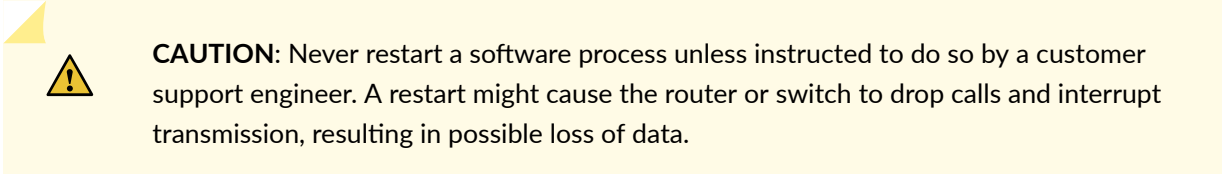
Syntax (Junos OS Evolved)

```
restart (BdL2Token | aft-sysinfo | agentd | alarmd | arpd | audit-process | bcmd_evo | bfdd |
bios-manager | charonctl | chassis-control | class-of-service | clksynced | cmevod | command-
handler | command-relay | configd | ddosd | dfwd-junos-relay | diskmgmt | distributor | dot1x-
protocol | dot1xd-agent | edo | emfca | ethernet-connectivity-fault-management | ethernet-link-
fault-management | event-processing | evo-aftmand-zx | evo-cda-zx | evo-cda-zx-diag | evo-jet-
sdk-broker | evoaft-jvisiond |  fabricHub | fabspoked-fchip | fabspoked-pfe | fabtokend | fibd |
fibd-proxy | firewall | fpa | fwstatsd | gcd | hwddual | hwdfpc | hwdspmb | icmpd | idmd-dest-
usage-class | idmd-src-usage-class | idmdbd | idmdcounter | idmdfabtoken | idmdfilter |
idmdfilterterm | idmdfwgretunnel | idmdifd | idmdifl | idmdnh | idmdoffchip32 | idmdoffchip64 |
idmdonchip | dmdpolicer | idmdrtb | idmdsensor |idmdsgid | idmdstp | ifstatsd | imgd | interface-
control | jdhcpd | jinsightd | jsd | jstatsd | kfirewall-agent | l2agent | l2ald | l2cpd | l2cpd-
agent | lacp | license-check | lldpd | mem-mgmt | mfilterd | mgd | mgd-api | mgd-pfe | mgmt-ethd
| mib-process | mplsoamd | mstr | mstrzk | msvcsd | mstrzk | msvcsd | mustd | na-grpcd | na-mqtt
| ndp | netdefaultsd | nlsd | objmon | objping-server | ofp | ofp-command | opticmand |
orchestratord | packetio-zx | pccd | pci-agent | pdevmand | pfestatsd | picd | ppman | ppmd |
ppmdagent | resild | routing | rpcserviced | rpdfw | securityd | sflowd | sinetd | smartd-agent-
monitor | snmp | snmpd-subagent | svcsd | syscmdd | sysepochman | sysman | sysman-ui | trace-
```

```
relay | trace-writer | xmlproxyd | ztp)
<gracefully | immediately | soft>
```

Description

Restart a Junos OS process.



CAUTION: Never restart a software process unless instructed to do so by a customer support engineer. A restart might cause the router or switch to drop calls and interrupt transmission, resulting in possible loss of data.

For Junos OS Evolved, the `restart` command also triggers a restart of the dependent applications (apps). In order to inform you which dependent apps are being restarted the following message will be logged when the `restart` command is used:

`App restarting <app name>. Related apps that may be impacted - <related-app name>` . For example: `Jan 14 11:42:08 RE0 sysman[5100]: SYSTEM_APP_RESTARTING_WITH_RELAPPS_EVENT: App restarting re0-ifmand. Related apps that may be impacted - aggd`

Starting in Junos OS Evolved Release 20.1R1, if you specify `restart` *app-name* and the application is not supposed to run on the platform, the error message is as follows:

```
user@device> restart fabspoked-pfe
Restart failed for fabspoked-pfe on node re0. Application is not running.
```

The `restart` command expands all applications names including applications that are not required for the current platform. Therefore, a user could try to do a restart for an application that is not running for the current platform. This error message communicates that the restart failed because the application was not running on the system.

Options

none Same as `gracefully`.

adaptive-services (Optional) Restart the configuration management process that manages the configuration for stateful firewall, Network Address Translation (NAT), intrusion

	detection services (IDS), and IP Security (IPsec) services on the Adaptive Services PIC.
all-chassis	(TX Matrix and TX Matrix Plus routers only) (Optional) Restart the software process on all chassis.
all-lcc	(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process on all T640 routers connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process on all T1600 routers connected to the TX Matrix Plus router.
all-members	(MX Series routers only) (Optional) Restart the software process for all members of the Virtual Chassis configuration.
all-sfc	(TX Matrix Plus routers only) (Optional) For a TX Matrix Plus router, restart the software processes for the TX Matrix Plus router (or switch-fabric chassis).
ancpd-service	(Optional) Restart the Access Node Control Protocol (ANCP) process, which works with a special Internet Group Management Protocol (IGMP) session to collect outgoing interface mapping events in a scalable manner.
application-identification	(Optional) Restart the process that identifies an application using intrusion detection and prevention (IDP) to allow or deny traffic based on applications running on standard or nonstandard ports.
application-security	(Optional) Restart the application security process.
audit-process	(Optional) Restart the RADIUS accounting process that gathers statistical data that can be used for general network monitoring, analyzing, and tracking usage patterns, for billing a user based on the amount of time or type of services accessed.
auto-configuration	(Optional) Restart the Interface Auto-Configuration process.
autoinstallation	(EX Series switches only) (Optional) Restart the autoinstallation process.
bbe-stats-service	(MX Series routers only) (Optional) Restart bbe-statsd, the BBE statistics collection and management process.
captive-portal-content-delivery	(Optional) Restart the HTTP redirect service by specifying the location to which a subscriber's initial Web browser session is redirected, enabling initial provisioning and service selection for the subscriber.

ce-l2tp-service	(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Universal Edge Layer 2 Tunneling Protocol (L2TP) process, which establishes L2TP tunnels and Point-to-Point Protocol (PPP) sessions through L2TP tunnels.
chassis-control	(Optional) Restart the chassis management process.
class-of-service	(Optional) Restart the class-of-service (CoS) process, which controls the router's or switch's CoS configuration.
clksyncd-service	(Optional) Restart the external clock synchronization process, which uses synchronous Ethernet (SyncE).
commitd-service	(Optional) Restart the committed services.
database-replication	(EX Series switches and MX Series routers only) (Optional) Restart the database replication process.
datapath-trace-service	(Optional) Restart the packet path tracing process.
dhcp	(EX Series switches only) (Optional) Restart the software process for a Dynamic Host Configuration Protocol (DHCP) server. A DHCP server allocates network IP addresses and delivers configuration settings to client hosts without user intervention.
dhcp-service	(Optional) Restart the Dynamic Host Configuration Protocol process.
dialer-services	(EX Series switches only) (Optional) Restart the ISDN dial-out process.
diameter-service	(Optional) Restart the diameter process.
disk-monitoring	(Optional) Restart disk monitoring, which checks the health of the hard disk drive on the Routing Engine.
dlsw	(QFX Series only) (Optional) Restart the data link switching (DLSw) service.
dot1x-protocol	(EX Series switches only) (Optional) Restart the port-based network access control process.
dynamic-flow-capture	(Optional) Restart the dynamic flow capture (DFC) process, which controls DFC configurations on Monitoring Services III PICs.
ecc-error-logging	(Optional) Restart the error checking and correction (ECC) process, which logs ECC parity errors in memory on the Routing Engine.

ethernet-connectivity-fault-management	(Optional) Restart the process that provides IEEE 802.1ag Operation, Administration, and Management (OAM) connectivity fault management (CFM) database information for CFM maintenance association end points (MEPs) in a CFM session.
ethernet-link-fault-management	(EX Series switches and MX Series routers only) (Optional) Restart the process that provides the OAM link fault management (LFM) information for Ethernet interfaces.
ethernet-switching	(EX Series switches only) (Optional) Restart the Ethernet switching process.
event-processing	(Optional) Restart the event process (eventd).
extensible-subscriber-services	(Optional) Restart the extensible subscriber services process.
fibre-channel	(QFX Series only) (Optional) Restart the Fibre Channel process.
fipsd	(Optional) Restart the fipsd services.
firewall	(Optional) Restart the firewall management process, which manages the firewall configuration and enables accepting or rejecting packets that are transiting an interface on a router or switch.
general-authentication-service	(EX Series switches and MX Series routers only) (Optional) Restart the general authentication process.
gprs-process	(Optional) Restart the General Packet Radio Service (GPRS) process.
gracefully	(Optional) Restart the software process.
iccp-service	(Optional) Restart the Inter-Chassis Communication Protocol (ICCP) process.
idp-policy	(Optional) Restart the intrusion detection and prevention (IDP) protocol process.
immediately	(Optional) Immediately restart the software process.
interface-control	(Optional) Restart the interface process, which controls the router's or switch's physical interface devices and logical interfaces.
ipmi	(Optional) Restart the intelligent platform management interface process.
ipsec-key-management	(Optional) Restart the IPsec key management process.
isdn-signaling	(QFX Series only) (Optional) Restart the ISDN signaling process, which initiates ISDN connections.

jflow-service	(Optional) Restart jflow service process.
jnu-management	(Optional) Restart jnu management process.
jnx-wmicd-service	(Optional) Restart jnx wmicd service process.
jsrp-service	(Optional) Restart the Juniper Services Redundancy Protocol (jsrdp) process, which controls chassis clustering.
kernel-health-monitoring	(Optional) Restart the Routing Engine kernel health monitoring process, which enables health parameter data to be sent from kernel components to data collection applications. When you change the polling interval through `sysctl kern.jkhmd_polling_time_secs`, you must restart the kernel health monitoring process for the new polling interval to take effect.
kernel-replication	(Optional) Restart the kernel replication process, which replicates the state of the backup Routing Engine when graceful Routing Engine switchover (GRES) is configured.
l2-learning	(Optional) Restart the Layer 2 address flooding and learning process.
l2cpd-service	(Optional) Restart the Layer 2 Control Protocol process, which enables features such as Layer 2 protocol tunneling and nonstop bridging.
l2tp-service	(M10, M10i, M7i, and MX Series routers only) (Optional) Restart the Layer 2 Tunneling Protocol (L2TP) process, which sets up client services for establishing Point-to-Point Protocol (PPP) tunnels across a network and negotiating Multilink PPP if it is implemented.
l2tp-universal-edge	(MX Series routers only) (Optional) Restart the L2TP process, which establishes L2TP tunnels and PPP sessions through L2TP tunnels.
lacp	(Optional) Restart the Link Aggregation Control Protocol (LACP) process. LACP provides a standardized means for exchanging information between partner systems on a link to allow their link aggregation control instances to reach agreement on the identity of the LAG to which the link belongs, and then to move the link to that LAG, and to enable the transmission and reception processes for the link to function in an orderly manner.
lcc *number*	(TX Matrix and TX Matrix Plus routers only) (Optional) For a TX Matrix router, restart the software process for a specific T640 router that is connected to the TX Matrix router. For a TX Matrix Plus router, restart the software process for a specific router that is connected to the TX Matrix Plus router. Replace *number* with the following values depending on the LCC configuration:

- 0 through 3, when T640 routers are connected to a TX Matrix router in a routing matrix.
- 0 through 3, when T1600 routers are connected to a TX Matrix Plus router in a routing matrix.
- 0 through 7, when T1600 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.
- 0, 2, 4, or 6, when T4000 routers are connected to a TX Matrix Plus router with 3D SIBs in a routing matrix.

license-service (EX Series switches only) (Optional) Restart the feature license management process.

link-management (TX Matrix and TX Matrix Plus routers and EX Series switches only) (Optional) Restart the Link Management Protocol (LMP) process, which establishes and maintains LMP control channels.

lldpd-service (EX Series switches only) (Optional) Restart the Link Layer Discovery Protocol (LLDP) process.

local (MX Series routers only) (Optional) Restart the software process for the local Virtual Chassis member.

local-policy-decision-function (Optional) Restart the process for the Local Policy Decision Function, which regulates collection of statistics related to applications and application groups and tracking of information about dynamic subscribers and static interfaces.

logical-system-service (Optional) Restart the logical system service process.

mac-validation (Optional) Restart the Media Access Control (MAC) validation process, which configures MAC address validation for subscriber interfaces created on demux interfaces in dynamic profiles on MX Series routers.

member *member-id* (MX Series routers only) (Optional) Restart the software process for a specific member of the Virtual Chassis configuration. Replace *member-id* with a value of `0` or `1`.

mib-process (Optional) Restart the Management Information Base (MIB) version II process, which provides the router's MIB II agent.

mobile-ip (Optional) Restart the Mobile IP process, which configures Junos OS Mobile IP features.

mountd-service	(EX Series switches and MX Series routers only) (Optional) Restart the service for NFS mount requests.
mpls-traceroute	(Optional) Restart the MPLS Periodic Traceroute process.
mspd	(Optional) Restart the Multiservice process.
multicast-snooping	(EX Series switches and MX Series routers only) (Optional) Restart the multicast snooping process, which makes Layer 2 devices, such as VLAN switches, aware of Layer 3 information, such as the media access control (MAC) addresses of members of a multicast group.
named-service	(Optional) Restart the DNS Server process, which is used by a router or a switch to resolve hostnames into addresses.
network-access-service	(QFX Series only) (Optional) Restart the network access process, which provides the router's Challenge Handshake Authentication Protocol (CHAP) authentication service.
network-security	(Optional) Restart the network security process.
network-security-trace	(Optional) Restart the network security trace process.
nfsd-service	(Optional) Restart the Remote NFS Server process, which provides remote file access for applications that need NFS-based transport.
ntpd-service	(Optional) Restart the Network Time Protocol (NTP) process.
packet-triggered-subscribers	(Optional) Restart the packet-triggered subscribers and policy control (PTSP) process, which allows the application of policies to dynamic subscribers that are controlled by a subscriber termination device.
peer-selection-service	(Optional) Restart the Peer Selection Service process.
pgcp-service	(Optional) Restart the pgcpd service process running on the Routing Engine. This option does not restart pgcpd processes running on mobile station PICs. To restart pgcpd processes running on mobile station PICs, use the `services pgcp gateway` option.
pgm	(Optional) Restart the process that implements the Pragmatic General Multicast (PGM) protocol for assisting in the reliable delivery of multicast packets.

pic-services-logging	(Optional) Restart the logging process for some PICs. With this process, also known as fsad (the file system access daemon), PICs send special logging information to the Routing Engine for archiving on the hard disk.
pki-service	(Optional) Restart the PKI Service process.
ppp	(Optional) Restart the Point-to-Point Protocol (PPP) process, which is the encapsulation protocol process for transporting IP traffic across point-to-point links.
ppp-service	(Optional) Restart the Universal edge PPP process, which is the encapsulation protocol process for transporting IP traffic across universal edge routers.
pppoe	(Optional) Restart the Point-to-Point Protocol over Ethernet (PPPoE) process, which combines PPP that typically runs over broadband connections with the Ethernet link-layer protocol that allows users to connect to a network of hosts over a bridge or access concentrator.
profilerd	(Optional) Restart the profiler process.
protected-system-domain-service	(Optional) Restart the Protected System Domain (PSD) process.
redundancy-interface-process	(Optional) Restart the ASP redundancy process.
remote-operations	(Optional) Restart the remote operations process, which provides the ping and traceroute MIBs.
rest-api	(Optional) Restart the rest api process.
root-system-domain-service	(Optional) Restart the Root System Domain (RSD) service.
routing	(ACX Series routers, QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the routing protocol process.
routing <logical-system *logical-system-name*>	(Optional) Restart the routing protocol process, which controls the routing protocols that run on the router or switch and maintains the routing tables. Optionally, restart the routing protocol process for the specified logical system only.
sampling	(Optional) Restart the sampling process, which performs packet sampling based on particular input interfaces and various fields in the packet header.
sampling-route-record	(Optional) Restart the sampling route record process.

sbc-configuration-process	(Optional) Restart the session border controller (SBC) process of the border signaling gateway (BSG).
scc	(TX Matrix routers only) (Optional) Restart the software process on the TX Matrix router (or switch-card chassis).
scc-chassisd	(Optional) Restart the scc chassisd process.
sdk-service	(Optional) Restart the SDK Service process, which runs on the Routing Engine and is responsible for communications between the SDK application and Junos OS. Although the SDK Service process is present on the router, it is turned off by default.
secure-neighbor-discovery	(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the secure Neighbor Discovery Protocol (NDP) process, which provides support for protecting NDP messages.
security-intelligence	(Optional) Restart security intelligence process.
security-log	(Optional) Restart the security log process.
sfc *number*	(TX Matrix Plus routers only) (Optional) Restart the software process on the TX Matrix Plus router (or switch-fabric chassis). Replace *number* with `0`.
service-deployment	(Optional) Restart the service deployment process, which enables Junos OS to work with the Session and Resource Control (SRC) software.
services	(Optional) Restart a service.
services pgcp gateway *gateway-name*	(Optional) Restart the pgcpd process for a specific border gateway function (BGF) running on an MS-PIC. This option does not restart the pgcpd process running on the Routing Engine. To restart the pgcpd process on the Routing Engine, use the `pgcp-service` option.
sflow-service	(EX Series switches only) (Optional) Restart the flow sampling (sFlow technology) process.
simple-mail-client-service	(Optional) Restart the simple mail client service process.
snmp	(Optional) Restart the SNMP process, which enables the monitoring of network devices from a central location and provides the router's or switch's SNMP master agent.

soft	(Optional) Reread and reactivate the configuration without completely restarting the software processes. For example, BGP peers stay up and the routing table stays constant. Omitting this option results in a graceful restart of the software process.
static-routed	(Optional) Restart the static routed process.
static-subscribers	(Optional) Restart the static subscribers process, which associates subscribers with statically configured interfaces and provides dynamic service activation and activation for these subscribers.
statistics-service	(Optional) Restart the process that manages the Packet Forwarding Engine statistics.
subscriber-management	(Optional) Restart the Subscriber Management process.
subscriber-management-helper	(Optional) Restart the Subscriber Management Helper process.
system-log-vital	(Optional) Restart system log vital process.
tunnel-oamd	(Optional) Restart the Tunnel OAM process, which enables the Operations, Administration, and Maintenance of Layer 2 tunneled networks. Layer 2 protocol tunneling (L2PT) allows service providers to send Layer 2 protocol data units (PDUs) across the provider's cloud and deliver them to Juniper Networks EX Series Ethernet Switches that are not part of the local broadcast domain.
uac-service	(Optional) Restart the Unified Access Control (UAC) process.
usb-control	(MX Series routers) (Optional) Restart the USB control process.
user-ad-authentication	(Optional) Restart User ad Authentication process
vrrp	(ACX Series routers, EX Series switches, and MX Series routers only) (Optional) Restart the Virtual Router Redundancy Protocol (VRRP) process, which enables hosts on a LAN to make use of redundant routing platforms on that LAN without requiring more than the static configuration of a single default route on the hosts.
web-management	(QFX Series, EX Series switches, and MX Series routers only) (Optional) Restart the Web management process.

Required Privilege Level

reset

Output Fields

When you enter this command, you are provided feedback on the status of your request.

Sample Output

restart interfaces

```
user@host> restart interfaces
interfaces process terminated
interfaces process restarted
```

restart interface-control gracefully

```
user@host> restart interface-control gracefully
Interface control process started, pid 41129
```

restart interface-control (Junos OS Evolved)

```
user@host> restart interface-control
interface-control restart requested
Restarted aggd on re0
Restarted ifmand on re0
```

Release Information

Command introduced before Junos OS Release 7.4.

Options added:

- `dynamic-flow-capture` in Junos OS Release 7.4.
- `dlsw` in Junos OS Release 7.5.
- `event-processing` in Junos OS Release 7.5.
- `ppp` in Junos OS Release 7.5.
- `l2ald` in Junos OS Release 8.0.
- `link-management` in Junos Release 8.0.
- `pgcp-service` in Junos OS Release 8.4.
- `sbc-configuration-process` in Junos OS Release 9.5.
- `services pgcp gateway` in Junos OS Release 9.6.
- `sfc` and `all-sfc` for the TX Matrix Router in Junos OS Release 9.6.
- Command introduced before Junos OS Release 9.2 on SRX Series devices.
- `bbe-stats-service` in Junos OS Release 18.4R1 on MX Series routers.
- `kernel-health-monitoring` in Junos OS Release 19.1R1.
- Introduced in Junos OS Evolved Release 19.1R1.

RELATED DOCUMENTATION

Overview of Operational Mode Commands

show captive-portal firewall

IN THIS SECTION

- Syntax | **943**
- Description | **943**

- Options | 943
- Required Privilege Level | 944
- Output Fields | 944
- Sample Output | 944
- Release Information | 945

Syntax

```
show captive-portal firewall
<brief | detail>
<interface-name>
<interface-name detail>
```

Description

Display information about the firewall filters for each user that is authenticated on each captive portal interface.

Options

none	Display all the firewall filters on all captive portal interfaces.
brief | detail	(Optional) Display the specified level of output.
interface-name	(Optional) Display all the terms of the firewall filters for the specified interface.
***interface-name* detail**	(Optional) Display all of the terms of the firewall filters for the specified interface.

Required Privilege Level

view

Output Fields

Output fields for the `show captive-portal firewall` command include any action modifier specified in firewall filters except policers. Policers are not supported in the terms of the internally generated dynamic firewall filters that are created when multiple supplicants authenticate on 802.1X-enabled interfaces.

Sample Output

show captive-portal firewall brief

```
user@switch> show captive-portal firewall brief
Captive Portal Information:
Interface      State           MAC address          User
ge-0/0/1.0     Connecting
ge-0/0/10.0    Connecting      00:30:48:8c:66:bd    No User
```

show captive-portal firewall (Specific Interface)

```
user@switch> show captive-portal firewall ge-0/0/10.0
Filter name: dot1x_ge-0/0/10
Counters:
Name                            Bytes              Packets
dot1x_ge-0/0/10_CP_arp           7616                  119
dot1x_ge-0/0/10_CP_dhcp             0                    0
dot1x_ge-0/0/10_CP_http             0                    0
dot1x_ge-0/0/10_CP_https            0                    0
dot1x_ge-0/0/10_CP_t_dns            0                    0
dot1x_ge-0/0/10_CP_u_dns            0                    0
```

show captive-portal firewall

```
user@switch> show captive-portal firewall
Filter name: dot1x_ge-0/0/0
Counters:
Name                                Bytes              Packets
dot1x_ge-0/0/0_CP_arp                   0                    0
dot1x_ge-0/0/0_CP_dhcp                  0                    0
dot1x_ge-0/0/0_CP_http                  0                    0
dot1x_ge-0/0/0_CP_https                 0                    0
dot1x_ge-0/0/0_CP_t_dns                 0                    0
dot1x_ge-0/0/0_CP_u_dns                 0                    0
Filter name: dot1x_ge-0/0/1
Counters:
Name                                Bytes              Packets
dot1x_ge-0/0/1_CP_arp                   0                    0
dot1x_ge-0/0/1_CP_dhcp                  0                    0
dot1x_ge-0/0/1_CP_http                  0                    0
dot1x_ge-0/0/1_CP_https                 0                    0
dot1x_ge-0/0/1_CP_t_dns                 0                    0
dot1x_ge-0/0/1_CP_u_dns                 0                    0
Filter name: dot1x_ge-0/0/10
Counters:
Name                                Bytes              Packets
dot1x_ge-0/0/10_CP_arp               7616                  119
dot1x_ge-0/0/10_CP_dhcp                 0                    0
dot1x_ge-0/0/10_CP_http                 0                    0
dot1x_ge-0/0/10_CP_https                0                    0
dot1x_ge-0/0/10_CP_t_dns                0                    0
dot1x_ge-0/0/10_CP_u_dns                0                    0
Filter name: dot1x_ge-0/0/11
```

Release Information

Command introduced in Junos OS Release 10.1.

RELATED DOCUMENTATION

- show captive-portal authentication-failed-users
- show captive-portal interface
- clear captive-portal
- Example: Setting Up Captive Portal Authentication on an EX Series Switch
- Configuring Captive Portal Authentication (CLI Procedure)

show dhcp client binding

IN THIS SECTION

- Syntax | 946
- Description | 947
- Options | 947
- Required Privilege Level | 947
- Output Fields | 948
- Sample Output | 949
- Release Information | 950

Syntax

```
show dhcp client binding
[<address> |interface <interface-name>]
 routing-instance <routing-instance name>
[brief | detail | summary ]
logical-system
tenant
```

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.
routing-instance <routing-instance name>	(Optional) Display DHCP binding information for DHCP clients on the specified routing instance.
interface <interface-name>	(Optional) Perform this operation on the specified interface.
brief	(Optional) Display brief information about the active client bindings.
detail	(Optional) Display detailed client binding information.
summary	(Optional) Display a summary of DHCP client information.
logical-system	(Optional) Displays the DHCP binding information for DHCP clients on the specified logical system.
tenant	(Optional) Displays the DHCP binding information for DHCP clients on the specified tenant system.

Required Privilege Level

view

Output Fields

Table 21 on page 948 lists the output fields for the `show dhcp client binding` command. Output fields are listed in the approximate order in which they appear.

Table 21: show dhcp client binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Server	IP address of the DHCP server.
Expires	Number of seconds in which the lease expires.
State	State of the address binding table on the DHCP local server.
Interface	Interface on which the request was received.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds in which the lease expires.
Lease Start	Date and time at which the client's IP address lease started.
Vendor Identifier	Vendor identifier.
Server Identifier	IP address of the DHCP server.
Client IP Address	IP address of the DHCP client.

Sample Output

show dhcp client binding

```
user@host> show dhcp client binding
2 clients, (2 bound,  0 init, 0 discover, 0 renew, 0 rebind)

            IP address      Hardware address     Server      Expires     State      Interface
            10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND      fe-0/0/1.0
            20.1.1.90       00:0a:12:00:12:34    20.1.1.1    568         BOUND      fe-0/0/2.0
```

command-name

```
user@host> show dhcp client binding interface fe-0/0/1.0 detail
Client Interface: fe-0/0/1.0
               Hardware address:       00:0a:12:00:12:12
               State:                  BOUND
               Lease Expires:          2010-09-16 14:45:41 UTC
               Lease Expires in:       528 seconds
               Lease Start:            2010-09-16 14:35:41 UTC
               Vendor Identifier:      ether
               Server Identifier:      10.1.1.1
               Client IP Address:      10.1.1.89
               update server           enabled

           DHCP Options :
               Name: name-server, Value: [ 10.209.194.131, 198.51.110.2, 192.0.2.3 ]
               Name: server-identifier, Value: 10.1.1.1
               Name: router, Value: [ 10.1.1.80 ]
               Name: domain-name, Value: example-50
```

command-name

```
user@host> show dhcp client binding 10.1.1.89
IP address      Hardware address     Server      Expires     State      Interface
         10.1.1.89       00:0a:12:00:12:12    10.1.1.1    348         BOUND      fe-0/0/1.0
```

command-name

```
user@host> show dhcp client binding tenant TSYS1 routing-instance R1
IP address        Hardware address   Expires     State      Interface
       33.33.33.3        00:50:56:b0:b8:21  1628        BOUND      ge-0/0/3.0
```

command-name

```
user@host> show dhcp client binding detail tenant TSYS1 routing-instance R1
Client Interface/Id: ge-0/0/3.0
     Hardware Address:             00:50:56:b0:b8:21
     State:                        BOUND(LOCAL_CLIENT_STATE_BOUND)
     Lease Expires:                2018-04-26 16:24:34 UTC
     Lease Expires in:             1626 seconds
     Lease Start:                  2018-04-26 15:51:14 UTC
     Server Identifier:            11.11.11.1
     Client IP Address:            33.33.33.3
     Update Server                 No

    DHCP options:
    Name: dhcp-lease-time, Value: 33 minutes, 20 seconds
    Name: server-identifier, Value: 11.11.11.1
    Name: router, Value: [ 33.33.33.1 ]
    Name: subnet-mask, Value: 255.255.255.0
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

The `logical-system` and `tenant` options are introduced in Junos OS Release 18.4R1.

RELATED DOCUMENTATION

clear dhcp client binding | 879

show dhcp client statistics

IN THIS SECTION

- Syntax | 951
- Description | 951
- Options | 951
- Required Privilege Level | 952
- Output Fields | 952
- Sample Output | 954
- Release Information | 955

Syntax

```
show dhcp client statistics
<routing-instance routing-instance-name >
logical-system
tenant
```

Description

Displays the DHCP client statistics.

Options

routing-instance routing-instance-name	(Optional) Display the statistics for DHCP clients on the specified routing instance.

logical-system	(Optional) Displays the DHCP statistics information for DHCP clients on the specified logical system.
tenant	(Optional) Displays the DHCP statistics information for DHCP clients on the specified tenant system.

Required Privilege Level

view

Output Fields

Table 22 on page 952 lists the output fields for the `show dhcp client statistics` command. Output fields are listed in the approximate order in which they appear.

Table 22: show dhcp client statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the 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.

Table 22: show dhcp client statistics *(Continued)*

Field Name	Field Description
Messages received	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP protocol data units (PDUs) received • DHCPOFFER—Number of DHCP PDUs of type OFFER received • DHCPACK—Number of DHCP PDUs of type ACK received • DHCPNACK—Number of DHCP PDUs of type NACK received • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW received

Table 22: show dhcp client statistics *(Continued)*

Field Name	Field Description
Messages sent	Number of DHCP messages sent. • BOOTREQUEST—Number of BOOTP protocol data units (PDUs) transmitted • DHCPDECLINE—Number of DHCP PDUs of type DECLINE transmitted • DHCPDISCOVER—Number of DHCP PDUs of type DISCOVER transmitted • DHCPREQUEST—Number of DHCP PDUs of type REQUEST transmitted • DHCPINFORM—Number of DHCP PDUs of type INFORM transmitted • DHCPRELEASE—Number of DHCP PDUs of type RELEASE transmitted • DHCPRENEW—Number of DHCP PDUs of type RENEW transmitted • DHCPREBIND—Number of DHCP PDUs of type REBIND transmitted

Sample Output

show dhcp client statistics

```
user@host> show dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    BOOTREPLY                 0
    DHCPOFFER                 0
    DHCPACK                   0
```

```
    DHCPNAK                    0
    DHCPFORCERENEW             0
Messages sent:
    BOOTREQUEST                0
    DHCPDECLINE                0
    DHCPDISCOVER               0
    DHCPREQUEST                0
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPRENEW                  0
    DHCPREBIND                 0
```

show dhcp client statistics tenant TSYS1 routing-instance R1

```
user@host> show dhcp client statistics tenant TSYS1 routing-instance R1
Packets dropped:
    Total                      0

   Messages received:
    BOOTREPLY                  14
    DHCPOFFER                  4
    DHCPACK                    10
    DHCPNAK                    0
    DHCPFORCERENEW             0

  Messages sent:
    BOOTREQUEST                17
    DHCPDECLINE                0
    DHCPDISCOVER               4
    DHCPREQUEST                10
    DHCPINFORM                 0
    DHCPRELEASE                3
    DHCPRENEW                  6
    DHCPREBIND                 0
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

The `logical-system` and `tenant` option is introduced in Junos OS Release 18.4R1.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

clear dhcp client statistics | 881

show dhcp relay binding

IN THIS SECTION

- Syntax | 956
- Description | 957
- Options | 957
- Required Privilege Level | 957
- Output Fields | 957
- Sample Output | 958
- Release Information | 959

Syntax

```
Show dhcp relay binding
[<address> |interface <interface-name>]
routing-instance <routing-instance name>
[brief | detail | summary]
```

Description

Display the address bindings in the Dynamic Host Configuration Protocol (DHCP) relay 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.
routing-instance <routing-instance name>	(Optional) Display DHCP binding information on the specified routing instance.
interface <interface-name>	(Optional) Perform this operation on the specified interface.
brief	(Optional) Display brief information about the active client bindings.
detail	(Optional) Display detailed client binding information.
summary	(Optional) Display a summary of DHCP client information.

Required Privilege Level

view

Output Fields

Table 23 on page 958 lists the output fields for the `show dhcp relay binding` command. Output fields are listed in the approximate order in which they appear.

Table 23: show dhcp relay binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp relay binding

```
user@host> show dhcp relay binding detail
IP address       Hardware address   Type     Lease expires            State
       100.20.32.1      90:00:00:01:00:01  active   2007-01-17 11:38:47 PST  rebind
       100.20.32.3      90:00:00:02:00:01  active   2007-01-17 11:38:41 PST  rebind
       100.20.32.4      90:00:00:03:00:01  active   2007-01-17 11:38:01 PST  rebind
       100.20.32.5      90:00:00:04:00:01  active   2007-01-17 11:38:07 PST  rebind
       100.20.32.6      90:00:00:05:00:01  active   2007-01-17 11:38:47 PST  rebind
```

command-name

```
user@host> show dhcp relay binding 100.20.32.1
Active binding information:
           IP address               100.20.32.1
           Hardware address         90:00:00:01:00:01

       Lease information:
          Type                DHCP
          Obtained at         2007-01-17 11:28:47 PST
          Expires at          2007-01-17 11:38:47 PST

       > show dhcp relay binding 100.20.32.1 detail
       Active binding information:
           IP address              100.20.32.1
           Hardware address        90:00:00:01:00:01
           Request received on     fe-0/0/2.0, relayed by 100.20.32.2

       Lease information:
           Type                DHCP
           Obtained at         2007-01-17 11:28:47 PST
           Expires at          2007-01-17 11:38:47 PST
           State               rebind
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

clear dhcp relay binding | 883

show dhcp relay statistics

IN THIS SECTION

- Syntax | 960
- Description | 960
- Options | 960
- Required Privilege Level | 961
- Output Fields | 961
- Sample Output | 962
- Release Information | 962

Syntax

```
show dhcp relay statistics
[<routing-instance>]
```

Description

Display Dynamic Host Configuration Protocol (DHCP) relay statistics.

Options

routing-instance (Optional) Display the DHCP relay statistics on the specified routing instance.

Required Privilege Level

view

Output Fields

Table 24 on page 961 lists the output fields for the `show dhcp relay statistics` command. Output fields are listed in the approximate order in which they appear.

Table 24: show dhcp relay statistics

Field Name	Field Description
Messages received	Number of DHCP messages sent. • 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 • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received
Messages sent	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show dhcp relay statistics

```
user@host> show dhcp relay statistics
Messages received:
    BOOTREQUEST                0
    DHCPDECLINE                0
    DHCPDISCOVER               0
    DHCPINFORM                 0
    DHCPRELEASE                0
    DHCPREQUEST                0

Messages sent:
    BOOTREPLY                  0
    DHCPOFFER                  0
    DHCPACK                    0
    DHCPNAK                    0
    DHCPFORCERENEW             0
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

clear dhcp relay statistics | 885

show dhcp server binding

IN THIS SECTION

- Syntax | 963
- Description | 963
- Options | 963
- Required Privilege Level | 964
- Output Fields | 964
- Sample Output | 965
- Release Information | 965

Syntax

```
show dhcp server binding
[interface <interface name>]
<brief | detail | summary | verbose>
<ip-address | MAC address>
<routing-instance routing-instance-name>
```

Description

Display the address bindings in the client table on the Dynamic Host Configuration Protocol (DHCP) local server.

Options

interface <interface name>	(Optional) Display information about active client bindings on the specified interface.

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`.
ip-address	Display DHCP binding information for a specific client identified by the specified IP address.
MAC address	Display DHCP binding information for a specific client identified by the specified MAC address.
routing-instance routing-instance-name	(Optional) Display information about active client bindings for DHCP clients on the specified routing instance.

Required Privilege Level

view

Output Fields

Table 25 on page 964 lists the output fields for the show dhcp server binding command. Output fields are listed in the approximate order in which they appear.

Table 25: show dhcp server binding Output Fields

Field Name	Field Description
IP address	IP address of the DHCP client.
Hardware address	Hardware address of the DHCP client.
Request received on	Interface on which the request was received.
Type	Type of DHCP packet processing performed on the device.

Table 25: show dhcp server binding Output Fields *(Continued)*

Field Name	Field Description
Obtained at	Date and time at which the client's IP address lease started.
Expires at	Date and time at which the client's IP address lease expires.
State	State of the address binding table on the DHCP local server.

Sample Output

show dhcp server binding

```
user@host> show dhcp server binding 100.20.32.1 detail
Active binding information:
               IP address             100.20.32.1
               Hardware address       90:00:00:01:00:01
               Request received on    fe-0/0/2.0, relayed by 100.20.32.2

           Lease information:
               Type                   DHCP
               Obtained at            2007-01-17 11:28:47 PST
               Expires at             2007-01-17 11:38:47 PST
               State                  rebind
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

clear dhcp server binding | 886

show dhcp server statistics

IN THIS SECTION

- Syntax | 966
- Description | 966
- Options | 966
- Required Privilege Level | 967
- Output Fields | 967
- Sample Output | 968
- Release Information | 969

Syntax

```
show dhcp server statistics
<routing-instance>
```

Description

Display Dynamic Host Configuration Protocol (DHCP) local server statistics.

Options

routing-instance (Optional) Display information about 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

Output Fields

Table 26 on page 967 lists the output fields for the `show dhcp server statistics` command. Output fields are listed in the approximate order in which they appear.

Table 26: show dhcp server statistics

Field Name	Field Description
Packets dropped	Number of packets discarded by the 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.
Messages received	Number of DHCP messages sent. • 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 • DHCPREQUEST—Number of DHCP PDUs of type REQUEST received • DHCPINFORM—Number of DHCP PDUs of type INFORM received • DHCPRELEASE—Number of DHCP PDUs of type RELEASE received

Table 26: show dhcp server statistics *(Continued)*

Field Name	Field Description
Messages sent	Number of DHCP messages received. • BOOTREPLY—Number of BOOTP PDUs transmitted • DHCPOFFER—Number of DHCP PDUs of type OFFER transmitted • DHCPACK—Number of DHCP PDUs of type ACK transmitted • DHCPNACK—Number of DHCP PDUs of type NACK transmitted • DHCPFORCERENEW—Number of DHCP PDUs of type FORCERENEW transmitted

Sample Output

show 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
    DHCPFORCERENEW            0
```

Release Information

Statement introduced in Junos OS Release 12.1X44-D10.

RELATED DOCUMENTATION

clear dhcp server statistics | 888

show dhcpv6 client binding

IN THIS SECTION

- Syntax | 969
- Description | 970
- Options | 970
- Required Privilege Level | 970
- Output Fields | 970
- Sample Output | 971
- Release Information | 972

Syntax

```
show dhcpv6 client binding
interface interface-name
routing-instance <routing-instance-name>
[brief | detail | summary]
```

Description

Display the address bindings in the Dynamic Host Configuration Protocol version 6 (DHCPv6) client table.

Options

interface *interface-name*	(Optional) Perform this operation on the specified interface.
routing-instance *routing-instance-name*	(Optional) Display DHCPv6 binding information for DHCPv6 clients on the specified routing instance.
brief	(Optional) Display brief information about the active client bindings.
detail	(Optional) Display detailed client binding information.
summary	(Optional) Display a summary of DHCPv6 client information.

Required Privilege Level

view

Output Fields

Table 27 on page 970 lists the output fields for the `show dhcpv6 client binding` command. Output fields are listed in the approximate order in which they appear.

Table 27: show dhcpv6 client binding Output Fields

Field Name	Field Description
Hardware Address	Hardware address of the DHCPv6 client.

Table 27: show dhcpv6 client binding Output Fields *(Continued)*

Field Name	Field Description
State	State of the address-binding table on the DHCPv6 local server.
Lease Expires	Date and time at which the client's IP address lease expires.
Lease Expires in	Number of seconds until the lease expires.
Lease Start	Date and time at which the client's IP address lease started.
Client DUID	The DHCPv6 client's unique identifier.
Bind type	The bind type.
Client Type	The type of DHCPv6 client. The client type can be autoconfig or stateful.
Rapid Commit	Two-message exchange option for address assignment.
Server IP Address	IP address of the DHCPv6 server.
Client IP Address	IP address of the DHCPv6 client.

Sample Output

show dhcpv6 client binding

```
user@host> show dhcpv6 client binding
IP prefix                Expires        ClientType     State  Interface       Client DUID
    2001:db8::b2b7:8631:d968:8d5e/128    96              STATEFUL      BOUND ge-0/0/1.0
LL_TIME0x3-0x0-2c:6b:f5:62:39:c1
```

command-name

```
user@host> show dhcpv6 client binding detail
Client Interface: ge-0/0/1.0
             Hardware Address:             2c:6b:f5:62:39:c1
             State:                        BOUND(DHCPV6_CLIENT_STATE_BOUND)
             Lease Expires:                2012-08-07 15:52:19 UTC
             Lease Expires in:             116 seconds
                Lease Start:                  2012-08-07 15:50:19 UTC
             Client DUID                   VENDOR0x00000583-0x3000103f
                Bind Type:                       IA_NA
                ClientType :                    STATEFUL
             Rapid Commit                  Off
             Server Ip Address:            fe80::230:48ff:fe5d:5bf7
             Client IP Address:            2001:db8::655b:3c80:2deb:1a3/128

        DHCP options:
            Name: server-identifier, Value: LL_TIME0x1-0x17acddab-00:30:48:5d:5b:f7
            Name: vendor-opts, Value: 000005830002aaaa
            Name: sip-server-list, Value: 2000::300 2000::302 2000::303 2000::304
            Name: dns-recursive-server, Value: 2000::ff2000::fe
            Name: domain-search-list, Value: 076578616d706c6503636f6d00
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

RELATED DOCUMENTATION

clear dhcpv6 client binding | 890

show dhcpv6 client statistics

IN THIS SECTION

- Syntax | 973
- Description | 973
- Options | 973
- Required Privilege Level | 974
- Output Fields | 974
- Sample Output | 976
- Release Information | 976

Syntax

```
show dhcpv6 client statistics
routing-instance<routing-instance-name>
```

Description

Display Dynamic Host Configuration Protocol (DHCPv6) client statistics.

Options

routing-instance <routing-instance-name>	(Optional) Display the statistics for DHCPv6 clients on the specified routing instance.

Required Privilege Level

view

Output Fields

Table 28 on page 974 lists the output fields for the `show dhcpv6 client statistics` command. Output fields are listed in the approximate order in which they appear.

Table 28: show dhcpv6 client statistics Output Fields

Field Name	Field Description
Dhcpv6 Packets dropped	Number of packets discarded by the DHCPv6 local server because of errors. Only nonzero statistics appear in the DHCPv6 Packets dropped output. When all of the Packets dropped statistics are 0 (zero), only the Total field appears.

Table 28: show dhcpv6 client statistics Output Fields *(Continued)*

Field Name	Field Description
Messages sent	Number of DHCPv6 messages sent. • DHCPV6_DECLINE—Number of DHCPv6 PDUs of type DECLINE transmitted • DHCPV6_SOLICIT—Number of DHCPv6 PDUs of type SOLICIT transmitted • DHCPV6_INFORMATION_REQUEST—Number of DHCPv6 PDUs of type INFORMATION REQUEST transmitted • DHCPV6_RELEASE—Number of DHCPv6 PDUs of type RELEASE transmitted • DHCPV6_REQUEST—Number of DHCPv6 PDUs of type REQUEST transmitted • DHCPV6_CONFIRM—Number of DHCPv6 PDUs of type CONFIRM transmitted • DHCPV6_RENEW—Number of DHCPv6 PDUs of type RENEW transmitted • DHCPV6_REBIND—Number of DHCPv6 PDUs of type REBIND transmitted
Messages received	Number of DHCPv6 messages received. • DHCPV6_ADVERTISE—Number of DHCPv6 PDUs of type ADVERTISE received • DHCPV6_REPLY—Number of DHCPv6 PDUs of type REPLY received • DHCPV6_RECONFIGURE—Number of DHCPv6 PDUs of type RECONFIGURE received

Sample Output

show dhcpv6 client statistics

```
user@host> show dhcpv6 client statistics
Dhcpv6 Packets dropped:
            Total               0

            Messages sent:
            DHCPV6_DECLINE             0
            DHCPV6_SOLICIT             3
            DHCPV6_INFORMATION_REQUEST 6
            DHCPV6_RELEASE             1
            DHCPV6_REQUEST             2
            DHCPV6_CONFIRM             0
            DHCPV6_RENEW               0
            DHCPV6_REBIND              0

            Messages received:
            DHCPV6_ADVERTISE           3
            DHCPV6_REPLY               3
            DHCPV6_RECONFIGURE         0
```

Release Information

Statement introduced in Junos OS Release 12.1X45-D10.

NOTE: This command is not supported in Junos OS Evolved because it is not needed. Stateless DHCPv4 and DHCPv6 relay are supported and enabled by default, so Junos OS Evolved does not maintain states or records of statistics or bindings for DHCP clients.

RELATED DOCUMENTATION

clear dhcpv6 client statistics | 892

show dhcpv6 relay binding

IN THIS SECTION

- Syntax | 977
- Description | 977
- Options | 978
- Required Privilege Level | 978
- Output Fields | 979
- Sample Output | 982
- Release Information | 989

Syntax

```
show dhcpv6 relay binding
<address>
<brief>
<detail>
<interface interface-name>
<interfaces-vlan>
<interfaces-wildcard>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
<summary>
```

Description

Display the DHCPv6 address bindings in the Dynamic Host Configuration Protocol (DHCP) client table.

Options

address	(Optional) One of the following identifiers for the DHCPv6 client whose binding state you want to show: • *CID*—The specified Client ID (CID). • *ipv6-prefix*—The specified IPv6 prefix. • *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 dhcpv6 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 S-VLAN ID.
interfaces-vlan	(Optional) Interface VLAN ID or S-VLAN ID interface on which to show binding state information.
interfaces-wildcard	(Optional) 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 DHCPv6 client information.

Required Privilege Level

view

Output Fields

Table 29 on page 979 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
number clients,(*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* rebinding, *number* releasing)	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 IPv6 Excluded Prefix	IPv6 Prefix of the DHCP client excluded.	detail
Client DUID	DHCP for IPv6 Unique Identifier (DUID) of the client.	brief detail
Client IPv6 Address	IPv6 address assigned to the subscriber.	detail
Session Id	Session ID of the subscriber session.	brief detail
Expires	Number of seconds in which the lease expires.	brief detail

Table 29: show dhcpv6 relay binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
State	State of the DHCPv6 relay address binding table on the DHCPv6 client: • BOUND—Client has an active IP address lease. • INIT—Initial state. • REBINDING—Client is broadcasting a request to renew the IP address lease. • RECONFIGURE—Client is broadcasting a request to reconfigure 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
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

Table 29: show dhcpv6 relay binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
`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`

Table 29: show dhcpv6 relay binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
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
Dual Stack Group	Name of the dual-stack group for the DHCPv6 binding.	detail
Dual Stack Peer Address	Address of the dual-stack DHCPv4 peer.	detail

Sample Output

show dhcpv6 relay binding

```
user@host> show dhcpv6 relay binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:3c4d:15::/64    1           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
2001:db8:3c4d:16::/64    2           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:02
2001:db8:3c4d:17::/64    3           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:03
2001:db8:3c4d:18::/64    4           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:04
2001:db8:3c4d:19::/64    5           83720    BOUND    ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:05
2001:db8:3c4d: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 dhcp6 relay binding 2001:db8:1111:2222::/64 detail
Session Id:  1
     Client IPv6 Prefix:                  2001:db8:3c4d: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:                      2001:db8:aaaa:bbbb::1
     Server Interface:                    none
     Relay Address:                       2001:db8:1111:2222::
     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:db8:3c4d: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:                      2001:db8:aaaa:bbbb::1
     Server Interface:                    none
     Relay Address:                       2001:db8:1111:2222::
     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:db8:3c4d: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:                      2001:db8:aaaa:bbbb::1
     Server Interface:                    none
     Relay Address:                       2001:db8:1111:2222::
     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 (Dual-Stack)

```
user@host> show dhcpv6 relay binding detail
Session Id:  2
     Client IPv6 Prefix:                  2001:db8:ffff:0:4::/64
     Client IPv6 Address:                 2001:db8:3000:8003::1/128
     Client DUID:                         LL0x1-00:00:64:01:01:02
     State:                               BOUND(DHCPV6_RELAY_STATE_BOUND)
     Lease Expires:                       2016-10-17 07:39:25 PDT
     Lease Expires in:                    3450 seconds
     Lease Start:                         2016-10-17 06:39:25 PDT
     Last Packet Received:                2016-10-17 06:39:25 PDT
     Incoming Client Interface:           ae0.3221225472
     Client Interface Svlan Id:           2000
```

```
     Client Interface Vlan Id:              1
     Server Ip Address:                     2001:db8:3000::2
     Server Interface:                      none
     Client Profile Name:                   my-dual-stack
     Client Id Length:                      10
     Client Id:                             /0x00030001/0x00006401/0x0102
     Dual Stack Group:                      group1
     Dual Stack Peer Address:               192.0.2.4
```

show dhcpv6 relay binding detail (Multi-Relay Topology)

```
user@host > show dhcpv6 relay binding detail
Session Id:  13
     Client IPv6 Prefix:                    2001:db8:3000:0:8001::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:          2001:db8:4000::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:db8:3c4d:15::/64   41           78837     BOUND   ge-1/0/0.0
LL_TIME0x1-0x4bfa26af-00:10:94:00:00:01
```

show dhcpv6 relay binding (Subscriber with Multiple Addresses)

```
user@host> show dhcpv6 relay binding
Prefix                  Session Id  Expires  State    Interface    Client DUID
2001:db8:1001::1:24/128          23          593      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:1001::1:1c/128          23          393      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:1001::1:14/128          23          193      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::300/120           23          293      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::200/120           23          193      BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
2001:db8:3001::100/120           23          93       BOUND    ge-9/0/9.0
LL_TIME0x1-0x55306754-00:10:94:00:00:02
```

When DHCPv6 relay binding is configured with prefix exclude option, we get the following output:

```
user@host> show dhcpv6 relay binding detail
Session Id:  6
     Hardware Address:                    00:10:94:00:00:01
     Client IPv6 Address:                 7001:2:3::d/128
     Lease Expires:                       2017-12-11 07:45:27 IST
     Lease Expires in:                    9999952 seconds
     Preferred Lease Expires:             2017-12-11 07:45:27 IST
     Preferred Lease Expires in:          9999952 seconds
     Client IPv6 Prefix:                  7001::1000:0:0:0/68
     Client IPv6 Excluded Prefix:         7001::1fff:ffff:ffff:ff00/120
     Lease Expires:                       2017-12-11 07:45:27 IST
     Lease Expires in:                    9999952 seconds
     Preferred Lease Expires:             2017-12-11 07:45:27 IST
     Preferred Lease Expires in:          9999952 seconds
     Client DUID:                         LL_TIME0x1-0x599553b0-00:10:94:00:00:01
     State:                               BOUND(DHCPV6_RELAY_STATE_BOUND)
     Lease Start:                         2017-08-17 13:58:33 IST
     Last Packet Received:                2017-08-17 13:58:48 IST
     Incoming Client Interface:           ge-0/0/0.100
     Client Interface Vlan Id:            100
     Server Ip Address:                   7002::1
     Server Interface:                    none
```

```
    Client Id Length:                   14
    Client Id:                          /0x00010001/0x599553b0/0x00109400/0x0001
    Generated Circuit ID:               ge-0/0/0:100
```

show dhcpv6 relay binding detail (Subscriber with Multiple Addresses)

```
user@host> show dhcpv6 relay binding detail
Session Id:  3
    Client IPv6 Address:                2001:db8:1001::1:2/128
    Lease Expires:                      2015-05-15 02:34:51 PDT
    Lease Expires in:                   24 seconds
    Preferred Lease Expires:            2015-05-15 02:34:51 PDT
    Preferred Lease Expires in:         24 seconds
    Client IPv6 Address:                2001:db8:1001::1:12/128
    Lease Expires:                      2015-05-15 02:41:31 PDT
    Lease Expires in:                   424 seconds
    Preferred Lease Expires:            2015-05-15 02:41:31 PDT
    Preferred Lease Expires in:         424 seconds
    Client IPv6 Address:                2001:db8:1001::1:a/128
    Lease Expires:                      2015-05-15 02:38:11 PDT
    Lease Expires in:                   224 seconds
    Preferred Lease Expires:            2015-05-15 02:38:11 PDT
    Preferred Lease Expires in:         224 seconds
    Client IPv6 Prefix:                 2001:db8:3001::/120
    Lease Expires:                      2015-05-15 02:34:51 PDT
    Lease Expires in:                   24 seconds
    Preferred Lease Expires:            2015-05-15 02:34:51 PDT
    Preferred Lease Expires in:         24 seconds
    Client IPv6 Prefix:                 2001:db8:3001::200/120
    Lease Expires:                      2015-05-15 02:38:11 PDT
    Lease Expires in:                   224 seconds
    Preferred Lease Expires:            2015-05-15 02:38:11 PDT
    Preferred Lease Expires in:         224 seconds
    Client IPv6 Prefix:                 2001:db8:3001::100/120
    Lease Expires:                      2015-05-15 02:36:31 PDT
    Lease Expires in:                   124 seconds
    Preferred Lease Expires:            2015-05-15 02:36:31 PDT
    Preferred Lease Expires in:         124 seconds
    Client DUID:                        LL_TIME0x1-0x55554c6e-00:10:94:00:00:02
    State:                              BOUND(DHCPV6_RELAY_STATE_BOUND)
    Lease Start:                        2015-05-15 02:34:21 PDT
```

```
    Last Packet Received:                  2015-05-15 02:34:22 PDT
    Incoming Client Interface:             ge-9/0/9.0
    Client Interface Vlan Id:              111
    Demux Interface:                       demux0.3221225475
    Server Ip Address:                     2001:db8:5001::1
    Server Interface:                      none
    Client Profile Name:                   DHCP-IPDEMUX-PROF
    Client Id Length:                      14
    Client Id:                             /0x00010001/0x55554c6e/0x00109400/0x0002
    Generated Circuit ID:                  ge-9/0/9:111
    Generated Remote ID Enterprise Number: 1411
    Generated Remote ID:                   ge-9/0/9:111
```

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:DB8:19::/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:DB8:19::/32     31       79681    BOUND    demux0.1073741825
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:C9::/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:DB8:19::/32     33       79681    BOUND    ge-1/3/0.110
LL_TIME0x1-0x4d5d009f-00:10:94:00:00:01
2001:DB8:C9::/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)
```

Release Information

Command introduced in Junos OS Release 11.4.

interfaces-vlan and *interfaces-wildcard* options introduced in Junos OS Release 12.1.

RELATED DOCUMENTATION

Viewing and Clearing DHCP Bindings

clear dhcpv6 relay binding | **893**

show dhcpv6 relay statistics

IN THIS SECTION

- Syntax | **990**
- Description | **990**
- Options | **990**
- Required Privilege Level | **991**
- Output Fields | **991**

Sample Output | 995
Release Information | 996

Syntax

```
show dhcpv6 relay statistics
<bulk-leasequery-connections>
<leasequery>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Display Dynamic Host Configuration Protocol for IPv6 (DHCPv6) relay statistics.

Options

bulk-leasequery-connections	(Optional) Display DHCPv6 relay bulk leasequery statistics.
leasequery	(Optional) Display information about DHCPv6 relay individual leasequery statistics.
logical-system *logical-system-name*	(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.
routing-instance *routing-instance-name*	(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.

Required Privilege Level

view

Output Fields

Table 30 on page 992 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`	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. • `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. • `Client MAC validation`—Number of packets discarded because validation of the client MAC address failed. • `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	Number of DHCPv6 messages received. • 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 • DHCPV6_RELAY_FORW—Number of DHCPv6 RELAY-FORW PDUs received. • DHCPV6_LEASEQUERY_REPLY—Number of DHCPv6 replies received from the DHCPv6 sever • DHCPV6_LEASEQUERY_DATA—xxxx • DHCPV6_LEASEQUERY_DONE—The leasequery is complete

Table 30: show dhcpv6 relay statistics Output Fields *(Continued)*

Field Name	Field Description
Messages sent	Number of DHCPv6 messages sent. • 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 • DHCPV6_RELAY_REPL—Number of DHCPv6 RELAY-REPL PDUs transmitted. • DHCP6_LEASEQUERY—Number of DHCP leasequery messages transmitted
Packets forwarded	Number of packets forwarded by the extended DHCPv6 relay agent application. • FWD REQUEST—Number of DHCPv6 REQUEST packets forwarded • FWD REPLY—Number of DHCPv6 REPLY packets forwarded
External Server Response	State of the external DHCP server responsiveness.
Total Requested Servers	Total number of servers with which the DHCP relay agent has requested a bulk leasequery connection.
Total Attempted Servers	Total number of servers with which the DHCP relay agent has attempted to create a bulk leasequery connection.
Total Connected	Total number of servers that have formed a bulk leasequery connection with the DHCP relay agent.
Total Terminated by Server	Total number of servers that have terminated a bulk leasequery connection with the DHCP relay agent.

Table 30: show dhcpv6 relay statistics Output Fields *(Continued)*

Field Name	Field Description
`Total Max Attempted`	Total number of servers where the DHCP relay agent reached the maximum retry limit when it attempted to create a bulk leasequery connection.
`Total Closed due to Errors`	Total number of bulk leasequery connections that closed due to an internal error on the DHCP relay agent.
`In-Flight Connected`	Number of current bulk leasequery connections on the DHCP relay agent.
`Bulk Leaasequery Reply Packet Retries`	Number of bulk leasequery reply packets that the DHCP relay agent has retried.

Sample Output

show dhcpv6 relay statistics

```
user@host> show dhcpv6 relay statistics
DHCPv6 Packets dropped:
    Total                       2
    Lease Time Violation        1
    Client MAC validation       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_FORW           0
    DHCPV6_LEASEQUERY_REPLY     0
    DHCPV6_LEASEQUERY_DATA      0
    DHCPV6_LEASEQUERY_DONE      0

Messages sent:
    DHCPV6_ADVERTISE            0
    DHCPV6_REPLY                0
    DHCPV6_RECONFIGURE          0
    DHCPV6_RELAY_REPL           0
    DHCPV6_LEASEQUERY           0

Packets forwarded:
    Total                       4
    FWD REQUEST                 2
    FWD REPLY                   2

External Server Response:
    State                     Responding
```

show dhcpv6 relay statistics bulk-leasequery-connections

```
user@host> show dhcpv6 relay statistics bulk-leasequery-connections

Total Requested Servers:    0
Total Attempted Servers:    0
Total Connected:            0
Total Terminated by Server: 0
Total Max Attempted:        0
Total Closed due to Errors: 0
In-Flight Connected:        0
Bulk Leasequery Reply Packet Retries:   0
```

Release Information

Command introduced in Junos OS Release 11.4.

`bulk-leasequery-connections` option introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

clear dhcpv6 relay statistics | 898

DHCPv6 Client MAC Address Validation to Prevent Session Hijacking

show dhcpv6 server binding (View)

IN THIS SECTION

- Syntax | 997
- Description | 997
- Options | 998
- Required Privilege Level | 998
- Output Fields | 998
- Sample Output | 1000
- Release Information | 1003

Syntax

```
show dhcpv6 server binding
<brief | detail | summary>
<interface interface-name>
<routing-instance routing-instance-name>
```

Description

Display the address bindings in the client table for DCHPv6 local server.

Options

- 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`.
- interface *interface-name*—(Optional) Display information about active client bindings on the specified interface.
- routing-instance *routing-instance-name*—(Optional) Display information about active client bindings for DHCPv6 clients on the specified routing instance.
-

Required Privilege Level

view

Output Fields

Table 31 on page 998 lists the output fields for the `show dhcpv6 server binding` command. Output fields are listed in the approximate order in which they appear.

Table 31: show dhcv6p server binding Output Fields

Field Name	Field Description	Level of Output
number clients, (*number* init, *number* bound, *number* selecting, *number* requesting, *number* renewing, *number* releasing)	Summary counts of the total number of DHCPv6 clients and the number of DHCPv6 clients in each state.	summary

Table 31: show dhcv6p server binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Prefix	Client's DHCPv6 prefix.	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 DHCPv6 local server: • BOUND—Client has active IP address lease. • INIT—Initial state. • RELEASE—Client is releasing IP address lease. • RECONFIGURE—Client has received reconfigure message from server. • 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 DUID	Client's DHCP Unique Identifier (DUID).	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

Table 31: show dhcv6p server binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
Lease Start	Date and time at which the client's address lease was obtained.	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 Id length	Length of the DHCPv6 client ID, in bytes.	detail
Client Id	ID of the DHCPv6 client.	detail
Server Id	ID type and ID of the DHCPv6 server.	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
```

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(bound)
     Lease Expires:                        2009-07-21 10:41:15 PDT
     Lease Expires in:                     86308 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:                            /0x00010001/0x02e159c0/0x00109400/0x0001      Server
Id:                            <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>

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:                     86308 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      Server
Id:                            <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>
```

show dhcpv6 server binding interface

```
user@host> show dhcp6 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 dhcp6 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
     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      Server
Id:                            <VENDOR 2198142976/4a4e3131324143433741464300000000000000000>
```

show dhcpv6 server binding prefix

```
user@host> show dhcp6 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
     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:bd8:1111:2222::/64 8          86235    BOUND    ge-1/0/0.0
LL_TIME0x1-0x2e159c0-00:10:94:00:00:03
```

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)
```

Release Information

Command introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

clear dhcpv6 server binding (Local Server) | 905

show dhcpv6 server statistics

IN THIS SECTION

Syntax | 1004

- Description | **1004**
- Options | **1004**
- Required Privilege Level | **1005**
- Output Fields | **1005**
- Sample Output | **1008**
- Release Information | **1009**

Syntax

```
show dhcpv6 server statistics
<bulk-leasequery-connections>
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Display extended Dynamic Host Configuration Protocol for IPv6 (DHCPv6) local server statistics.

Options

bulk-leasequery-connections	(Optional) Display information about DHCPv6 local server bulk leasequery statistics.
logical-system *logical-system-name*	(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.
routing-instance *routing-instance-name*	(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.

Required Privilege Level

view

Output Fields

Table 32 on page 1006 lists the output fields for the `show dhcpv6 server statistics` command. Output fields are listed in the approximate order in which they appear.

Table 32: show dhcpv6 server statistics Output Fields

Field Name	Field Description
`Packets dropped`	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. • `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 • `Client MAC validation`—Number of packets discarded because validation of the client MAC address failed. • `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

Table 32: show dhcpv6 server statistics Output Fields *(Continued)*

Field Name	Field Description
	• `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
`Advertise Delay`	Number of DHCP advertise messages delayed. • `DELAYED`—Number of DHCPv6 advertise packets that have been sent after being delayed. • `INPROGRESS`—Number of DHCPv6 advertise packets that are in the delay queue. • `TOTAL`—Total number of delayed DHCPv6 advertise messages; sum of `DELAYED` and `INPROGRESS`.
`Messages received`	Number of DHCPv6 messages received. • `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. • `DHCPV6_LEASEQUERY`—Number of DHCPv6 leasequery messages received.

Table 32: show dhcpv6 server statistics Output Fields *(Continued)*

Field Name	Field Description
`Messages sent`	Number of DHCPv6 messages sent. • `DHCPV6_ADVERTISE`—Number of DHCPv6 ADVERTISE PDUs transmitted. • `DHCPV6_REPLY`—Number of DHCPv6 ADVERTISE PDUs transmitted. • `DHCPV6_LOGICAL_NAK`—Number of logical NAK messages sent, signifying T1 and T2 timers with values of zero; subset of `DHCPV6_REPLY` counter. (Displays only at `verbose` level. • `DHC6_RECONFIGURE`—Number of DHCPv6 RECONFIGURE PDUs transmitted. • `DHCPV6_RELAY_REPL`—Number of DHCPv6 RELAY-REPL PDUs transmitted. • `DHCPV6_RELAY_FORW`—Number of DHCPv6 RELAY-FORW PDUs transmitted. • `DHCPV6_LEASEQUERY_REPLY`—Number of DHCPv6 leasequery replies transmitted to the DHCPv6 relay agent. • `DHCPV6_LEASEQUERY_DATA`—Number of DHCPv6 LEASEQUERY-DATA packets transmitted. • `DHCPV6_LEASEQUERY_DONE`—Number of DHCPv6 LEASEQUERY-DONE packets sent.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
    Total                     2
    Lease Time Violation      1
    Client MAC validation     1

Advertise Delay:
    DELAYED                   3
```

```
    INPROGRESS                 9
    TOTAL                     12

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

    DHCPV^_LEASEQUERY          0

Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
    DHCPV6_LEASEQUERY_REPLY    0
    DHCPV6_LEASEQUERY_DATA     0
    DHCPV6_LEASEQUERY_DONE     0
```

show dhcpv6 server statistics bulk-leasequery-connections

```
user@host> show dhcpv6 server statistics bulk-leasequery-connections

Total Accepted Connections:                    0
Total Not-Accepted Connections:                0
Connections Closed due to Errors:              0
Connections Closed due to max-empty-replies:   0
In-flight Connections:                         0
```

Release Information

Command introduced in Junos OS Release 9.6.

`bulk-leasequery-connections` option introduced in Junos OS Release 16.1.

RELATED DOCUMENTATION

clear dhcpv6 server statistics | 907

DHCPv6 Client MAC Address Validation to Prevent Session Hijacking

show dhcpv6 server statistics (View)

IN THIS SECTION

- Syntax | 1010
- Description | 1010
- Options | 1011
- Required Privilege Level | 1011
- Output Fields | 1011
- Sample Output | 1014
- Release Information | 1014

Syntax

```
show dhcpv6 server statistics
<logical-system logical-system-name>
<routing-instance routing-instance-name>
```

Description

Display DHCPv6 local server statistics.

Options

logical-system *logical-system-name* — (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.

routing-instance *routing-instance-name* — (Optional) Display information about 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.

Required Privilege Level

view

Output Fields

Table 33 on page 1012 lists the output fields for the `show dhcpv6 server statistics` command. Output fields are listed in the approximate order in which they appear.

Table 33: show dhcpv6 server statistics Output Fields

Field Name	Field Description
`Dhcpv6 Packets dropped`	Number of packets discarded by the 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. • `Total`—Total number of packets discarded by the DHCPv6 local server • `Authentication`—Number of packets discarded because they could not be authenticated • `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 • `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 DHCPv6 local server could not send

Table 33: show dhcpv6 server statistics Output Fields *(Continued)*

Field Name	Field Description
`Messages received`	Number of DHCPv6 messages received. • `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 from a relay by the DHCPv6 server. • `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`	Number of DHCPv6 messages sent. • `DHCPV6_ADVERTISE`—Number of DHCPv6 ADVERTISE PDUs transmitted. • `DHCPV6_REPLY`—Number of DHCPv6 ADVERTISE PDUs transmitted. • `DHC6_RECONFIGURE`—Number of DHCPv6 RECONFIGURE PDUs transmitted. • `DHCPV6_RELAY_REPL`—Number of DHCPv6 RELAY-REPL PDUs sent from DHCPv6 server to DHCPv6 relay.

Sample Output

show dhcpv6 server statistics

```
user@host> show dhcpv6 server statistics
Dhcpv6 Packets dropped:
    Total               0

Messages received:
    DHCPV6_DECLINE             0
    DHCPV6_SOLICIT             9
    DHCPV6_INFORMATION_REQUEST 0
    DHCPV6_RELEASE             0
    DHCPV6_REQUEST             5
    DHCPV6_CONFIRM             0
    DHCPV6_RENEW               0
    DHCPV6_REBIND              0
    DHCPV6_RELAY_FORW          0
   Messages sent:
    DHCPV6_ADVERTISE           9
    DHCPV6_REPLY               5
    DHCPV6_RECONFIGURE         0
    DHCPV6_RELAY_REPL          0
```

Release Information

Command introduced in Junos OS Release 10.4.

RELATED DOCUMENTATION

clear dhcpv6 server statistics (Local Server) | 909

show route protocol

IN THIS SECTION

- Syntax | 1015
- Syntax (EX Series Switches) | 1015
- Description | 1015
- Options | 1016
- Required Privilege Level | 1017
- Output Fields | 1017
- Sample Output | 1018
- Release Information | 1022

Syntax

```
show route protocol protocol
<brief | detail | extensive | terse>
<logical-system (all | logical-system-name)>
```

Syntax (EX Series Switches)

```
show route protocol protocol
<brief | detail | extensive | terse>
```

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 | *logical-system-name*) (Optional) Perform this operation on all logical systems or on a particular logical system.

protocol Protocol from which the route was learned:

- `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

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 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 direct

```
user@host> show route protocol direct

inet.0: 335843 destinations, 335844 routes (335394 active, 0 holddown, 450 hidden)
+ = Active Route, - = Last Active, * = Both

172.16.8.0/24         *[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
172.16.30.0/24      *[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

2001:db8::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 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 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
172.16.233.5/32      *[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
172.16.233.5/32      *[OSPF/10] 20:26:20, metric 1
```

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
172.16.233.9/32      *[RIP/100] 00:03:59, metric 1
```

Release Information

Command introduced before Junos OS Release 7.4.

`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.

RELATED DOCUMENTATION

- *show route*
- *show route detail*
- *show route extensive*
- *show route terse*

show system services dhcp binding

IN THIS SECTION

- Syntax | **1023**
- Description | **1023**
- Options | **1024**
- Required Privilege Level | **1024**
- Output Fields | **1024**
- Sample Output | **1025**
- Release Information | **1027**

Syntax

```
show system services dhcp binding
<detail>
<address>
```

Description

(EX Series switches only) Display Dynamic Host Configuration Protocol (DHCP) server client binding information.

Options

none Display brief information about all active client bindings.

detail (Optional) Display detailed information about all active client bindings.

address (Optional) Display detailed client binding information for the specified IP address only.

Required Privilege Level

view and system

Output Fields

Table 34 on page 1024 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 34: 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

Table 34: show system services dhcp binding Output Fields *(Continued)*

Field Name	Field Description	Level of Output
`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`
`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
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

clear system services dhcp binding | 910

show system services dhcp client

IN THIS SECTION

- Syntax | 1027
- Description | 1028
- Options | 1028
- Required Privilege Level | 1028
- Output Fields | 1028
- Sample Output | 1030
- Sample Output | 1031
- Sample Output | 1031
- Release Information | 1032

Syntax

```
show system services dhcp client
<                    interface-name                >
<statistics>
```

Description

Display information about DHCP clients.

Options

- none—Display DHCP information for all interfaces.
- *interface-name*—(Optional) Display DHCP information for the specified interface.
- `statistics`—(Optional) Display DHCP client statistics.

Required Privilege Level

view and system

Output Fields

Table 35 on page 1028 lists the output fields for the `show system services dhcp client` command. Output fields are listed in the approximate order in which they appear.

Table 35: show system services dhcp client Output Fields

Field Name	Field Description
`Logical Interface Name`	Name of the logical interface.
`Client Status`	State of the client binding.
`Vendor Identifier`	Vendor ID.
`Server Address`	IP address of the DHCP server.

Table 35: show system services dhcp client Output Fields *(Continued)*

Field Name	Field Description
`Address obtained`	IP address obtained from the DHCP server.
`Lease Obtained at`	Date and time the lease was obtained.
`Lease Expires in`	(EX Series switches only) Time the current lease expires in (seconds).
`Lease Expires at`	Date and time the lease expires.
`DHCP Options`	• `Name: server-identifier`, `Value:` IP address of the name server. • `Name: device`, `Value:` IP address of the name device. • `Name: domain-name`, `Value:` Name of the domain.
`Packets dropped`	`Total` packets dropped.
`Messages received`	`Number of the following DHCP messages received:` • `DHCPOFFER`—First packet received on a logical interface when DHCP is enabled. • `DHCPACK`—When received from the server, the client sends an ARP request for that address and adds a (ARP response) timer for 4 seconds and stops the earlier timer added for DHCPACK. • `DHCPNAK`—When a DHCPNAK is received instead of DHCPACK, the logical interface sends a DHCPDISCOVER packet.

Table 35: show system services dhcp client Output Fields *(Continued)*

Field Name	Field Description
Messages sent	Number of the following DHCP messages sent: • DHCPDECLINE—Packet sent when ARP response is received and there is a conflict. The logical interface sends a new DHCPDISCOVER packet. • DHCPDISCOVER—Packet sent on the interface for which the DHCP client is enabled. • DHCPREQUEST—Packet sent to the DHCP server after accepting the DHCPOFFER. After sending the DHCPREQUEST, the device adds a retransmission-interval timer. • DHCPINFORM—Packet sent to the DHCP server for local configuration parameters. • DHCPRELEASE—Packet sent to the DHCP server to relinquish network address and cancel remaining lease. • DHCPRENEW—Packet sent to the DHCP server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be unicast directly to the server. • DHCPREBIND—Packet sent to any server to renew the address. The next message to be sent will be a DHCPREQUEST message, which will be broadcast.

Sample Output

show system services dhcp client

```
user@host> show system services dhcp client
Logical Interface name         ge-0/0/34.0
        Hardware address        00:1f:12:38:5f:e5
        Client status           bound
        Address obtained        10.0.0.2
```

```
        Update server           disabled
        Lease obtained at       2013-12-23 08:11:40 UTC
        Lease expires in        93
        Lease expires at        2013-12-23 08:13:20 UTC

DHCP options:
    Name: server-identifier, Value: 10.0.0.1
    Code: 1, Type: ip-address, Value: 255.255.255.0
```

Sample Output

show system services dhcp client ge-0/0/34.0

```
user@host> show system services dhcp client ge-0/0/34.0
 Logical Interface name         ge-0/0/34.0
        Hardware address        00:1f:12:38:5f:e5
        Client status           bound
        Address obtained        10.0.0.2
        Update server           disabled
        Lease obtained at       2013-12-23 08:11:40 UTC
        Lease expires in        87
        Lease expires at        2013-12-23 08:13:20 UTC

DHCP options:
    Name: server-identifier, Value: 10.0.0.1
    Code: 1, Type: ip-address, Value: 255.255.255.0
```

Sample Output

show system services dhcp client statistics

```
user@host> show system services dhcp client statistics
Packets dropped:
    Total                     0
Messages received:
    DHCPOFFER                 0
```

```
    DHCPACK                  8
    DHCPNAK                  0
Messages sent:
    DHCPDECLINE              0
    DHCPDISCOVER             0
    DHCPREQUEST              1
    DHCPINFORM               0
    DHCPRELEASE              0
    DHCPRENEW                7
    DHCPREBIND               0
```

Release Information

Command introduced in Junos OS Release 8.5.

Command introduced in Junos OS Release 9.0 for EX Series switches.

RELATED DOCUMENTATION

dhcp (DHCP Client) | 441

request system services dhcp | 923

show system services dhcp conflict

IN THIS SECTION

- Syntax | 1033
- Description | 1033
- Options | 1033
- Required Privilege Level | 1033
- Output Fields | 1033
- Sample Output | 1034

- Release Information | 1034

Syntax

```
show system services dhcp conflict
```

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

Output Fields

Table 36 on page 1034 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 36: 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               10.0.0.1
2004-08-04 04:23:12 PDT  Ping              10.0.0.2
2004-08-05 21:06:44 PDT  Client            10.0.0.3
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

clear system services dhcp conflict | 912

show system services dhcp global

IN THIS SECTION

- Syntax | 1035
- Description | 1035
- Options | 1035
- Required Privilege Level | 1036
- Output Fields | 1036
- Sample Output | 1036
- Release Information | 1037

Syntax

```
show system services dhcp global
```

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

Output Fields

Table 37 on page 1036 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 37: 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
```

Release Information

Command introduced before Junos OS Release 7.4.

show system services dhcp pool

IN THIS SECTION

- Syntax | **1038**
- Description | **1038**
- Options | **1038**
- Required Privilege Level | **1038**
- Output Fields | **1038**
- Sample Output | **1040**
- Release Information | **1041**

Syntax

```
show system services dhcp pool
<detail>
<subnet-address>
```

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

Output Fields

Table 38 on page 1039 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 38: 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`	(*subnet-address* option only) Subnet to which the specified address pool belongs.	None specified
`Address range`	(*subnet-address* 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`
`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`

Table 38: show system services dhcp pool Output Fields *(Continued)*

Field Name	Field Description	Level of Output
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
192.0.2.0/24 192.0.2.2     192.0.2.254     192.0.2.1
```

show system services dhcp pool subnet-address

```
user@host> show system services dhcp pool 192.0.2.0/24

Pool information:
    Subnet                    192.0.2.0/24
    Address range             192.0.2.2 - 192.0.2.254
    Addresses assigned        2/253
```

show system services dhcp pool subnet-address detail

```
user@host> show system services dhcp pool 192.0.2.0/24 detail

Pool information:
    Subnet                    192.0.2.0/24
    Address range             192.0.2.2 - 192.0.2.254
    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: { 192.0.2.1 }
    Name: server-identifier, Value: 192.0.2.1
    Code: 19, Type: flag, Value: off
    Code: 40, Type: string, Value: domain.tld
    Code: 32, Type: ip-address, Value: 192.0.2.1
```

Release Information

Command introduced before Junos OS Release 7.4.

show system services dhcp relay-statistics

IN THIS SECTION

- Syntax | **1042**
- Description | **1042**
- Required Privilege Level | **1042**
- Output Fields | **1042**
- Sample Output | **1043**
- Release Information | **1044**

Syntax

```
show system services dhcp relay-statistics
```

Description

Display information about the DHCP relay.

Required Privilege Level

view and system

Output Fields

Table 39 on page 1042 lists the output fields for the `show system services dhcp relay-statistics` command. Output fields are listed in the approximate order in which they appear.

Table 39: show system services dhcp relay-statistics Output Fields

Field Name	Field Description
`Received packets`	Total DHCP packets received.
`Forwarded packets`	Total DHCP packet forwarded.

Table 39: show system services dhcp relay-statistics Output Fields *(Continued)*

Field Name	Field Description
`Dropped packets`	Total DHCP packets dropped for the following reasons: • `Due to a missing interface in the relay database`—Number of packets discarded because they did not belong to a configured interface. • `Due to a missing matching routing instance`—Number of packets discarded because they did not belong to a configured routing instance. • `Due to an error during packet read`—Number of packets discarded because of a system read error. • `Due to an error during packet send`—Number of packets that the DHCP relay application could not send. • `Due to an invalid server address`—Number of packets discarded because an invalid server address was specified. • `Due to a missing valid local address`—Number of packets discarded because there was no valid local address. • `Due to a missing route to the server or client`—Number of packets discarded because there were no addresses available for assignment.

Sample Output

show system services dhcp relay-statistics

```
user@host> show system services dhcp relay-statistics
  Received packets: 4
  Forwarded packets: 4
  Dropped packets: 4
    Due to missing interface in relay database: 4
    Due to missing matching routing instance: 0
```

```
    Due to an error during packet read: 0
    Due to an error during packet send: 0
    Due to invalid server address: 0
    Due to missing valid local address: 0
    Due to missing route to server/client: 0
```

Release Information

Command introduced in Junos OS Release 8.5 .

RELATED DOCUMENTATION

dhcp (DHCP Client) | 441

show system services dhcp statistics

IN THIS SECTION

- Syntax | 1044
- Description | 1045
- Options | 1045
- Required Privilege Level | 1045
- Output Fields | 1045
- Sample Output | 1047
- Release Information | 1048

Syntax

```
show system services dhcp statistics
```

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

Output Fields

Table 40 on page 1045 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 40: 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.

Table 40: show system services dhcp statistics Output Fields *(Continued)*

Field Name	Field Description
`Packets dropped`	Total number of packets dropped and number of packets dropped because of: • 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
`Messages received`	Number of the following message types sent from DHCP clients and received by the DHCP server: • BOOTREQUEST • DHCPDECLINE • DHCPDISCOVER • DHCPINFORM • DHCPRELEASE • DHCPREQUEST

Table 40: show system services dhcp statistics Output Fields *(Continued)*

Field Name	Field Description
`Messages sent`	Number of the following message types sent from the DHCP server to DHCP clients: • 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
```

Release Information

Command introduced before Junos OS Release 7.4.

RELATED DOCUMENTATION

clear system services dhcp statistics | 914