



---

# JunosE™ Software for E Series™ Broadband Services Routers

## DHCP Local Server

Release

14.3.x



---

Published: 2013-07-15

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

Copyright © 2013, Juniper Networks, Inc. All rights reserved.

Juniper Networks, Junos, Steel-Belted Radius, NetScreen, and ScreenOS are registered trademarks of Juniper Networks, Inc. in the United States and other countries. The Juniper Networks Logo, the Junos logo, and JunosE are trademarks of Juniper Networks, Inc. All other trademarks, service marks, registered trademarks, or registered service marks are the property of their respective owners.

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

Products made or sold by Juniper Networks or components thereof might be covered by one or more of the following patents that are owned by or licensed to Juniper Networks: U.S. Patent Nos. 5,473,599, 5,905,725, 5,909,440, 6,192,051, 6,333,650, 6,359,479, 6,406,312, 6,429,706, 6,459,579, 6,493,347, 6,538,518, 6,538,899, 6,552,918, 6,567,902, 6,578,186, and 6,590,785.

*JunosE™ Software for E Series™ Broadband Services Routers DHCP Local Server*  
Release 14.3.x  
Copyright © 2013, Juniper Networks, Inc.  
All rights reserved.

Revision History  
July 2013—FRS JunosE 14.3.x

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

#### YEAR 2000 NOTICE

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

#### END USER LICENSE AGREEMENT

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

# Table of Contents

	About the Documentation . . . . .	xi
	E Series and JunosE Documentation and Release Notes . . . . .	xi
	Audience . . . . .	xi
	E Series and JunosE Text and Syntax Conventions . . . . .	xi
	Obtaining Documentation . . . . .	xiii
	Documentation Feedback . . . . .	xiii
	Requesting Technical Support . . . . .	xiii
	Self-Help Online Tools and Resources . . . . .	xiv
	Opening a Case with JTAC . . . . .	xiv
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>How DHCP Local Server Works . . . . .</b>	<b>3</b>
	Embedded DHCP Local Server Overview . . . . .	3
	DHCP Local Server and Client Configuration . . . . .	3
	Equal-Access Mode Overview . . . . .	4
	Local Pool Selection and Address Allocation . . . . .	4
	The Connection Process . . . . .	5
	Standalone Mode Overview . . . . .	6
	Local Pool Selection and Address Allocation . . . . .	6
	Server Management Table . . . . .	8
	DHCP Local Server Prerequisites . . . . .	8
	DHCP Local Server Configuration Tasks . . . . .	9
<b>Chapter 2</b>	<b>DHCP Unique IDs for DHCPv6 Clients and Servers . . . . .</b>	<b>11</b>
	DHCP Unique ID for Clients and Servers Overview . . . . .	11
<b>Chapter 3</b>	<b>AAA Authentication for DHCPv6 Local Server Standalone Mode . . . . .</b>	<b>13</b>
	Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview . . . . .	13
	Accounting for IPv6 Subscribers with DHCPv6 Local Server Standalone Mode . . . . .	15
	Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information . . . . .	15
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 4</b>	<b>Configuration Tasks for DHCPv4 Local Server . . . . .</b>	<b>19</b>
	Configuring DHCP Local Address Pools . . . . .	19
	Basic Configuration of DHCP Local Address Pools . . . . .	19
	Linking Local Address Pools . . . . .	21

	Setting Grace Periods for Address Leases . . . . .	21
	Configuring the DHCP Local Server . . . . .	23
	Basic Configuration of DHCP Local Server . . . . .	23
	Limiting the Number of IP Addresses Supplied by DHCP Local Server . . . . .	24
	Excluding IP Addresses from Address Pools . . . . .	25
	Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces . . . . .	25
	Differentiating Between Clients with the Same Client ID or Hardware Address . . . . .	25
	Logging Out DHCP Local Server Subscribers . . . . .	27
	Clearing an IP DHCP Local Server Binding . . . . .	27
	Using SNMP Traps to Monitor DHCP Local Server Events . . . . .	27
	Using DHCP Local Server Event Logs . . . . .	28
	Configuring AAA Authentication for DHCP Local Server Standalone Mode . . . . .	29
<b>Chapter 5</b>	<b>Configuration Tasks for DHCPv6 Local Server . . . . .</b>	<b>33</b>
	Configuring the DHCPv6 Local Server . . . . .	33
	Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode . . . . .	35
	Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers . . . . .	37
<b>Chapter 6</b>	<b>Removal of DHCPv6 Client Bindings . . . . .</b>	<b>39</b>
	Deleting DHCPv6 Client Bindings . . . . .	39
<b>Chapter 7</b>	<b>Interoperation of SRC Client and DHCP Local Server . . . . .</b>	<b>41</b>
	Configuring the Router to Work with the SRC Software . . . . .	41
<b>Chapter 8</b>	<b>Configuring Baselines for DHCP Local Server Statistics . . . . .</b>	<b>45</b>
	Setting Baselines for DHCP Statistics . . . . .	45
	Setting a Baseline for DHCP Relay and Relay Proxy . . . . .	45
	Setting a Baseline for DHCP Proxy Server Statistics . . . . .	45
	Setting a Baseline for DHCP External Server Statistics . . . . .	46
	Setting a Baseline for DHCP Local Server Statistics . . . . .	46
<b>Chapter 9</b>	<b>Configuration Commands . . . . .</b>	<b>47</b>
	clear ip dhcp-local binding . . . . .	48
	dhcp delete-binding . . . . .	49
	default-router . . . . .	52
	dns-server . . . . .	53
	domain-name . . . . .	54
	grace-period . . . . .	55
	ip dhcp-local pool . . . . .	56
	ip dhcp-local auto-configure agent-circuit-identifier . . . . .	57
	ip dhcp-local excluded-address . . . . .	58
	ip dhcp-local limit . . . . .	59
	ip dhcp-local unique-client-ids . . . . .	60
	ip dhcp-local auth domain . . . . .	61
	ip dhcp-local auth include . . . . .	62
	ip dhcp-local auth password . . . . .	63
	ip dhcp-local auth user-prefix . . . . .	64
	ip dhcp-local auth domain . . . . .	65
	ipv6 dhcpv6-local delegated-prefix . . . . .	66

	ipv6 dhcpv6-local dns-domain-search . . . . .	67
	ipv6 dhcpv6-local dns-server . . . . .	68
	ipv6 dhcpv6-local duid-type . . . . .	69
	ipv6 dhcpv6-local prefix-lifetime . . . . .	70
	ipv6 local pool . . . . .	71
	ipv6 dhcpv6-local auth domain . . . . .	72
	ipv6 dhcpv6-local auth password . . . . .	73
	ipv6 dhcpv6-local auth user-prefix . . . . .	74
	ipv6 dhcpv6-local duid-type . . . . .	75
	lease . . . . .	76
	link . . . . .	77
	logout subscribers . . . . .	78
	netbios-name-server . . . . .	80
	netbios-node-type . . . . .	81
	network . . . . .	82
	reserve . . . . .	84
	server-address . . . . .	85
	service dhcp-local . . . . .	86
	service dhcpv6-local . . . . .	87
	snmpTrap . . . . .	88
	use-release-grace-period . . . . .	89
	warning . . . . .	90
	service dhcp-local . . . . .	91
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Monitoring DHCP Local Address Pools . . . . .</b>	<b>95</b>
	Monitoring DHCP Local Address Pools . . . . .	95
<b>Chapter 11</b>	<b>Monitoring Tasks for DHCPv4 Local Server . . . . .</b>	<b>99</b>
	Monitoring DHCP Local Server Authentication Information . . . . .	99
	Monitoring DHCP Local Server Configuration . . . . .	100
	Monitoring DHCP Local Server Leases . . . . .	101
	Monitoring DHCP Local Server Statistics . . . . .	102
	Monitoring the Maximum Number of Available Leases . . . . .	105
	Monitoring Static IP Address and MAC Address Pairs Supplied by DHCP Local Server . . . . .	106
<b>Chapter 12</b>	<b>Monitoring Tasks for DHCPv6 Local Server . . . . .</b>	<b>109</b>
	Monitoring DHCPv6 Local Server Authentication Information . . . . .	109
	Monitoring DHCPv6 Local Server Binding Information . . . . .	110
	Monitoring DHCPv6 Local Server DNS Search Lists . . . . .	110
	Monitoring DHCPv6 Local Server DNS Servers . . . . .	111
	Monitoring DHCPv6 Local Server Prefix Lifetime . . . . .	111
	Monitoring DHCPv6 Local Server Statistics . . . . .	112
<b>Chapter 13</b>	<b>Monitoring Commands . . . . .</b>	<b>115</b>
	show ip dhcp-local . . . . .	116
	show ip dhcp-local auth . . . . .	117
	show ip dhcp-local binding . . . . .	118

show ip dhcp-local excluded . . . . .	119
show ip dhcp-local leases . . . . .	120
show ip dhcp-local limits . . . . .	121
show ip dhcp-local pool . . . . .	122
show ip dhcp-local reserved . . . . .	123
show ip dhcp-local statistics . . . . .	124
show ipv6 dhcpv6-local auth config . . . . .	125
show ipv6 dhcpv6-local binding . . . . .	126
show ipv6 dhcpv6-local dns-domain-searchlist . . . . .	127
show ipv6 dhcpv6-local dns-servers . . . . .	128
show ipv6 dhcpv6-local prefix-lifetime . . . . .	129
show ipv6 dhcpv6-local statistics . . . . .	130

## Part 4

## Index

Index . . . . .	133
-----------------	-----

# List of Figures

<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>How DHCP Local Server Works . . . . .</b>	<b>3</b>
	Figure 1: Non-PPP Equal Access via the Router . . . . .	6
<b>Part 2</b>	<b>Configuration</b>	
<b>Chapter 7</b>	<b>Interoperation of SRC Client and DHCP Local Server . . . . .</b>	<b>41</b>
	Figure 2: Non-PPP Equal-Access Configuration Example . . . . .	42





# List of Tables

	<b>About the Documentation . . . . .</b>	<b>xi</b>
	Table 1: Notice Icons . . . . .	xii
	Table 2: Text and Syntax Conventions . . . . .	xii
<b>Part 1</b>	<b>Overview</b>	
<b>Chapter 1</b>	<b>How DHCP Local Server Works . . . . .</b>	<b>3</b>
	Table 3: Local Pool Selection in Equal-Access Mode . . . . .	5
	Table 4: Local Pool Selection in Standalone Mode Without AAA Authentication . . . . .	7
	Table 5: Local Pool Selection in Standalone Mode with AAA Authentication . . . . .	7
<b>Part 3</b>	<b>Administration</b>	
<b>Chapter 10</b>	<b>Monitoring DHCP Local Address Pools . . . . .</b>	<b>95</b>
	Table 6: show ip dhcp-local pool Output Fields . . . . .	96
<b>Chapter 11</b>	<b>Monitoring Tasks for DHCPv4 Local Server . . . . .</b>	<b>99</b>
	Table 7: show ip dhcp-local auth Output Fields . . . . .	100
	Table 8: show ip dhcp-local Output Fields . . . . .	101
	Table 9: show ip dhcp-local leases Output Fields . . . . .	102
	Table 10: show ip dhcp-local statistics output fields. . . . .	103
	Table 11: show ip dhcp-local limits Output Fields . . . . .	106
	Table 12: show ip dhcp-local reserved Output Fields . . . . .	107
<b>Chapter 12</b>	<b>Monitoring Tasks for DHCPv6 Local Server . . . . .</b>	<b>109</b>
	Table 13: show ipv6 dhcpv6-local auth config Output Fields . . . . .	109
	Table 14: show ipv6 dhcpv6-local binding Output Fields . . . . .	110
	Table 15: show ipv6 dhcpv6-local dns-domain-searchlist Output Fields . . . . .	111
	Table 16: show ipv6 dhcpv6-local dns-servers Output Fields . . . . .	111
	Table 17: show ipv6 dhcpv6-local prefix-lifetime Output Fields . . . . .	112
	Table 18: show ipv6 dhcpv6-local statistics Output Fields . . . . .	112



# About the Documentation

- E Series and JunosE Documentation and Release Notes on page xi
- Audience on page xi
- E Series and JunosE Text and Syntax Conventions on page xi
- Obtaining Documentation on page xiii
- Documentation Feedback on page xiii
- Requesting Technical Support on page xiii

## E Series and JunosE Documentation and Release Notes

---

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

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

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

## Audience

---

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

## E Series and JunosE Text and Syntax Conventions

---

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

Table 1: Notice Icons

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

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

Table 2: Text and Syntax Conventions

Convention	Description	Examples
<b>Bold text like this</b>	Represents commands and keywords in text.	<ul style="list-style-type: none"> <li>Issue the <b>clock source</b> command.</li> <li>Specify the keyword <b>exp-msg</b>.</li> </ul>
<b>Bold text like this</b>	Represents text that the user must type.	<b>host1(config)#traffic class low-loss1</b>
Fixed-width text like this	Represents information as displayed on your terminal's screen.	<b>host1#show ip ospf 2</b>  Routing Process OSPF 2 with Router ID 5.5.0.250  Router is an Area Border Router (ABR)
<i>Italic text like this</i>	<ul style="list-style-type: none"> <li>Emphasizes words.</li> <li>Identifies variables.</li> <li>Identifies chapter, appendix, and book names.</li> </ul>	<ul style="list-style-type: none"> <li>There are two levels of access: <i>user</i> and <i>privileged</i>.</li> <li><i>clusterId</i>, <i>ipAddress</i>.</li> <li><i>Appendix A, System Specifications</i></li> </ul>
Plus sign (+) linking key names	Indicates that you must press two or more keys simultaneously.	Press Ctrl + b.
<b>Syntax Conventions in the Command Reference Guide</b>		
Plain text like this	Represents keywords.	terminal length
<i>Italic text like this</i>	Represents variables.	<i>mask</i> , <i>accessListName</i>

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

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

## Obtaining Documentation

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

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

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

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

## Documentation Feedback

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

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

## Requesting Technical Support

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

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

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

## Self-Help Online Tools and Resources

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

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

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

## Opening a Case with JTAC

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

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

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

## PART 1

# Overview

- [How DHCP Local Server Works on page 3](#)
- [DHCP Unique IDs for DHCPv6 Clients and Servers on page 11](#)
- [AAA Authentication for DHCPv6 Local Server Standalone Mode on page 13](#)





## CHAPTER 1

# How DHCP Local Server Works

- [Embedded DHCP Local Server Overview on page 3](#)
- [Equal-Access Mode Overview on page 4](#)
- [Standalone Mode Overview on page 6](#)
- [DHCP Local Server Prerequisites on page 8](#)
- [DHCP Local Server Configuration Tasks on page 9](#)

## Embedded DHCP Local Server Overview

---

The router offers an embedded DHCP server, known as the DHCP local server. The DHCP local server has two modes: equal-access and standalone.



**NOTE:** E Series routers also support an embedded DHCP version 6 (DHCPv6) local server. The DHCPv6 local server provides a subset of the features of the DHCP local server. For information about configuring the DHCPv6 local server, see [“Configuring the DHCPv6 Local Server” on page 33](#).

- In equal-access mode, the DHCP local server works with the Juniper Networks SRC software to provide an advanced subscriber configuration and management service.
- In standalone mode, the DHCP local server provides a basic DHCP service, and also allows you to configure AAA authentication for incoming DHCP clients. Also, after successful authentication, the DHCP local server uses the information in the client's AAA subscriber record together with the client's DHCP parameters to select the IP address pool used for address assignment.

DHCP local server also supports RADIUS accounting, including interim accounting, in standalone mode. This feature allows you to use RADIUS start and stop attributes to track user events such as the lifetime of an IP address.

## DHCP Local Server and Client Configuration

You can use DHCP to configure the router to allow remote access to non-PPP clients. DHCP-based access is also an alternative to PPP in environments such as Public Wireless LANs (PWLANS). In PWLANS, a user scans for available broadband networks, then is redirected to a web-based authentication mechanism to request service.

DHCP provides address assignment information for users. Authentication, authorization, and accounting are separate processes, and are up to the Internet service provider (ISP) to define.

The DHCP local server can configure a client with the following DHCP options:

- Default router
- DNS server
- Domain name
- Lease time
- Grace period for address lease
- NetBIOS name server
- NetBIOS node type
- Subnet mask

**Related  
Documentation**

- [Equal-Access Mode Overview on page 4](#)
- [Standalone Mode Overview on page 6](#)
- [DHCP Local Server Prerequisites on page 8](#)
- [DHCP Local Server Configuration Tasks on page 9](#)
- [Viewing and Deleting DHCP Client Bindings](#)

---

## Equal-Access Mode Overview

In equal-access mode, the router enables access to non-PPP users. Non-PPP equal access requires the use of the router's DHCP local server and SRC software, which communicates with a RADIUS server.

The DHCP local server performs the following functions in equal-access mode:

- Communicates with SRC software.
- Assigns an IP address that enables the subscriber to access services.

## Local Pool Selection and Address Allocation

The DHCP local server selects a DHCP pool from which to allocate an address using a number of parameters in a certain predefined sequence. The router compares the parameters with the local DHCP pools in the order presented in [Table 3 on page 5](#). When the router finds a match, it selects a pool based on the match and does not examine other parameters.

**Table 3: Local Pool Selection in Equal-Access Mode**

Field	How the DHCP Local Server Uses the Field
Framed IP address	<p>The client's entry can be configured with a framed IP address, which the DHCP local server can get from the SRC software (formerly the SDX software).</p> <p>If the router selects a pool using a framed IP address, the DHCP local server attempts to allocate the framed IP address from the pool. If the framed IP address is not available, then the server allocates the next available address in the pool to the client.</p>
Pool name	Each DHCP local pool has a pool name. The client's entry can also be configured with a pool name, which the DHCP local server can get from the SRC software. The SRC software must be configured to send RADIUS attributes to DHCP.
Domain name	<p>You can use a domain name as the name of a DHCP local pool. If the client logs onto the SRC software and RADIUS authenticates the client using a domain name, the DHCP local server receives the domain name from the SRC software.</p> <p>If the client's domain name does not match the name of the DHCP local pool, the router attempts to match the client's domain name to the domain name field within the pool.</p>
Giaddr	A DHCP local pool is configured with a network address. A gateway IP address (giaddr), which indicates a client's subnetwork, can be presented to the DHCP local server in the client's DHCP request message. The giaddr field in the DHCP request message contains the IP address of a DHCP relay agent. The router attempts to match the giaddr address in the DHCP request message with the network address of a DHCP local pool.
Received interface IP address	The router uses the IP address of the interface on which the DHCP packet is being processed and attempts to match it with the network address of a DHCP local pool. If the interface address matches with the IP address configured in the DHCP local address pool on the router, that pool is used to delegate the address to the client.

## The Connection Process

The following sequence describes how the subscriber connects to the network for the first time using equal-access mode. [Figure 1 on page 6](#) illustrates the process.

1. The subscriber's computer boots and issues a DHCP request.
2. The DHCP local server uses the SRC client to issue a COPS request to retrieve address pool information.
3. After standard DHCP negotiations, the DHCP local server supplies an IP address to the subscriber's computer from a local address pool, as described in the previous section.

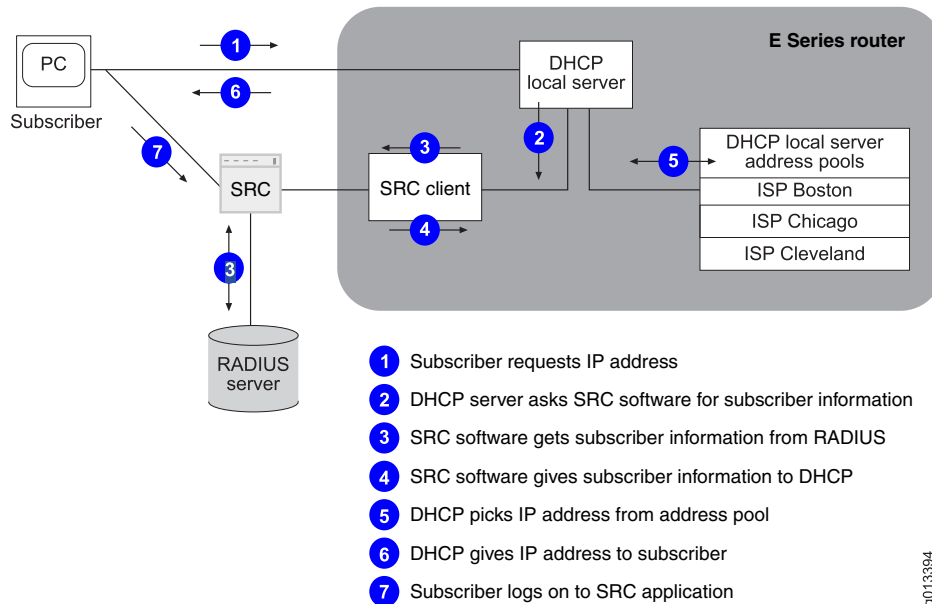
The router maintains a host route that maps the IP address to the router's interface associated with the subscriber's computer.

4. The subscriber's computer retains the IP address until the subscriber turns off the computer.



**NOTE:** If a DHCP client attempts to renew its address and the DHCP server receives the request on a different interface than the interface that the client originally used, the DHCP server sends a NAK message to the client, forcing the client to begin the DHCP connection process again.

Figure 1: Non-PPP Equal Access via the Router



#### Related Documentation

- [Embedded DHCP Local Server Overview on page 3](#)
- [Standalone Mode Overview on page 6](#)
- [DHCP Local Server Prerequisites on page 8](#)
- [DHCP Local Server Configuration Tasks on page 9](#)

## Standalone Mode Overview

In standalone mode, the DHCP local server operates as a basic DHCP server. Clients are not authenticated by default; however, you can optionally configure the DHCP local server to use AAA authentication for the incoming clients. The DHCP local server receives DHCP client requests for addresses, selects DHCP local pools from which to allocate addresses, distributes addresses to the clients, and maintains the resulting DHCP bindings in a server management table.

### Local Pool Selection and Address Allocation

In standalone mode, the DHCP local server selects a pool to allocate an address for a client; the SRC software is never notified or queried. The process used depends on whether AAA authentication is configured.

- If AAA authentication is not configured, the DHCP local server selects a pool by matching the local pool network address to the giaddr or the received interface IP address. The router compares the parameters with the local DHCP pools in the order presented in [Table 4 on page 7](#). When the router finds a match, it selects a pool based on the match and does not examine other parameters.

**Table 4: Local Pool Selection in Standalone Mode Without AAA Authentication**

Field	How the DHCP Local Server Uses the Field
Giaddr	A giaddr, which indicates a client's subnetwork, can be presented to the DHCP local server in the client DHCP REQUEST message. The giaddr field in the DHCP request message usually contains the IP address of a DHCP relay agent. The router attempts to match the giaddr address in the DHCP request message with the network address of a DHCP local pool. If it finds a match, the router uses the matching DHCP local pool.
Received interface IP address	The router uses the IP address of the interface on which the DHCP packet is being processed and attempts to match it with the network address of a DHCP local pool.

After the router selects a DHCP local pool, the DHCP local server first tries to find a reserved IP address for the client in the selected pool. If no reserved address is available, the router attempts to allocate a client's requested IP address. If the requested IP address is not available, the router allocates the next available address in the pool. If a grace period is configured for the pool, the router assigns the grace period to the allocated address. If no addresses are available in a pool, the DHCP local server attempts to allocate an address from the linked pool, if such a pool is configured.

- If AAA authentication is configured (as described in [“Configuring AAA Authentication for DHCP Local Server Standalone Mode” on page 29](#)) and the authentication is successful, the local server selects an IP address pool based on the order presented in [Table 5 on page 7](#). When the router finds a match, it selects a pool based on the match and does not examine other parameters.

**Table 5: Local Pool Selection in Standalone Mode with AAA Authentication**

Field	How the DHCP Local Server Uses the Field
Framed IP address	<p>The client's RADIUS entry can be configured with a framed IP address, which the DHCP local server can get from the AAA server when the client is authenticated.</p> <p>If the AAA server specifies a framed IP address, the DHCP local server attempts to allocate the address pool that contains the framed IP address and allocates that address from the pool. If the framed IP address is not available, then the server allocates the next available address in the pool to the client.</p>
Pool name	<p>Each DHCP local pool has a pool name. The client's RADIUS entry can also be configured with a pool name, which the DHCP local server can get from the AAA server when the client is authenticated. The AAA server must be configured to send RADIUS attributes to DHCP.</p> <p>If AAA specifies an address pool name, the local server finds the pool with the matching name and allocates an address from that pool.</p>

Table 5: Local Pool Selection in Standalone Mode with AAA Authentication (*continued*)

Field	How the DHCP Local Server Uses the Field
Domain name	<p>You can use a domain name as the name of a DHCP local pool. If RADIUS authenticates the client using a domain name, the DHCP local server receives the domain name from the AAA server.</p> <p>If the client's domain name does not match the name of the DHCP local pool, the router attempts to match the client's domain name to the domain name field within the pool.</p>
Giaddr	A DHCP local pool is configured with a network address. A gateway IP address (giaddr), which indicates a client's subnetwork, can be presented to the DHCP local server in the client's DHCP request message. The giaddr field in the DHCP request message usually contains the IP address of a DHCP relay server. The router attempts to match the giaddr address in the DHCP request message with the network address of a DHCP local pool.
Received interface IP address	The router uses the IP address of the interface on which the DHCP packet is being processed and attempts to match it with the network address of a DHCP local pool. If the interface address matches with the IP address configured in the DHCP local address pool on the router, that pool is used to delegate the address to the client.

## Server Management Table

For each client that makes requests of the DHCP local server, the router keeps an entry in the server management table. The entry defines client-specific information and state information. The router uses this table to identify clients when it receives subsequent messages and to maintain the state of each client within the DHCP protocol. In addition, the table contains information that may be transferred to and from the SRC software.

### Related Documentation

- [Embedded DHCP Local Server Overview on page 3](#)
- [Equal-Access Mode Overview on page 4](#)
- [DHCP Local Server Prerequisites on page 8](#)
- [DHCP Local Server Configuration Tasks on page 9](#)

## DHCP Local Server Prerequisites

Before you configure DHCP local server, you need to configure interfaces. You can configure ATM or Ethernet interfaces for DHCP local server. These interfaces can be numbered or unnumbered. Because subscribers connect to the router from different subnetworks, you must configure an IP address for each subnetwork on the interface. This action provides connectivity between the subnetwork and the router.

To configure a numbered IP address for DHCP local server:

1. Select an ATM or Ethernet interface.
2. Assign the primary IP address for one subnetwork to this interface.
3. Assign secondary IP addresses for all other subnetworks to this interface.

To configure an unnumbered IP address for DHCP local server:

1. Specify a loopback interface.
2. Assign the primary IP address for one subnet to the loopback interface.
3. Assign secondary IP addresses for all other subnets to the loopback interface.
4. Select an ATM or Ethernet interface.
5. Configure an unnumbered IP address associated with the loopback interface on the ATM or Ethernet interface.

For information about defining IP addresses, see the *Configuring IP* chapter in *JunosE IP, IPv6, and IGP Configuration Guide*.

- Related Documentation**
- [IP Profiles](#)
  - [Setting Up an Unnumbered Interface](#)

---

## DHCP Local Server Configuration Tasks

---

This section covers the configuration tasks for equal-access and standalone modes. Perform the appropriate procedure:

1. For both equal-access and standalone modes, configure the DHCP local server.  
[See “Configuring AAA Authentication for DHCP Local Server Standalone Mode” on page 29](#) for a sample configuration.
2. For standalone mode, optionally configure the router to use AAA authentication for DHCP requests from subscribers.  
[See “Configuring AAA Authentication for DHCP Local Server Standalone Mode” on page 29](#) for a sample configuration.
3. For non-PPP equal access, configure the router to work with the SRC software.  
[See “Configuring the Router to Work with the SRC Software” on page 41](#) for a sample configuration.

- Related Documentation**
- [Embedded DHCP Local Server Overview on page 3](#)
  - [Equal-Access Mode Overview on page 4](#)
  - [Standalone Mode Overview on page 6](#)





## CHAPTER 2

# DHCP Unique IDs for DHCPv6 Clients and Servers

- [DHCP Unique ID for Clients and Servers Overview on page 11](#)

## DHCP Unique ID for Clients and Servers Overview

---

Each entity in a DHCP operation, the client and the server, has a DHCP unique identifier (DUID). DHCP clients use DUIDs to identify a server in messages where a server needs to be identified. DHCP servers use DUIDs to determine the configuration parameters to be used for clients and in the association of addresses with clients.

The DUID is contained in the client identifier and server identifier options. The DUID is stable for any specific client or server. The DHCPv6 application uses DUIDs based on link-layer addresses for both the client and server identifier options. An Identity Association for Prefix Delegation option is a collection of prefixes assigned to a requesting router. A requesting router can have more than one Identity Association for Prefix Delegation option; for example, one for each of its interfaces. Each Identity Association for Prefix Delegation is denoted by an Identity Association identifier. The Identity Association identifier is chosen by the requesting router and is unique among the Identity Association identifiers that are present in the Identity Association for Prefix Delegation options on the requesting router. A client binding is indexed by a DUID.

When an IPv6 DHCP client requests two prefixes with the same DUID but different Identity Association identifiers on two different interfaces, these prefixes are considered to be for two different clients, and the interface information is maintained for both the clients. Clients and servers identify DUIDs as opaque values and compare DUIDs only to check for their equality. Clients and servers do not process DUIDs for other information.

A DUID consists of a two-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 (DUID-EN)
- Type 3—Link-layer address (DUID-LL)

The Type 1 DUID consists of a two-octet type field that contains the value 1, a two-octet hardware type code, four 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 Type 2 DUID is assigned by the vendor to the device and contains the vendor's registered private enterprise number as maintained by the IANA, followed by a unique identifier assigned by the vendor.

The Type 3 DUID contains a two-octet type field that stores the value 3, a two-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.

By default, the DHCPv6 local server application in JunosE Software uses the Type 2 server DUID for allocation of IPv6 prefixes from the delegating router, which is an E Series router configured as a DHCPv6 local server to requesting routers, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client. In scenarios in which the CPE does not support the Type 2 DUID, or if the service provider uses a DUID type other than Type 2, the verification of identity of servers and clients by each other using DUIDs does not happen successfully. In such network environments, configuring the DUID type on the DHCPv6 local server to be other than the default value of Type 2 enables correct identity verification of clients and servers.

You can configure the type of DUID using the **ipv6 dhcpv6-local duid-type** *duidType* command in Global Configuration mode to be either Type 2 or Type 3. These two types are currently supported by the DHCPv6 local server application in JunosE Software. The Type 1 DUID is not supported by the DHCPv6 local server in JunosE Software. However, DHCPv6 clients support DUID Types 1, 2, and 3. The **ipv6 dhcpv6-local duid-type** command enables you to specify the DUID type that matches with the DUID type that the service providers use in their networks and also provides flexibility to DHCP subscribers to use a DUID type that suits their requirements. The DHCPv6 local server uses the configured DUID type in its communication with the client.

The DUID type conforms to the following guidelines:

- The DUID type is unique across all the virtual routers on the chassis.
- The DUID type is persistent across a system reload.
- The DUID type is retained after a switchover.
- You cannot modify the DUID type when at least one active DHCP client connection exists.

To support the Type 3 DUID, the DHCPv6 local server uses a combination of the chassis ID and virtual router ID as the DUID. When you remove the configured DUID type using the **no ipv6 dhcpv6-local duid-type** command, the router reverts to the default Type 2 DUID. All the binding requests from the clients are acknowledged with the default server ID if the Type 2 DUID is on the DHCPv6 local server.

**Related  
Documentation**

- [Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers on page 37](#)
- [ipv6 dhcpv6-local duid-type on page 69](#)

## CHAPTER 3

# AAA Authentication for DHCPv6 Local Server Standalone Mode

- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
- [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)

## Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview

---

You can use the DHCPv6 local server to perform authentication and accounting of IPv6 subscribers that are directly connected using Ethernet VLAN links to the router. For PPP subscribers, authentication and accounting operations are performed by the underlying PPP module; the DHCPv6 local server only delegates IPv6 prefixes to requesting clients. IPv6 subscribers that are connected over PPP links and IPv6 subscribers that are connected over Ethernet and VLAN interfaces can coexist on a virtual router when you configure the DHCPv6 local server for standalone mode with AAA authentication.

For PPP subscribers, the PPP module authenticates users during the establishment of the PPP session and sends the authentication token to the DHCPv6 local server for allocation of IPv6 prefixes. For IPv6 subscribers, the DHCPv6 local server performs the AAA authentication of clients that are logging in. Prefix delegation for IPv6 subscribers occurs only if the prefix is configured on the interface or if the interface address matches with any of the prefix ranges configured in the IPv6 local address pool on the router. When you configure standalone mode with AAA authentication for the DHCPv6 local server, delegation of prefixes is performed based on the Access-Accept and Access-Reject messages the AAA server sends in response to the client authentication request.

The DHCPv6 local server enables you to optionally configure AAA-based authentication of standalone mode DHCPv6 clients. By default, clients are not authenticated in standalone mode. Typically, an incoming DHCPv6 client does not provide a username—therefore, the DHCPv6 local server constructs a username based on the user's attachment parameters and optional DHCP parameters. AAA uses the constructed username to authenticate the incoming client and create the AAA subscriber record for the client. The information in the AAA subscriber record is then used to determine the IP address pool from which to assign the address for the DHCP client.

You can include the following parameters in the username:

- User prefix
- Circuit type
- Circuit identifier
- Domain name

The complete format of the username is as follows:

*user-prefix.circuit-type.circuit-identifier@domain*

The elements of the username are defined as follows:

- user-prefix—A configured string per DHCPv6 local server.
- circuit-type—Specifies the circuit type of the interface on which the DHCPv6 client's request was received. Possible values are atm, eth, or vlan.
- circuit-identifier—Specifies the circuit identifier of the interface on which the DHCPv6 client's request was received. The interface identifier has one of the following formats:
  - atm—slot.port.vpi.vci
  - eth—slot.port.0.0
  - vlan—slot.port.svlan.vlan
- domain—Name of the user domain for each DHCPv6 local server.

You can construct the username by using only the user-prefix attribute, using a combination of the user-prefix and domain attributes, or using other optional attributes that are specified. If you remove the domain configuration, the '@' character is removed from the username. The username is valid only when the nondomain portion consists of at least one character, either using the configuration of a non-null user-prefix or using the inclusion of at least one optional username parameter.

The authentication process starts before the Advertise message is sent from the DHCPv6 local server to the client. If the authentication of the subscriber is successful, the DHCPv6 local server sends the Advertise packet to the client in response to DHCPv6 Solicit messages that are received from the client. When the authentication request is sent to the AAA server, the DHCPv6 local server includes the constructed username, password, interface ID, authentication type, and the interface on which the request was received from the user. The AAA server uses this information during authentication and accounting updates. The authentication and accounting attributes that are sent to the RADIUS server are based on RADIUS attributes configured for inclusion in RADIUS messages using the **radius include** command.

This mode of operation for the DHCPv6 local server is called standalone mode with AAA authentication. The default mode of operation for the DHCPv6 local server is standalone mode without AAA authentication that interoperates with the existing capabilities of PPP and non-PPP subscribers.

## Accounting for IPv6 Subscribers with DHCPv6 Local Server Standalone Mode

The PPP application handles the transmission of accounting information to the AAA server. The DHCPv6 local server uses the authentication token that the AAA server generates while authenticating the IPv6 user to send the interim accounting updates to the AAA server. The starting and termination of accounting is performed during the authentication phase based on the receipt of the DHCP release packets from clients or the lease expiration of the assigned address.

The Acct-Start message is sent to the RADIUS server after the AAA server receives the message about successful authentication. You can use the **aaa service accounting interval** command to specify the default service interim accounting interval. Service Manager uses this interval value for service accounting when the Service-Interim-Acct-Interval attribute is not configured. Based on the configured interval, the DHCPv6 local server generates interim accounting information. The Acct-Stop message is sent to the RADIUS server when a client binding is removed. The accounting functionality of the DHCPv6 local server is similar to the accounting operations of the DHCPv4 local server.

### Related Documentation

- [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)
- [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)
- [Monitoring DHCPv6 Local Server Authentication Information on page 109](#)

## Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information

The following cases describe the behavior of the **show subscribers** command, used to view details on active subscribers logged in to the router, when AAA and RADIUS authentication mechanisms are used to authenticate IPv6 subscribers:

- If you do not disable AAA authentication on the default router for IP subscribers by using the **aaa authentication ip default none** command and do not map the domain name of the user with the virtual router by using the **aaa domain-map** command, details regarding the logged-in subscribers are not displayed in the output of the **show subscribers** and **show subscribers ipv6** commands. In such cases, you can use the output of the **show subscribers summary** command to view the summary information of the subscribers that are logged in.
- If you disable AAA authentication on the default router for IP subscribers by entering the **aaa authentication ip default none** command and map the domain name of the user with the virtual router by using the **aaa domain-map** command, you can view the details of the active subscribers using the output of the **show subscribers**, **show subscribers ipv6**, and **show subscribers summary** commands.
- If you configure RADIUS authentication for IP subscribers on the default router by using the **aaa authentication ip default radius** command and the Virtual-Router VSA attribute [26-1] is returned from the RADIUS server in the Access-Accept message, the subscriber details are displayed in the output of the **show subscribers** command. Also, you can

use the **show subscribers summary** command to view the consolidated information on active subscribers.

- If you configure RADIUS authentication for IP subscribers on the default router by using the **aaa authentication ip default radius** command and the Ipv6-Virtual-Router VSA attribute [26-45] is returned from the RADIUS server in the Access-Accept message, the subscriber details are displayed in the output of the **show subscribers ipv6** command. Also, you can use the **show subscribers summary** command to view the consolidated information on active subscribers.

**Related  
Documentation**

- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
- [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)
- [Monitoring DHCPv6 Local Server Authentication Information on page 109](#)
- *show subscribers*
- *aaa authentication default*
- *aaa domain-map*

## PART 2

# Configuration

- [Configuration Tasks for DHCPv4 Local Server on page 19](#)
- [Configuration Tasks for DHCPv6 Local Server on page 33](#)
- [Removal of DHCPv6 Client Bindings on page 39](#)
- [Interoperation of SRC Client and DHCP Local Server on page 41](#)
- [Configuring Baselines for DHCP Local Server Statistics on page 45](#)
- [Configuration Commands on page 47](#)





## CHAPTER 4

# Configuration Tasks for DHCPv4 Local Server

- [Configuring DHCP Local Address Pools on page 19](#)
- [Configuring the DHCP Local Server on page 23](#)
- [Configuring AAA Authentication for DHCP Local Server Standalone Mode on page 29](#)

## Configuring DHCP Local Address Pools

---

Tasks to configure DHCP local address pool include:

- [Basic Configuration of DHCP Local Address Pools on page 19](#)
- [Linking Local Address Pools on page 21](#)
- [Setting Grace Periods for Address Leases on page 21](#)

### Basic Configuration of DHCP Local Address Pools

To configure the DHCP local address pool:

1. Specify the pool name and access DHCP Local Pool Configuration mode.

```
host1(config)#ip dhcp-local pool ispBoston
host1(config-dhcp-local)#
```

2. Specify the IP address of the router for the subscriber's computer to use for traffic destined for locations beyond the local subnetwork.

```
host1(config-dhcp-local)#default-router 10.10.1.1
```

The default router must be on the same subnetwork as the local server pool IP addresses that you configure with the **network** command.

You specify the IP address of a primary server, and optionally, the IP address of a secondary server.

3. (Optional) Assign a DNS server to an address pool. Some DHCP clients request the DHCP local server to assign a DNS server.

```
host1(config-dhcp-local)#dns-server 10.10.1.1
```

4. (Optional) Specify a domain name that can be returned to the subscriber if requested.

```
host1(config-dhcp-local)#domain-name ispBoston
```

The name of the domain must match the name you specified for the RADIUS vendor-specific attribute (VSA) and for authentication, authorization, accounting, and address assignment.

5. Specify the time period for which the supplied IP address is valid.

```
host1(config-dhcp-local)#lease 0 0 24
```

Specify the number of days, and optionally, the number of hours, minutes, and seconds. Use the keyword **infinite** to specify a lease that does not expire. The default lease time is 30 minutes.

6. (Optional) Link the DHCP local address pool being configured to another local address pool. See [“Linking Local Address Pools” on page 21](#) for more information about linking local address pools.

```
host1(config-dhcp-local)#link ispChicago
```

7. (Optional) Assign a NetBIOS server for subscribers. Some DHCP clients request the DHCP local server to assign a NetBIOS server.

```
host1(config-dhcp-local)#netbios-name-server 10.10.1.1 10.10.1.2
```

Specify the IP address of a primary server and, optionally, the address of a secondary server.

8. (Optional) Specify NetBIOS node type.

```
host1(config-dhcp-local)#netbios-node-type b-node
```

Specify one of the following types of NetBIOS nodes. By default, the node type is unspecified.

- **b-node**—Broadcast
- **p-node**—Peer-to-peer
- **m-node**—Mixed
- **h-node**—Hybrid

9. Specify the IP addresses that the DHCP local server can provide from an address pool.

```
host1(config-dhcp-local)#network 10.10.1.0 255.255.0.0
```

Use the **force** keyword with the **no** version of the command to delete the address pool even if the pool is in use.

10. For both equal-access and standalone modes, you can reserve an IP address for a specific MAC address.

```
host1(config-dhcp-local)#reserve 10.10.13.8 0090.1a10.0552
```

11. For standalone mode, you can specify the DHCP server address that is sent to DHCP clients.

```
host1(config-dhcp-local)#server-address 10.10.20.0
```

12. (Optional) Enable Simple Network Management Protocol (SNMP) traps for local address pool utilization, including normal, linked, and shared address pools. Traps are generated based on threshold values for utilization. You can define threshold values

by using the warning command. See [“Using SNMP Traps to Monitor DHCP Local Server Events” on page 27](#) for more information about SNMP and local address pools.

```
host1(config-dhcp-local)#snmpTrap
host1(config-dhcp-local)#warning 50 40
```

13. (Optional) Configure a grace period for address leases allocated from the current DHCP local address pool. Specify the number of days and, optionally, the number of hours, minutes, and seconds in the grace period.

```
host1(config-dhcp-local)#grace-period 0 12
```

This command applies only to address leases that expire. Use the **use-release-grace-period** command to also apply the configured grace period to the local pool addresses that are explicitly released by clients. See [“Setting Grace Periods for Address Leases” on page 21](#) for more information about grace periods.

14. (Optional) Specify that the grace period is applied to addresses that have been explicitly released by clients. By default, the grace period is applied only to address leases that expire, not to addresses that have been released. See [“Setting Grace Periods for Address Leases” on page 21](#) for more information about grace periods.

```
host1(config-dhcp-local)#use-release-grace-period
```

## Linking Local Address Pools

In both equal-access mode and standalone mode, you can link a DHCP local pool to another local pool. The linked pool serves as a backup pool. If no addresses are available in a pool, the DHCP local server attempts to allocate an address from the linked pool. The address pools that are linked are viewed as a group.

## Setting Grace Periods for Address Leases

The JunosE Software enables you to configure a grace period for a particular local address pool—the grace period is applied to all address leases associated with the address pool. The grace period is the amount of time that a client continues to retain its address lease after the lease expires or is released. An address cannot be assigned to any other client during the grace period. When the grace period expires, the address is released back to the address pool.

Grace periods help to ensure that a DHCP client retains its previously assigned IP address in situations that might normally cause a lease termination followed by a new address assignment. For example, if a client loses its lease due to a network disruption, the grace period enables the client to be reassigned the same address when the client requests an address after the network stabilizes. Grace periods are also useful during client reboots and in cases where a non-compliant or unreliable DHCP implementation triggers a lease renewal.

You configure a grace period for a local address pool. The grace period is immediately applied to all addresses that are allocated from the pool, including previously allocated addresses that are currently active—the new grace period takes precedence over a previously configured grace period for the address pool.



**NOTE:** Configuring a new grace period that is shorter than the address pool current grace period immediately terminates any existing address leases that are in the grace period state and that have already exceeded the length of the new grace period.

An address continues to be counted against the address pool resources while in a grace period. For example, if the address pool is exhausted, a new address cannot be assigned to other clients.

Client address leases enter the grace period in two ways—the lease might expire or the address can be explicitly released by the client. In both cases the address remains unavailable to other clients and can only be reapplied to the original client during the grace period. The address is released back to the address pool if the grace period expires before the address is reapplied to the original client.

When you configure a grace period, by default it is applied to address leases that *expire*, but not to addresses that are *released* by clients. However, you can optionally apply the grace period to released addresses.

#### Related Documentation

- [Linking Local Address Pools on page 21](#)
- [Setting Grace Periods for Address Leases on page 21](#)
- [SNMP Traps to Monitor DHCP Local Server Events](#) section in [Configuring the DHCP Local Server on page 23](#)
- [default-router on page 52](#)
- [dns-server on page 53](#)
- [domain-name on page 54](#)
- [grace-period on page 55](#)
- [ip dhcp-local pool on page 56](#)
- [lease on page 76](#)
- [link on page 77](#)
- [netbios-name-server on page 80](#)
- [netbios-node-type on page 81](#)
- [network on page 82](#)
- [reserve on page 84](#)
- [server-address on page 85](#)
- [snmpTrap on page 88](#)
- [use-release-grace-period on page 89](#)
- [warning on page 90](#)

## Configuring the DHCP Local Server

Tasks to configure the DHCP local server include:

- [Basic Configuration of DHCP Local Server on page 23](#)
- [Limiting the Number of IP Addresses Supplied by DHCP Local Server on page 24](#)
- [Excluding IP Addresses from Address Pools on page 25](#)
- [Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces on page 25](#)
- [Differentiating Between Clients with the Same Client ID or Hardware Address on page 25](#)
- [Logging Out DHCP Local Server Subscribers on page 27](#)
- [Clearing an IP DHCP Local Server Binding on page 27](#)
- [Using SNMP Traps to Monitor DHCP Local Server Events on page 27](#)
- [Using DHCP Local Server Event Logs on page 28](#)

### Basic Configuration of DHCP Local Server

Before you configure a DHCP local server, you must identify which mode to activate (standalone mode or equal-access mode). Use equal-access mode, if you use the Session and Resource Control (SRC) software for address allocation and managing the subscribers. If you do not use SRC for managing subscribers, use standalone mode. SRC contributes to the address pool selection and so when you use standalone mode, SRC is not used for address allocation.

If you do not specify a mode, equal-access mode is activated, by default. When you activate equal-access mode, common open policy service usage for policy provisioning (COPS-PR) and SRC client are automatically started on the virtual router.

To configure the DHCP local server:

1. Enable the DHCP local server for either equal-access or standalone mode.
 

```
host1(config)#service dhcp-local equal-access
host1(config)#service dhcp-local standalone
```
2. (Optional) Specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or to a particular interface or subinterface. See [“Limiting the Number of IP Addresses Supplied by DHCP Local Server” on page 24](#) for more information about limiting the number of IP addresses.
 

```
host1(config)#ip dhcp-local limit ethernet 6
```
3. (Optional) Specify any addresses that the DHCP local server must not assign. See [“Excluding IP Addresses from Address Pools” on page 25](#) for more information.



**NOTE:** You can specify this command multiple times on the CLI and the excluded address must fall within a network that has been specified in the DHCP local pool.

**host1(config)#ip dhcp-local excluded-address 10.10.3.4**

4. (Optional) Enable general DHCP local server traps. See [“Using SNMP Traps to Monitor DHCP Local Server Events” on page 27](#).

**host1(config)#ip dhcp-local snmpTraps**

5. (Optional) Configure the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages. See [“Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces” on page 25](#).

**host1(config)#ip dhcp-local auto-configure agent-circuit-identifier**

6. (Optional) Specify that DHCP local server use an optional method to differentiate between clients with duplicate client IDs or hardware addresses. Any changes you make have no effect on currently bound clients. See [“Differentiating Between Clients with the Same Client ID or Hardware Address” on page 25](#).

**host1(config)# ip dhcp-local unique-client-ids**

7. Configure the DHCP local address pool that supplies IP addresses to subscribers who want to access a domain. See [“Configuring DHCP Local Address Pools” on page 19](#) for more information about configuring address pools.

## Limiting the Number of IP Addresses Supplied by DHCP Local Server

You can specify the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or POS access interface type, or to a particular interface or subinterface.

You can set global limits for a given interface type—all interfaces of that type that are subsequently created, whether dynamically or statically, inherit that limit value.

You can also set an individual interface limit for a specific interface and override the global limit configured for that interface type. For example, suppose the VLAN interface type limit is five. You can specify a limit of 10 for the VLAN interface FastEthernet 1/0.100. All other VLAN interfaces retain the global limit of five.

The global limits for interface types and the individual interface limits set on static interfaces are kept in NVS. These values are restored during a switchover or a reload.

When you assign an individual limit to a dynamic interface, that limit is in force only until either a switchover or reload takes place. After the switchover or reload, if the action that caused the dynamic interface to be created occurs again, a new dynamic interface is created. The new dynamic interface then inherits the limit set by the global values based on the type of interface that is created.

- To set a global limit for an interface type:

**host1(config)#ip dhcp-local limit ethernet 6**

- To set a limit for a specific interface:

**host1(config)#ip dhcp-local limit interface atm 3/1 15**



**NOTE:** Limits that you specify on dynamic interfaces are not restored after a switchover or reboot.

## Excluding IP Addresses from Address Pools

You can use the **ip dhcp-local excluded-address** command to specify IP addresses that you do not want the DHCP local server to supply from the default address pool. You might exclude addresses if because those addresses are already used by devices on the subnet.

You can exclude a single IP address or a range of addresses. To exclude a range, you specify the start-of-range IP address and the end-of-range IP address.

- To exclude a specific IP address:

```
host1(config)#ip dhcp-local excluded-address 10.10.3.4
```

- To exclude a range of IP addresses:

```
host1(config)#ip dhcp-local excluded-address 10.10.3.4 10.10.3.100
```

## Configuring DHCP Local Server to Support Creation of Dynamic Subscriber Interfaces

You can use the **ip dhcp-local auto-configure agent-circuit-identifier** command to configure the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages.

- Use this command within a specific virtual router context.
- This command requires that the user's DHCP control traffic and data traffic traverse the same client-facing ingress port on the E Series router.

The use of the option 82 field enables you to stack an IP interface that is associated with a particular subscriber over a dynamically created VLAN; the VLAN is dynamically created based on the agent-circuit-id option (suboption 1) that is contained in the DHCP option 82 field.

For information about configuring agent-circuit-id-based dynamic VLAN subinterfaces, see the *Configuring Dynamic Interfaces Using Bulk Configuration* chapter in *JunosE Link Layer Configuration Guide*.

## Differentiating Between Clients with the Same Client ID or Hardware Address

A JunosE Software feature enables the DHCP local server to create unique client IDs to support roaming clients and to manage situations in which two clients in the network have the same hardware address.



**NOTE:** This feature replaces the previous router behavior for DHCP local server client roaming and duplicate address support. The `ip dhcp-local unique-client-ids` command replaces the `ip dhcp-local inhibit-roaming` command, which has been removed from the CLI and has no effect on the DHCP local server.

You can configure the method DHCP local server uses when the router receives a DISCOVER or REQUEST packet that contains a client ID or hardware address that matches the ID or address of a currently bound client on another subnet or subinterface.

In the default configuration, the DHCP local server uses the DHCP client's subnet or subinterface to differentiate duplicate clients and support client roaming. When a new client, with a duplicate ID or hardware address, requests an address lease, DHCP assigns that client a new address and lease—the existing client's lease is unchanged.

The following table describes how the DHCP local server differentiates between a new DHCP client with the same ID or hardware address as a currently bound DHCP client. The determination is based on whether the DHCP clients exist on the same or on different subnets and subinterfaces.

Location of DHCP Clients with Identical IDs or Addresses	How DHCP Local Server Differentiates Clients
On different subinterfaces in the same subnet	By unique subinterface
On the same subinterface in different subnets	By unique subnet
On different subinterfaces in different subnets	By unique subinterface and unique subnet
On the same subinterface in the same subnet	DHCP local server <i>cannot distinguish clients</i> with identical IDs or identical hardware addresses in this configuration

In the optional configuration, you use the `ip dhcp-local unique-client-ids` command to disable the use of the DHCP client's subnet or subinterface to differentiate between clients with duplicate client IDs or hardware addresses. When DHCP receives the request from a duplicate ID or address, DHCP terminates the address lease for the existing client and returns the address to its original address pool. DHCP then assigns a new address and lease to the new client.

We strongly recommend that you enable the `ip dhcp-local unique-client-ids` command in the following situations:

- When duplicate client IDs and duplicate hardware addresses do not exist in your network



- When the DHCP local server application interacts with DHCP relays in your network that do not support duplicate client IDs or duplicate hardware addresses

Enabling the **ip dhcp-local unique-client-ids** command in these cases enables you to properly manage DHCP clients that roam to different subnets.

The DHCP relay agent application and the DHCP relay proxy application do not support duplicate client IDs or duplicate hardware addresses.

## Logging Out DHCP Local Server Subscribers

You can use the **logout subscribers** command from Privileged Exec mode to log out DHCP local server subscribers. For example, you might use this feature if you want to force a user to request a new lease or if you want to recover functional resources. The **logout subscribers** command, unlike the **clear ip address binding** command (described in “Clearing an IP DHCP Local Server Binding” on page 27), does not terminate the subscriber’s user session or management representation.

This command applies to DHCP local server local-access and standalone clients, as well as to PPP users. You can log out **all** subscribers, or log out subscribers by **username**, **domain**, **virtual-router**, or **port**.

## Clearing an IP DHCP Local Server Binding



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

You can use the **clear ip dhcp-local binding** command to force the removal of a connected user’s IP address lease and associated route configuration. Using this command enables you to:

- Recover functional resources from a user who has not explicitly terminated connectivity and whose lease is unexpired.
- Discontinue connectivity to a user, prompting or forcing the user to request a new lease in order to reestablish network connectivity.

## Using SNMP Traps to Monitor DHCP Local Server Events

The DHCP local server supports configurable global SNMP traps that monitor events related to the DHCP local server and local SNMP traps that are related to address pool utilization. You use the **ip dhcp-local snmpTraps** command to enable the global SNMP traps for DHCP local server.

The DHCP local server’s global SNMP trap generates severity level 1 (alert), 2 (critical), and 3 (error) events. This trap helps administrators monitor DHCP local server general health, error statistics, address lease status, and protocol events. The global SNMP trap generates a severity level 4 (warning) event when a duplicate MAC address is detected. The global SNMP trap information is captured in the `dhcpLocalGeneral` logging category.

SNMP also traps events related to address pool utilization. You use the **warning** command to define the maximum and minimum threshold values and the **snmpTrap** command to generate traps when utilization occurs above or below the defined values.

For linked or shared pools, SNMP treats the members of the pool as a group, and uses the values configured for the first pool in the chain as the group's threshold.

The address pool utilization SNMP trap information is captured in the `dhcpLocalPool` logging category.



**NOTE:** You must configure your SNMP management client to read the MIB objects, and your SNMP trap collector must be capable of decoding the new traps. For information about setting up SNMP, see the *Configuring SNMP* chapter in *JunosE System Basics Configuration Guide*.

---

## Using DHCP Local Server Event Logs

To troubleshoot and monitor your DHCP local server, use the following system event logs:

- `dhcpLocalClients`—DHCP local server client events and duplicate MAC address detection
- `dhcpLocalGeneral`—DHCP local server infrastructure-related events and number of client threshold events



**NOTE:** The `dhcpLocalGeneral` category replaces the `dhcpLocalServerGeneral` category.

- 
- `dhcpLocalHighAvailability`—DHCP high availability events
  - `dhcpLocalPool`—DHCP local address pool events, including normal, linked, and shared pools
  - `dhcpLocalProtocol`—DHCP local server protocol events

See the *JunosE System Event Logging Reference Guide* for additional information about the DHCP local server logs.

### Related Documentation

- [Configuring DHCP Local Address Pools on page 19](#)
- [Configuring AAA Authentication for DHCP Local Server Standalone Mode on page 29](#)
- [clear ip dhcp-local binding on page 48](#)
- [dhcp delete-binding on page 49](#)
- [ip dhcp-local auto-configure agent-circuit-identifier on page 57](#)
- [ip dhcp-local excluded-address on page 58](#)
- [ip dhcp-local limit on page 59](#)

- [ip dhcp-local unique-client-ids on page 60](#)
- [logout subscribers on page 78](#) command
- [service dhcp-local on page 86](#)
- [ipv6 local pool on page 71](#)

## Configuring AAA Authentication for DHCP Local Server Standalone Mode

The DHCP local server enables you to optionally configure AAA-based authentication of standalone mode DHCP clients. In addition to providing increased security, AAA authentication also provides RADIUS-based input to IP address pool selection for standalone mode clients. By default, clients are not authenticated in standalone mode.

Typically, an incoming DHCP client does not provide a username—therefore, the DHCP local server constructs a username based on the user's attachment parameters and optional DHCP parameters. AAA uses the constructed username to authenticate the incoming client and create the AAA subscriber record for the client. The information in the AAA subscriber record is then used to determine the IP address pool from which to assign the address for the DHCP client. You can include the following elements in the username:

Attachment Parameters	DHCP Parameters
domain	circuit ID
user prefix	circuit type
–	MAC address
–	option 82
–	virtual router name



**NOTE:** The nondomain portion of a constructed username must contain at least one character. Otherwise, the DHCP local server rejects the DHCP client without performing the AAA authentication request.

When using authentication, AAA accepts the DHCP client as a subscriber—this enables you to use **show** commands to monitor configuration information and statistics about the client. You can also use the **logout subscriber** command to manage subscribers.

To configure AAA-based authentication for DHCP local server standalone mode clients:



**CAUTION:** Configuring authentication on the DHCP local server requires that you first disable the DHCP local server for standalone mode. Doing so removes

your entire DHCP local server configuration. Therefore, if you want to configure authentication, do so before you have otherwise configured the DHCP local server.

- .....
1. Disable the DHCP local server for standalone mode.

```
host1(config)#no service dhcp-local standalone
```

2. Enable AAA-based authentication for DHCP local server standalone mode clients.

```
host1(config)#service dhcp-local standalone authenticate
```

3. Specify the password that authenticates a locally configured DHCP standalone mode client. In DHCP standalone mode, the password is presented to AAA in an authentication request.

```
host1(config)#ip dhcp-local auth password to4tooL8
```

4. Specify the domain for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.

```
host1(config)#ip dhcp-local auth domain ISP1.com
```

5. Specify the user-prefix for a username that is locally configured for a DHCP standalone mode client. The locally configured username is presented to AAA in an authentication request.

```
host1(config)#ip dhcp-local auth user-prefix ERX4-Boston
```

6. Include optional information as part of the locally configured username for a DHCP standalone mode client. The optional information becomes part of the AAA subscriber record, and is then used to determine the IP address pool from which to assign the address for the DHCP client.

Use the following keywords to include specific information:

- **circuit-identifier**—Specifies the circuit identifier of the interface on which the DHCP client's request was received.
- **circuit-type**—Specifies the circuit type of the interface on which the DHCP client's request was received.
- **mac-address**—Specifies the DHCP client's MAC address.
- **option82**—Specifies the DHCP client's option 82 value.
- **virtual-router-name**—Specifies the DHCP local server's virtual router name.

```
host1(config)#ip dhcp-local auth include virtual-router-name
host1(config)#ip dhcp-local auth include circuit-type
host1(config)#ip dhcp-local auth include circuit-identifier
```

7. (Optional) Verify your authentication configuration.

```
host1(config)#show ip dhcp-local auth config
```

DHCP Local Server Authentication Configuration

User-Prefix : ERX4-Boston  
Domain : ISP1.com  
Password : to4TooL8  
Virtual Router : included  
Circuit Type : included  
Circuit ID : included  
MAC Address : excluded  
Option 82 : excluded

DHCP Local Server DHCP Options Configuration

RADIUS DHCP Options : excluded

**Related  
Documentation**

- [ip dhcp-local auth domain on page 61](#)
- [ip dhcp-local auth include on page 62](#)
- [ip dhcp-local auth password on page 63](#)
- [ip dhcp-local auth user-prefix on page 64](#)
- [service dhcp-local on page 86](#)



# Configuration Tasks for DHCPv6 Local Server

- [Configuring the DHCPv6 Local Server on page 33](#)
- [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)
- [Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers on page 37](#)

## Configuring the DHCPv6 Local Server

---

In addition to the embedded DHCP local server that is used for IP version 4 (IPv4) address support, E Series routers include an embedded DHCPv6 local server. This server enables the router to function as a server for the DHCP protocol for IP version 6 (IPv6). The DHCPv6 local server sends and receives packets via IPv6 and informs IPv6 of the routing requirements of the router clients.

The DHCPv6 local server provides the following IPv6 address support:

- Delegates IPv6 prefixes to client routers; each client can have one prefix; prefixes and DNS information can be locally configured or derived from RADIUS via AAA.
- Provides DNS server information to directly connected router clients.



**NOTE:** You must add a vendor-specific attribute to RADIUS to enable E Series routers to retrieve IPv6 Domain Name System (DNS) addresses.



**NOTE:** If an IPv6 prefix is not available to be delegated to requesting DHCPv6 clients, the delegating server sends the Identity Association for Prefix Delegation option, where each Identity Association for Prefix Delegation option consists of an Identity Association identifier and associated configuration information, in an Advertise message that includes a Status Code option containing the value NoPrefixAvail. For example, when a RADIUS server is used for authentication of DHCPv6 clients and the server is configured to disable the delegation of prefixes, in response to DHCPv6 Solicit messages that are received from the client, the server sends Identity Association for Prefix Delegation options in an Advertise message to the client.



**NOTE:** If you configure the IPv6 prefix to be delegated to the client using RADIUS attributes and the client is authenticated by the RADIUS server, it is not necessary to configure the prefix associated with it using this procedure. In such a scenario, the prefix derives its settings from the Framed-IPv6-Prefix [23] or the Delegated-IPv6-Prefix [97] RADIUS IETF attributes.



**NOTE:** The DHCPv6 local server supports the DHCPv6 Rapid Commit option (DHCPv6 option 14). When a DHCPv6 client includes the DHCPv6 Rapid Commit option in the Solicit messages, the server recognizes this option and the client terminates the waiting process as soon as it receives a Reply message with the Rapid Commit option from the server. The server and client then use a two-message exchange (Solicit and Reply) to configure clients, rather than the default four-method exchange (Solicit, Advertise, Request, and Reply). The two-message exchange provides faster client configuration, and is beneficial in environments in which networks are under a heavy load.

Use the following steps to configure the DHCPv6 local server:

1. Enable the DHCPv6 local server.

```
host1(config)#service dhcpv6-local
```

2. Specify the IPv6 prefix and lifetime that are to be delegated to the DHCPv6 client. The specified prefix is delegated by the DHCPv6 local server when requested by the client.

```
host1(config-if)#ipv6 dhcpv6-local delegated-prefix 2001:db8:17::/48 lifetime infinite
```

Use the **lifetime** keyword to specify the time period for which the prefix is valid. This lifetime overrides the default lifetime that is set in Global Configuration mode. If no lifetime is specified, the default lifetime is assigned.

- Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
  - Use the keyword **infinite** to specify a lifetime that does not expire.
3. Specify the name of a DNS domain for DHCPv6 clients in the current virtual router to search. You can specify a maximum of four DNS domains for a DHCPv6 local server's search list.

```
host1(config)#ipv6 dhcpv6-local dns-domain-search xyzcorporation.com  
host1(config)#ipv6 dhcpv6-local dns-domain-search xyzcorp.com
```

4. Specify the IPv6 address of the DNS server and to assign the server to the DHCPv6 clients in the current virtual router. You can specify a maximum of four DNS servers.

```
host1(config)#ipv6 dhcpv6-local dns-server 2001:db8:18::
```



- Set the default lifetime for which a prefix delegated by this DHCPv6 local server is valid. This default is overridden by an interface-specific lifetime.

**host1(config)#ipv6 dhcpv6-local prefix-lifetime infinite**

- Specify the number of days and, optionally, the number of hours, minutes, and seconds. You cannot specify a lifetime of zero (that is, you cannot set the days, hours, minutes, and seconds fields all to zero).
  - Use the keyword **infinite** to specify a lifetime that does not expire.
- Specify the DHCP unique identifier (DUID) type to be used in the communication between the DHCPv6 local server and clients. You can configure the type of DUID to be either Type 2 or Type 3. These two types are currently supported by the DHCPv6 local server application in JunosE Software. The Type 1 DUID is not supported by JunosE Software.

**host1(config)#ipv6 dhcpv6-local duid-type 3**

- (Optional) Specify the maximum number of IPv6 prefixes that the DHCPv6 local server can delegate to each ATM interface, Ethernet subnet, VLAN interface, or POS access interface, or to a particular interface of subinterface. For more information about the limiting of delegated IPv6 prefixes, see *Limiting the Maximum Number of IPv6 Prefixes Delegated Per Interface by the DHCPv6 Local Server Overview*.

- To set the maximum number of IPv6 prefixes globally for an interface type:

**host1(config)#ipv6 dhcpv6-local limit vlan 300**

- To set the maximum number of IPv6 prefixes for a particular interface:

**host1(config)#ipv6 dhcpv6-local limit interface gigabitEthernet 6/0 500**

#### Related Documentation

- *Monitoring the Maximum Number of IPv6 Prefixes Delegated Per Interface by the DHCPv6 Local Server*
- [ip dhcp-local auth domain on page 61](#)
- [ipv6 dhcpv6-local delegated-prefix on page 66](#)
- [ipv6 dhcpv6-local dns-domain-search on page 67](#)
- [ipv6 dhcpv6-local dns-server on page 68](#)
- [ipv6 dhcpv6-local duid-type on page 69](#)
- [ipv6 dhcpv6-local limit](#)
- [ipv6 dhcpv6-local prefix-lifetime on page 70](#)
- [service dhcpv6-local on page 87](#)

## Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode

When using authentication, AAA accepts the DHCPv6 client as a subscriber—this enables you to use **show** commands to monitor configuration information and statistics about the client. You can also use the **logout subscriber** command to manage subscribers.



**NOTE:** The nondomain portion of a constructed username must contain at least one character. Otherwise, the DHCPv6 local server rejects the DHCPv6 client without performing the AAA authentication request.



**CAUTION:** Configuring authentication on the DHCPv6 local server requires that you first disable the DHCPv6 local server for standalone mode. Your entire DHCPv6 local server configuration is removed when you disable the DHCPv6 local server. Therefore, if you want to configure authentication, you must set up the authentication parameters before you configure the DHCPv6 local server for other attributes.

To configure AAA-based authentication for DHCPv6 local server standalone mode clients:

1. Disable the DHCPv6 local server for standalone mode.

```
host1(config)#no service dhcpv6-local standalone
```

2. Enable AAA-based authentication for DHCPv6 local server standalone mode clients.

```
host1(config)#service dhcpv6-local standalone authenticate
```

3. Specify the password that authenticates a locally configured DHCPv6 standalone mode client. In DHCPv6 standalone mode, the password is presented to AAA in an authentication request.

```
host1(config)#ip dhcpv6-local auth password to4tooL8
```

4. Specify the domain for a username that is locally configured for a DHCPv6 standalone mode client. The locally configured user-prefix is presented to AAA in an authentication request.

```
host1(config)#ip dhcpv6-local auth domain ISP1.com
```

5. Specify the user-prefix for a username that is locally configured for a DHCPv6 standalone mode client. The locally configured username is presented to AAA in an authentication request.

```
host1(config)#ip dhcpv6-local auth user-prefix ERX4-Boston
```

6. Include optional information as part of the locally configured username for a DHCPv6 standalone mode client. The optional information becomes part of the AAA subscriber record, and is then used to determine the IP address pool from which to assign the address for the DHCPv6 client.

Use the following keywords to include specific information:

- **circuit-identifier**—Specifies the circuit identifier of the interface on which the DHCPv6 client's request was received.
- **circuit-type**—Specifies the circuit type of the interface on which the DHCPv6 client's request was received.

```
host1(config)#ipv6 dhcpv6-local auth include circuit-identifier
host1(config)#ipv6 dhcpv6-local auth include circuit-type
```

7. (Optional) Verify your authentication configuration.

```
host1(config)#show ipv6 dhcpv6-local auth config
```

```
DHCPv6 Local Server Authentication Configuration
User-Prefix      : userPrefix
Domain           : domain
Password         : password
Circuit Type     : excluded
Circuit ID       : excluded
```

#### Related Documentation

- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
- [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)
- [Monitoring DHCPv6 Local Server Authentication Information on page 109](#)
- [ipv6 dhcpv6-local auth domain on page 72](#)
- [ipv6 dhcpv6-local auth password on page 73](#)
- [ipv6 dhcpv6-local auth user-prefix on page 74](#)
- [service dhcpv6-local on page 87](#)

## Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers

You can configure the type of DHCP unique identifier (DUID) using the **ipv6 dhcpv6-local duid-type** *duidType* command in Global Configuration mode to be either Type 2 or Type 3. These two types are currently supported by the DHCPv6 local server application in JunosE Software. The Type 1 DUID is not supported by the DHCPv6 local server in JunosE Software. However, DHCPv6 clients support DUID Types 1,2, and 3.

To configure the DUID type:

1. Enable the DHCPv6 local server.

```
host1(config)#service dhcpv6-local
```

2. Specify the DUID type to be used during the identity verification of the server and the client.

```
host1(config)#ipv6 dhcpv6-local duid 3
```

In this example, the DUID type is set as Type 3, which is used by devices that have a permanently connected network interface with a link-layer address, and do not have a nonvolatile, writable stable storage.



**NOTE:** You must enable the DHCPv6 local server using the **service dhcpv6-local** command before configuring the DUID type. Otherwise, an error message states that the DHCPv6 local server is not configured on the router.

- Related Documentation**
- [DHCP Unique ID for Clients and Servers Overview on page 11](#)
  - [ipv6 dhcpv6-local duid-type on page 69](#)

# Removal of DHCPv6 Client Bindings

- [Deleting DHCPv6 Client Bindings on page 39](#)

## Deleting DHCPv6 Client Bindings

---

The JunosE Software enables you to manage your router's DHCPv6 local server client bindings. The client binding associates an IPv6 prefix with a unique DHCP ID (DUID) of the subscriber client. To view information about current DHCPv6 client bindings and track lease times of a specific client binding, use the **show ipv6 dhcpv6—local binding** command.

To delete a client binding and the associated route configuration when the DHCPv6 client binding is no longer needed, use the **dhcpv6 delete-binding** command. You can delete the DHCPv6 client bindings instead of waiting for the lease timer to expire. Use the following keywords and variables with the **dhcpv6 delete-binding** command to specify (filter) the client bindings you want to delete:

- **all**—All DHCPv6 local server client bindings
- *ipv6Prefix*—IPv6 prefix (address and subnetwork mask) of the DHCPv6 clients; for example, 2002:2:4:1::/64
- *string*—Local address pool name; for example, server4pool



**NOTE:** After a stateful SRP switchover, in a scaled environment, the interface strings associated with DHCPv6 client bindings might not be displayed in the output of the **show** commands used to view information about client bindings if you issue the **show** command immediately after a stateful SRP switchover. These **show** commands display interface strings in the output only if the restoration of IPv6 interfaces on the router is complete after the SRP warm switchover. After the restoration of IPv6 interfaces is complete, interface strings are displayed properly in the output of the **show** commands available for this purpose.

You can remove all DHCPv6 client bindings, all DHCPv6 client bindings of a particular type, or a specified DHCPv6 client binding that meets the deletion criteria you specify.

- To delete all DHCPv6 client bindings on virtual router vr1:

**host1:vr1#dhcpv6 delete-binding all**

- To delete DHCPv6 client bindings with the specified IPv6 prefix:

**host1:vr1#dhcpv6 delete-binding 2002:2:4:1::/64**

- To delete a group of DHCPv6 client bindings that were assigned prefix from the local pool:

**host1:vr2#dhcpv6 delete-binding server4pool**

The router does not notify the DHCPv6 client when you use the **dhcpv6 delete-binding** command. To verify that the DHCPv6 client bindings have been deleted, use the **show ipv6 dhcpv6-local binding** command.

In JunosE Release 11.3.0, when DHCPv6 client bindings are brought up over a PPPv6 session, on a router that acts as an L2TP network server (LNS) and is enabled for stateful line module switchover, the client bindings are removed when the primary line module fails and the spare line module takes over as the primary. This behavior occurs because the underlying dynamic IPv6 over PPP interface goes down temporarily (when the subscriber session is disrupted briefly) before the interface becomes operational again on the newly active primary module. When the dynamic IPv6 over PPP interface goes down temporarily (when the stateful switchover process is in progress), the DHCPv6 client binding and the access route for that interface are deleted. Similarly, DHCPv6 bindings are deleted when a PPP subscriber logs out and then back in. In such scenarios, the client needs to send a renew or rebind request to the DHCP server to enable the DHCPv6 binding to be re-created.

Beginning with JunosE Release 12.0.0, DHCPv6 client bindings and access routes that are created over a PPPv6 session on an LNS device enabled for stateful line module switchover are retained when the dynamic IPv6 over PPP interface temporarily goes down during the stateful switchover operation. DHCPv6 client bindings and the associated route configuration are deleted only when the interface is deleted and not during the interface down event.

DHCPv6 client bindings and access routes that are created over a PPPv6 session, on a router that acts as an LNS and is enabled for stateful line module switchover, are retained when the dynamic IPv6 over PPP interface goes down temporarily during the stateful switchover operation. When the stateful switchover procedure is complete, the interface is re-created on the newly active primary module and the DHCPv6 bindings are also retained. The same behavior of preservation of DHCPv6 bindings is applicable when a PPPv6 subscriber logs out and then back in.

**Related  
Documentation**

- [Monitoring DHCPv6 Local Server Binding Information on page 110](#)
- *dhcpv6 delete-binding*
- [show ipv6 dhcpv6-local binding on page 126](#)

## CHAPTER 7

# Interoperation of SRC Client and DHCP Local Server

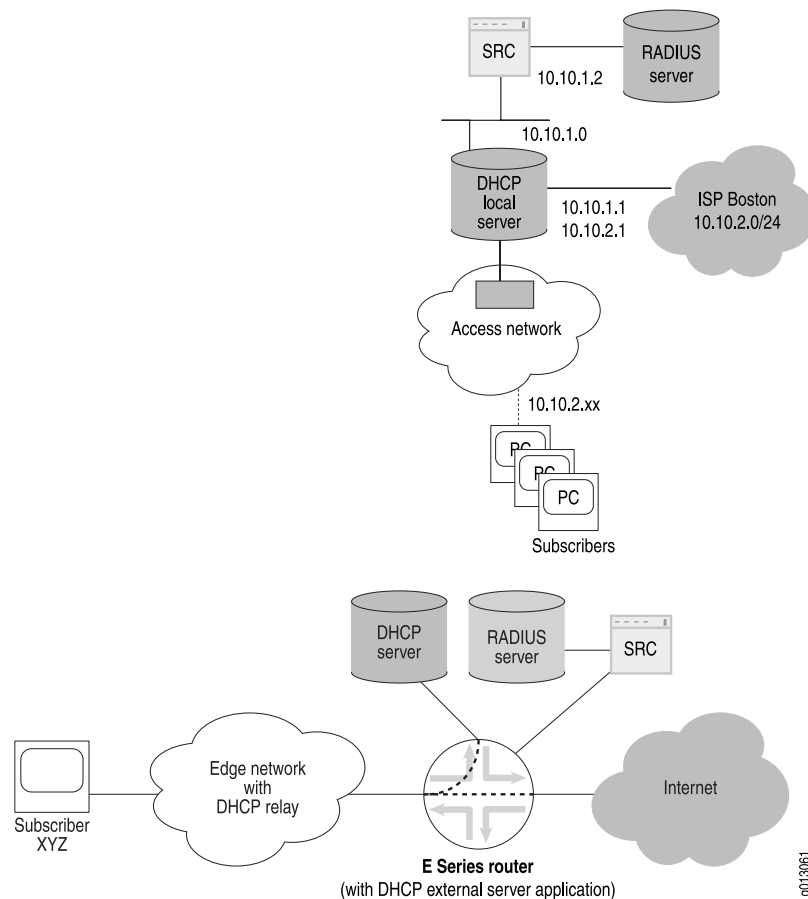
- [Configuring the Router to Work with the SRC Software on page 41](#)

### Configuring the Router to Work with the SRC Software

E Series Broadband Services Routers have an embedded SRC client that interacts with the SRC software. For information about configuring the SRC client, see *SRC Client Configuration Overview*.

[Figure 2 on page 42](#) shows the scenario for this example. Subscribers obtain access to ISP Boston via a router. Subscribers log in through the SRC software, and a RADIUS server provides authentication.

Figure 2: Non-PPP Equal-Access Configuration Example



The following steps describe how to configure this scenario.

1. Configure interfaces on the router.

```
host1(config)#interface loopback 0
host1(config-if)#ip address 10.10.1.1 255.255.255.255
host1(config-if)#ip address 10.10.2.1 255.255.255.255 secondary
host1(config-if)#exit
host1(config)#interface fastEthernet 2/0
host1(config-if)#ip unnumbered loopback 0
```

2. Configure the parameters to enable the router to forward authentication requests to the RADIUS server.

```
host1(config)#radius authentication server 10.10.1.2
host1(config)#udp-port 1645
host1(config)#key radius
```

3. Specify the authentication method.

```
host1(config)#aaa authentication ppp default radius
```

Or

```
host1(config)#aaa authentication ppp default none
```



4. Enable the DHCP local server.

```
host1(config)#service dhcp-local
```

5. Specify the IP addresses that are in use, so that the DHCP local server cannot assign these addresses.

```
host1(config)#ip dhcp-local excluded-address 10.10.1.1
```

```
host1(config)#ip dhcp-local excluded-address 10.10.1.2
```

6. Configure the DHCP local server to provide IP addresses to subscribers of ISP Boston.

```
host1(config)ip dhcp-local pool ispBoston
```

```
host1(config-dhcp-local)#network 10.10.2.0 255.255.255.0
```

```
host1(config-dhcp-local)#domain-name ispBoston
```

```
host1(config-dhcp-local)#default-router 10.10.2.1
```

```
host1(config-dhcp-local)#lease 0 0 10
```

```
host1(config-dhcp-local)#ip dhcp-local limit atm 5
```

7. Configure the SRC client.

```
host1(config)#sscc enable
```

```
host1(config)#sscc retryTimer 200
```

```
host1(config)#sscc primary address 10.10.1.2 port 3288
```

#### Related Documentation

- *Configuring the SRC Client*
- *aaa authentication default*
- [default-router on page 52](#)
- [domain-name on page 54](#)
- *interface fastEthernet*
- *interface loopback*
- *ip address*
- [ip dhcp-local excluded-address on page 58](#)
- [ip dhcp-local limit on page 59](#)
- [ip dhcp-local pool on page 56](#)
- *ip unnumbered*
- *key*
- [lease on page 76](#)
- [network on page 82](#)
- *radius authentication server*
- *sscc address*
- *sscc enable*
- *sscc retryTimer*
- *udp-port*



## CHAPTER 8

# Configuring Baselines for DHCP Local Server Statistics

- [Setting Baselines for DHCP Statistics on page 45](#)

## Setting Baselines for DHCP Statistics

---

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

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

Tasks to set a baseline for DHCP statistics are:

1. [Setting a Baseline for DHCP Relay and Relay Proxy on page 45](#)
2. [Setting a Baseline for DHCP Proxy Server Statistics on page 45](#)
3. [Setting a Baseline for DHCP External Server Statistics on page 46](#)
4. [Setting a Baseline for DHCP Local Server Statistics on page 46](#)

### Setting a Baseline for DHCP Relay and Relay Proxy

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

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

```
host1#baseline dhcp relay
```

There is no **no** version.

### Setting a Baseline for DHCP Proxy Server Statistics

To set a baseline for DHCP proxy server statistics.

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

```
host1#baseline dhcp server
```

There is no **no** version.

## Setting a Baseline for DHCP External Server Statistics

To set a baseline for DHCP external server statistics.

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

```
host1#baseline ip dhcp-external
```

There is no **no** version.

## Setting a Baseline for DHCP Local Server Statistics

To set a baseline for DHCP local server statistics:

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

```
host1#baseline ip dhcp-local
```

There is no **no** version.

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

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

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

To set a baseline for DHCPv6 local server statistics:

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

```
host1#baseline ipv6 dhcpv6-local
```

## CHAPTER 9

# Configuration Commands

## clear ip dhcp-local binding

---

**Syntax** clear ip dhcp-local binding *ipAddress*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Clears the specified IP DHCP address binding. There is no **no** version.



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **dhcp delete-binding** command.

**Options** • *ipAddress*—DHCP IP address binding to clear

**Mode** Privileged Exec

## dhcp delete-binding

**Syntax** To delete the DHCP client with the specified binding ID:

```
dhcp delete-binding bindingId
```

To delete all DHCP client bindings or all DHCP client bindings of a particular type on the specified subnet:

```
dhcp delete-binding { all | all-local | all-external | all-relay-proxy } [ subnetAddress ]
```

To delete DHCP client bindings of a particular type on the specified subnet:

```
dhcp delete-binding { local | external | relay-proxy } [ subnetAddress ]
```

To delete DHCP client bindings for the specified IP prefix:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] ip-prefix ipPrefix
```

To delete DHCP client bindings for the specified interface string:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] interface string
```

To delete DHCP client bindings without a lower-layer interface:

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] no-interface
```

To delete DHCP client bindings for the specified agent-circuit-id suboption (suboption 1) string of the DHCP relay agent information option (option 82):

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] circuit-id string
```

To delete DHCP client bindings for the specified agent-remote-id suboption (suboption 2) string of the DHCP relay agent information option (option 82):

```
dhcp delete-binding [ local | external | relay-proxy ] [ subnetAddress ] remote-id string
```

**Release Information** Command introduced in JunosE Release 8.1.0.

**local**, **external**, **relay-proxy**, **interface**, **no-interface**, **ip-prefix**, **circuit-id**, and **remote-id** keywords and *subnetAddress*, *ipAddress*, and *string* variables added in JunosE Release 9.3.0.

**Description** Deletes the specified DHCP client bindings. There is no **no** version.



**NOTE:** This command replaces the deprecated **clear ip dhcp-local binding** and **dhcp-external delete-binding** commands, which may be removed completely in a future release.

- Options**
- *bindingId*—DHCP binding ID for a specific client
  - *all*—Specifies all DHCP local server, DHCP external server, and DHCP relay proxy client bindings
  - *all-local*—Specifies all DHCP local server client bindings
  - *all-external*—Specifies all DHCP external server client bindings
  - *all-relay-proxy*—Specifies all DHCP relay proxy client bindings
  - *local*—Specifies DHCP local server client bindings that meet the deletion criteria
  - *external*—Specifies DHCP external server client bindings that meet the deletion criteria
  - *relay-proxy*—Specifies DHCP relay proxy client bindings that meet the deletion criteria
  - *subnetAddress*—IP address of the subnet on which the DHCP clients reside
  - *ipPrefix*—IP prefix (address and subnetwork mask) of the DHCP clients; for example, 10.10.10.0/24
  - *no-interface*—Specifies DHCP clients without a lower-layer interface; use this keyword to delete DHCP client bindings configured over dynamic interfaces for which the lower-layer interface has been shut down
  - *string*—Regular expression string that represents the interface, circuit ID, or remote ID to be matched; you must enclose elements containing a space within double quotes (“*one element*”)

Each element is either a literal string, a metacharacter, or a combination. You can remove the special meaning of a metacharacter by preceding it with a backslash (\). Regular expressions support the following metacharacters:

- *^* Matches the beginning of the input string. Alternatively, when used as the first character within brackets—*[^ ]*—matches any number except the ones specified within the brackets.
- *\$* Matches the end of the input string
- *.* (period) Matches any single character, including white space
- *\** Matches 0 or more sequences of the immediately previous character or pattern.
- *+* Matches 1 or more sequences of the immediately previous character or pattern
- *?* Matches 0 or 1 sequence of the immediately previous character or pattern
- *( )* Specifies patterns for multiple use when followed by one of the multiplier metacharacters: asterisk *\**, plus sign *+*, or question mark *?*
- *[ ]* Matches any enclosed character; specifies a range of single characters
- *–* (hyphen) Used within brackets to specify a range of AS or community numbers
- *\_* (underscore) Matches a *^*, a *\$*, a comma, a space, a *{*, or a *}*. Placed on either side of a string to specify a literal and disallow substring matching. Numerals enclosed by underscores can be preceded or followed by any of the characters listed above
- *|* Matches characters on either side of the metacharacter; logical OR



You must specify the interface string as a regular expression without spaces; for example, `fastEthernet1.1/100` or `fastEthernet.*100`

The following rules apply for representing nonprintable character sequences in the circuit ID string or the remote ID string:

- To represent the binary sequence `0d 0a` (hex), use the string `'\\r\\n'`. This consists of four ASCII characters: `5c` for `\\`, `72` for `r`, `5c` for `\\`, and `6e` for `n`.

For example, to match the sequence `74 65 73 74 0d 0a 6f 6e 65` (hex), use the string `'test\\r\\nnone'`. In this string, `74` is represented by `t`, `65` is represented by `e`, `73` is represented by `s`, `74` is represented by `t`, `0d 0a` is represented by `\\r\\n`, `6f` is represented by `o`, `6e` is represented by `n`, and `65` is represented by `e`.

- To represent the binary sequence `0d 00` (hex), use the string `'\\r'`. This consists of two ASCII characters: `5c` for `\\`, and `72` for `r`.
- To represent the binary sequence `0a 00` (hex), use the string `'\\n'`. This consists of two ASCII characters: `5c` for `\\`, and `6e` for `n`.

For example, to match the sequence `74 65 73 74 0a 00 6f 6e 65` (hex), use the string `'test\\nnone'`. In this string, `74` is represented by `t`, `65` is represented by `e`, `73` is represented by `s`, `74` is represented by `t`, `0a 00` is represented by `\\n`, `0a` is represented by `\\n`, `6f` is represented by `o`, `6e` is represented by `n`, and `65` is represented by `e`.

- To represent all other cases, use the string `'\\xab'`, where `ab` is a hex code of the byte. For example, to represent byte `3A`, use `'\\x3a'`. This consists of four ASCII characters: `5c` for `\\`, `78` for `x`, `33` for `3`, and `61` for `a`.

As another example, to match the sequence `74 65 73 74 f3 6f 6e 65` (hex), use the string `'test\\xf3one'`. In this string, `74` is represented by `t`, `65` is represented by `e`, `73` is represented by `s`, `74` is represented by `t`, byte `F3` is represented by `\\xf3`, `6f` is represented by `o`, `6e` is represented by `n`, and `65` is represented by `e`.

**Mode** Privileged Exec

## default-router

---

**Syntax**    `default-router ipAddressPrimary [ ipAddressSecondary ]`  
              `no default-router`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies the IP address of the router that the subscriber's computer will use for traffic destined for locations beyond the local subnet. The default router must be on the same subnet as the local server pool addresses configured with the **network** command. The **no** version removes the association between the address pool and the router.

**Options**

- *ipAddressPrimary*—IP address of preferred router
- *ipAddressSecondary*—IP address of secondary router

**Mode**    DHCP Local Pool Configuration

## dns-server

---

**Syntax**    `dns-server ipAddressPrimary [ ipAddressSecondary ]`  
              `no dns-server`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Assigns a DNS server to an address pool. The **no** version removes the association between the address pool and the DNS server.

**Options**    • *ipAddressPrimary*—IP address of preferred DNS server  
              • *ipAddressSecondary*—IP address of secondary DNS server

**Mode**    DHCP Local Pool Configuration

## domain-name

---

**Syntax** From DHCP Local Pool Configuration mode:

domain-name *domainName*

no domain-name

From IPsec Identity Configuration mode:

[ no ] domain-name *domainName*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** From DHCP Local Pool Configuration mode, specifies a domain name that can be returned to the subscriber of an address pool if requested. The **no** version removes the association between the address pool and the domain name.

From IPsec Identity mode, specifies the domain name that the router uses in IKE authentication messages and to generate certificate requests. The **no** version removes the domain name.

**Options**

- *domainName*—Name of the domain
- *domainName*—Name used in certificate requests and in IKE authentication messages; up to 60 characters

**Mode** DHCP Local Pool Configuration, IPsec Identity Configuration

## grace-period

---

**Syntax**    `grace-period days [ hours [ minutes [ seconds ] ] ]`  
`no grace-period`

**Release Information**    Command introduced in JunosE Release 8.0.0.

**Description**    Configures the grace period for address leases allocated from the current DHCP local address pool. When the address lease expires, the address enters the grace period, when the address continues to be unavailable to other clients and can only be reassigned to the original client. This command applies only to expired releases—to optionally apply the grace period to addresses that are *explicitly released* by a client, you must enable the **use-release-grace-period** command. The **no** version restores the default, in which no grace period is associated with the local address pool.

- Options**
- *days*—Number of days in the grace period; in the range 0–32767
  - *hours*—Number of hours in the grace period; in the range 0–23
  - *minutes*—Number of minutes in the grace period; in the range 0–59
  - *seconds*—Number of seconds in the grace period; in the range 0–59

**Mode**    DHCP Local Pool Configuration

## ip dhcp-local pool

---

**Syntax** [ no ] ip dhcp-local pool { *poolName* | default }

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Accesses DHCP Local Pool Configuration mode. The DHCP local server uses pool names other than default to maintain configuration information for subscribers to a particular domain. The **no** version prevents the DHCP local server from supplying IP addresses from the specified pool.

- Options**
- *poolName*—Name of the address pool
  - default—Specifies the default address pool

**Mode** Global Configuration

## **ip dhcp-local auto-configure agent-circuit-identifier**

---

**Syntax** [ no ] ip dhcp-local auto-configure agent-circuit-identifier

**Release Information** Command introduced in JunosE Release 7.3.0.

**Description** Configures the DHCP local server to support the creation of dynamic subscriber interfaces built over dynamic VLANs that are based on the agent-circuit-id option (suboption 1) of the option 82 field in DHCP messages. This command is specific to a virtual router. The **no** version disables the autoconfigure feature.

**Mode** Global Configuration

## ip dhcp-local excluded-address

---

**Syntax** [ no ] ip dhcp-local excluded-address *ipAddressStart* *ipAddressStop*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Specifies IP addresses that the DHCP local server should not supply from the default address pool because those addresses are already used by devices on the subnet. The **no** version allows the DHCP local server to supply the specified IP address.

- Options**
- *ipAddressStart*—Single IP address or start of the range of IP addresses that the DHCP local server should not supply
  - *ipAddressStop*—End of the range of IP addresses that the DHCP local server should not supply

**Mode** Global Configuration



## ip dhcp-local limit

**Syntax** ip dhcp-local limit  
 { atm | ethernet | pos | vlan | interface *InterfaceType InterfaceSpecifier* } *value*  
 no ip dhcp-local limit [ atm | ethernet | pos | vlan  
 | interface *InterfaceType InterfaceSpecifier* ]

**Release Information** Command introduced before JunosE Release 7.1.0.  
**interface** keyword and *interfaceType* and *interfaceSpecifier* variables added in JunosE Release 7.1.0.  
**pos** keyword added in JunosE Release 10.0.0.

**Description** Specifies the maximum number of IP addresses that the DHCP local server can supply to each VPI/VCI, VLAN, Ethernet subnetwork, or POS access interface, or to a particular interface or subinterface. The **no** version restores the default address limit value, 48000.

- Options**
- atm—Specifies the limit for VPIs and VCIs
  - ethernet—Specifies the limit for Ethernet subnets
  - pos—Specifies the limit for POS access interfaces
  - vlan—Specifies the limit for VLANs
  - *interfaceType*—Interface type; see *Interface Types and Specifiers*
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
  - *value*—Maximum number of leases, in the range 0–96000; default is 48000

**Mode** Global Configuration

## ip dhcp-local unique-client-ids

---

**Syntax** [ no ] ip dhcp-local unique-client-ids

**Release Information** Command introduced in JunosE Release 8.0.0.

**Description** Configures the method that DHCP local server uses when it receives a DHCP DISCOVER or REQUEST packet from a client ID or hardware address that matches the client ID or hardware address of a currently bound client on another subnet or subinterface.

Use this command to specify that DHCP local server uses a method that considers a request from a client with a duplicate client ID or hardware address to be from a roaming client—the server then terminates the currently bound client's existing lease and assigns a new address to the requesting client.

The **no** version restores the default behavior, in which DHCP local server uses the DHCP client's subnet or subinterface to differentiate between two clients that use the same client ID or hardware address—the DHCP server processes requests in the normal manner.



.....  
**NOTE:** This command replaces the **ip dhcp-local inhibit-roaming** command, which has been removed from the CLI.  
.....

**Mode** Global Configuration

## ip dhcp-local auth domain

---

**Syntax** [ no ] ip dhcp-local auth domain *domainName*

**Release Information** Command introduced in JunosE Release 7.1.0.

**Description** Specifies a domain name for a username that is locally configured for a DHCP standalone mode client. In standalone mode, the locally configured username is presented to AAA in an authentication request. The **no** version removes the domain name.

**Options** • *domainName*—String of 1–32 characters used as the domain name

**Mode** Global Configuration

## ip dhcp-local auth include

---

**Syntax** [ no ] ip dhcp-local auth include { circuit-identifier | circuit-type | mac-address | option82 | virtual-router-name | radius-dhcp-options }

**Release Information** Command introduced in JunosE Release 7.1.0.  
**radius-dhcp-options** keyword added in JunosE Release 11.3.0.

**Description** Includes optional information as part of the locally configured username for a DHCP standalone mode client. In standalone mode, the username is presented to AAA in an authentication request. The **no** version removes the specified optional information.

- Options**
- circuit-identifier—Specifies the circuit identifier of the interface on which the DHCP client's request was received
  - circuit-type—Specifies the circuit type of the interface on which the DHCP client's request was received
  - mac-address—Specifies the DHCP client's MAC address
  - option82—Specifies the DHCP client's Option 82 value
  - virtual-router-name—Specifies the DHCP local server's virtual router name
  - radius-dhcp-options—Specifies the DHCP options returned from the RADIUS server

**Mode** Global Configuration

## ip dhcp-local auth password

---

**Syntax** [ no ] ip dhcp-local auth password *password*

**Release Information** Command introduced in JunosE Release 7.1.0.

**Description** Assigns a password used to authenticate a locally configured DHCP standalone mode client. In DHCP standalone mode, the password is presented to AAA in an authentication request. The **no** version removes the password.

**Options** • *password*—String of 1–32 characters used as the password

**Mode** Global Configuration

## ip dhcp-local auth user-prefix

---

**Syntax** [ no ] ip dhcp-local auth user-prefix *userNamePrefix*

**Release Information** Command introduced in JunosE Release 7.1.0.

**Description** Specifies a user prefix for a username that is locally configured for a DHCP standalone mode client. In DHCP standalone mode, the username is presented to AAA in an authentication request. The **no** version removes the user prefix.

**Options**

- *userNamePrefix*—String of 1–32 characters used as the prefix for a locally configured username

**Mode** Global Configuration

## ip dhcp-local auth domain

---

**Syntax** [ no ] ip dhcp-local auth domain *domainName*

**Release Information** Command introduced in JunosE Release 7.1.0.

**Description** Specifies a domain name for a username that is locally configured for a DHCP standalone mode client. In standalone mode, the locally configured username is presented to AAA in an authentication request. The **no** version removes the domain name.

**Options** • *domainName*—String of 1–32 characters used as the domain name

**Mode** Global Configuration

## ipv6 dhcpv6-local delegated-prefix

---

**Syntax**    `ipv6 dhcpv6-local delegated-prefix ipv6Prefix`  
              `[ lifetime { days [ hours [ minutes [ seconds ] ] ] | infinite } ]`  
  
              `no ipv6 dhcpv6-local delegated-prefix`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies the IPv6 prefix and lifetime that is to be delegated, when requested, to the DHCPv6 client on this interface by the DHCPv6 local server. This lifetime overrides the default lifetime that is set in Global Configuration mode. If no lifetime is specified, the default lifetime is used. The **no** version removes the IPv6 prefix from the interface.

- Options**
- *ipv6Prefix*—Prefix that defines the IPv6 interface
  - *days*—Number of days in the lifetime; in the range 0–32768
  - *hours*—Number of hours in the lifetime; in the range 0–24
  - *minutes*—Number of minutes in the lifetime; in the range 0–60
  - *seconds*—Number of seconds in the lifetime; in the range 0–60
  - *infinite*—Assigns a lifetime that does not expire

**Mode**    Interface Configuration



## ipv6 dhcpv6-local dns-domain-search

---

**Syntax** [ no ] ipv6 dhcpv6-local dns-domain-search *dnsDomainName*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Adds the specified DNS domain name to the domain search list. The **no** version removes the specified domain name from the search list.

**Options** • *dnsDomainName*—Name of DNS domain name

**Mode** Global Configuration

## ipv6 dhcpv6-local dns-server

---

**Syntax** [ no ] ipv6 dhcpv6-local dns-server *ipv6Address*

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Assigns the specified DNS server to all DHCPv6 clients in the current virtual router. The **no** version removes the specified DNS server.

**Options** • *ipv6Address*—IPv6 address of the DNS server

**Mode** Global Configuration

## ipv6 dhcpv6-local duid-type

**Syntax** `ipv6 dhcpv6-local duid-type duidType`

`no ipv6 dhcpv6-local duid-type`

**Release Information** Command introduced in JunosE Release 12.2.0.

**Description** Specifies the DHCP unique identifier (DUID) type that the DHCPv6 local server running on the router uses in communication with the DHCPv6 client and for verifying the identity of the client. Both the server and the client are identified by a DUID. By default, the DHCPv6 local server uses the Type 2 server DUID in the communication between the delegating router and the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client. The **no** version removes the configured DUID type and the router reverts to the default Type 2 DUID for the client to identify the server.

**Options** • *duidType*—DUID type can be either 2 or 3; the default value is 2



**NOTE:** You must enable the DHCPv6 local server using the **service dhcpv6-local** command before configuring the DUID type. Otherwise, an error message states that the DHCPv6 local server is not configured on the router.

**Mode** Global Configuration

**Related Documentation**

- [DHCP Unique ID for Clients and Servers Overview on page 11](#)
- [Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers on page 37](#)

## ipv6 dhcpv6-local prefix-lifetime

---

**Syntax**    `ipv6 dhcpv6-local prefix-lifetime { days [ hours [ minutes [ seconds ] ] ] | infinite }`  
              `no ipv6 dhcpv6-local prefix-lifetime`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Sets the default lifetime for which a prefix delegated by this DHCPv6 local server is valid. This default is overridden by the interface-specific lifetime. The **no** version restores the default lifetime to 1 day.

- Options**
- *days*—Number of days in the lifetime; in the range 0–32768
  - *hours*—Number of hours in the lifetime; in the range 0–24
  - *minutes*—Number of minutes in the lifetime; in the range 0–60
  - *seconds*—Number of seconds in the lifetime; in the range 0–60
  - *infinite*—Assigns a lifetime that does not expire

**Mode**    Global Configuration

## ipv6 local pool

---

**Syntax**    `ipv6 local pool poolName`  
              `no ipv6 local pool poolName [ force ]`

**Release Information**    Command introduced in JunosE Release 10.1.0.

**Description**    Accesses IPv6 Local Pool Configuration mode. Specifies the IPv6 local address pool from which prefixes are allocated to the requesting router in networks that use DHCPv6. The **no** version removes the IPv6 local pool.

- Options**
- *poolName*—Name of the IPv6 local address pool to be used to delegate prefixes to the requesting routers or DHCPv6 clients; string of up to 16 alphanumeric characters
  - *force*—Forcibly deletes an IPv6 local address pool from which prefixes have been allocated. When a pool from which prefixes have been assigned to DHCPv6 clients is deleted, the corresponding DHCPv6 bindings are also deleted.

**Mode**    Global Configuration

## ipv6 dhcpv6-local auth domain

---

**Syntax** [ no ] ipv6 dhcpv6-local auth domain *domainName*

**Release Information** Command introduced in JunosE Release 12.2.0.

**Description** Specifies a domain name for a username that is locally configured for a DHCPv6 standalone mode client. In standalone mode, the locally configured username is presented to AAA in an authentication request. The **no** version removes the configured domain, which is the default behavior.

**Options** • *domainName*—String of 1–32 characters used as the domain name

**Mode** Global Configuration

**Related Documentation**

- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
- [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)
- [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)

---

## ipv6 dhcpv6-local auth password

---

<b>Syntax</b>	[ no ] ipv6 dhcpv6-local auth password <i>password</i>
<b>Release Information</b>	Command introduced in JunosE Release 12.2.0.
<b>Description</b>	Assigns a password used to authenticate a locally configured DHCPv6 standalone mode client. In DHCPv6 standalone mode, the password is presented to AAA in an authentication request. The <b>no</b> version removes the password configured for the user, which is the default behavior.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>password</i>—String of 1–32 characters used as the password</li></ul>
<b>Mode</b>	Global Configuration
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13</a></li><li>• <a href="#">Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15</a></li><li>• <a href="#">Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35</a></li></ul>

## ipv6 dhcpv6-local auth user-prefix

---

**Syntax** [ no ] ipv6 dhcpv6-local auth user-prefix *userNamePrefix*

**Release Information** Command introduced in JunosE Release 12.2.0.

**Description** Specifies a user prefix for a username that is locally configured for a DHCPv6 standalone mode client. In DHCPv6 standalone mode, the username is presented to AAA in an authentication request. The **no** version removes the user prefix, which is the default behavior.

**Options**

- *userNamePrefix*—String of 1–32 characters used as the prefix for a locally configured username

**Mode** Global Configuration

**Related Documentation**

- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
- [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)
- [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)



## ipv6 dhcpv6-local duid-type

**Syntax** `ipv6 dhcpv6-local duid-type duidType`

`no ipv6 dhcpv6-local duid-type`

**Release Information** Command introduced in JunosE Release 12.2.0.

**Description** Specifies the DHCP unique identifier (DUID) type that the DHCPv6 local server running on the router uses in communication with the DHCPv6 client and for verifying the identity of the client. Both the server and the client are identified by a DUID. By default, the DHCPv6 local server uses the Type 2 server DUID in the communication between the delegating router and the requesting router, which is the customer premises equipment (CPE) at the edge of the remote client site that acts as the DHCP client. The **no** version removes the configured DUID type and the router reverts to the default Type 2 DUID for the client to identify the server.

**Options** • *duidType*—DUID type can be either 2 or 3; the default value is 2



**NOTE:** You must enable the DHCPv6 local server using the **service dhcpv6-local** command before configuring the DUID type. Otherwise, an error message states that the DHCPv6 local server is not configured on the router.

**Mode** Global Configuration

**Related Documentation**

- [DHCP Unique ID for Clients and Servers Overview on page 11](#)
- [Configuring the Type of DHCP Unique ID for DHCPv6 Local Servers on page 37](#)

## lease

---

**Syntax**    `lease { days [ hours [ minutes [ seconds ] ] ] | infinite }`  
`no lease`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies the time period for which the supplied IP address is valid. The **no** version restores the default lease time, 30 minutes.



.....  
**NOTE:** Ensure that DHCP clients have a minimum lease of 120 minutes before you begin a unified in-service software upgrade to prevent unwanted lease expirations due to the length of the unified ISSU process.  
.....

- Options**
- *days*—Number of days for which the IP address is valid; in the range 0–32768
  - *hours*—Number of hours for which the IP address is valid in the range 0–24
  - *minutes*—Number of minutes for which the IP address is valid; in the range 0–60
  - *seconds*—Number of seconds for which the IP address is valid; in the range 0–60
  - *infinite*—Assigns a lease that does not expire

**Mode**    DHCP Local Pool Configuration

## link

---

**Syntax**    `link poolName`

`no link`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Links the pool currently being configured to another DHCP local address pool. The linked pool acts as a backup pool. The **no** version removes the link.

**Options**    • *poolName*—Name of pool to which you want to link the pool currently being configured

**Mode**    DHCP Local Pool Configuration

## logout subscribers

**Syntax** logout subscribers { all | domain *domainName* | icr-partition *icrPartitionId* | port *interfaceSpecifier* | interface { lag } *interfaceLocation* | username *userName* | virtual-router *vrName* }

**Release Information** Command introduced before JunosE Release 7.1.0.  
**icr-partition** keyword and *icrPartitionLocationId* variable added in JunosE Release 10.3.0  
**interface** and **lag** keywords and *interfaceLocation* variable added in JunosE Release 12.2.0

**Description** Logs out the authenticated PPP or DHCP local server users. Also, logs out subscribers based on the ICR partition ID. There is no **no** version.

- Options**
- **all**—Logs out all PPP or DHCP local server sessions.
  - **domainName**—Logs out active PPP or DHCP local server sessions whose usernames have the mentioned domain name.
  - **icr-partition**—Logs out subscribers based on the location ID of the partition in the ICR cluster.
  - **icrPartitionLocationID**—A unique identifier for each ICR partition on a chassis; a maximum of 128 characters. Note that this ID is different from the partition ID, which is configured using the **ip vrrp vrid icr-partition partitionId** command. The partition location ID that you specify here is a combination of the interface within the chassis on which the ICR partition is configured and the VRRP ID, which is system-defined and nonconfigurable.
  - **interfaceSpecifier**—Location of the port with active PPP subscribers; format varies according to interface type; see *Interface Types and Specifiers*.
  - **lag**—Displays subscribers based on the LAG interface
  - **interfaceLocation**—Location of the member interfaces in a LAG bundle for which subscribers that logged in to those interfaces are displayed; format varies according to interface type; see *Interface Types and Specifiers*.
  - **userName**—Logs out active PPP or DHCP local server sessions whose names match the username.



**NOTE:** You must specify the complete username with the domain name (if available) regardless of the status of the strip domain feature on a virtual router or AAA domain map.

- **vrName**—Logs out active PPP or DHCP local server sessions whose interfaces are bound to a specific virtual router.

**Mode** Privileged Exec

- Related Documentation**
- *Domain Name and Realm Name Overview*
  - [Configuring the DHCP Local Server on page 23](#)
  - *aaa strip-domain*
  - *strip-domain*

## netbios-name-server

---

**Syntax** netbios-name-server *ipAddressPrimary* [ *ipAddressSecondary* ]  
no netbios-name-server

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Assigns a NetBIOS server to subscribers of an address pool. The **no** version removes the association between the address pool and the NetBIOS server.

- Options**
- *ipAddressPrimary*—IP address of preferred NetBIOS server
  - *ipAddressSecondary*—IP address of secondary DNS server

**Mode** DHCP Local Pool Configuration

## netbios-node-type

---

**Syntax**    netbios-node-type *nodeType*  
              no netbios-node-type

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Specifies a NetBIOS node type. The **no** version restores the default situation, in which the node type is unspecified.

**Options**    • *nodeType*—One of the following types of NetBIOS servers:

- b-node—NetBIOS Broadcast node
- p-node—NetBIOS Peer-to-Peer node
- m-node—NetBIOS mixed node
- h-node—NetBIOS hybrid node

**Mode**    DHCP Local Pool Configuration

## network

---

**Syntax** For BGP:

```
[ no ] network { networkNumber [ [ mask ] networkMask ] | ipv6Prefix | rtfPrefix }  
[ route-map mapTag ] [ weight weight ] [ backdoor ]
```

For DHCP local server:

```
network networkAddress { networkMask | prefix }
```

```
no network [ force ]
```

For RIP:

```
[ no ] network networkAddress [ networkMask ]
```

**Release Information** Command introduced before JunosE Release 7.1.0.  
*rtMemNlri* variable added in JunosE Release 9.0.0.  
*rtMemNlri* variable replaced by *rtfPrefix* variable in JunosE Release 9.1.0.

**Description** For BGP, does one of the following:

- Configures a BGP speaker with an IPv6 or IPv4 prefix originating within its AS that it advertises to its peers if a non-BGP route to the prefix exists in the IP forwarding table. The **no** version removes the prefix.
- Originates a RT-MEM-NLRI route for the prefix that represents the route-target membership NLRI. This route is advertised to all peers that have negotiated the route-target address family. The advertisement is used by the speaker to exhibit interest in or request routes from a specific VPN that is not configured locally. The **no** version removes the prefix.

For DHCP local server, specifies IP addresses that the DHCP local server can provide from an address pool. The **no** version removes the network address and mask.

For RIP, enables RIP on a specific network (not on a range of networks). If you do not associate a network with RIP, the router cannot advertise the network in any RIP update. The **no** version disables RIP on a specific network. If you do not specify a network mask, the router applies the natural mask. Use the **ip rip** commands to configure RIP attributes on the network.

- Options**
- *networkNumber*—Prefix that BGP will advertise
  - *networkMask*—Subnet mask for the network
  - *ipv6Prefix*—IPv6 prefix that BGP will advertise
  - *rtfPrefix*—Prefix representing the route-target membership NLRI (RT-MEM-NLRI), in the format *asNumber:extendedCommunity/prefixLength* (for example, 320:320:524/36) where:



- *asNumber*—AS number for origin of route target information, in the range 1–4294967295
- *extendedCommunity*—Two-part number in the format *number1:number2* that identifies an extended community of VPNs, in the format *number1 : number2*, where:
  - *number1*—Autonomous system (AS) number, in the range 1–4294967295, or an IP address
  - *number2*—Unique integer, in the range 1–4294967295; 32 bits if *number1* is a 16-bit AS number; 16 bits if *number1* is an IP address or a 32-bit AS number
- *prefixLength*—Number that specifies the length of the route prefix, in the range 32–96
- *mapTag*—Name of the route map; a string of up to 32 alphanumeric characters; does not currently work with *rtMemNlri*
- *weight*—Number in the range 0–65535; default value is 32768; assigns an absolute weight to the network route that overrides a weight assigned by the **redistribute** command
- *backdoor*—Lowers the preference of an EBGp route to the specified prefix by setting the administrative distance to the value of an internal BGP route. Use this option to favor an IGP backdoor route over an EBGp route to a specific network. BGP does not advertise the prefix specified with this option.
- *networkAddress*—IP address of the network
- *prefix*—Network prefix
- *force*—Deletes address pool even if the pool is in use

**Mode**    Address Family Configuration (BGP, RIP), DHCP Local Pool Configuration (for DHCP local server), Router Configuration (BGP, RIP)

## reserve

---

**Syntax**    *reserve ipAddress macAddress*  
              *no reserve ipAddress*

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    For DHCP local server clients, reserves an IP address for a specific MAC address. The **no** version removes the reservation.

**Options**    • *ipAddress*—IP address to reserve  
              • *macAddress*—MAC address for which the IP address is reserved.

**Mode**    DHCP Local Pool Configuration

## server-address

---

**Syntax**    `server-address address`

`no server-address [ address ]`

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Sets the DHCP server address that is sent to DHCP clients. The **no** version removes server address.

**Options**    • *address*—DHCP server address

**Mode**    DHCP Local Pool Configuration

## service dhcp-local

---

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

**Release Information** Command introduced before JunosE Release 7.1.0.

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

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

**Mode** Global Configuration

## service dhcpv6-local

---

<b>Syntax</b>	[ no ] service dhcpv6-local [ standalone [ authenticate ] ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0. <b>standalone</b> and <b>authenticate</b> keywords added in JunosE Release 12.2.0.
<b>Description</b>	Enables the DHCPv6 local server. In standalone mode, the <b>authenticate</b> keyword enables AAA-based authentication for incoming DHCPv6 clients. The <b>no</b> version disables the DHCPv6 local server and does not save the previous settings.
<b>Options</b>	<ul style="list-style-type: none"><li>• standalone—Configures the router as a DHCPv6 local server</li><li>• authenticate—Enables AAA-based authentication of incoming DHCPv6 clients</li></ul>
<b>Mode</b>	Global Configuration
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13</a></li><li>• <a href="#">Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15</a></li><li>• <a href="#">Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35</a></li></ul>

## snmpTrap

---

**Syntax** [ no ] snmpTrap

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Enables SNMP traps for DHCP local address pool utilization. You can set the maximum and minimum threshold values for local address pool utilization by using the [warning](#) command. The **no** version disables SNMP traps for local address pool utilization.

**Mode** DHCP Local Pool Configuration

## use-release-grace-period

---

**Syntax** [ no ] use-release-grace-period

**Release Information** Command introduced in JunosE Release 8.0.0.

**Description** Applies the grace period, which is specified by the **grace-period** command, to the DHCP local address pool addresses that are explicitly released by clients. When a client releases an address, the address enters the grace period and can be reassigned only to the original client. The **no** version restores the default, which disables the use of the grace period for explicitly released addresses.

**Mode** DHCP Local Pool Configuration

## warning

---

**Syntax**    warning *maximumUtilization minimumUtilization*  
              no warning

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Sets the minimum and maximum threshold values for DHCP local address pool utilization. A local address pool can be linked to a second local address pool so that when the first pool utilization reaches 100%, the DHCP local server uses the second pool. The utilization of addresses is calculated for all the pools that are in the linked pools and they are collectively considered as an aggregated pool group for generation of SNMP traps. By default, the minimum and maximum threshold for SNMP traps to be triggered are 75 percent and 85 percent, respectively.

If you issue the ***snmp-server*** command, SNMP traps are generated when utilization occurs above or below the specified threshold values. The **no** version restores the default threshold values for local address pool utilization.

- Options**    • *maximumUtilization*—Maximum utilization value for the DHCP local address pool  
              • *minimumUtilization*—Minimum utilization value for the DHCP local address pool

**Mode**    DHCP Local Pool Configuration



## service dhcp-local

---

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

**Release Information** Command introduced before JunosE Release 7.1.0.

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

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

**Mode** Global Configuration



## PART 3

# Administration

- [Monitoring DHCP Local Address Pools on page 95](#)
- [Monitoring Tasks for DHCPv4 Local Server on page 99](#)
- [Monitoring Tasks for DHCPv6 Local Server on page 109](#)
- [Monitoring Commands on page 115](#)



## CHAPTER 10

# Monitoring DHCP Local Address Pools

- [Monitoring DHCP Local Address Pools on page 95](#)

## Monitoring DHCP Local Address Pools

---

**Purpose** Display the DHCP local pool configurations.

**Action** To display information about the local address pool:

```
host1#show ip dhcp-local pool
```

```
*****
Pool Name - ispBoston
Pool Id - 6
Domain Name - ispBoston
Network - 10.10.0.0
Mask - 255.255.255.0
NETBIOS Node Type - 1
Lease - Days:0 Hours:0 Minutes:24 Seconds:0
Grace Period - Days:0 Hours:0 Minutes:10 Seconds:0
Grace period for released leases enabled
DNS Servers
  10.10.1.1
NETBIOS Name Servers
  10.10.1.1
  10.10.1.2
Default Routers
  10.10.1.3
Server Address - 10.10.20.8
Linked Pool - cable5
High utilization threshold - 85%
Abated utilization threshold - 75%
Current utilization - 0%
Utilization trap disabled.
Shared pool allocations - 25
```

To display information about local address pool groups:

```
host1#show ip dhcp-local pool groups
```

```
  DHCP Local Server Pool Groups
  There is 1 group configured
*****
Group Name: pool8_7-1-Group
  Total Addresses Available: 145
  Total Addresses In Use:    0
  High Utilization Thresh:   85%
```

```

Abated Utilization Thresh: 75%
Current Utilization:      0%
Trap Enabled:             no
===== Pools =====
pool8_7-1
pool8_7-2
pool8_7-3
pool8_7-4
pool8_7-5

```

**Meaning** [Table 6 on page 96](#) lists the **show ip dhcp-local pool** command output fields.

**Table 6: show ip dhcp-local pool Output Fields**

Field Name	Field Description
Pool Name	Name of the DHCP local pool
Pool Id	ID of the pool
Domain Name	Domain name assigned to the pool
Network	Addresses that the DHCP local server can provide from the pool
Mask	Subnet mask that goes with the network address
NETBIOS Node Type	Type of NetBIOS server:  1 = Broadcast  2 = Peer-to-peer  4 = Mixed  8 = Hybrid
Lease	Time for which the supplied IP address is valid
Grace Period	Length of grace period
Grace period for released leases	Status of the grace period for released leases; enabled or disabled
DNS Servers	Address of each DNS server assigned to the pool
NETBIOS Name Servers	NetBIOS server assigned to subscribers
Default Routers	Address of default router used for subscribers
Server Address	DHCP server address that is sent to subscribers
Linked Pool	Names of any pools that are linked to this pool

Table 6: show ip dhcp-local pool Output Fields (*continued*)

Field Name	Field Description
High utilization threshold	<p>Threshold at or above which the utilization trap is triggered, if the trap is enabled</p> <p>For linked pools, utilization is calculated based on the usage of all pools in the group</p>
Abated utilization threshold	<p>Threshold below which the utilization trap is triggered, if the trap is enabled</p> <p>For linked pools, utilization is calculated based on the usage of all pools in the group</p>
Current utilization	<p>Percentage of local address pools currently used</p> <p>For linked pools, utilization is calculated based on the usage of all pools in the group</p>
Utilization trap	<p>Status of the utilization trap which is generated when the high utilization, abated utilization, or 100% utilization is reached</p> <p>For linked pools, utilization is calculated based on the usage of all pools in the group</p>
Shared pool allocations	Number of addresses allocated to shared pools
Group Name	Group name; based on the name of the original pool
Total Addresses Available	Number of addresses in the group
Total Addresses In Use	Number of addresses currently being used
Trap Enabled	Status of utilization trap, yes or no
Pools	Names of pools in the group

**Related Documentation**

- [show ip dhcp-local pool on page 122](#)





## CHAPTER 11

# Monitoring Tasks for DHCPv4 Local Server

- [Monitoring DHCP Local Server Authentication Information on page 99](#)
- [Monitoring DHCP Local Server Configuration on page 100](#)
- [Monitoring DHCP Local Server Leases on page 101](#)
- [Monitoring DHCP Local Server Statistics on page 102](#)
- [Monitoring the Maximum Number of Available Leases on page 105](#)
- [Monitoring Static IP Address and MAC Address Pairs Supplied by DHCP Local Server on page 106](#)

### Monitoring DHCP Local Server Authentication Information

---

**Purpose** Display the DHCP local server's AAA authentication configuration information and statistics.

**Action** To display DHCP local server AAA authentication configuration:

```
host1#show ip dhcp-local auth config
```

DHCP Local Server Authentication Configuration

```
User-Prefix      : ERX4-Boston
Domain           : ISP1.com
Password         : to4Tool8
Virtual Router   : included
Circuit Type     : included
Circuit ID       : included
MAC Address      : excluded
Option 82        : excluded
```

DHCP Local Server DHCP Options Configuration

RADIUS DHCP Options : excluded

To display DHCP local server AAA authentication statistics:

```
host1#show ip dhcp-local auth statistics
```

DHCP Local Server Authentication Statistics

```
-----
Item                      Count
-----
auth requests             10
auth request failures     0
```

auth grants	9
auth denies	1

**Meaning** [Table 7 on page 100](#) lists the **show ip dhcp-local auth** command output fields.

**Table 7: show ip dhcp-local auth Output Fields**

Field Name	Field Description
User-Prefix	Client's user prefix
Domain	Client's domain
Password	Password used to authenticate client
Virtual Router	Client's virtual router; excluded or included
Circuit Type	Client's circuit type; excluded or included
Circuit ID	Client's circuit ID; excluded or included
MAC Address	Client's MAC address; excluded or included
Option 82	Status of client's option 82 field; excluded or included
RADIUS DHCP Options	Status of the DHCP options returned from the RADIUS server; excluded or included
auth requests	Number of authorization requests received by this DHCP local server
auth request failures	Number of authorization requests that have failed
auth grants	Number of authorization requests that have been granted
auth denies	Number of authorization requests that have been denied

**Related Documentation** • [show ip dhcp-local auth on page 117](#)

## Monitoring DHCP Local Server Configuration

**Purpose** Display the DHCP local server's configuration information.

**Action** To display configuration settings for DHCP local server:

```
host1#show ip dhcp-local
```

```
*****
```

```
    DHCP Local Server Configuration
```

```
Mode: Standalone
```

```
SNMP Traps Enabled - no
```

```
Unique Client IDs - enabled
```

**Meaning** [Table 8 on page 101](#) lists the **show ip dhcp-local** command output fields.

**Table 8: show ip dhcp-local Output Fields**

Field Name	Field Description
Mode	DHCP local server mode, equal-access or standalone
SNMP Traps Enabled	Status of DHCP local traps support, yes or no
Unique Client IDs	Status of duplicate client ID and duplicate hardware address detection, enabled or disabled

**Related Documentation**

- [show ip dhcp-local on page 116](#)

## Monitoring DHCP Local Server Leases

**Purpose** Display lease information for a specific IP address or for all DHCP local server leases.

**Action** To display information about a specific DHCP local server lease:

```
host1#show ip dhcp-local leases 192.168.0.3
```

```

                                Dhcp Local Leases
                                -----
Address      Hardware      Lease      Initiated/Renewed
-----
192.168.0.3  10-06-10-00-10-33  120       THU SEP 08 2005 08:02:11 UTC
Address      Expiration      Remaining
-----
192.168.0.3  THU SEP 08 2005 08:04:11 UTC  79
Address      Initial Lease Start
-----
192.168.0.3  THU SEP 08 2005 08:01:12 UTC

```

To display information about all DHCP local server leases:

```
host1#show ip dhcp-local leases
```

```

                                Dhcp Local Leases
                                -----
Address      Hardware      Lease      Initiated/Renewed
-----
192.168.0.2  10-06-10-00-10-32  120       THU JUL 06 2006 08:02:11 UTC
192.168.0.3  10-06-10-00-10-33  120       THU JUL 06 2006 08:02:11 UTC
192.168.55.4  10-06-10-00-10-34  (600)     THU JUL 06 2006 09:57:22 UTC
192.168.55.5  10-06-10-00-10-35  infinite  THU JUL 06 2006 08:03:10 UTC
Address      Expiration      Remaining
-----
192.168.0.2  THU JUL 06 2006 08:04:11 UTC  80
192.168.0.3  THU JUL 06 2006 08:04:11 UTC  80
192.168.55.4  THU JUL 06 2006 10:07:22 UTC  575
192.168.55.5  THU JUL 06 2006 08:04:11 UTC  infinite
Address      Initial Lease Start
-----

```

```

10.1.0.2      THU JUL 06 2006 08:01:12 UTC
10.1.0.3      THU JUL 06 2006 08:01:12 UTC
192.168.55.4  THU JUL 06 2006 09:54:19 UTC
192.168.55.5  THU JUL 06 2006 08:03:10 UTC

```

**Meaning** [Table 9 on page 102](#) lists the **show ip dhcp-local leases** command output fields.

**Table 9: show ip dhcp-local leases Output Fields**

Field Name	Field Description
Address	IP address
Hardware	MAC address of the subscriber's computer
Lease	Infinite, or the number of seconds in which the IP address is available; grace period in parentheses for clients in the grace period
Initiated/Renewed	Day, date, and time the lease was most recently initiated or renewed; start time of grace period for clients in the grace period
Expiration	Day, date, and time the lease expires; expiration time of grace period for clients in the grace period
Remaining	Infinite, or the number of seconds remaining in the lease, if any; remaining time of grace period for clients in the grace period
Initial Lease Start	Day, date, and time the lease was initiated

**Related Documentation** • [show ip dhcp-local leases on page 120](#)

## Monitoring DHCP Local Server Statistics

**Purpose** Display statistics for the DHCP local server.

**Action** To display all DHCP local server statistics:

```
host1#show ip dhcp-local statistics
```

```
DHCP Local Server Statistics
```

```

-----
            Item                Count
-----
memUsage                184
bindings                  2
--Receive Statistics--
discover                  8
request(accept)          10
request(renew)             6
request(rebind)           2
request(other)            6
decline                   0
release                   6
inform                    0

```

```

total in packet      38
in error             0
in discard           0
unknown client packet 6
--Transmit Statistics--
offer                8
ack(accept)          10
ack(renew)            6
ack(rebind)           2
nak                   6
nak(renew)            0
nak(rebind)           0
total out packet     32
out error             0
out discard           0

```

To display DHCP local server statistics for a specific interface:

```
host1#show ip dhcp-local statistics interface atm 4/0.32
```

```

DHCP Local Server SubInterface Statistics
Interface          Item                      Count
-----
ATM4/0.32
Receive Statistics
discover            4
request(accept)     5
request(renew)       1
request(rebind)      1
request(other)       3
decline             0
release             3
inform              0
total in packet     17
in error             0
in discard           0
unknown client packet 3
Transmit Statistics
offer                4
ack(accept)          5
ack(renew)            1
ack(rebind)           1
nak                   3
nak(renew)            0
nak(rebind)           0
total out packet     14
out error             0
out discard           0

```

**Meaning** [Table 10 on page 103](#) lists the `show ip dhcp-local statistics` command

**Table 10: show ip dhcp-local statistics output fields.**

Field Name	Field Description
memUsage	Number of bytes of memory used by the DHCP local server
bindings	Number of leased IP addresses currently assigned
Receive Statistics	Statistics for packets that have been received

Table 10: show ip dhcp-local statistics output fields. (*continued*)

Field Name	Field Description
discover	Number of DHCP discover messages received
request(accept)	Number of DHCP requests accepted
request(renew)	Number of DHCP requests for renewal received
request(rebind)	Number of DHCP requests for rebinding received
request(other)	Number of DHCP unknown requests received
decline	Number of DHCP decline messages received
release	Number of DHCP release messages received
inform	Number of DHCP inform messages received
total in packet	Number of packets received
in error	Number of packets received with errors that prevent further processing; count is independent of the message-type counters
in discard	Number of packets received that are discarded due to system resource issues; count is independent of the message-type counters
unknown client packet	Number of nonrequest packets that have no entry in the local server database received
Transmit Statistics	Statistics for packets that have been transmitted
offer	Number of DHCP offer messages sent
ack(accept)	Number of DHCP acknowledgments sent in response to accepted requests
ack(renew)	Number of DHCP acknowledgments sent in response to renewal requests
ack(rebind)	Number of DHCP acknowledgments sent in response to rebinding requests
nak	Number of DHCP NAK messages sent in response to requests that cannot be bound or that are unknown to this local server
nak(renew)	Number of DHCP NAK messages sent in response renewal requests
nak(rebind)	Number of DHCP NAK messages sent in response to rebinding requests

Table 10: show ip dhcp-local statistics output fields. (continued)

Field Name	Field Description
total out packet	Number of packets sent by the DHCP local server
out error	Number of packets that cannot be transmitted due to protocol errors or configuration errors; count is independent of the message-type counters
out discard	Number of packets that cannot be transmitted due to system resource issues; count is independent of the message-type counters

**Related Documentation** • [show ip dhcp-local statistics on page 124](#)

## Monitoring the Maximum Number of Available Leases

**Purpose** Display the maximum number of leases available for each VPI/VCI, VLAN, Ethernet subnetwork, or POS access interface type, or for a specific interface or subinterface.

**Action** To display the maximum number of leases available for each interface type:

```
host1(config)#show ip dhcp-local limits
```

```
*****
```

```
      DHCP Local Server Address Limits
ATM Limit      - 48000
VLAN Limit     - 48000
POS Limit      - 1000
Ethernet Limit - 48000
```

To display information about the maximum number of leases for a specific interface:

```
host1(config)#show ip dhcp-local limits interface atm 3/1
```

```
      Dhcp Local Interface Limits
      -----
Interface  Limit  Count  Denied  Total
-----
atm 3/1    300    127    5       29
```

To display information about the maximum number of leases on all interfaces:

```
host1(config)#show ip dhcp-local limits interface
```

```
      Dhcp Local Interface Limits
      -----
Interface  Limit  Count  Denied  Total
-----
fastEthernet0/0  200    0      0       0
atm 3/1        300    127    5       29
atm 4/2        5000    0      0       0
atm 5/1        5000    15     2       5
pos 2/1        1000    0      0       0
```

**Meaning** [Table 11 on page 106](#) lists the **show ip dhcp-local limits** command output fields.

**Table 11: show ip dhcp-local limits Output Fields**

Field Name	Field Description
ATM Limit	Number of leases available for each VPI/VCI
VLAN Limit	Number of leases available for each VLAN
POS Limit	Number of leases available for each POS access interface
Ethernet Limit	Number of leases available for each Ethernet subnet
Limit	Number of leases available to the specified interface or subinterface; indicates the configured value for the interface type unless a specific lease value is configured for the particular interface
Count	Number of active leases on the interface
Denied	Number of lease requests denied during the current denial period; this number is reset to zero (and the denial period restarted) when the number of active leases no longer exceeds the configured limit
Total Denied	Total number of lease requests denied on the interface since the interface became active

**Related Documentation** • [show ip dhcp-local limits on page 121](#)

## Monitoring Static IP Address and MAC Address Pairs Supplied by DHCP Local Server

**Purpose** Display the static IP address/MAC address pairs that the DHCP local server supplies in standalone mode.

**Action** To display information about static IP address/MAC address pairs:

```
host1#show ip dhcp-local reserved
```

```

                                Dhcp Reserved Addresses
                                -----
    Pool      Address          Hardware
    -----
cablemodem  10.44.44.100  12-34-12-34-12-34-00-00-00-00-00-00-00-00-00-00
cablemodem  10.44.44.101  22-33-22-33-22-33-00-00-00-00-00-00-00-00-00-00

```

**Meaning** [Table 12 on page 107](#) lists the **show ip dhcp-local reserved** command output fields.



Table 12: show ip dhcp-local reserved Output Fields

Field Name	Field Description
Pool	Name of pool in which the address is reserved
Address	IP address that is reserved
Hardware	Address for which the IP address is reserved

**Related Documentation**

- [show ip dhcp-local reserved on page 123](#)



# Monitoring Tasks for DHCPv6 Local Server

- [Monitoring DHCPv6 Local Server Authentication Information on page 109](#)
- [Monitoring DHCPv6 Local Server Binding Information on page 110](#)
- [Monitoring DHCPv6 Local Server DNS Search Lists on page 110](#)
- [Monitoring DHCPv6 Local Server DNS Servers on page 111](#)
- [Monitoring DHCPv6 Local Server Prefix Lifetime on page 111](#)
- [Monitoring DHCPv6 Local Server Statistics on page 112](#)

## Monitoring DHCPv6 Local Server Authentication Information

**Purpose** Display the DHCPv6 local server's AAA authentication configuration information.

**Action** To display the DHCPv6 local server's AAA authentication configuration:

```
host1#show ipv6 dhcpv6-local auth config
```

DHCPv6 Local Server Authentication Configuration

```
User-Prefix      : userPrefix
Domain           : domain
Password         : password
Circuit Type     : excluded
Circuit ID       : excluded
```

**Meaning** [Table 13 on page 109](#) lists the **show ipv6 dhcpv6-local auth config** command output fields.

**Table 13: show ipv6 dhcpv6-local auth config Output Fields**

Field Name	Field Description
User-Prefix	Client's user prefix
Domain	Client's domain
Password	Password used to authenticate client
Circuit Type	Client's circuit type; excluded or included
Circuit ID	Client's circuit ID; excluded or included

- Related Documentation**
- [Authentication and Accounting of IPv6 Subscribers Using the DHCPv6 Local Server Overview on page 13](#)
  - [Interoperation of Authentication of IPv6 Clients and Display of Active Subscriber Information on page 15](#)
  - [Configuring AAA Authentication for DHCPv6 Local Server Standalone Mode on page 35](#)
  - [show ipv6 dhcpv6-local auth config on page 125](#)

## Monitoring DHCPv6 Local Server Binding Information

**Purpose** Display the mapping between one or more IPv6 addresses and the DHCP unique ID of the subscriber's computer.

**Action** To display the DHCP binding information for an IPv6 address:

```
host1#show ipv6 dhcpv6-local binding 2001:db8:4::/48
```

Prefix	Client DUID	Lease	Intf
2001:db8:4::/48	<LL 1/00A0DE113502>	infinite	FastEthernet 3/6.1

**Meaning** [Table 14 on page 110](#) lists the **show ipv6 dhcpv6-local binding** command output fields.

Table 14: show ipv6 dhcpv6-local binding Output Fields

Field Name	Field Description
Prefix	IPv6 address
Client DUID	DHCP unique ID of subscriber's computer
Lease	Time for which the IPv6 address is available in seconds, or infinite
Intf	Router's interface that is associated with the subscriber's computer

- Related Documentation**
- [show ipv6 dhcpv6-local binding on page 126](#)

## Monitoring DHCPv6 Local Server DNS Search Lists

**Purpose** Display the DHCPv6 local servers DNS search list.

**Action** To display the DNS search list for DHCPv6 local servers:

```
host1#show ipv6 dhcpv6-local dns-domain-searchlist
Domain 1: xyzcorporation.net
Domain 2: xyzcorp.com
Domain 3: financeDomain.com
Domain 4: researchDomain.com
```

**Meaning** [Table 15 on page 111](#) lists the `show ipv6 dhcpv6-local dns-domain-searchlist` command output fields.

**Table 15: show ipv6 dhcpv6-local dns-domain-searchlist Output Fields**

Field Name	Field Description
Domain	Domains in the search list

**Related Documentation** • [show ipv6 dhcpv6-local dns-domain-searchlist on page 127](#)

## Monitoring DHCPv6 Local Server DNS Servers

**Purpose** Display a list of DNS servers configured on the DHCPv6 local server.

**Action** To display the list of DNS servers:

```
host1#show ipv6 dhcpv6-local dns-servers
DNS server 1: 2001:db8:18::
DNS server 2: 2001:db8:19::
DNS server 3: 2001:db8:20::
DNS server 4: 2001:db8:21::
```

**Meaning** [Table 16 on page 111](#) lists the `show ipv6 dhcpv6-local dns-servers` command output fields.

**Table 16: show ipv6 dhcpv6-local dns-servers Output Fields**

Field Name	Field Description
DNS server	IPv6 address of the DNS server

**Related Documentation** • [show ipv6 dhcpv6-local dns-servers on page 128](#)

## Monitoring DHCPv6 Local Server Prefix Lifetime

**Purpose** Display the DHCPv6 default prefix lifetime.

**Action** To display the DHCPv6 default prefix lifetime:

```
host1#show ipv6 dhcpv6-local prefix-lifetime
default prefix lifetime is 1 day, 12 hours, 30 minutes
```

**Meaning** [Table 17 on page 112](#) lists the `show ipv6 dhcpv6-local prefix-lifetime` command output fields.

Table 17: show ipv6 dhcpv6-local prefix-lifetime Output Fields

Field Name	Field Description
default prefix lifetime	Number of days, hours, and minutes

**Related Documentation**

- [show ipv6 dhcpv6-local prefix-lifetime on page 129](#)

## Monitoring DHCPv6 Local Server Statistics

**Purpose** Display statistics for the DHCPv6 local server.

**Action** To display DHCPv6 local server statistics:

```
host1#show ipv6 dhcpv6-local statistics
```

```
DHCPv6 Local Server Statist
```

```
-----
      Item              Count
-----
memUsage                136
bindings                1
solicit rx              1
request(accept) rx      1
request(renew) rx       0
decline rx              0
release rx              0
inform rx               0
confirm rx              0
rebind rx               0
reconfigure tx          0
advertise tx             1
successful reply tx     1
failed reply tx          0
unknown msgs            0
bad msgs                 0
```

**Meaning** [Table 18 on page 112](#) lists the `show ipv6 dhcpv6-local statistics` command output fields.

Table 18: show ipv6 dhcpv6-local statistics Output Fields

Field Name	Field Description
memUsage	Number of bytes of memory used by DHCPv6 local server
bindings	Number of leased IPv6 prefixes currently assigned
solicit rx	Number of DHCPv6 solicit messages received
request(accept) rx	Number of DHCPv6 request messages received
request(renew) rx	Number of DHCPv6 requests for renewal received
decline rx	Number of DHCPv6 decline messages received

Table 18: show ipv6 dhcpv6-local statistics Output Fields (*continued*)

Field Name	Field Description
release rx	Number of DHCPv6 release messages received
inform rx	Number of DHCPv6 information-request messages received
confirm rx	Number of DHCPv6 confirm messages received
rebind rx	Number of DHCPv6 rebind messages received
reconfigure tx	Number of DHCPv6 reconfigure messages transmitted
advertise tx	Number of DHCPv6 advertise messages transmitted
successful reply tx	Number of reply messages transmitted with success reply code
failed reply tx	Number of reply messages transmitted with reply codes other than success
unknown msgs	Unused field; always 0
bad msgs	Number of messages with errors received by the DHCPv6 local server

**Related  
Documentation**

- [show ipv6 dhcpv6-local statistics on page 130](#)





## CHAPTER 13

# Monitoring Commands

## show ip dhcp-local

---

**Syntax**    show ip dhcp-local

**Release Information**    Command introduced in JunosE Release 7.2.0.

**Description**    Displays DHCP local server configuration information, including the status of SNMP traps and client roaming support.

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCP Local Server Configuration on page 100](#)

## show ip dhcp-local auth

---

<b>Syntax</b>	show ip dhcp-local auth { config   statistics [ delta ] } [ <i>filter</i> ]
<b>Release Information</b>	Command introduced in JunosE Release 7.1.0.
<b>Description</b>	Displays information about the DHCP local server authentication configuration.
<b>Options</b>	<ul style="list-style-type: none"><li>• config—Specifies that configuration information is shown</li><li>• statistics—Specifies that statistics are shown</li><li>• delta—Displays baselined statistics</li><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring DHCP Local Server Authentication Information on page 99</a></li></ul>

## show ip dhcp-local binding

---

**Syntax** show ip dhcp-local binding [ *ipAddress* | interface *interfaceType* *interfaceValue* ]  
[ *filter* ]

**Release Information** Command introduced before JunosE Release 7.1.0.

**Description** Displays DHCP local server binding information for DHCP local server clients.



**NOTE:** This command is deprecated and might be removed completely in a future release. The function provided by this command has been replaced by the **show dhcp binding** command.

- Options**
- *ipAddress*—IP address of the subscriber's personal computer
  - *interfaceType*—Interface type; see *Interface Types and Specifiers*
  - *interfaceSpecifier*—Particular interface; format varies according to interface type; see *Interface Types and Specifiers*
  - *filter*—See *Filtering show Commands*

**Mode** Privileged Exec

**Related Documentation**

- *Monitoring DHCP Bindings (Local Server Binding Information)*

## show ip dhcp-local excluded

---

<b>Syntax</b>	show ip dhcp-local excluded [ <i>filter</i> ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0.
<b>Description</b>	Displays IP addresses that have been excluded. These are addresses that the DHCP local server does not allocate because they are already used by devices on the subnet.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring the Maximum Number of Available Leases on page 105</a></li></ul>

## show ip dhcp-local leases

---

**Syntax**    show ip dhcp-local leases [ *ipAddress* ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays DHCP local server lease and binding information.

- Options**
- *ipAddress*—Specific IP address
  - *filter*—See *Filtering show Commands*

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring the Maximum Number of Available Leases on page 105](#)

---

## show ip dhcp-local limits

---

<b>Syntax</b>	show ip dhcp-local limits [ interface <i>InterfaceType</i> <i>InterfaceSpecifier</i>   <i>filter</i> ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0. <b>interface</b> keyword and <i>interfaceType</i> and <i>interfaceSpecifier</i> variables added in JunosE Release 7.1.0.
<b>Description</b>	Displays the maximum number of leases available for each VPI/VCI, VLAN, and Ethernet subnetwork, or for a particular interface or subinterface from the DHCP local server.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>interfaceType</i>—Interface type; see <i>Interface Types and Specifiers</i></li><li>• <i>interfaceSpecifier</i>—Particular interface; format varies according to interface type; see <i>Interface Types and Specifiers</i></li><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring the Maximum Number of Available Leases on page 105</a></li></ul>

## show ip dhcp-local pool

---

**Syntax**    show ip dhcp-local pool [ groups ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays the configuration of DHCP local pools.

- Options**
- groups—Displays DHCP local server pool group information
  - *filter*—See *Filtering show Commands*

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCP Local Address Pools on page 95](#)



## show ip dhcp-local reserved

---

<b>Syntax</b>	show ip dhcp-local reserved [ <i>filter</i> ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0.
<b>Description</b>	Displays the static IP address/MAC address pairs that the DHCP local server supplies in standalone mode. This command does not display address pairs that the DHCP local server supplies in non-PPP equal access mode.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring Static IP Address and MAC Address Pairs Supplied by DHCP Local Server on page 106</a></li></ul>

## show ip dhcp-local statistics

---

<b>Syntax</b>	show ip dhcp-local statistics [ interface [ <i>interfaceType</i> <i>interfaceSpecifier</i> ] ] [ delta ] [ <i>filter</i> ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0.
<b>Description</b>	Displays statistics for the DHCP local server.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>interfaceType</i>—Interface type; see <i>Interface Types and Specifiers</i></li><li>• <i>interfaceSpecifier</i>—Particular interface; format varies according to interface type; see <i>Interface Types and Specifiers</i></li><li>• delta—Displays baselined statistics</li><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring DHCP Local Server Statistics on page 102</a></li></ul>

## **show ipv6 dhcpv6-local auth config**

---

**Syntax**    show ipv6 dhcpv6-local auth config

**Release Information**    Command introduced in JunosE Release 12.2.0.

**Description**    Displays information about the DHCPv6 local server authentication configuration.

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCPv6 Local Server Authentication Information on page 109](#)

## show ipv6 dhcpv6-local binding

---

**Syntax**    show ipv6 dhcpv6-local binding [ *ipv6Prefix* ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays the mapping between the token or enduring IPv6 prefix and the DHCP unique ID (DUID) of the client computer.

**Options**

- *ipv6Prefix*—IPv6 address of the subscriber's personal computer
- *filter*—See *Filtering show Commands*

**Mode**    Privileged Exec

**Related Documentation**

- [Monitoring DHCPv6 Local Server Binding Information on page 110](#)

## **show ipv6 dhcpv6-local dns-domain-searchlist**

---

<b>Syntax</b>	show ipv6 dhcpv6-local dns-domain-searchlist [ <i>filter</i> ]
<b>Release Information</b>	Command introduced before JunosE Release 7.1.0.
<b>Description</b>	Displays the DHCPv6 local server's DNS search list.
<b>Options</b>	<ul style="list-style-type: none"><li>• <i>filter</i>—See <i>Filtering show Commands</i></li></ul>
<b>Mode</b>	Privileged Exec
<b>Related Documentation</b>	<ul style="list-style-type: none"><li>• <a href="#">Monitoring DHCPv6 Local Server DNS Search Lists on page 110</a></li></ul>

## show ipv6 dhcpv6-local dns-servers

---

**Syntax**    show ipv6 dhcpv6-local dns-servers [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays DNS servers that are configured on the DHCPv6 local server.

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

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCPv6 Local Server DNS Servers on page 111](#)

## show ipv6 dhcpv6-local prefix-lifetime

---

**Syntax**    show ipv6 dhcpv6-local prefix-lifetime [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays the DHCPv6 default prefix lifetime.

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

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCPv6 Local Server Prefix Lifetime on page 111](#)

## show ipv6 dhcpv6-local statistics

---

**Syntax**    show ipv6 dhcpv6-local statistics [ *delta* ] [ *filter* ]

**Release Information**    Command introduced before JunosE Release 7.1.0.

**Description**    Displays statistics for the DHCPv6 local server.

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

**Mode**    Privileged Exec

**Related Documentation**    • [Monitoring DHCPv6 Local Server Statistics on page 112](#)



## PART 4

# Index

- [Index on page 133](#)



# Index

## A

AAA authentication	
scenarios in which show subscribers command output varies	
domain name mapped with the virtual router.....	15
domain name not mapped with the virtual router.....	15
active subscriber details, viewing	
with AAA authentication configured on default router	
show subscribers command.....	15
with RADIUS authentication configured on default router	
show subscribers command.....	15
show subscribers ipv6 command.....	15
show subscribers summary command.....	15
authentication of IPv6 clients	
and behavior of the show subscribers command.....	15

## B

B-RAS commands	
dhcp delete-binding.....	49
grace-period.....	55
logout subscribers.....	78
use-release-grace-period.....	89
baseline commands	
baseline dhcp relay.....	45
baseline dhcp server.....	45
baseline dhcp-local.....	46
baseline dhcpv6-local.....	46
baseline ip dhcp-external.....	46
BGP commands	
network.....	82

## C

clear ip commands	
clear ip dhcp-local binding .....	28

conventions	
notice icons.....	xi
text and syntax.....	xii
customer support.....	xiii
contacting JTAC.....	xiii

## D

DHCP (Dynamic Host Configuration Protocol)	
giaddr.....	5, 8
option 82.....	29, 30
DHCP client bindings	
indexing using DUID.....	11
requests from clients	
acknowledged using default DUID type by server.....	11
DHCP commands	
clear ip dhcp-local binding.....	48
ip dhcp-local auth domain.....	61, 65
ip dhcp-local auth include.....	62
ip dhcp-local auth password.....	63
ip dhcp-local auth user-prefix.....	64
service dhcp-local.....	86, 91
service dhcpv6-local.....	87
show ip dhcp-local auth.....	117
DHCP local address pools	
configuring.....	19
grace periods.....	21
linking.....	21
DHCP local server.....	25
configuring.....	23
configuring authentication.....	29
duplicate clients.....	25
equal-access mode.....	4
address allocation.....	4
configuring.....	9
connection process.....	4
local pool selection.....	4
overview.....	4
local address pool group.....	21, 97
local pool selection, equal-access.....	4
using domain name.....	5
using framed IP address.....	5
using giaddr.....	5
using pool name.....	5
local pool selection, standalone.....	6
using giaddr.....	6
using received interface IP address.....	6
logging information.....	28
modes.....	3

overview.....	3	use-release-grace-period.....	21
RADIUS accounting support for.....	3	warning.....	21
standalone mode		DHCP unique identifier See DUID	
address allocation.....	6, 29	dhcp-local-server-configuration-overview.....	9
authentication.....	29	DHCPv6 client bindings	
configuring.....	9	deleting.....	39
local pool selection.....	6	dhcpv6 delete-binding command.....	40
overview.....	6	DHCPv6 local server	
unique client IDs.....	25	accounting for IPv6 subscribers	
DHCP local server commands		standalone mode with AAA	
ip dhcp-local		authentication.....	15
auto-configureagent-circuit-identifier.....	57	Advertise message	
link.....	77	authentication of subscribers.....	14
network.....	82	authentication of IPv6 subscribers	
reserve.....	84	connected using Ethernet links.....	13
server-address.....	85	connected using VLAN links.....	13
show ip dhcp-local excluded.....	119	configuring.....	33
show ip dhcp-local leases.....	120	configuring authentication.....	35
show ip dhcp-local pool.....	122	configuring DUID type.....	37
show ip dhcp-local reserved.....	123	IPv6.....	33
DHCP local server traps		prefix delegation	
logging.....	27	with standalone mode configured.....	13
DHCP local server:local pool selection, equal-access		with standalone mode for PPP	
using received interface IP address.....	5	subscribers.....	13
DHCP local server:local pool selection, standalone		standalone mode	
with AAA		address allocation.....	35
using domain name.....	8	authentication.....	35
using framed IP address.....	7	standalone mode with AAA authentication	
using giaddr.....	8	construction of username.....	13
using pool name.....	7	standalone mode with AAA authentication,	
using received IP address.....	8	overview.....	13
DHCP local server:local pool selection, standalone		standalone mode without AAA authentication,	
without AAA		overview.....	13
using giaddr.....	7	using DUID in identity verification of clients.....	11
using received interface IP address.....	7	using DUID types that suit the client and service	
DHCP pool commands		provider networks.....	11
default-router.....	21	DHCPv6 local server commands	
dns-server.....	21	ipv6 dhcpv6-local auth domain.....	72
domain-name.....	21	ipv6 dhcpv6-local auth password.....	73
grace-period.....	21	ipv6 dhcpv6-local auth user-prefix.....	74
lease.....	21	ipv6 dhcpv6-local delegated-prefix.....	66
link.....	21	ipv6 dhcpv6-local dns-domain-search.....	67
netbios-name-server.....	21	ipv6 dhcpv6-local dns-server.....	68
netbios-node-type.....	21	ipv6 dhcpv6-local duid.....	69, 75
network.....	21	ipv6 dhcpv6-local prefix-lifetime.....	70
reserve.....	21	show ipv6 dhcpv6-local dns-servers.....	128
server-address.....	21	show ipv6 dhcpv6-local prefix-lifetime.....	129
snmpTrap.....	21	show ipv6	
		dhcpv6-localdns-domain-searchlist.....	127

- digital certificate commands
    - domain-name.....54
  - documentation set
    - comments on.....xiii
  - DUID
    - conformance standards.....11
    - default type on DHCPv6 local server.....11
    - format and example.....11
    - Identity Association for Prefix Delegation option and.....11
    - Identity Association identifier and.....11
    - indexing client bindings.....11
    - prerequisite for configuring DUID type.....37
    - type, configuring on DHCPv6 local server.....37
    - types of
      - Type 1, contents and format.....11
      - Type 2, contents and format.....11
      - Type 3, contents and format.....11
    - types supported
      - by DHCP client.....11
      - by DHCPv6 local server.....11
    - used in client and server exchanges.....11
  - duplicate clients.....25
  - Dynamic Host Configuration Protocol. *See* DHCP
- E**
- equal-access DHCP local server.....4
- G**
- giaddr.....5
- I**
- Identity Association for Prefix Delegation
    - and its interoperation with DUID.....11
    - contains Identity Association identifier collection of prefixes.....11
  - Identity Association identifier
    - chosen by the requesting router.....11
    - using to denote Identity Association for Prefix Delegation options.....11
  - interfaces
    - configuring for DHCP local server.....8
  - ip dhcp-local auth domain command.....31, 35
  - ip dhcp-local auth include command.....31
  - ip dhcp-local auth password.....31
  - ip dhcp-local auth user-prefix command.....31
- ip dhcp-local commands
    - ip dhcp-local auto-configure
      - agent-circuit-identifier.....28
    - ip dhcp-local excluded-address.....28
    - ip dhcp-local limit.....28
    - ip dhcp-local pool.....21
    - ip dhcp-local unique-client-ids.....28
  - IPsec identity commands
    - domain-name.....54
  - IPv6 DHCP local server.....33
    - monitoring.....110, 111
  - ipv6 dhcpv6-local auth domain command.....37
  - ipv6 dhcpv6-local auth password.....37
  - ipv6 dhcpv6-local auth user-prefix command.....37
  - ipv6 dhcpv6-local commands
    - ipv6 dhcpv6-local delegated-prefix.....33
    - ipv6 dhcpv6-local dns-domain-search.....33
    - ipv6 dhcpv6-local dns-server.....33
    - ipv6 dhcpv6-local limit.....33
    - ipv6 dhcpv6-local prefix-lifetime.....33
  - IPv6 local address pool commands
    - ipv6 local pool.....71
  - IPv6 subscribers
    - accounting of
      - using DHCPv6 local server, standalone mode.....13
    - accounting of, DHCPv6 local server configured with standalone authentication mode.....15
    - authentication of
      - using DHCPv6 local server, standalone mode.....13
- L**
- logging. *See* specific feature, product, or protocol
  - logout subscribers command.....29
- M**
- MAC (media access control) addresses
    - duplicate.....27, 28
  - manuals
    - comments on.....xiii
- N**
- non-PPP equal access
    - configuration example.....41
    - requirements.....4

non-PPP equal access commands	
default-router .....	52
dns-server .....	53
domain-name.....	54
ip dhcp-local excluded-address.....	58
ip dhcp-local limit.....	59
ip dhcp-local pool.....	56
ip dhcp-local unique-client-ids.....	60
lease .....	76
netbios-name-server.....	80
netbios-node-type.....	81
show ip dhcp-local.....	116
show ip dhcp-local binding.....	118
show ip dhcp-local limits.....	121
show ip dhcp-local statistics.....	124
show ipv6 dhcpv6-local auth config .....	125
show ipv6 dhcpv6-local binding.....	126
show ipv6 dhcpv6-local statistics.....	130
notice icons.....	xi
<b>O</b>	
option 82.....	29, 30
<b>P</b>	
PPP subscribers	
DHCPv6 local server: standalone mode	
delegation of prefixes.....	13
<b>R</b>	
RADIUS authentication	
scenarios in which show subscribers command	
output varies	
IPv6 virtual router name contained in	
Access-Accept message.....	15
RADIUS configured on default router.....	15
RADIUS not configured on default	
router.....	15
virtual router name returned in	
Access-Accept message.....	15
RIP commands	
network.....	82
<b>S</b>	
service commands	
service dhcp-local.....	28
service dhcp-local authenticate.....	29
service dhcpv6-local .....	33
service dhcpv6-local standalone	
authenticate.....	35
service dhcp-local command.....	31
service dhcpv6-local command.....	37
Session and Resource Control. See SRC software	
show ip dhcp-local commands	
show ip dhcp-local.....	100
show ip dhcp-local auth.....	99
show ip dhcp-local limits.....	105
show ip dhcp-local pool.....	95
show ip dhcp-local reserved.....	106
show ip dhcp-local statistics.....	101, 102
show ipv6 dhcpv6-local commands	
show ipv6 dhcpv6-local auth.....	109
show ipv6 dhcpv6-local binding.....	110
show ipv6 dhcpv6-local	
dns-domain-searchlist.....	110
show ipv6 dhcpv6-local dns-servers.....	111
show ipv6 dhcpv6-local prefix-lifetime.....	111
show ipv6 dhcpv6-local statistics.....	112
SNMP commands	
snmpTrap.....	88
warning.....	90
SNMP traps	
configuring for DHCP local servers.....	27
SRC (Session and Resource Control) software.....	41
standalone DHCP local server.....	6
standalone mode	
with and without AAA authentication	
DHCPv6 local server functionality.....	13
standalone mode with AAA authentication	
DHCPv6 local server	
accounting of IPv6 subscribers.....	15
DHCPv6 local server, parameters in username	
circuit identifier.....	13
circuit type.....	13
domain name.....	13
user prefix.....	13
virtual router.....	13
support, technical See technical support	
<b>T</b>	
technical support	
contacting JTAC.....	xiii
text and syntax conventions.....	xii
Type 1 DUID	
not supported by DHCPv6 local server.....	37
Type 2 DUID	
default type present on DHCPv6 local	
server.....	37

Type 3 DUID  
  configured using ipv6 dhcpv6-local duid-type  
  command.....[37](#)

